State of Nevada
Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board

NOTICE OF PUBLIC MEETING

Wednesday, April 24, 2024 ~ 4:30pm

Location: Board Office ~ 6170 Mae Anne Avenue, Suite 1, Reno, Nevada 89523

Supporting materials relating to this meeting will be physically available but in an effort to reduce costs and preserve resources, attendees are encouraged to access electronic copies on the Board's website at https://www.nvspeechhearing.org/about/Minutes.asp

Teleconference Access

ZOOM VIDEO & AUDIO:
https://us02web.zoom.us/j/86748672519?pwd=SFVzZGhIZVMySmJyVHdTVkt1L0dBdz09

AUDIO ONLY BY TELEPHONE: (669) 900-6833

Meeting ID: 867 4867 2519 **Passcode:** 841579

If you are outside the United States or need **toll-free telephone access**, please contact the Board office at board@nvspeechhearing.org or (775) 787-3421 to request a toll-free number no later than 3:00pm Pacific on the day of the meeting.

Public Comment

Any person wishing to make public comment may attend the meeting and provide comment as follows:
1) In person at the physical location(s) listed above, 2) Virtually through the Zoom teleconference video link listed above, or 3) Telephonically through the Zoom telephone number listed above.
Please see additional public comment instructions at the end of this agenda.

AGENDA

The **STATE OF NEVADA SPEECH-LANGUAGE PATHOLOGY, AUDIOLOGY AND HEARING AID DISPENSING BOARD** may: (a) address agenda items out of sequence (b) combine agenda items or (c) pull or remove items from the agenda at any time. The Board may convene in closed session to consider the character, alleged misconduct, professional competence or physical or mental health of a person. (NRS 241.020, NRS 241.030).
Action by the Board on any item may be to approve, deny, amend, or table.

1. **Call to Order, Confirmation of Quorum**
2. **Public Comment**

   No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020)

3. **Approval of the Minutes: Board Meeting of February 21, 2024** *(for possible action)*
4. **Public Hearing on Proposed Regulations LCB File R108-23** *(informational only)*
   a. Introduction to Proposed Regulations LCB File R108-23 *(informational only*
   b. Public Comment on Proposed Regulations LCB File R108-23 *(informational only)*

   No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020)

5. **Consideration to Adopt Proposed Regulations LCB File R108-23** *(for possible action)*

6. **Update and Report Out from Strategies 360 on Legislative and Lobbying Activities for 2024 Interim and 2025 Legislative Session** *(for possible action)*

7. **Consideration to Approve Proposed Revisions to NRS 637B for Inclusion in 2025 Legislative Effort with Recommendations from Advisory Committee on Fitting and Dispensing Hearing Aids and Speech-Language Pathology Subcommittee** *(for possible action)*

   a. **Revisions Related to Audiology: Report Out and Recommendations from Advisory Committee on Fitting and Dispensing Hearing Aids** *(for possible action)*
      1) NRS 637B.050 "Practice of audiology" defined. *(for possible action)*
      2) NRS 637B.075 Sponsor" defined. *(for possible action)*
      3) NRS 637B.100 Creation; number, appointment and qualifications of members; terms; vacancies. *(for possible action)*
      4) NRS 637B.175 Fees. *(for possible action)*
      5) NRS 637B.191 Regulations concerning examinations for, period of validity of, renewal and reinstatement of licenses; placement of license on inactive status. *(for possible action)*
      6) NRS 637B.236 Apprentices: Supervision of and responsibility for work; selection of hearing aid; signing of audiogram or sales document. *(for possible action)*
      7) NRS 637B.242 Sale of hearing aids by catalog, mail or Internet: Conditions; records; regulations. *(for possible action)*
      8) NRS 637B.243 Audiograms for use of physician or member of related profession. *(for possible action)*

   b. **Revisions Related to Fitting and Dispensing Hearing Aids** *(for possible action)*
      1) Clarification on Recommendations Made for Revisions to NRS 637B and NAC 637B Regarding HAS License Requirements *(for possible action)*
      2) NRS 637B.044 "Hearing aid" defined and NRS 637B.NEW "Over-the-counter hearing aid" defined. *(for possible action)*
      3) NRS 637B.055 "Practice of fitting and dispensing hearing aids" defined. *(for possible action)*
         (a) "Ordering the Use of" Language *(for possible action)*
         (b) Cerumen Management & Definition *(for possible action)*
         (c) Tinnitus Care & Definition *(for possible action)*
      4) Review and Recommendation to the Board on Possible Revisions to Examination Requirements in NRS 637B and NAC 637B for HAS License to Engage in the Practice of Fitting and Dispensing Hearing Aids *(for possible action)*

   c. **Revisions Related to Speech-Language Pathology** *(for possible action)*
      1) NRS New SLP Assistants *(for possible action)*
      2) NRS New Telesupervision *(for possible action)*
      3) NRS 637B.060 "Practice of speech-language pathology" defined. *(for possible action)*

8. **Disciplinary Matters: Case No. S23-02 Recommended for Dismissal** *(for possible action)*

9. **Executive Director's Report**
   a. Licensure Statistics *(for possible action)*
   b. FY24 Q3 Financial Report *(for possible action)*
   c. Board Member Appointments/Reappointments *(for possible action)*
   d. Complaints *(for possible action)*

10. **Review and Approval of Revised FY25 Budget and Contracts for Bookkeeping Services and Licensing Database** *(for possible action)*
    a. Revised FY25 Budget and New Sole Source Contract with Numbers, Inc. for Bookkeeping Services *(for possible action)*
    b. Consideration of Technology Risk Assessment as Recommended by Nevada Office of the CIO for Previously Approved Albertson Consulting Contract for Licensing Database *(for possible action)*

11. **Report from Legal Counsel** *(informational only)*

12. **Reports from Board Chair and Members**
    a. Report from Board Chair and Board Members *(for possible action)*
    b. 2024 Proposed Meeting Schedule: Next meeting proposed: Wednesday, July 24, 2024 at 4:30pm. Teleconference hosted via Zoom and in-person at the Reno Board Office *(for possible action)*
    c. Future Agenda Items *(for possible action)*
       1) Welcome New Board Member Appointments
       2) Election of Board Chair/Vice Chair (as needed)
       3) Comprehensive Review of Proposed Revisions to NRS 637B to Pursue in 2025 Legislative Session
       4) Update on Progress of Proposed Regulations LCB File R108-23
       5) Update and Report Out from Strategies 360 on Legislative and Lobbying Activities for 2024 Interim and 2025 Legislative Session
       6) Other Items As Proposed

13. **Public Comment**

No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020)

14. **Adjournment** *(for possible action)*

PUBLIC COMMENT

Public comment is welcomed by the Board. Public comment will be limited to five minutes per person and comments based on viewpoint will not be restricted. A public comment time will be available prior to action items on the agenda and on any matter not specifically included on the agenda as the last item on the agenda. At the discretion of the Board Chair, additional public comment may be heard when that item is reached. The Board Chair may allow additional time to be given a speaker as time allows and in their sole discretion. (NRS 241.020, NRS 241.030). Prior to the commencement and conclusion of a contested case or a quasi-judicial proceeding that may affect the due process rights of an individual, the Board may refuse to consider public comment. (NRS 233B.126).

ACCOMMODATIONS

Persons with disabilities who require special accommodations or assistance at the meeting should contact the Board office at (775) 787-3421 or email at board@nvspeechhearing.org no later than 48 hours prior to the meeting. Requests for special accommodations made after this time frame cannot be guaranteed.

AGENDA POSTING & DISSEMINATION

This meeting has been properly noticed and posted in the following locations:

- Nevada Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board Website and Office, 6170 Mae Anne Avenue, Suite 1, Reno, Nevada 89523
- State of Nevada Public Notices Website: www.notice.nv.gov

This agenda has been sent to all members of the Board and other interested persons who have requested an agenda from the Board. Persons who wish to continue to receive an agenda and notice must request so in writing on an annual basis.

SUPPORTING MATERIALS

Supporting material relating to public meetings of the Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board is available at the Board's administrative office located at 6170 Mae Anne Avenue, Suite 1, Reno, Nevada 89523 on the Board's website at https://www.nvspeechhearing.org/about/Minutes.asp or by contacting Jennifer R. Pierce, Executive Director by phone at (775) 787-3421 or email at board@nvspeechhearing.org. Anyone desiring additional information regarding the meeting is invited to call the Board office at (775) 787-3421 or board@nvspeechhearing.org.

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 1

Call to Order, Confirmation of Quorum

Call to Order, Confirmation of Quorum.

Action: Meeting Called to Order

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 2

Public Comment

No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020).

CHAIR/VICE CHAIR: PLEASE READ PRIOR TO CALLING FOR PUBLIC COMMENT:

I will now review the instructions for providing public comment during this meeting:

Any person wishing to make public comment may attend this meeting and provide public comment in one of the following ways:

1. Attend the meeting and provide public comment in-person at the physical location; OR

2. Attend the meeting and provide public comment virtually through the Zoom teleconference video link listed on the agenda; OR

3. Attend the meeting and provide public comment telephonically through the Zoom telephone number listed at the end of the meeting agenda with additional public comment instructions.

Public comment is welcomed by the Board.

- Public comment will be limited to five minutes per person and comments based on viewpoint will not be restricted.

- A public comment time will be available prior to action items on the agenda and on any matter not specifically included on the agenda as the last item on the agenda.

- At the discretion of the Board Chair, additional public comment may be heard when that item is reached.

- The Board Chair may allow additional time to be given a speaker as time allows and in their sole discretion.

- Prior to the commencement and conclusion of a contested case or a quasi-judicial proceeding that may affect the due process rights of an individual, the Board may refuse to consider public comment.

Action: None – Informational Only

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 3

Approval of the Minutes: Board Meeting of February 21, 2024

The minutes of the Board Meeting of February 21, 2024 are presented for approval.

Attachment on next page: *Minutes Not Yet Approved 2024 2 21*

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

MINUTES OF PUBLIC MEETING

Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

February 21, 2024

Members Present:	Andrea Menicucci, Lynee Anderson, Shawn Binn, Jennifer Joy-Cornejo, Branden Murphy, Adrienne Williams
Members Absent:	Timothy Hunsaker
Staff Present:	Jennifer Pierce, Executive Director Stacey Whittaker, Licensing Coordinator Henna Rasul, Sr. Deputy Attorney General, Board Counsel
Public Present:	Nancy Kuhles, Elyse Monroy, Belz & Case "Note-Taking Bot"

Call to Order, Confirmation of Quorum

Andrea Menicucci called the meeting to order at 4:32pm. A roll call confirmed a quorum was present, and Timothy Hunsaker was noted as excused absent.

Public Comment

Andrea Menicucci introduced this agenda item and read the following statement pursuant to AB219 (2023):

> "I will now review the instructions for providing public comment during this meeting: Any person wishing to make public comment may attend this meeting and provide public comment in one of the following ways: 1. Attend the meeting and provide public comment in-person at the physical location; OR 2. Attend the meeting and provide public comment virtually through the Zoom teleconference video link listed on the agenda; OR 3. Attend the meeting and provide public comment telephonically through the Zoom telephone number listed above. Please see additional public comment instructions at the end of this agenda. Public comment is welcomed by the Board. Public comment will be limited to five minutes per person and comments based on viewpoint will not be restricted. A public comment time will be available prior to action items on the agenda and on any matter not specifically included on the agenda as the last item on the agenda. At the discretion of the Board Chair, additional public comment may be heard when that item is reached. The Board Chair may allow additional time to be given a speaker as time allows and in their sole discretion. Prior to the commencement and conclusion of a contested case or a quasi-judicial proceeding that may affect the due process rights of an individual, the Board may refuse to consider public comment."

Ms. Menicucci then called for public comment. There was no public comment.

Approval of the Minutes: Board Meeting and Public Workshop of January 24, 2024

Andrea Menicucci asked if there were any corrections or revisions to the minutes of the meeting and Public Workship of January 24, 2024 and none were noted, so she called for a motion. Adrienne Williams made a motion to approve the minutes of January 24, 2024 as written. Shawn Binn seconded the motion. The motion passed unanimously.

Minutes have not yet been approved and are subject to revision at the next meeting.

Consideration for Review and Approval of Revised FY24 Budget and Contracts for Legislative Services and Licensing Database

Ms. Pierce explained the draft contracts presented during this meeting for the Board's final review and approval, along with a revised FY24 budget with additional expenses added for legislative services in support of the attached contract:

- Revised FY24 Budget: Presented with additional expenses added to cover legislative services in support of the proposed contract to be provided by Strategies 360 in FY24 (April – June), drafted to begin April 1, 2024. Other line items were also adjusted to reflect expenses that were originally budgeted higher than costs actually invoiced.
- Contract DRAFT – Strategies 360: Presented for approval to begin April 1, 2024 and end June 30, 2025 in support of the Board's legislative efforts.
- Contract DRAFT – Albertson Consulting, Inc.: Presented for approval to begin July 1, 2024 and end June 30, 2028. Ms. Pierce explained that a Sole Source Solicitation Waiver has been submitted to the state Purchasing Division in support of this contract as the system is currently in use and is a proprietary program customized by the vendor to this Board's licensing and regulatory needs.

Andrea Menicucci called for questions and there were none and no further discussion was held. Ms. Menicucci called for a motion. Jennifer Joy-Cornejo made a motion to approve the proposed contracts with Strategies 360 and Albertson Consulting, Inc. as drafted, as well as the revised FY24 budget as presented. Adrienne Williams seconded the motion. The motion passed unanimously. Following the motion, Jennifer Joy-Cornejo pointed out that the legislative services line item on the budget only included the amount but not the name of the firm (Strategies 360), and Ms. Pierce stated that she would correct the line item. Andrea Menicucci further suggested, and Ms. Pierce agreed to ask Strategies 360 to attend the April Board Meeting and provide updates on their scope of work and planned timeline for support throughout the session.

Public Comment

There was no public comment.

Adjournment

Andrea Menicucci adjourned the meeting at 4:44pm.

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 4

Public Hearing on Proposed Regulations LCB File R108-23

a. Introduction to Proposed Regulations LCB File R108-23

The proposed regulations do the following:

- **Section 1:** Increases the hearing aid dispensing practical examination fee from $200 to $250.
- **Section 2:** Eliminates the requirement for a Reinstatement Application to include certification by AAA, ASHA, or NBC-HIS.
- **Section 3:** Authorizes the Board, under certain circumstances, to approve and accept a passing score on the written hearing aid dispensing examination taken within the past 24 months (extended from current 12 months).
- **Section 4:** Allows the Board to provide by mail or electronic mail any notice to a licensee that is required by law or regulation.
- **Section 5:** Eliminates the provision that the Board will maintain a list of approved programs of academic training for Hearing Aid Specialist Apprentices.
- **Section 6:** Makes a conforming change to refer to an unlicensed assistant rather than an office assistant, aide, or technician.
- **Section 7:** Amends/expands the duties that may be delegated by a hearing aid specialist or dispensing audiologist to an unlicensed assistant.
- **Sections 8 and 9:** Eliminate obsolete references to the repealed federal regulation regarding medical evaluation or waiver for hearing aids.
- **Section 9:** Repeals the requirement that all formal written communications and documents be addressed to the Board and not to individual members of the Board or its staff.

Attachment on next page: *LCB File R108-23*

Action: None – Informational Only

b. Public Comment on Proposed Regulations LCB File R108-23

No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020).

Action: None – Informational Only

REVISED PROPOSED REGULATION OF THE SPEECH-LANGUAGE PATHOLOGY, AUDIOLOGY AND HEARING AID DISPENSING BOARD

LCB File No. R108-23

February 28, 2024

EXPLANATION – Matter in *italics* is new; matter in brackets [~~omitted material~~] is material to be omitted.

AUTHORITY: § 1, NRS 637B.132 and 637B.175; §§ 2-4 and 7, NRS 637B.132 and 637B.191; §§ 5 and 6, NRS 637B.132 and 637B.194; §§ 8 and 9, NRS 637B.132.

A REGULATION relating to audiology; revising certain fees relating to licensure to engage in the practice of audiology, speech-language pathology or fitting and dispensing hearing aids; revising provisions relating to the written examination for a license to engage in the practice of fitting and dispensing hearing aids; authorizing hearing aid specialists, audiologists or dispensing audiologists to delegate certain duties to unlicensed assistants; prohibiting a hearing aid specialist, audiologist or dispensing audiologist from delegating certain duties to an unlicensed assistant that require professional or advanced training for the practice of audiology or fitting and dispensing hearing aids; revising provisions relating to waivers of certain medical evaluations; eliminating the requirement to address certain written communications and documents to the Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law requires the Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board to adopt regulations establishing standards of practice for persons licensed or endorsed to engage in the practice of audiology, speech-language pathology or fitting and dispensing hearing aids. (NRS 637B.132)

Existing law requires the Board to charge and collect certain fees established by the Board, including a fee for the renewal of a license in an amount not to exceed $100. (NRS 637B.175) Existing regulations set forth the fee for the renewal of a standard, provisional or temporary license. (NAC 637B.030) **Section 1** of this regulation establishes a fee of $50 for the renewal of an inactive license. **Section 1** further increases the examination fee from $200 to $250.

Existing regulations set forth certain requirements an applicant must meet to reinstate his or her license, including that the applicant include with the application for reinstatement proof satisfactory of his or her certification by the American Board of Audiology, the American Speech-Language-Hearing Association or the National Board for Certification in Hearing Instrument Sciences or a successor organization, as applicable. (NAC 637B.0365) **Section 2** of this regulation eliminates this requirement.

Existing law requires the Board to adopt regulations regarding the examination that is required concerning the practice of fitting and dispensing hearing aids. (NRS 637B.194) Existing regulations authorize the Board, under certain circumstances, to approve and accept a passing score on a written examination taken within the immediately preceding 12 months. (NAC 637B.0373) **Section 3** of this regulation instead authorizes the Board, under certain circumstances, to approve and accept a passing score on a written examination taken within the immediately preceding 24 months.

Existing regulations provide that the Board will mail any notice to a licensee that is required by law or regulation to the last known residential address of the licensee but authorize the Board to provide notice to a licensee by electronic mail upon the written consent of the licensee. (NAC 637B.0385) **Section 4** of this regulation provides instead that the Board will provide by mail or electronic mail any notice to a licensee that is required by law or regulation.

Existing law and regulations provide that: (1) a customized program of academic training for an apprentice who is completing in-service training under the supervision of a sponsor to become eligible to apply for a license to engage in the practice of fitting and dispensing hearing aids must be submitted to the Board for evaluation and approval; and (2) the Board will maintain a list of approved programs of academic training. (NRS 637B.025; NAC 637B.0392) **Section 5** of this regulation eliminates the provision that the Board will maintain a list of approved programs of academic training.

Existing regulations authorize a hearing aid specialist or dispensing audiologist to delegate certain duties to an office assistant, aide or technician who is not licensed. (NAC 637B.0442) **Section 7** of this regulation: (1) authorizes a hearing aid specialist, audiologist or dispensing audiologist to instead delegate certain duties to an unlicensed assistant; (2) provides that a hearing aid specialist, audiologist or dispensing audiologist may only delegate duties to an unlicensed assistant that are within the scope of his or her license or endorsement issued by the Board; (3) provides that a hearing aid specialist, audiologist or dispensing audiologist is responsible and civilly liable for any negligence or incompetence of an unlicensed assistant in performing a delegated duty; and (4) prohibits a hearing aid specialist, audiologist or dispensing audiologist from delegating certain duties to an unlicensed assistant that require professional or advanced training for the practice of audiology or fitting and dispensing hearing aids. **Section 6** of this regulation makes conforming changes to refer to an unlicensed assistant rather than an office assistant, aide or technician.

Existing regulations: (1) set forth certain requirements concerning a waiver by a client of a medical evaluation required by federal regulations; and (2) require a hearing aid specialist or dispensing audiologist to prepare and retain a copy of any such waiver. (NAC 637B.0444, 637B.045) Those federal regulations have been repealed. (21 C.F.R. § 801.421; 87 Fed. Reg. 50, 698-01 (Oct. 17, 2022)) **Sections 8 and 9** of this regulation eliminate obsolete references to the repealed federal regulation.

Existing regulations require that all formal written communications and documents be addressed to the Board and not to individual members of the Board or its staff. (NAC 637B.700) **Section 9** further repeals this requirement.

Section 1. NAC 637B.030 is hereby amended to read as follows:

637B.030 The Board will charge and collect the following fees:

Application fee	$150
Fee for a standard license or provisional license	100
Fee for a temporary license	50
Fee for a limited license	25
Fee for renewal of a standard license or provisional license	100
Fee for renewal of ~~[a]~~ ***an inactive or*** temporary license	50
Reinstatement fee for a standard license or provisional license expired 30 days or more	100
Reinstatement fee for a standard license or provisional license expired less than 30 days	75
Examination fee	~~[200]~~ ***250***
Fee for converting to a different type of license	50
Fee for each additional license or endorsement	50
Fee for obtaining license information	50

Sec. 2. NAC 637B.0365 is hereby amended to read as follows:

637B.0365 1. An applicant for reinstatement of his or her license shall include with the application for reinstatement:

(a) Proof satisfactory that the applicant has completed the continuing education that is required of a licensee for the year immediately preceding the application for reinstatement.

(b) The fees imposed by the Board pursuant to NRS 637B.175 for the reinstatement of a license.

~~[(c) Proof satisfactory of his or her certification by the American Board of Audiology, the American Speech-Language-Hearing Association or the National Board for Certification in Hearing Instrument Sciences or a successor organization, as applicable.]~~

2. The reinstatement of a license that has been expired for 30 days or more must not be retroactive.

3. An application to reinstate a license must be submitted not later than 3 years after the date on which the license expired.

Sec. 3. NAC 637B.0373 is hereby amended to read as follows:

637B.0373 1. The examination prescribed by the Board pursuant to NRS 637B.194 must consist of a written portion and a practical portion. The examination may also include a portion that tests the familiarity of an applicant with the provisions of this chapter and chapter 637B of NRS and all other federal laws and regulations relevant to the practice of fitting and dispensing hearing aids in this State.

2. To be eligible to take the examination set forth in subsection 1, an applicant must:

(a) File a completed application with the Executive Director of the Board; and

(b) Pay the examination fee prescribed by NAC 637B.030.

3. The Board will establish the passing score for the examination set forth in subsection 1.

4. If an applicant does not achieve a passing score on the examination set forth in subsection 1, as established by the Board pursuant to subsection 3, he or she may retake the examination not sooner than 30 days after the date of the previous examination upon payment of the examination fee prescribed by NAC 637B.030.

5. The Board may approve and accept a passing score obtained on a written examination taken within the immediately preceding ~~[12]~~ ***24*** months if the examination taken by the applicant was substantially the same as the written portion of the examination prescribed by the Board.

Sec. 4. NAC 637B.0385 is hereby amended to read as follows:

637B.0385 1. Each licensee shall:

(a) Maintain with the Board the licensee's current residential address, business address or other contact information, including, without limitation, the telephone number and electronic mail address of the licensee, if available.

(b) Notify the Board of any change in the information maintained pursuant to paragraph (a) not later than 30 days after the change.

2. ~~[Except as otherwise provided in subsection 3, the]~~ ***The*** Board will provide by United States mail to the last known residential address ***or by electronic mail to the last known electronic mail address*** of the licensee provided pursuant to paragraph (a) of subsection 1 any notice to a licensee that is required by law or regulation.

~~[3. The Board may provide a notice to a licensee by electronic mail upon the prior written consent of the licensee.]~~

Sec. 5. NAC 637B.0392 is hereby amended to read as follows:

637B.0392 1. The academic portion of the in-service training of an apprentice required by NAC 637B.0391 must be specific to the training and education necessary to perform competently the duties and responsibilities necessary for the practice of fitting and dispensing hearing aids and must include, without limitation, training and education concerning:

(a) Laws and rules relating to ethics;

(b) Federal laws and rules governing hearing aids;

(c) Infection controls;

(d) Basic hearing science;

(e) Hearing instrument science and fitting practices; and

(f) Audiometric testing and masking.

2. Except as otherwise provided in subsection 3, a customized program of academic training and a proposed curriculum must be submitted to the Board for evaluation and approval.

3. A program of academic training accepted by the National Board for Certification in Hearing Instrument Sciences, the International Hearing Society or an accredited institution of higher education that meets the minimum requirements of subsection 1 does not require the approval of the Board.

~~[4. The Board will maintain a list of approved programs of academic training.]~~

Sec. 6. NAC 637B.0398 is hereby amended to read as follows:

637B.0398 1. A sponsor of an apprentice shall:

(a) Except as otherwise provided in subsection 3, provide direct supervision to the apprentice;

(b) Determine the competency level of the apprentice to perform tasks relating to fitting and dispensing hearing aids;

(c) Evaluate the work of the apprentice;

(d) Document the training provided to and the direct supervision of the apprentice; and

(e) Provide written notification to the Board if:

(1) The apprentice is no longer under the sponsorship of the sponsor;

(2) The apprentice withdraws from or terminates his or her in-service training;

(3) The sponsor withdraws as a sponsor for the apprentice;

(4) The apprentice has completed 1 year of in-service training under the direct supervision of the sponsor and the sponsor believes that the apprentice is competent to work without physical on-site supervision; or

(5) The apprentice successfully completes all the requirements for in-service training.

2. All work completed by an apprentice must be reviewed daily and signed by the sponsor and the apprentice.

3. An apprentice is not required to be under the direct supervision of a sponsor when performing any of the duties that may be delegated to an ~~[office]~~ ***unlicensed*** assistant ~~[, aide or technician]~~ pursuant to ~~[subsection 1 of]~~ NAC 637B.0442.

4. An apprentice shall not maintain, run or operate an office or a satellite office in which hearing aids are fitted and dispensed without the approval of the Board.

5. As used in this section, “direct supervision” means:

(a) During the first year of the in-service training of an apprentice, being physically on-site at the same location as the apprentice.

(b) After the first year of the in-service training of an apprentice and upon attaining the approval of the Board, daily communication with the apprentice without the requirement of being physically on-site at the same location as the apprentice.

Sec. 7. NAC 637B.0442 is hereby amended to read as follows:

637B.0442 1. Except as otherwise provided in ~~[subsection 2,]~~ ***this section,*** a hearing aid specialist ***, audiologist*** or dispensing audiologist may delegate certain duties to an ~~[office]~~ ***unlicensed*** assistant ~~[, aide or technician who is not licensed pursuant to this chapter and chapter 637B of NRS and does not possess the professional or advanced training required for the practice of fitting and dispensing hearing aids]~~ if ~~[the]~~ ***:***

(a) The duty being delegated is within the scope of the license or endorsement of the hearing aid specialist, audiologist or dispensing audiologist; and

(b) The hearing aid specialist ***, audiologist*** or dispensing audiologist determines, before delegating a duty, that the ~~[office]~~ ***unlicensed*** assistant ~~[, aide or technician]~~ possesses the necessary knowledge, competence, training and skills to perform the duty.

2. If a hearing aid specialist, audiologist or dispensing audiologist delegates a duty to an unlicensed assistant, the hearing aid specialist, audiologist or dispensing audiologist is responsible and civilly liable for any negligence or incompetence of the unlicensed assistant in performing the duty.

3. The duties that may be delegated to an ~~[office]~~ ***unlicensed*** assistant ~~[, aide or technician]~~ pursuant to this section include, without limitation:

(a) Cleaning ~~[a]~~ hearing ~~[aid;]~~ ***aids and amplification devices;***

(b) Repairing or replacing a broken part of a hearing aid with the same part;

(c) Replacing a thin tube or dome with a similar size or style;

(d) Replacing filters;

(e) Returning to a client a repaired hearing aid that does not require fitting, programming or adjusting;

(f) Accepting an in-office return of a hearing aid if a receipt is provided to the client to document proof of the return; ~~[and]~~

(g) Performing clerical, secretarial and general administrative duties, including, without limitation, providing information that is readily available to the general public ~~[.~~

~~2.]~~ ***;***

(h) Greeting, escorting and scheduling clients;

(i) Packaging and mailing orders of earmolds, repaired devices and returns to manufacturers or laboratories;

(j) Maintaining inventories of supplies and checking the function of equipment;

(k) Performing checks on hearing aids and other amplification devices;

(l) Performing troubleshooting and minor repairs to hearing aids, earmolds and other amplification devices;

(m) Performing electroacoustic analysis of hearing aids and other amplification devices;

(n) Demonstrating alerting and assistive listening devices;

(o) Verbally instructing a client in proper ear hygiene;

(p) Assisting a hearing aid specialist, audiologist or dispensing audiologist with treatment programs;

(q) Assisting a hearing aid specialist, audiologist or dispensing audiologist with setup and technical tasks;

(r) Preparing materials for an ear impression;

(s) Maintaining and restocking test and treatment rooms;

(t) Performing equipment maintenance and biological checks;

(u) Performing infection control duties within the clinic;

(v) Assisting a client in completing a case history or other relevant forms;

(w) Interacting with a manufacturer or supplier of hearing instruments regarding the status of an order or repair; and

(x) Translating and interpreting only if the unlicensed assistant is fluent in a language other than English and has the necessary training and skills to perform such translation or interpretation.

4. The following duties that involve direct physical contact with a client or a hearing-related procedure or instrument may be delegated to an unlicensed assistant pursuant to this section:

(a) Instructing a client in the proper use and care of hearing aids and other amplification devices;

(b) Conducting hearing and tympanometric screening on older children and adults without interpretation;

(c) Conducting an otoacoustic emission screening;

(d) Performing a nondiagnostic otoscopy;

(e) Performing a pure-tone audiologic reassessment on an established client;

(f) Preparing a client for electronystagmography and videonystagmography or evoked testing;

(g) Assisting a hearing aid specialist, audiologist or dispensing audiologist in testing the hearing of a pediatric client; and

(h) Performing a pure-tone hearing screening and universal newborn hearing screening test.

5. A hearing aid specialist ***, audiologist*** or dispensing audiologist shall not delegate any duty to an ~~[office]~~ ***unlicensed*** assistant ~~[, aide or technician]~~ pursuant to this section that requires professional or advanced training for the practice of ***audiology or*** fitting and dispensing hearing aids. Duties that may not be delegated pursuant to this section include, without limitation:

(a) Removing a hearing aid from or placing a hearing aid into a client’s ear;

(b) Programming, adjusting or fitting a hearing aid;

(c) Conducting an interview, examination or evaluation relating to a client's hearing or hearing loss; ~~[and]~~

(d) ~~[Conducting]~~ ***Except for the duties that may be delegated to an unlicensed assistant pursuant to subsection 4, conducting*** any activity involving direct physical contact with a client and a hearing-related procedure or instrument ~~[.;]~~ ***;***

(e) Determining case selection or evaluation protocols;

(f) Interpreting observations or data into a diagnostic statement of a clinical management strategy or procedure;

(g) Participating in a team or case conference or on any interdisciplinary team without the presence of a supervising audiologist or an audiologist designated by the supervising audiologist;

(h) Writing, developing or modifying a client's individualized treatment plan;

(i) Assisting a client without following the treatment plan prepared by the respective hearing aid specialist, audiologist or dispensing audiologist without proper supervision;

(j) Composing or signing any formal document such as a treatment plan, reimbursement form, progress note or other report, as applicable;

(k) Transmitting or disclosing clinical information, either verbally or in writing, to anyone, including, without limitation, the client, without the approval of the supervising hearing aid specialist, audiologist or dispensing audiologist;

(l) Selecting a client for treatment services or discharging a client from treatment services;

(m) Counseling or consulting with a client, a family member of a client or others regarding the client's status or treatment services or making referrals for additional services; and

(n) An unlicensed assistant referring to himself or herself, either verbally or in writing, with a title other than one designated by the supervising hearing aid specialist, audiologist or dispensing audiologist.

Sec. 8. NAC 637B.045 is hereby amended to read as follows:

637B.045 1. A speech-language pathologist or audiologist shall prepare and retain health care records for each client he or she treats in accordance with NRS 629.051. As used in this subsection, "health care records" has the meaning ascribed to it in NRS 629.021.

2. A hearing aid specialist or dispensing audiologist shall prepare and retain records of fitting, servicing or dispensing a hearing aid for each client he or she treats. The records must be retained for not less than 5 years after the record is prepared and may be created, authenticated and stored in a computer system that limits access to those records or is maintained in any other form which ensures that the records are easily accessible by the hearing aid specialist or dispensing audiologist. Each record must include, without limitation:

(a) The name, address, telephone number and date of birth of the client;

(b) The medical history of the client as it relates to his or her loss of hearing;

(c) The dates on which the hearing aid was delivered, fitted and adjusted, and notations of all procedures performed on such dates, and, if applicable, the date of return or attempted return of the hearing aid;

(d) Audiograms of the client;

(e) The specifications of the hearing aid, including the serial number of the hearing aid as indicated by the manufacturer of the hearing aid;

(f) The settings for the hearing aid;

(g) The progress and disposition of the case; ***and***

(h) A copy of the contract for the sale of the hearing aid. ~~[; and~~

~~(i) A copy of any waiver of the medical evaluation required by 21 C.F.R. § 801.421.]~~

Sec. 9. NAC 637B.0444 and 637B.700 are hereby repealed.

TEXT OF REPEALED SECTIONS

637B.0444 Requirements concerning waiver by client of medical evaluation. (NRS 637B.132) If a hearing aid specialist or dispensing audiologist offers a client a waiver of the medical evaluation required by 21 C.F.R. § 801.421, the hearing aid specialist or dispensing audiologist shall:

1. Verbally explain the waiver to the client before the client signs the waiver; and

2. Provide the written waiver on a form separate from any other form that the client is required to sign.

637B.700 Address for written communications and documents to Board. (NRS 637B.132) All formal written communications and documents must be addressed to the Board and not to individual members of the Board or its staff.

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 5

Consideration to Adopt Proposed Regulations LCB File R108-23

The Board will consider adoption of the proposed regulations taking into consideration comments from the public.

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 6

Update and Report Out from Strategies 360 on Legislative and Lobbying Activities for 2024 Interim and 2025 Legislative Session

Izack Tenorio of Strategies, 360 will provide the Board with an update on plans and activities related to the 2024 Interim and planned BDR in the 2025 legislative session.

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 7

Consideration to Approve Proposed Revisions to NRS 637B for Inclusion in 2025 Legislative Effort with Recommendations from Advisory Committee on Fitting and Dispensing Hearing Aids and Speech-Language Pathology Subcommittee

A number of NRS sections have been reviewed and approved by the Board for inclusion in the planned 2025 BDR. The NRS sections below are either 1) proposed for inclusion in the 2025 BDR and presented for the Board's review and approval, or 2) are still under consideration. It is hoped that a final draft of all proposed NRS revisions will be ready for review at the Board's July 2024 meeting.

a. Revisions Related to Audiology: Report Out and Recommendations from Advisory Committee on Fitting and Dispensing Hearing Aids

The proposed revisions in this section relate to the Board's approval to seek repeal of NRS 637B.205, eliminating examination and endorsement requirements for an Audiologist to fit and dispense hearing aids. The revisions below were reviewed and recommended by the Advisory Committee on Fitting and Dispensing Hearing Aids at its April 10, 2024 meeting. <u>It is proposed that the Board approve these recommended revisions.</u>

Note: Revisions highlighted in gray have already been approved by the Board.

1) NRS 637B.050 "Practice of audiology" defined.

"Practice of audiology" means the application of principles, methods and procedures relating to hearing and balance, hearing disorders and related speech and language disorders and includes, without limitation:

1. The conservation of auditory system functions;
2. Screening, identifying, assessing and interpreting, preventing and rehabilitating auditory and balance system disorders;
3. The ordering the use of, selection, fitting, programming and dispensing of hearing aids, the programming of cochlear implants and other technology which assists persons with hearing loss and training persons to use such technology; ["only when holding the dispensing endorsement required pursuant to NRS 637B.205".]
4. Providing vestibular and auditory rehabilitation, cerumen management and associated counseling services;
5. Conducting research on hearing and hearing disorders for the purpose of modifying disorders in communication involving speech, language and hearing;
6. Providing referral services for medical diagnosis and treatment; and
7. At the request of a physician, participating in the diagnosis of a person.

2) NRS 637B.075 Sponsor" defined.

"Sponsor" means a hearing aid specialist or [dispensing] audiologist who is responsible for the direct supervision and in-service training of an apprentice in the practice of fitting and dispensing hearing aids.

3) NRS 637B.100 Creation; number, appointment and qualifications of members; terms; vacancies.

1. The Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board, consisting of seven members
appointed by the Governor, is hereby created.
2. The Governor shall appoint:
   (a) Three members who are speech-language pathologists, each of whom must practice in a different setting, including, without limitation, a university, public school, hospital or private practice;
   (b) Two members who are audiologists[, at least one of whom must be a dispensing audiologist];
   (c) One member who is a hearing aid specialist; and
   (d) One member who is a representative of the general public. This member must not be:
      (1) A speech-language pathologist, a hearing aid specialist or an audiologist; or
      (2) The spouse or the parent or child, by blood, marriage or adoption, of a speech-language pathologist, a hearing aid specialist or an audiologist.
3. Each member of the Board who is an audiologist, a speech-language pathologist or a hearing aid specialist must:
   (a) Have practiced, taught or conducted research in his or her profession for the 3 years immediately preceding the appointment; and
   (b) Hold a current license issued pursuant to this chapter.
4. A person who is a stockholder in a manufacturer of hearing aids may not be selected to or serve as a member of the Board.
5. After the initial terms, each member of the Board serves a term of 3 years.
6. A member of the Board shall not serve for more than two terms.
7. If a vacancy occurs during the term of a member, the Governor shall appoint a person similarly qualified to replace that member for the remainder of the unexpired term.

4) NRS 637B.175 Fees.

1. The Board shall charge and collect only the following fees whose amounts must be determined by the Board, but may not exceed:

Application fee	[$150]	**$ 300**
License fee	[100]	**200**
Fee for the renewal of a license	[100]	**200**
Reinstatement fee	[100]	**300**
Examination fee	[300]	**500**
Fee for converting to a different type of license		50
Fee for each additional license [or endorsement]		50
Fee for obtaining license information	[50]	**200**

2. If an applicant submits an application for a license by endorsement pursuant to NRS 637B.204, the Board shall collect not more than one-half of the fee set forth in subsection 1 for the initial issuance of the license.
3. All fees are payable in advance and may not be refunded.

5) NRS 637B.191 Regulations concerning examinations for, period of validity of, renewal and reinstatement of licenses; placement of license on inactive status.

1. The Board shall adopt regulations prescribing:
   (a) The examinations required pursuant to NRS 637B.160 and concerning the practice of audiology and the practice of speech-language pathology;
   (b) The period for which a license issued pursuant to the provisions of this chapter is valid which, except as otherwise provided in NRS 637B.200 and 637B.202, must be not less than 1 year; and
   (c) The manner in which a license [or endorsement] issued pursuant to this chapter must be renewed, which may include requirements for continuing education.

2. The Board may adopt regulations providing for the late renewal of a license and the reinstatement of an expired license, except that the Board must not renew or reinstate a license more than 3 years after the license expired.
3. The Board may, at the request of a person licensed pursuant to this chapter, place a license on inactive status if the holder of the license:
   (a) Does not engage in, or represent that the person is authorized to engage in, the practice of audiology, speech-language pathology or fitting and dispensing hearing aids in this State; and
   (b) Satisfies any requirements for continuing education prescribed by the Board pursuant to this section.

6) NRS 637B.236 Apprentices: Supervision of and responsibility for work; selection of hearing aid; signing of audiogram or sales document.

1. All work performed by a licensed apprentice must be directly supervised by a hearing aid specialist or [dispensing] audiologist, and the hearing aid specialist or [dispensing] audiologist is responsible and civilly liable for the negligence or incompetence of the licensed apprentice under his or her supervision.
2. Any selection of a hearing aid for a customer made by a licensed apprentice must be approved by a hearing aid specialist or [dispensing] audiologist.
3. Any audiogram or sales document prepared by a licensed apprentice must be signed by the apprentice and the supervising hearing aid specialist or [dispensing] audiologist.
4. As used in this section:
   (a) "Incompetence" means a lack of ability to practice safely and skillfully as a licensed apprentice arising from:
      (1) A lack of knowledge or training; or
      (2) An impaired physical or mental capability, including an alcohol or other substance use disorder.
   (b) "Negligence" means a deviation from the normal standard of professional care exercised generally by apprentices.

7) NRS 637B.242 Sale of hearing aids by catalog, mail or Internet: Conditions; records; regulations.

(1) A hearing aid specialist or [dispensing] audiologist licensed pursuant to this chapter may sell hearing aids by catalog, mail or the Internet if[:]

[(a) The hearing aid specialist or dispensing audiologist has received:

(1) A written statement signed by:

(I) A physician or physician assistant licensed pursuant to chapter 630 or 633 of NRS, an advanced practice registered nurse licensed pursuant to NRS 632.237, an audiologist or a hearing aid specialist which verifies that he or she has performed an otoscopic examination of the person to whom the hearing aid will be sold and the results of the examination indicate that the person may benefit from the use of a hearing aid;

(II) A physician or physician assistant licensed pursuant to chapter 630 or 633 of NRS, an audiologist or a hearing aid specialist which verifies that he or she has performed an audiometric examination of the person to whom the hearing aid will be sold and the results of the examination indicate that the person may benefit from the use of a hearing aid; and

(III) A dispensing audiologist or a hearing aid specialist which verifies that an ear impression has been taken of the person to whom the hearing aid will be sold; or

(2) A waiver of the medical evaluation signed by the person to whom the hearing aid will be sold as authorized pursuant to 21 C.F.R. § 801.421(a)(2); and]

[(b) T]the person to whom the hearing aid will be sold has signed a statement acknowledging that the hearing aid specialist or [dispensing] audiologist is selling him or her the hearing aid by catalog, mail or the Internet based upon the information submitted by the person in accordance with this section.

(2) A hearing aid specialist or [dispensing] audiologist who sells hearing aids by catalog, mail or the Internet pursuant to this section shall maintain a record of each sale of a hearing aid made pursuant to this section for not less than 5 years.

(3) The Board may adopt regulations to carry out the provisions of this section, including, without limitation, the information that must be included in each record required to be maintained pursuant to subsection 2.

8) NRS 637B.243 Audiograms for use of physician or member of related profession.

A hearing aid specialist or [dispensing] audiologist, upon request by a physician or a member of a related profession specified by the Board, may make audiograms for the physician's or member's use in consultation with a person who suffers from impaired hearing.

Action: Approve, Table, or Take No Action on the Matter

b. Revisions Related to Fitting and Dispensing Hearing Aids: Report Out and Recommendations from Advisory Committee on Fitting and Dispensing Hearing Aids

1) Clarification on Recommendations Made for Revisions to NRS 637B and NAC 637B Regarding HAS License Requirements

The Committee considered a recommendation to clarify its recommendation for the training required for a Standard HAS license if the NBC-HIS requirement is removed. The intention of the original recommendation was that this experience be independent practice experience, not supervised training. As such, the minutes of the January 16, 2024 were corrected as follows "to require 1 year of licensed independent dispensing experience for a Standard HAS applicant who is licensed or has prior training/experience. It is proposed that the Board approve this clarified recommendation.

Action: Approve, Table, or Take No Action on the Matter

2) NRS 637B.044 "Hearing aid" defined and NRS 637B.NEW "Over-the-counter hearing aid" defined

The Committee reviewed potential revisions to this definition in the context of the FDA Final Rule on Over-the-Counter Hearing aids, assessing the current NRS definition and examples from FDA, the Code of Federal Regulations (CFR), and North Carolina, and recommended the Board retain the current NRS definition of a hearing aid with the addition of the CFR definition and add the new over-the-counter hearing aid definition to the planned NRS revisions. No action by the Board is proposed at this time as draft revisions will be presented to the Committee at its next meeting for a final recommendation to the Board.

Action: Approve, Table, or Take No Action on the Matter

3) NRS 637B.055 "Practice of fitting and dispensing hearing aids" defined.

This section of NRS has been under review and revision since 2021, and the proposed version below was presented to the Board at its January 2024 meeting. Concerns were raised specific to the addition of cerumen management and the matter was sent back to the Committee for further deliberation and recommendation.

"Ordering the Use of" Language: Guidance on the FDA Final Rule indicated there was no need to revise state laws & regulations to address "prescribing" traditional hearing aids, however IHS has recommended that states add this "ordering the use of" language to clarify scope of practice. This was reviewed and recommended for revision by the Advisory Committee, and it is proposed that the Board approve this recommendation.

Cerumen Management & Definition: After much discussion around acceptable scope of practice and risks, the Committee recommended adding this to the scope of practice with prescribed guidelines similar to this in place in Tennessee. No action by the Board is proposed at this time as draft revisions will be presented to the Committee at its next meeting for a final recommendation to the Board.

Tinnitus Care & Definition: After discussion around acceptable scope of practice and risks, the Committee recommended adding this to the scope of practice with verbiage that includes a requirement for a practitioner to have completed "a Board-approved certification or course in tinnitus care", as well as a new definition for tinnitus care. No action by the Board is proposed at this time as draft revisions will be presented to the Committee at its next meeting for a final recommendation to the Board.

Action: Approve, Table, or Take No Action on the Matter

4) **Review and Recommendation to the Board on Possible Revisions to Examination Requirements in NRS 637B and NAC 637B for HAS License to Engage in the Practice of Fitting and Dispensing Hearing Aids**
Following the discussions on HAS training and licensing requirements at the January 2024 Committee and Board meetings, the Board office received a request from IHS for the Board to consider waiving both the written and practical dispensing examinations for an applicant holding current NBC-HIS certification. IHS suggests that since NBC-HIS certification includes an exam demonstrating skills and knowledge, a person who has passed that exam and is maintaining board certification should be able to move from one state, where licensed, to another without taking the entry licensure exam.

Currently, NAC 637B allows the Board to accept a passing score within the past 12 months on the Written ILE exam, and this has been identified to extend to 24 months in the Board's current revision in LCB File R108-23 scheduled for a public hearing later this month.

- Florida's HAS license requirements were cited as an example, though Florida does not require a practical examination.
- 40 states currently require a HAS applicant to pass both a written and practical examination, and 9 states require only a written examination.
- Many states indicate some level of reciprocity granted, but the number of states that fully waive examination requirements for those holding NBC-HIS certification and/or out-of-state licensure is unknown.
- In addition to a waiver for NBC-HIS certification, the Committee may consider whether to recommend a waiver for either exam when an applicant has passed the same IHS version of either exam in another state.

Consensus following discussion was that it seemed reasonable to consider accepting a score on the same or a "substantially equivalent" exam from an applicant holding an out-of-state license in good standing, and to consider accepting current NBC-HIS certification in lieu of the Written ILE exam.

The matter was tabled with plans to review drafted examples of NRS and NAC revisions at the next meeting to better visualize the changes and further consider recommendations. No action was taken.

No action by the Board is proposed at this time as the Committee will discuss the matter further at its next meeting.

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

c. **Revisions Related to Speech-Language Pathology: Report Out and Recommendations from SLP Subcommittee**

The Speech-Language Pathology Subcommittee was established by the Board at its January 24, 2024 meeting and been tasked with making recommendations on the three matters below for inclusion in a BDR during the 2025 legislative session to revise NRS 637B and potential related revisions to NAC 637B:

- Licensing SLP Assistants (NRS New Section)
- Telesupervision (NRS New Section)
- Addressing FEES Procedure in SLP Scope of Practice NRS 637B.060

The Committee is comprised of the following nine (9) Board and non-Board members:

- Kim Reddig, M.S. CCC-SLP, ASHA & WCSD, SLP Subcommittee Chair
- Shawn Binn, CCC-SLP, Board Member
- Marvelee Clayworth, M.S., CCC-SLP Carson City School District, SLP Department Chair
- Christy Fleck, Ph.D., CCC-SLP, Asst Professor of Speech Language Pathology, Nevada State University
- Nancy Kuhles, M.S., CCC-SLP ASHA Fellow & NSHA Coalition Co-Chair
- Branden Murphy, MSNed, RN, CPN, Board Member
- Katrina Nicholas, PhD, CCC-SLP, Asst Professor of Speech Language Pathology, Nevada State University
- Andrea Menicucci, CCC-SLP, Board Chair
- Adrienne Williams, CCC-SLP, Board Member

The Committee met on February 21, 2024 and March 25, 2024, and will meet again May 21, 2024. It is hoped that final recommendations on NRS revisions will be ready for the Board to consider at its July 2024 meeting in preparation for the planned BDR. While no action has been made to make formal recommendations to the Board, progress has been made during work sessions on potential NRS and NAC language. No action by the Board is requested at this time as draft revisions will be presented to the Subcommittee at its next meeting to consider final recommendations to the Board.

1) **NRS NEW SLP Assistants; and**
2) **NRS NEW Telesupervision**

The following sections have been drafted, reviewed and discussed by the Committee, and scheduled for recommendation at its next meeting:

- Definitions
  - NRS NEW: “ Speech-Language Pathology Assistant” Defined; “Supervising Speech-Language Pathologist” Defined.
  - NAC NEW: “Direct Supervision” Defined; “Indirect Supervision” Defined; “Medically Fragile” Defined; “Supervision” Defined; “Plan Of Care” Defined; “Provisional Licensee” Defined; And “Telesupervision” Defined.
- Qualifications/Education/Examination:
  - NRS NEW: Speech-language pathology assistants**:** Educational requirements; Speech-language pathology assistants**:** Regulations; and Examination for licensure as a speech-language pathology assistant.
- Scope of Practice/Prohibited Activities
  - NRS NEW: Requirements For Speech-Language Pathology Assistant or Provisional Licensee to Assist in Practice of Speech-Language Pathology.
  - NAC NEW: Speech-Language Therapy Assistant or Provisional Licensee: Delegation of Duties By Supervising Speech-Language Pathologist; Limitations; and Speech-language pathology assistant prohibited from performing certain activities; disciplinary action.

- Continuing Education:
  - NAC 637B.400 Requirements for renewal of standard or provisional license; records; audits; excess credits may not be carried forward.
- Fees for Application, License, & Renewal
  - NRS 637B.175 Fees.
  - NAC 637B.030 Schedule of fees.

The following sections have been drafted, reviewed and discussed by the Committee, and are scheduled for recommendation at its next meeting:

- SLPA Supervision: NAC: Qualifications to act as a supervising speech-language pathologist; supervision ratios; Speech-language pathology assistant or provisional licensee: Verification to Board of employment and supervision; notice of termination; number of primary supervisors required per employer of record; and Speech-language pathology assistant or provisional licensee: Practice under supervision of supervising speech-language pathologist.
- TBD: Supervision of Student Interns and Clinical Fellows
- Applicability of Chapter/Alignment With NDE Assistants: NRS 637B.080 Applicability of chapter.
- TBD: SLPA Telepractice

3) NRS 637B.060 "Practice of speech-language pathology" defined to address Flexible Endoscopic Evaluation of Swallowing (FEES) Procedure

Consensus in Committee discussions is to not recommend adding specific language regarding the FEES procedure, and instead, a slight revision to the wording in #5 of this section, *"The use of oral and nasal endoscopy for the purpose of vocal tract imaging and visualization"* could better encompass the range of tools used by SLPs without being too prescriptive. No action by the Board is requested at this time as draft revisions will be presented to the Subcommittee at its next meeting to consider final recommendations to the Board.

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 8

Disciplinary Matters: Case S23-02 Recommended for Dismissal

Case #S23-02
The Complaint alleged unprofessional conduct, attempting to influence a client to derive financial benefits, failure to complete reports in a timely manner, premature termination of services, and conduct that is harmful to the public health and safety. After investigation and review of all documentation received on this complaint, it has been determined that there is insufficient evidence to file a formal complaint for hearing before the Board and the facts set forth in the accusations are insufficient to establish a violation of Chapter 637B of the Nevada Revised Statutes or the Nevada Administrative Code. This case is recommended for dismissal.

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 9

Executive Director’s Report

Please see the Written Executive Director’s Report.

Attachments on next page:

1. *ED Report 4 24 2024*
2. *FY24 Q3 Financial Reports*

Action: Approve, Table, or Take No Action on the Matter

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board
6170 Mae Anne Avenue, Suite 1, Reno, NV 89523
(775) 787-3421 / Fax (775) 746-4105
www.nvspeechhearing.org Email board@nvspeechhearing.org

EXECUTIVE DIRECTOR'S REPORT

April 24, 2024

a. Licensure Statistics

The following chart provides licensing statistics for the period January 1, 2024 through March 31, 2024 with a net increase of 2 licenses (64 issued/62 expired), a less than 1% increase from the prior quarter. This increase is the first increase in prior years' 2nd quarters since FY16.

Description	Total Licensees	Speech Pathologists	Audiologists	Dispensing Audiologists	Hearing Aid Specialists	Apprentices
Dec 31, 2023	**1592**	**1315**	**70**	**109**	**84**	**14**
Issued	64	53	4	1	5	1
Expired	62	50	5	2	2	3
Mar 31, 2023	**1594**	**1318**	**69**	**108**	**87**	**12**
Net Change	+2	+3	-1	-1	+3	-2
	+.13%	+.23%	-1%	-1%	+4%	-14%

b. FY24 Q3 Financial Report

The FY24 Q3 Financial Summary is attached for the Board's review, with both income and expenses ending less than the 75% target for the third quarter as listed below.

Profit and Loss Through Q3

- Total Revenue: $159,695.38 Percent of Budget: 72.92%
- Deferred Revenue: $89,889.59
- Total Expenses: $160,259.00 Percent of Budget: 73.58%
- **Net Income: $-563.62**

FY24 Q3 Balance Sheet

- Total Cash Assets: $213,113.88
- Total Liabilities: $106,458.117
- **Total Equity: $120,153.24** (Decrease of $1,867.41 from last quarter; Increase of $2,780.39 from FY23 Q3)

FY24 Q3 Deviations from Budget

One factor in the current summary is the expected repayment of legal fees due from the four Consent Decrees approved by the Board in October 2023 and January 2024 (see new line item *Fees* in Income section). To date, fines assessed in three of these cases have been paid in full, though a portion of one was paid during the current Q4 and will be reflected in the next summary. One case resulted in an almost $8,000 judgement and is being repaid in installments and will take some time to recoup.

Legal fees continue to increase due to complaint cases and additional Board and Committee/ Subcommittee meetings. During this quarter, there were no other unanticipated deviations.

c. Board Member Appointments/Reappointments

Name	Credential/Role	Location	Term	Term Expires	Eligible for Reappointment
Andrea Menicucci	SLP/Board Chair	Reno	2	7/1/2024	No
Timothy Hunsaker	AuD-D/Board Vice Chair	Las Vegas	2	7/1/2025	No
Lynee Anderson	BC-HIS	Reno	1	7/1/2024	Yes
Shawn Binn	SLP	Reno	1	9/30/2026	Yes
Jennifer Joy-Cornejo	AuD-D	Las Vegas	1	9/30/2026	Yes
Branden Murphy	Public Member	Las Vegas	1	11/30/2026	Yes
Adrienne Williams	SLP	Las Vegas	1	7/1/2025	Yes

Andrea Menicucci’s second term will expire on 7/1/2024, at which time a new member is expected to be appointed and the Board will be tasked with electing a new Chair. While she is terming off the Board, she is eligible to and has agreed to remain on as a member of the SLP Subcommittee. Lynee Anderson’s first term also expires 7/1/2024 and she is eligible to apply for reappointment.

d. Complaints

There was **one** open complaint case following the last report-out at the January 24, 2024 Board Meeting. **Three** new complaints were received in March & April 2024 respectively, with one screened out and two cases opened for investigation, totaling **three** open cases. **One** case will be presented in this meeting with a recommendation for dismissal, and if approved, **two open cases** will remain.

The Board received no reports of unlicensed practice since the January 2024 meeting.

BEASP

Profit Loss Budget vs. Actual

July 2023 through March 2024

	Approved Budget	Actuals July 23 - Mar 24	Remaining Balance	% of Budget Spent
Ordinary Income/Expense				
Income				
Fees	41,832.00	22,175.00	19,657.00	53.01%
License Fees	167,122.80	124,708.97	42,413.83	74.62%
Fines	0.00	7,603.36	-7,603.36	100.00%
Exams, List and Interest	10,050.42	5,208.05	4,842.37	51.82%
Total Income	219,005.22	159,695.38	59,309.84	72.92%
Expense				
Personnel Cost	162,922.53	120,494.17	42,428.36	73.96%
Attorney General / Legal Fees	8,000.00	8,095.83	-95.83	101.20%
Audit Fees	15,000.00	10,000.00	5,000.00	66.67%
Bank Service Charges	4,600.00	3,412.40	1,187.60	74.18%
Board Compensation	2,925.00	2,250.00	675.00	76.92%
Dues	550.00	440.00	110.00	80.00%
Equipment Purchase	500.00	836.67	-336.67	167.33%
Examinations	4,240.00	1,918.50	2,321.50	45.25%
Insurance	1,350.00	1,618.59	-268.59	119.90%
Licensing Program Subscription	7,650.00	5,466.64	2,183.36	71.46%
Meeting Expenses	100.00	0.00	100.00	0.00%
Office Lease	3,400.00	2,194.29	1,205.71	64.54%
Office Supplies	750.00	94.22	655.78	12.56%
Postage	400.00	275.86	124.14	68.97%
Printing	200.00	0.00	200.00	0.00%
Professional Fees				
Investigation Fees	1,000.00	0.00	1,000.00	0.00%
Accounting	3,000.00	2,250.00	750.00	75.00%
IT / Technical Support	500.00	265.00	235.00	53.00%
Total Professional Fees	4,500.00	2,515.00	1,985.00	55.89%
Telephone	525.00	646.83	-121.83	123.21%
Travel				
In-state Travel	200.00	0.00	200.00	0.00%
Out of State Travel	0.00	0.00	0.00	0.00%
Total Travel	200.00	0.00	200.00	0.00%
Total Expense	217,812.53	160,259.00	57,553.53	73.58%
Net Ordinary Income	1,192.69	-563.62	1,756.31	-47.26%
Net Income	**1,192.69**	**-563.62**	**1,756.31**	**-47.26%**

BEASP

Balance Sheet

As of March 31, 2024

	Mar 31, 2024
ASSETS	
Current Assets	
Checking/Savings	
Wells Fargo Bank - Checking	110,146.07
Wells Fargo Bank - Savings	102,967.81
Total Checking/Savings	213,113.88
Other Current Assets	
Accounts Receivable	6,546.51
Prepaid Expenses	5,614.97
Total Other Current Assets	12,161.48
Fixed Assets	
Capital Assets	1,335.99
Total Fixed Assets	1,335.99
TOTAL ASSETS	**226,611.35**
LIABILITIES & EQUITY	
Liabilities	
Current Liabilities	
Accounts Payable	
Accounts Payable	0.00
Total Accounts Payable	0.00
Other Current Liabilities	
Deferred Revenue	89,889.59
Paid Time Off	13,497.75
Payroll Liabilities	2,866.29
Payroll Tax Liability	204.48
Total Other Current Liabilities	106,458.11
Total Current Liabilities	106,458.11
Total Liabilities	106,458.11
Equity	
Invested in Capital Assets	1,335.99
Retained Earnings	119,380.87
Net Income	-563.62
Total Equity	120,153.24
TOTAL LIABILITIES & EQUITY	**226,611.35**

BEASP
Transaction Detail by Account
January through March 2024

Type	Date	Num	Name	Memo	Amount
Wells Fargo Bank - Checking					
Deposit	01/01/2024			Deposit	1,000.00
Check	01/02/2024	1823	Numbers, Inc.	Bookkeeping services	-750.00
Check	01/02/2024	1824	Attorney General	Legal fees	-408.30
Check	01/02/2024	1825	Coulson and Associates	Audit fees	-10,000.00
Check	01/02/2024	1826	Board of Occupational Therapy	Postage reimbursement	-46.68
Deposit	01/02/2024			Deposit	750.00
Liability Check	01/03/2024		QuickBooks Payroll Service	Payroll expense	-4,317.63
Deposit	01/03/2024			Deposit	950.00
Paycheck	01/04/2024	DD1308	Jennifer Pierce	Direct Deposit	0.00
Paycheck	01/04/2024	DD1309	Stacey Whittaker	Direct Deposit	0.00
Paycheck	01/04/2024	DD1310	Thomas D Sharkey	Direct Deposit	0.00
Check	01/04/2024		Voya	Payroll expense	-401.60
Deposit	01/04/2024			Deposit	250.00
Deposit	01/05/2024			Deposit	550.00
Deposit	01/06/2024			Deposit	200.00
Deposit	01/07/2024			Deposit	600.00
Check	01/08/2024		AT&T	Telephone expense	-27.89
Deposit	01/08/2024			Deposit	1,250.00
Check	01/09/2024	1827	Jennifer Simkins	Refund late fee	-75.00
Deposit	01/09/2024			Deposit	475.00
Deposit	01/10/2024			Deposit	225.00
Check	01/11/2024	1828	Jacqueline Hoppenrath	Refund endorsement fee	-50.00
Deposit	01/11/2024			Deposit	350.00
Deposit	01/12/2024			Deposit	225.00
Deposit	01/14/2024			Deposit	200.00
Deposit	01/15/2024			Deposit	200.00
Liability Check	01/16/2024	E-pay	US Treasury	Payroll expense	-3,006.52
Check	01/16/2024	ACH	Melissa Maestas	Examination fees	-100.00
Deposit	01/16/2024			Deposit	700.00
Liability Check	01/17/2024		QuickBooks Payroll Service	Payroll expense	-4,361.32
Check	01/17/2024	ACH	Tim Hunsaker	Board compensation	-75.00
Check	01/17/2024	ACH	Lynee Anderson V	Board compensation	-75.00
Check	01/17/2024	ACH	Jennifer Joy-Cornejo	Board compensation	-75.00
Deposit	01/17/2024			Deposit	100.00
Paycheck	01/18/2024	DD1311	Jennifer Pierce	Direct Deposit	0.00
Paycheck	01/18/2024	DD1312	Stacey Whittaker	Direct Deposit	0.00
Paycheck	01/18/2024	DD1313	Thomas D Sharkey	Direct Deposit	0.00
Check	01/18/2024	ACH	Voya	Payroll expense	-401.60
Deposit	01/18/2024			Deposit	525.00
Deposit	01/19/2024			Deposit	175.00
Deposit	01/20/2024			Deposit	100.00
Deposit	01/22/2024			Deposit	250.00
Deposit	01/23/2024			Deposit	525.00

BEASP

Transaction Detail by Account

January through March 2024

Deposit	01/24/2024			Deposit	200.00
Check	01/25/2024	ACH	Andrea Menicucci	Board compensation	-75.00
Check	01/25/2024	ACH	Tim Hunsaker	Board compensation	-75.00
Check	01/25/2024	ACH	Lynee Anderson V	Board compensation	-75.00
Check	01/25/2024	ACH	Jennifer Joy-Cornejo	Board compensation	-75.00
Check	01/25/2024	ACH	Adrienne Williams	Board compensation	-75.00
Check	01/25/2024	ACH	Shawn Binn	Board compensation	-75.00
Check	01/25/2024	ACH	Branden Murphy	Board compensation	-75.00
Check	01/25/2024	ACH	Wells Fargo	Postage, NCSB membership	-465.55
Deposit	01/25/2024			Deposit	150.00
Deposit	01/26/2024			Deposit	75.00
Deposit	01/27/2024			Deposit	25.00
Deposit	01/29/2024			Deposit	100.00
Deposit	01/30/2024			Deposit	400.00
Liability Check	01/31/2024		QuickBooks Payroll Service	Payroll expense	-4,398.25
Deposit	01/31/2024			Deposit	250.00
Deposit	01/31/2024			Interest	1.09
Paycheck	02/01/2024	DD1316	Thomas D Sharkey	Direct Deposit	0.00
Paycheck	02/01/2024	DD1315	Stacey Whittaker	Direct Deposit	0.00
Paycheck	02/01/2024	DD1314	Jennifer Pierce	Direct Deposit	0.00
Check	02/01/2024	ACH	Voya	Payroll expense	-401.60
Deposit	02/01/2024			Deposit	800.00
Check	02/01/2024	1829	Attorney General	Legal fees	-62.82
Deposit	02/02/2024			Deposit	825.00
Deposit	02/03/2024			Deposit	250.00
Deposit	02/05/2024			Deposit	450.00
Deposit	02/06/2024			Deposit	250.00
Check	02/06/2024	1830	Legislative Counsel Bureau	Legal fees	-750.00
Check	02/06/2024		AT&T	Telephone expense	-27.91
Deposit	02/07/2024			Deposit	400.00
Check	02/08/2024		Nevada Retail Network	Worker's comp	-600.00
Deposit	02/09/2024			Deposit	100.00
Deposit	02/10/2024			Deposit	450.00
Deposit	02/11/2024			Deposit	450.00
Deposit	02/12/2024			Deposit	450.00
Check	02/12/2024	1831	Greenbrae Trophy	Service award	-65.00
Check	02/12/2024		Wells Fargo	Merchant fees	-290.87
Deposit	02/12/2024			Deposit	250.00
Deposit	02/13/2024			Deposit	200.00
Liability Check	02/14/2024		QuickBooks Payroll Service	Payroll expense	-4,283.44
Deposit	02/14/2024			Deposit	450.00
Paycheck	02/15/2024	DD1317	Jennifer Pierce	Direct Deposit	0.00
Paycheck	02/15/2024	DD1318	Stacey Whittaker	Direct Deposit	0.00
Check	02/15/2024	ACH	Voya	Payroll expense	-401.60
Deposit	02/16/2024			Deposit	650.00

Deposit	02/17/2024			Deposit	350.00
Deposit	02/19/2024			Deposit	325.00
Deposit	02/20/2024			Deposit	175.00
Deposit	02/21/2024			Deposit	225.00
Deposit	02/22/2024			Deposit	400.00
Check	02/22/2024		Andrea Menicucci V	Board compensation	-75.00
Check	02/22/2024		Lynee Anderson V	Board compensation	-75.00
Check	02/22/2024		Jennifer Joy-Cornejo	Board compensation	-75.00
Check	02/22/2024		Adrienne Williams V	Board compensation	-75.00
Check	02/22/2024		Shawn Binn V	Board compensation	-75.00
Check	02/22/2024		Branden Murphy	Board compensation	-75.00
Deposit	02/23/2024			Deposit	100.00
Deposit	02/25/2024			Deposit	250.00
Deposit	02/26/2024			Deposit	100.00
Deposit	02/27/2024			Deposit	375.00
Liability Check	02/28/2024		QuickBooks Payroll Service	Payroll expense	-4,283.44
Deposit	02/28/2024			Deposit	200.00
Paycheck	02/29/2024	DD1319	Jennifer Pierce	Direct Deposit	0.00
Paycheck	02/29/2024	DD1320	Stacey Whittaker	Direct Deposit	0.00
Liability Check	02/29/2024	E-pay	US Treasury	Payroll expense	-4,500.62
Check	02/29/2024	ACH	Voya	Payroll expense	-401.60
Deposit	02/29/2024			Deposit	900.00
Deposit	02/29/2024			Interest	0.96
Deposit	03/01/2024			Deposit	700.00
Deposit	03/02/2024			Deposit	250.00
Deposit	03/03/2024			Deposit	400.00
Deposit	03/04/2024			Deposit	300.00
Check	03/04/2024	1832	Attorney General	Legal fees	-926.54
Deposit	03/05/2024			Deposit	250.00
Deposit	03/06/2024			Deposit	500.00
Check	03/06/2024	ACH	AT&T	Telephone expense	-27.90
Deposit	03/07/2024			Deposit	225.00
Deposit	03/08/2024			Deposit	250.00
Deposit	03/09/2024			Deposit	200.00
Deposit	03/10/2024			Deposit	500.00
Deposit	03/11/2024			Deposit	200.00
Deposit	03/12/2024			Deposit	350.00
Check	03/12/2024		Wells Fargo	Merchant fees	-192.45
Liability Check	03/13/2024		QuickBooks Payroll Service	Payroll expense	-4,283.44
Deposit	03/13/2024			Deposit	250.00
Check	03/13/2024	1833	Michael Hodes	Examination fees	-100.00
Paycheck	03/14/2024	DD1321	Jennifer Pierce	Direct Deposit	0.00
Paycheck	03/14/2024	DD1322	Stacey Whittaker	Direct Deposit	0.00
Check	03/14/2024	ACH	Voya	Payroll expense	-401.60
Deposit	03/14/2024			Deposit	250.00

	Deposit	03/15/2024			Deposit	1,431.85
	Deposit	03/16/2024			Deposit	225.00
	Deposit	03/18/2024			Deposit	100.00
	Deposit	03/19/2024			Deposit	600.00
	Deposit	03/20/2024			Deposit	375.00
	Deposit	03/21/2024			Deposit	50.00
	Deposit	03/22/2024			Deposit	700.00
	Deposit	03/23/2024			Deposit	200.00
	Deposit	03/25/2024			Deposit	550.00
	Check	03/25/2024		Wells Fargo	USPS	-19.20
	Check	03/25/2024	ACH	Adrienne Williams	Board compensation	-75.00
	Check	03/25/2024	ACH	Shawn Binn	Board compensation	-75.00
	Check	03/25/2024	ACH	Branden Murphy	Board compensation	-75.00
	Deposit	03/26/2024			Deposit	350.00
	Liability Check	03/27/2024		QuickBooks Payroll Service	Payroll expense	-4,398.25
	Deposit	03/27/2024			Deposit	250.00
	Paycheck	03/28/2024	DD1324	Stacey Whittaker	Direct Deposit	0.00
	Paycheck	03/28/2024	DD1323	Jennifer Pierce	Direct Deposit	0.00
	Paycheck	03/28/2024	DD1325	Thomas D Sharkey	Direct Deposit	0.00
	Liability Check	03/28/2024	E-pay	US Treasury	Payroll expense	-3,006.54
	Check	03/28/2024	ACH	Voya	Payroll expense	-401.60
	Deposit	03/28/2024			Deposit	550.00
	Deposit	03/29/2024			Deposit	525.00
	Deposit	03/30/2024			Deposit	100.00
	Deposit	03/31/2024			Interest	0.96
Total Wells Fargo Bank - Checking						-29,251.90

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 10

Review and Approval of Revised FY25 Budget and Contracts for Bookkeeping Services and Licensing Database

a. **Revised FY25 Budget and New Sole Source Contract with Numbers, Inc. for Bookkeeping Services**
A revision to the FY25 budget that was originally approved in January 2024 is attached, reflecting increases in the expenses listed below for an overall increase of $2,108 for the fiscal year. This budget was initially approved in January 2024 with an intentional deficit to cover the non-recurring cost of legislative services that are hoped to support passage of the Board's planned BDR. While anticipated FY25 revenue will likely not be sufficient to cover FY25 revenue, there are sufficient reserves to cover the deficit. Changes are noted in red.

- Bookkeeping Services: Increase from $750 to $900 per quarter ($3,000 to $3,600 annually
  The Board's current provider, Numbers, Inc., is increasing the monthly rate by $50, as no adjustment has been made since 2018. The Board formerly had a contract with this provider that expired in 2022 and has been paid on a quarterly invoice basis since then due to the low dollar amount. As a result of the increase, a new contract has been drafted for the Board's review and approval as the annual amount will total $3,600.

  The proposed new contract is attached for review and approval concurrently with this item.

- Office Supplies: Increase in for new QuickBooks Online + Payroll Core subscription at $1,836 annually
  The Board office was also just notified by Numbers, Inc. that the QuickBooks Desktop software they have used for 20+ years is being discontinued in the near future. This product was available for a flat annual fee to accountants, allowing for payroll processing for multiple companies in QuickBooks Desktop. After researching potential new options, they have recommended the Board convert to QuickBooks online with a payroll component add-on. This would be a monthly subscription totaling $1,836 annually ($153/month) as follows:
  - $90 QuickBooks Online
  - $45 Payroll Core
  - $18 Payroll Fees ($6 per employee * 3 employees. This will replace and be offset by removing the current $328 budgeted annually for direct deposit fees)

Attachments on next page:

1. *FY25 Budget DRAFT Revised*
2. *Numbers, Inc DRAFT Sole-Source Contract*

Action: Approve, Table, or Take No Action on the Matter

State of Nevada

Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board

FY25 BUDGET [APPROVED 1/24/2024 | REVISED 4/24/2024]

REVENUE						
Fees	New apps; late renewals		$ 41,832.00		$ 41,832.00	Same as FY24 Estimate
License Fees	New; renewals; reinstate; conversions		$ 167,122.80		$ 167,122.80	Same as FY24 Estimate
Exams, List, Interest	Exams; lists; verifications; interest		$ 10,050.42		$ 10,050.42	Same as FY24 Estimate
	Total Revenue		$ 219,005.22		$ 219,005.22	
EXPENSES		**CURRENT APPROVED**		**PROPOSED REVISED**		**Expense Narrative**
Personnel/Payroll			$ 164,930.96		$ 164,602.96	
	Executive Director	$ 101,012.91		$ 101,012.91		No change; remain at full-time hours in lieu of COLA increase.
	Licensing Coordinator	$ 40,448.38		$ 40,448.38		4% COLA increase ($1,555.71) per AB522, effective 7/1/2024.
	Investigator	$ 3,000.00		$ 3,000.00		
	Payroll Taxes	$ 11,000.00		$ 11,000.00		Change per COLA increase.
	Deferred Comp	$ 9,141.67		$ 9,141.67		ED Salary @ 9.05%. No change.
	Direct Deposit Fees	$ 328.00		$ -		Previously $328 annually ($4.00 per DD (JP/SW @ 52 = $208; Investigator @ 30 = $120)
Legal Fees	Attorney General		$ 8,000.00		$ 8,000.00	Est $154.36/hr: 9 mtgs @ 2 hrs ea= $2,778.48 + $5,221.52 complaints
Audit Fees	Coulson & Associates		$ 10,000.00		$ 10,000.00	Anticipated FY24 Audit
Bank Fees	Merchant Svcs/Checking		$ 4,600.00		$ 4,600.00	
Board Compensation	Salary		$ 3,525.00		$ 3,525.00	Board: 5 mtg @ 7 members x $75 each = $2,625; AC: 4 mtg @ 3 members x $75 each = $900
Dues	NCSB; RAN		$ 550.00		$ 550.00	NCSB $450; RAN $100
Equipment			$ 500.00		$ 500.00	No equipment anticipated.
Examinations			$ 4,840.00		$ 4,840.00	
Exam Proctors	Various	$ 2,400.00		$ 2,400.00		24 exams @ $100/proctor (Avg FY20-FY23 = 19)
Exam Materials	IHS	$ 2,440.00		$ 2,440.00		24 exams @ $100 each + $40 shipping (Avg FY20-FY23 = 19)
Insurance	Tort & Liability/Worker's Comp		$ 1,700.00		$ 1,700.00	Tort Liability $1,000 per FY24 increase; Worker's Comp $600
Database/Website	Albertson Consulting		$ 8,855.00		$ 8,855.00	Annual $8,000; SSL Certs $450; Support Overage $405 (3 hrs @ $135/hr)
Meeting Expense	Rooms/lunches		$ 100.00		$ 100.00	Recommend no-cost in-person meetings if held.
Ofc Lease/Cost Share	OT Board		$ 3,400.00		$ 3,400.00	Shared office, supplies, equipment, & internet.
Office Supplies	ZOOM, Office365, Staples, QBO		$ 750.00		$ 2,586.00	Zoom $150; Office365 $400; Misc $200; Quickbooks Online $1,836
Postage	USPS/OT Board		$ 400.00		$ 400.00	
Printing	State Printer		$ 200.00		$ 200.00	Envelopes, misc.
Professional Fees			$ 40,500.00		$ 41,100.00	
Accounting	Numbers Inc.	$ 3,000.00		$ 3,600.00		~~$750~~ $900/quarter
Investigation Fees	Various	$ 1,000.00		$ 1,000.00		Expert reviewer services.
Leg Services	Strategies 360	$ 36,000.00		$ 36,000.00		2025 Legislative Session Support
IT/Tech Support	Various	$ 500.00		$ 500.00		None used in FY21/FY22
Telephone/Tech	AT&T; State of NV IT		$ 525.00		$ 525.00	Local $300 ($25/mo). LD $25 ($2/month). Teleconference (if needed) $200.
Travel						
	Travel - In State	$ 200.00	$ 200.00	$ 200.00	$ 200.00	Local mileage. Reduce & hold all meetings via Zoom.
	Travel - Out of State	$ -		$ -		None planned.
	Total Operating Expenses		$ 253,575.96		$ 255,683.96	$ 2,108.00
	Revenue in Excess of Operating Expense		$ (34,570.74)		$ (36,678.74)	

CETS #:	
Solicitation #:	

CONTRACT FOR SERVICES OF INDEPENDENT CONTRACTOR FOR LESS THAN $50,000

A Contract Between the State of Nevada
Acting by and Through its

Agency Name:	Speech-Language Pathology, Audiology and Hearing Aid Dispensing Board
Address:	6170 Mae Anne Avenue, Suite 1
City, State, Zip Code:	Reno, NV 89523
Contact:	Jennifer R. Pierce, Executive Director
Phone:	(775) 787-3421
Fax:	(775) 746-4105
Email:	execdirector@nvspeechhearing.org

Contractor Name:	Numbers, Inc.
Address:	1285 Baring Blvd., #309
City, State, Zip Code:	Sparks, NV 89434
Contact:	Carol Woods
Phone:	(775) 742-2962
Fax:	
Email:	Carol Woods <carolwoods94123@yahoo.com>

WHEREAS, NRS 333.700 authorizes officers, departments, institutions, boards, commissions, and other agencies in the Executive Branch of the State Government which derive their support from public money in whole or in part to engage services of persons as independent contractors; and

WHEREAS, it is deemed that the service of Contractor is both necessary and in the best interests of the State of Nevada.

NOW, THEREFORE, in consideration of the aforesaid premises, the parties mutually agree as follows:

1. **CONTRACT TERM.** This Contract shall be effective as noted below, unless sooner terminated by either party as specified in ***Section 7, Contract Termination***. Contracts requiring approval of the Nevada Board of Examiners or the Clerk of the Board are not effective until such approval has occurred, however, after such approval, the effective date will be the date noted below.

Effective from:	7/1/2024	To:	6/30/2028

2. **NOTICE**. All communications, including notices, required or permitted to be given under this Contract shall be in writing and directed to the parties at the addresses stated above. Notices may be given: (a) by delivery in person; (b) by a nationally recognized next day courier service, return receipt requested; or (c) by certified mail, return receipt requested. If specifically requested by the party to be notified, valid notice may be given by facsimile transmission or email to the address(es) such party has specified in writing.

3. **SCOPE OF WORK**. The Scope of Work is described below, which is incorporated herein by reference:

DESCRIPTION OF SCOPE OF WORK:

Contractor will provide financial reporting and payroll services to include:

Financial Reporting:

- Monthly entry of bills, checks, and direct debit transactions into QuickBooks Online.
- Monthly entry/upload of customer payments into QuickBooks Online.
- Monthly bank reconciliations.
- Monthly budget vs. actual report.
- Quarterly financial close, including closing entries as needed (including deferred income) and preparation of financial reports.
- Year-end financial reports for your auditor with audit reconciliations.

Payroll Services:

- Management of bi-weekly payroll services including payroll, monthly 941 federal tax deposits, quarterly filings, and year end W-2s.
- Quarterly reporting for Nevada Unemployment Insurance
- Year-end issuance of 1099s and filing 1096 reports.

An Attachment must be limited to the Scope of Work to be performed by Contractor. Any provision, term or condition of an Attachment that contradicts the terms of this Contract, or that would change the obligations of the State under this Contract, shall be void and unenforceable.

4. **CONSIDERATION**. The parties agree that Contractor will provide the services specified in ***Section 3, Scope of Work*** at a cost as noted below:

$900	per	Quarter

Total Contract or installments payable at:	Upon invoice as services are provided.

Total Contract Not to Exceed:	$14,400.00

The State does not agree to reimburse Contractor for expenses unless otherwise specified in the Scope of Work or incorporated Attachments (if any). Any intervening end to a biennial appropriation period shall be deemed an automatic renewal (not changing the overall Contract term) or a termination as the result of legislative appropriation may require.

5. **BILLING SUBMISSION: TIMELINESS**. The parties agree that timeliness of billing is of the essence to the Contract and recognize that the State is on a Fiscal Year. All billings for dates of service prior to July 1 must be submitted to the State no later than the first Friday in August of the same calendar year. A billing submitted after the first Friday in August, which forces the State to process the billing as a stale claim pursuant to NRS 353.097, will subject Contractor to an administrative fee not to exceed one hundred dollars ($100.00). The parties hereby agree this is a reasonable estimate of the additional costs to the State of processing the billing as a stale claim and that this amount will be deducted from the stale claim payment due to Contractor.

6. **INSPECTION & AUDIT**. Contractor agrees to keep and maintain under generally accepted accounting principles (GAAP) and as required by State and federal law, complete and accurate records as are necessary to fully disclose to the State or United States Government, sufficient information to determine compliance with all State and federal regulations and statutes, and compliance with the terms of this contract, and agrees that such documents will be made available for inspection upon reasonable notice from authorized representatives of the State or Federal Government.

7. **CONTRACT TERMINATION**.

A. Termination Without Cause. Regardless of any terms to the contrary, this Contract may be terminated upon written notice by mutual consent of both parties. The State unilaterally may terminate this contract without cause by giving not less than thirty (30) days' notice in the manner specified in ***Section 2, Notice***. If this Contract is unilaterally terminated by the State, Contractor shall use its best efforts to minimize cost to the State and Contractor will not be paid for any cost that Contractor could have avoided.

B. State Termination for Non-Appropriation. The continuation of this Contract beyond the current biennium is subject to and contingent upon sufficient funds being appropriated, budgeted, and otherwise made available by the State Legislature and/or federal sources. The State may terminate this Contract, and Contractor waives any and all claims(s) for damages, effective immediately upon receipt of written notice (or any date specified therein) if for any reason the Contracting Agency's funding from State and/or federal sources is not appropriated or is withdrawn, limited, or impaired.

C. Termination with Cause for Breach. A breach may be declared with or without termination. A notice of breach and termination shall specify the date of termination of the Contract, which shall not be sooner than the expiration of the Time to Correct, if applicable, allowed under ***Subsection 7D***. This Contract may be terminated by either party upon written notice of breach to the other party on the following grounds:

1) If Contractor fails to provide or satisfactorily perform any of the conditions, work, deliverables, goods, or services called for by this Contract within the time requirements specified in this Contract or within any granted extension of those time requirements; or

2) If any state, county, city, or federal license, authorization, waiver, permit, qualification or certification required by statute, ordinance, law, or regulation to be held by Contractor to provide the goods or services required by this Contract is for any reason denied, revoked, debarred, excluded, terminated, suspended, lapsed, or not renewed; or

3) If Contractor becomes insolvent, subject to receivership, or becomes voluntarily or involuntarily subject to the jurisdiction of the Bankruptcy Court; or

4) If the State materially breaches any material duty under this Contract and any such breach impairs Contractor's ability to perform; or

5) If it is found by the State that any quid pro quo or gratuities in the form of money, services, entertainment, gifts, or otherwise were offered or given by Contractor, or any agent or representative of Contractor, to any officer or employee of the State of Nevada with a view toward securing a contract or securing favorable treatment with respect to awarding, extending, amending, or making any determination with respect to the performing of such contract; or

6) If it is found by the State that Contractor has failed to disclose any material conflict of interest relative to the performance of this Contract.

D. Time to Correct. Unless the breach is not curable, or unless circumstances do not permit an opportunity to cure, termination upon declared breach may be exercised only after service of formal written notice as specified in ***Section 2, Notice***, and the subsequent failure of the breaching party within fifteen (15) calendar days of receipt of that notice to provide evidence, satisfactory to the aggrieved party, showing that the declared breach has been corrected. Upon a notice of breach, the time to correct and the time for termination of the contract upon breach under ***Subsection 7C***, above, shall run concurrently, unless the notice expressly states otherwise.

8. **REMEDIES**. Except as otherwise provided for by law or this Contract, the rights and remedies of the parties shall not be exclusive and are in addition to any other rights and remedies provided by law or equity, including, without limitation, actual damages, and to a prevailing party reasonable attorneys' fees and costs. For purposes of an award of attorneys' fees to either party, the parties stipulate and agree that a reasonable hourly rate of attorneys' fees shall be one hundred and fifty dollars ($150.00) per hour. The State may set off consideration against any unpaid obligation of Contractor to any State agency in accordance with NRS 353C.190. In the event that Contractor voluntarily or involuntarily becomes subject to the jurisdiction of the Bankruptcy Court, the State may set off consideration against any unpaid obligation of Contractor to the State or its agencies, to the extent allowed by bankruptcy law, without regard to whether the procedures of NRS 353C.190 have been utilized.

9. **LIMITED LIABILITY**. The State will not waive and intends to assert available NRS Chapter 41 liability limitations in all cases. Contract liability of both parties shall not be subject to punitive damages. Damages for any State breach shall never exceed the amount of funds appropriated for payment under this Contract, but not yet paid to Contractor, for the Fiscal Year budget in existence at the time of the breach. Contractor's tort liability shall not be limited.

10. **INDEMNIFICATION AND DEFENSE**. To the fullest extent permitted by law, Contractor shall indemnify, hold harmless and defend, not excluding the State's right to participate, the State from and against all liability, claims, actions, damages, losses, and expenses, including, without limitation, reasonable attorneys' fees and costs, arising out of any breach of the obligations of Contractor under this Contract, or any alleged negligent or willful acts or omissions of Contractor, its officers, employees and agents. Contractor's obligation to indemnify the State shall apply in all cases except for claims arising solely from the State's own negligence or willful misconduct. Contractor waives any rights of subrogation against the State. Contractor's duty to defend begins when the State requests defense of any claim arising from this Contract.

11. **REPRESENTATIONS REGARDING INDEPENDENT CONTRACTOR STATUS.** Contractor represents that it is an independent contractor, as defined in NRS 333.700(2) and 616A.255, warrants that it will perform all work under this contract as an independent contractor, and warrants that the State of Nevada will not incur any employment liability by reason of this Contract or the work to be performed under this Contract. To the extent the State incurs any employment liability for the work under this Contract; Contractor will reimburse the State for that liability.

12. **INSURANCE SCHEDULE.** Unless expressly waived in writing by the Contracting Agency, Contractor must procure, maintain and keep in force for the duration of the Contract insurance conforming to the minimum requirements specified below. Each insurance policy shall provide for a waiver of subrogation against the State of Nevada, its officers, employees and immune contractors as defined in NRS 41.0307, for losses arising from work/materials/equipment performed or provided by or on behalf of Contractor. By endorsement to Contractor's automobile and general liability policies, the State of Nevada shall be named as an additional insured with respect to liability arising out of the activities performed by, or on behalf of Contractor. Contractor shall not commence work before Contractor has provided evidence of the required insurance in the form of a certificate of insurance and endorsement to the Contracting Agency of the State.

A. <u>Workers' Compensation and Employer's Liability Insurance.</u>

1) Contractor shall provide proof of worker's compensation insurance as required per Nevada Revised Statutes Chapters 616A through 616D inclusive.

2) If Contractor qualifies as a sole proprietor as defined in NRS Chapter 616A.310 and has elected to not purchase industrial insurance for himself/herself, the sole proprietor must submit to the contracting State agency a fully executed "Affidavit of Rejection of Coverage" form under NRS 616B.627 and NRS 617.210.

B. <u>Commercial General Liability – Occurrence Form</u>. The Policy shall include bodily injury, property damage and broad form contractual liability coverage.

1)	General Aggregate	$2,000,000
2)	Products – Completed Operations Aggregate	$1,000,000
3)	Personal and Advertising Injury	$1,000,000
4)	Each Occurrence	$1,000,000

C. <u>Professional Liability/Errors and Omissions Liability</u> The policy shall cover professional misconduct or lack of ordinary skill for those positions defined in the Scope of Work of this contract. In the event that the professional liability insurance required by this Contract is written on a claims-made basis, Contractor warrants that any retroactive date under the policy shall precede the effective date of this Contract; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of two (2) years beginning at the time work under this Contract is completed.

1)	Each Claim	$1,000,000
2)	Annual Aggregate	$2,000,000

Mail all required insurance documents to the Contracting Agency identified on page one of the Contract.

13. **WAIVER OF BREACH**. Failure to declare a breach or the actual waiver of any particular breach of the Contract or its material or nonmaterial terms by either party shall not operate as a waiver by such party of any of its rights or remedies as to any other breach.

14. **SEVERABILITY.** If any provision contained in this Contract is held to be unenforceable by a court of law or equity, this Contract shall be construed as if such provision did not exist and the non-enforceability of such provision shall not be held to render any other provision or provisions of this Contract unenforceable.

15. **STATE OWNERSHIP OF PROPRIETARY INFORMATION**. Any data or information provided by the State to Contractor and any documents or materials provided by the State to Contractor in the course of this Contract ("State Materials") shall be and remain the exclusive property of the State and all such State Materials shall be delivered into State possession by Contractor upon completion, termination, or cancellation of this Contract.

16. **PUBLIC RECORDS**. Pursuant to NRS 239.010, information or documents received from Contractor may be open to public inspection and copying. The State may have the duty to disclose unless a particular record is made confidential by law or a common law balance of interests.

17. **GENERAL WARRANTY**. Contractor warrants that all services, deliverables, and/or work products under this Contract shall be completed in a workmanlike manner consistent with standards in the trade, profession, or industry; shall conform to or exceed the specifications set forth in the incorporated attachments; and shall be fit for ordinary use, of good quality, with no material defects.

18. **DISCLOSURES REGARDING CURRENT OR FORMER STATE EMPLOYEES.** For the purpose of State compliance with NRS 333.705, Contractor represents and warrants that if Contractor, or any employee of Contractor who will be performing services under this Contract, is a current employee of the State or was employed by the State within the preceding 24 months, Contractor has disclosed the identity of such persons, and the services that each such person will perform, to the Contracting Agency.

19. **GOVERNING LAW: JURISDICTION**. This Contract and the rights and obligations of the parties hereto shall be governed by, and construed according to, the laws of the State of Nevada, without giving effect to any principle of conflict-of-law that would require the application of the law of any other jurisdiction. The parties consent to the exclusive jurisdiction of and venue in the First Judicial District Court, Carson City, Nevada for enforcement of this Contract, and consent to personal jurisdiction in such court for any action or proceeding arising out of this Contract.

20. **ENTIRE CONTRACT AND MODIFICATION**. This Contract and its Scope of Work constitute the entire agreement of the parties and as such are intended to be the complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Unless otherwise expressly authorized by the terms of this Contract, no modification or amendment to this Contract shall be binding upon the parties unless the same is in writing and signed by the respective parties hereto and approved by the Office of the Attorney General and the State Board of Examiners, as required. This form of Contract, including any amendments to the Contract, is not authorized for use if the "not to exceed" value ***Section 4, Consideration*** equals or exceeds $50,000. This Contract, and any amendments, may be executed in counterparts.

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be signed and intend to be legally bound thereby.

Independent Contractor's Signature Date

Independent Contractor's Title

State of Nevada Authorized Signature Date

Title

APPROVED BY BOARD OF EXAMINERS

Signature – Clerk of the Board of Examiners

On:

Date

Approved as to form by:

On:

Deputy Attorney General for Attorney General

Date

NUMBERS, INC.

April 16, 2024

Jennifer Pierce
Executive Director
State of Nevada Speech-Language Pathology,
Audiology & Hearing Aid Dispensing Board
Via email: board@nvspeechhearing.org

Dear Jennifer,

As we discussed, here is a proposed agreement for bookkeeping and payroll services for the Board.

Proposed Services:

Services to include:

- Entry of bills, checks and direct debit transactions into QuickBooks Online.
- Entry / upload of customer payments into QuickBooks Online.
- Monthly bank reconciliations.
- Monthly budget vs. actual report.
- Quarterly financial close - including closing entries as needed (including deferred income) and preparation of financial reports.
- Year end financial reports for your auditor with audit reconciliations.
- Management of bi-weekly payroll services, including payroll, tax deposits, quarterly filings, and year end W-2s..
- Issuing 1099s at year end, and filing of 1096 reports.

Fee Structure:

Services would be $300/month, paid quarterly during the first month of the quarter.

Please let me know if you have any questions.

Sincerely,

Carol Woods

Carol Woods, President

b. Consideration of Technology Risk Assessment as Recommended by Nevada Office of the CIO for Previously Approved Albertson Consulting Contract for Licensing Database

In January 2024, the Board approved a new sole-source contract with Albertson Consulting, Inc., the Board's current licensing and database provider, to continue services and comply with contract requirement changes in the State Administrative Manual.

The Board office submitted a sole-source solicitation waiver to the Purchasing Division but was notified that because the estimated value ($10,000 per fiscal year for four years) of the project is well below the threshold for formal competition ($25,000 per fiscal year) set by NAC 333.150, a waiver was not required. However, because this contract and the prior contract with Alberson Consulting, Inc. results in aggregated costs of $50,000 or more, the Board was required to submit a Technology Investment Notification (TIN), a detailed online questionnaire providing information about a technology initiative and is required regardless of funding source or state IT involvement to for state planning, security, and technical profile awareness.

Submission of the contract to Governor's Finance Office for approval requires inclusion of a TIN completion memo. Our TIN Completion memo is attached and recommends the Board conduct an assessment of identified risks, though the Board may still proceed with the contract. Albertson Consulting has provided the attached response to support the Board's review and assessment.

Specific areas recommended for assessment are as follows:

- Vendor Lock-in: The proprietary nature of the licensing program and the fact that maintenance and support are exclusively available from Albertson Consulting create a dependency on a single vendor. This dependency limits flexibility and potentially increases risk if the vendor fails to maintain high security standards or encounters operational difficulties.
- Data Security and Privacy: The SaaS regulatory database contains sensitive information that must be protected against unauthorized access, data breaches, and leaks. Ensuring the vendor adheres to stringent data protection standards, including encryption, access controls, and regular security assessments, is crucial.
- Compliance and Regulatory Requirements: As the software handles licensing and regulatory information, compliance with relevant legal and regulatory standards is paramount. This includes ensuring that Albertson Consulting's practices are in line with the state security requirements and any other applicable regulations concerning data systems contracting.
- Security Updates and Vulnerability Management: Given the evolving nature of cyber threats, it is vital to ensure that Albertson Consulting has an effective process for regularly updating the software and promptly addressing vulnerabilities.

Attachments on next page:

1. *TIN Completion Memo*
2. *Albertson Consulting TIN Risk Assessment Response*

Action: Approve, Table, or Take No Action on the Matter

Joe Lombardo
Governor

Timothy D. Galluzi
State Chief Information Officer

Darla J. Dodge
Deputy CIO– COO

David 'Ax' Axtell
Deputy CIO – CTO

Robert "Bob" Dehnhardt
Deputy CIO - CISO

STATE OF NEVADA
GOVERNOR'S OFFICE
Office of the Chief Information Officer
100 N. Stewart Street, Suite 100 │ Carson City, Nevada 89701
Phone: (775) 684-5800 │ www.it.nv.gov │ Fax: (775) 687-9097

MEMORANDUM

TO: Jennifer Pierce, Executive Director, NVSpeechHearing

CC: Tim Galluzi, State Chief Information Officer, OCIO
Robert Dehnhardt, State Chief Information Security Officer, OCIO
David Axtell, Deputy CIO - Chief Technology Officer, OCIO

FROM: Lisa Jean, TIN Administrator, OCIO

SUBJECT: TIN Completion Memo – NVSpeechHearing – TIN 846 – *Speech-Hearing Board Licensing Software* – BA B003

DATE: April 3, 2024

We have completed our review for the Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board's – *Speech-Hearing Board Licensing Software* – TIN 846.

The submitted TIN, for an estimated value of $8,000 in the FY24/FY25 biennium, $16,600 in FY26/FY27 biennium, and $8,500 in FY28 (100% Licensing Fees funding), is to contract with Albertson Consulting for maintenance and support for their software as a service (SaaS) regulatory database/licensing program and website hosting.

This contract is a continuation of an established hosting, maintenance, and support services agreement that was initiated in FY17. Maintenance and support for this platform are available exclusively from this vendor due to the proprietary nature of the licensing program. At this time, the board considers transitioning to a new licensing system and website hosting platform to be cost-prohibitive, as this board is small with limited funding and insufficient resources to stand up a new system.

Continuation of the Albertson Consulting program and website hosting presents several security concerns that warrant careful consideration. Given the proprietary nature of the software and the specialized services provided by Albertson Consulting, warrants consideration of the following security concerns:

Vendor Lock-in: The proprietary nature of the licensing program and the fact that maintenance and support are exclusively available from Albertson Consulting create a dependency on a single vendor. This dependency limits flexibility and potentially increases risk if the vendor fails to maintain high security standards or encounters operational difficulties.

Data Security and Privacy: The SaaS regulatory database contains sensitive information that must be protected against unauthorized access, data breaches, and leaks. Ensuring the vendor adheres to stringent data protection standards, including encryption, access controls, and regular security assessments, is crucial.

Compliance and Regulatory Requirements: As the software handles licensing and regulatory information, compliance with relevant legal and regulatory standards is paramount. This includes ensuring that Albertson Consulting's practices are in line with the state security requirements and any other applicable regulations concerning data systems contracting.

Security Updates and Vulnerability Management: Given the evolving nature of cyber threats, it is vital to ensure that Albertson Consulting has an effective process for regularly updating the software and promptly addressing vulnerabilities.

In light of these concerns, it is recommended that the Board conduct a comprehensive security assessment of Albertson Consulting's services, focusing on their adherence to best practices in data security, regulatory compliance, and system maintenance.

If there are to be any changes to enterprise services or utilizations, including: network, firewall, server, Active Directory (AD) integration, telecom, etc., please notify OCIO as soon as possible to avoid integration delays.

It is expected that this solution will follow state security standards and policies and be compliant with the Americans with Disabilities Act (ADA) to ensure accessibility to all authorized users.

A copy of this memo has been attached to the TIN.

If I can be of further assistance, please feel free to contact me.

Albertson Consulting Response to TIN Recommendations

April 2024

System Development Life Cycle

System Development Life Cycle

1. Purpose and Overview

The purpose of the Systems Development Life Cycle (SDLC) Standards is to describe the minimum required phases and considerations for developing and/or implementing new software and systems at Albertson Consulting.

2. Applies To

Albertson Consulting employees, vendors, independent contractors, etc. that do any type of software or systems development work under the auspices of Albertson Consulting.

In the event Albertson Consulting chooses to seek an exemption for reasons such as inability to meet specific points, tasks, or subtasks within the SDLC Policy or Standards, a SDLC Review Committee will convene in order to assess the specific merits of the exemption request(s) while still adhering to the main principles behind the SDLC Policy and Standards.

3. Policy Statement

All systems and software development work done at Albertson Consulting shall adhere to industry best practices with regard to a Systems (Software) Development Life Cycle. The minimum required phases and the tasks and considerations within these Systems development phases are outlined below. All of the following sub-tasks and considerations, as listed in the below respective standard development phases, are mandatory if the system or software development deals with Level 1 data in any way. Otherwise, the sub-tasks and considerations are recommended steps within the required standard development phases.

System Initiation:

- A need or opportunity is defined.
- Concept proposal is made.
- An initial feasibility study is conducted.
- A project charter (if necessary) is formulated.

System Requirements Analysis:

- Analyze user needs and develop user requirements.
- Create a detailed Functional Requirements Document.
- Break down the system, process, or problem into discrete units or modules and utilize diagrams and other visual tools in order to analyze the situation or need.
- Any security requirements must be defined.

System Design

- This phase transforms the requirements into a Design Document.
- The functions and operations of the system or software being designed are described in detail.

- A risk analysis should be done between the System Requirements and System Design phases.
- A final design review should be done to ensure the design addresses practicality, efficiency, cost, flexibility, and security.

System Construction (Procurement):

- This phase entails the transformation of the detailed design documents into a finished product or solution.
- Manual and automated testing at a unit or module level is done throughout this phase by the system or software developers. Security considerations are taken into account during testing.
- A third-party product may be utilized as a system or software solution if it best fits the user requirements and is more practical from a budgetary and/or resource perspective. However, all of the next phases should be followed regardless of whether the solution was developed in-house or purchased.

System Testing and Acceptance:

- This phase should validate or confirm that the developed system or software meets all functional requirements as captured during the System Requirements Analysis phase.
- Representatives separate from the development group should conduct internal Quality Assurance (QA) testing.
- Representative(s) from the user group should conduct user acceptance testing.
- Documentation during testing should detail and match testing criteria to specific requirements.
- While unit and module testing should be done throughout the entire SDLC, this phase entails holistic testing of the finished product and the final acceptance testing by the user(s).
- Final security assessment testing is now conducted.
- Any problems identified during the previous phases must be resolved or remediated before implementation.

System Implementation:

- The finished, tested, and user-accepted system or software is moved from the testing environment to production.
- All tools, code, or access mechanisms used for development or testing of the system or software must be removed from the software that is being moved into a production environment.
- Any necessary user training should be done prior to or during this phase.

System Maintenance

- This phase is the ongoing life of the system or software. Unlike the other phases, this phase only ends when the system or software is decommissioned.
- A customer/user support structure and any other necessary operational support processes should be in place.
- Any planned changes to the system or software should be scheduled, communicated, and documented.
- Continuous security penetration testing is conducted on the system or software throughout its life cycle at regularly scheduled intervals.
- Mandatory security testing is conducted when any major configuration or architecture change is made.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Exceptions to these standards and associated policy shall be allowed only if previous mutually approved by Albertson Consulting and Clients.

Web Application Security Policy

Table of Contents

Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors. It is crucial that any web application be assessed for vulnerabilities and any vulnerability be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within Albertson Consulting. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Albertson Consulting services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Albertson Consulting.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Albertson Consulting. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of Albertson Consulting is strictly prohibited unless approved.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.

c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

a) High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.

b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.

c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

a) Tenable.i
b) Trustwave PCI Compliance
c) OWASP Zed Attack Proxy (ZAP)

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

Application Testing

Application Testing

1. System Testing

ACI utilizes a proven strategy to identify, manage, and resolve issues. ACI testing strategy consists of three types of testing—Preliminary Testing (Static, Unit, and Development), Integration Testing, and System Testing— each aimed at helping us meet our clients' functional and deliverable requirements. Our focus on requirements traceability throughout your system implementation ensures that your business needs are met. Finally, when ACI's testing is done, we deploy the functionality to the UAT environment where we support clients in their execution of User Acceptance Testing. We conduct System Testing on each business process from end to end. The primary goal of System Testing is to validate that the developed functionality meets specified business objectives. System Testing ensures that all functional deliverables execute without defect in the client's actual business process. This level of testing validates that all rules function correctly as part of the larger process and not in isolation. System Testing covers database, functional, and security testing. System Tests occur iteratively between our Development and Quality Assurance (QA) teams. We perform a separate set of tests for each business process. If QA identifies any issues, they report them to Development
Preliminary Testing: Albertson Consulting Inc. Quality Assurance (QA) team executes various preliminary tests in the early stages of your project design and development.

2. Static Testing

Before programming even begins, ACI tests the documents that will be used to develop the new system. The purpose of Static Testing is to identify defects early on, before starting development. Our QA Specialists perform Static Tests on the Workflow Diagrams, Cheat Sheets, and Self-Documenting Specification documents. Our preliminary testing and defect correction of these documents ensures the development of a superior product in a shorter amount of time.

3. Unit Testing

(Functional Testing): Our Developers and QA Specialists will conduct Unit Tests throughout the development process to confirm that the configured and developed functionality performs according to specifications. Unit Tests occur iteratively between our Development and QA teams. Once all rules required by a business process are developed, the Developer informs QA and a Specialist is assigned. Albertson Consulting Inc. Developers Unit Test programming code in isolation from the integrated system, to verify that the software works according to specifications. Our QA Specialists perform a separate set of tests for each business process to verify low-level details of the screens, fields, and automation. We will update specifications (if needed) and code to resolve defects and re-execute testing until any and all issues are resolved.

4. Development Testing

Our QA team conducts Development Testing to confirm that developed or configured software functions according to requirements and properly interfaces with already programmed functionality. The intention of the Development Test is to "break" the software using standard industry testing techniques.

5. Integration Testing

Albertson Consulting Inc. works with our clients' technical staff to conduct Integration Testing. Integration Testing determines if our software properly interfaces with other systems and/or confirms that the website we have developed properly supports your business process needs. Integration Testing ensures that all inputs and outputs to your application are in place and functioning according to business process standards.

6. User Acceptance Testing

The objective of User Acceptance Testing (UAT) is for the client to validate that the system works as intended. UAT allows system users to confirm that they are able to use the new system to perform their job functions and that the system will meet their business requirements. To perform UAT effectively and ensure that the required functionality has been created, it is important that clients allocate sufficient staff resources and time to the endeavor. Albertson Consulting Inc. can provide training and guidance to designated client staff prior to beginning UAT to teach them how to test the system. We will also dedicate ample resources to resolving any identified issues quickly.

7. Load Testing

Load testing generally refers to the practice of modeling the expected usage of a software program by simulating multiple users accessing the program concurrently. Alberson Consulting leverages a combination of manual load testing and enterprise-grade load testing platform Neoload for automated testing across the complete software lifecycle, from component to full system-wide load tests.

2023

Last Updated: 1/1/2023

Backup / Disaster Recovery Plan

Backup / Disaster Recovery Plan

1. Backup Plan

Database

managed backups

Oracle and MySQL backups are managed by RDS automated backup feature. The automated backup feature of Amazon RDS enables point-in-time recovery for your DB Instance. Amazon RDS will back-up your database and transaction logs and store both for a user-specified retention period. This allows you to restore your DB Instance to any second during your retention period, up to the last five minutes. Automatic backup retention period is configured to thirty-five days. Data backups are encrypted at rest and in transit

snapshots

Daily full Oracle and MySQL snapshots are retained for thirty-five days in the disaster recovery environment in northern Virginia. Data snapshots are encrypted at rest and in transit.

File Backups

Files are backed up daily and all versions of the daily file backups are retained for 2 years and after 2 years the last version is saved indefinitely. Files backups are stored in non-publicly accessible 256-bit AES encrypted S3 buckets.

Backup client utilizes 256-bit AES encryption key to protect data in transit
Production files are synced to the DR environment every 15 minutes securely over site to site VPN.

Volume Snapshots

Daily volume snapshots are stored for 3 days in the production environment and also transferred and stored for 3 days in the DR environment in Virginia. Volume snapshots are encrypted at rest and in transit.

Instance Images

Instance images are refreshed on a monthly basis.

2. Backup testing

Backup health is monitored by daily reporting, alerts and consistency checks. Annual disaster recovery testing is performed in January.

3. Disaster Recovery Purpose and Objective

Albertson Consulting developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the features listed in the table above. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope

The scope of this DRP document addresses technical recovery only in the event of a significant disruption.

This disaster recovery plan provides:

- Guidelines for **determining plan activation**;
- Technical **response flow** and recovery strategy;

- Guidelines for **recovery procedures**;
- References to key **Business Resumption Plans** and technical dependencies;
- **Rollback procedures** that will be implemented to return to standard operating state;
- **Checklists** outlining considerations for escalation, incident management, and plan activation.

The specific objectives of this disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team.
-

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside Albertson Consulting. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

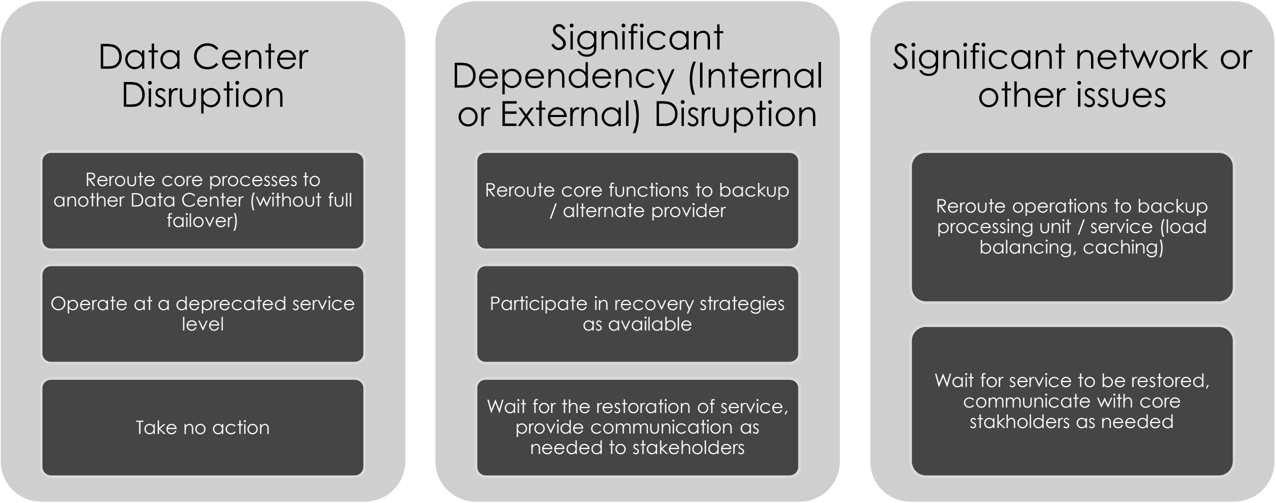
4. Dependencies

This section outlines the dependencies made during the development of this disaster recovery plan. If and when needed the DR TEAM will coordinate with their partner groups as needed to enable recovery.

Dependency	Assumptions
User Interface / Rendering Presentation components	- Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application). - Infrastructure and back-end services are still assumed to be active/running.
Business Intelligence / Reporting Processing components	- The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted). - Standard backup processes are not impacted, but the active / passive or mirrored processes are not functioning. - Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.
Network Layers Infrastructure components	- Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers. - Assumption is that terminal connections, serially attached devices and inputs are still functional.
Storage Layer Infrastructure components	- Loss of EBS, local area storage, or other storage component.
Database Layer Database storage components	- Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable
Hardware/Host Layer Hardware components	- Physical components are unavailable or affected by a given event
Virtualizations (VM's) Virtual Layer	- Virtual components are unavailable - Hardware and hosting services are accessible
Administration Infrastructure Layer	- Support functions are disabled such as management services, backup services, and log transfer functions. - Other services are presumed functional
Internal/External Dependencies	- Interfaces and intersystem communications corrupt or compromised

5. Disaster Recovery Strategies

The overall DR strategy of Albertson Consulting is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, reporting, etc.)



Data Center Disruption

- Reroute core processes to another Data Center (without full failover)
- Operate at a deprecated service level
- Take no action

Significant Dependency (Internal or External) Disruption

- Reroute core functions to backup / alternate provider
- Participate in recovery strategies as available
- Wait for the restoration of service, provide communication as needed to stakeholders

Significant network or other issues

- Reroute operations to backup processing unit / service (load balancing, caching)
- Wait for service to be restored, communicate with core stakholders as needed

6. Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.

Response Phase: The immediate actions following a significant event.

- On call personnel paged
- Decision made around recovery strategies to be taken
- Full recovery team identified

Resumption Phase: Activities necessary to resume services after team has been notified.

- Recovery procedures implemented
- Coordination with other departments executed as needed

Restoration Phase: Tasks taken to restore service to previous levels.

- Rollback procedures implemented
- Operations restored

Remediation Phase: Investigate cause of security breach or disaster

- Audit logs to determine case of breach or disaster

Response Phase

The following are the activities, parties and items necessary for a DR response in this phase. Please note these procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario).

Response Phase Recovery Procedures – All DR Event Scenarios

Step	Owner	Duration	Components
Identify issue, page on call / Designated Responsible Individual (DR TEAM)	DR TEAM	15 minutes	• Issue communicated / escalated • Priority set
Identify the team members needed for recovery	DR TEAM	15 minutes	Selection of core team members required for restoration phase from among the following groups: • Operations
Establish a Teams Meeting to coordinate next steps	DR TEAM	30 minutes	Team Meeting Alternate / backup communication tools: email, cell
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	DR TEAM	30 minutes	• Documentation / tracking of timelines and next decisions • Creation of disaster recovery event command center as needed

This information is also summarized by feature in Appendix A: Disaster Recovery Contacts - Admin Contact List.

In the event of a disaster clients will be updated by email notices, notices on our marketing site www.ebigpicture.com and your project manager will also be available by phone or email for any questions you may have.

Resumption Phase

During the resumption phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Backup data is stored at the hardware provider's vault building. The vault building is roughly 1 mile from the datacenter.

Data Center Recovery

Full Data Center Failover

Step	Owner	Duration	Components
Initiate Failover	DR TEAM	TBD	• Restoration procedures identified • Risks assessed for each procedure • Coordination points between groups defined • Issue communication process and triage efforts established
Complete Failover	DR TEAM	TBD	• Recovery steps executed, including handoffs between key dependencies
Test Recovery	DR TEAM	TBD	• Tests assigned and performed • Results summarized and communicated to group
Failover deemed successful	DR TEAM	TBD	•

Restoration Phase

During the restoration phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

Data Center Recovery

Full Data Center Restoration

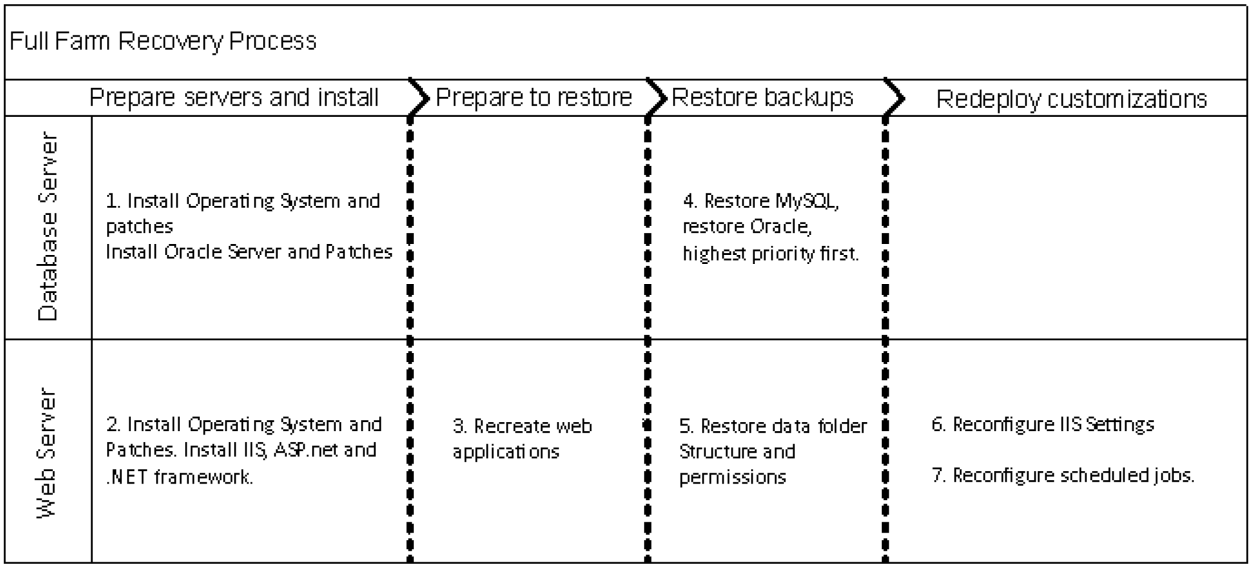
Step	Owner	Duration	Components
Determine whether failback to original Data Center will be pursued	DR TEAM	TBD	• Restoration procedures determined
Original data center restored	DR TEAM	TBD	• Server Farm level recovery
Complete Failback	DR Team	TBD	• Failback steps executed, including handoffs between key dependencies
Test Failback	DR Team	TBD	• Tests assigned and performed • Results summarized and communicated to group • Issues (if any) communicated to group
Determine whether failback was successful	DR TEAM	TBD	• Declaration of successful failback and communication to stakeholder group. • Disaster recovery procedures closed. • Results summarized, post mortem performed, and DRP updated (as needed).

The following section contains steps for the restoration procedures.

Full Server Farm Recovery

This section describes the process for recovering from a farm-level failure, for a: two-tier server farm consisting of a *database server and a web server* that provides provide web content.

The following diagram describes the recovery process for a farm.



Full Farm Recovery Process

	Prepare servers and install	Prepare to restore	Restore backups	Redeploy customizations
Database Server	1. Install Operating System and patches Install Oracle Server and Patches		4. Restore MySQL, restore Oracle, highest priority first.	
Web Server	2. Install Operating System and Patches. Install IIS, ASP.net and .NET framework.	3. Recreate web applications	5. Restore data folder Structure and permissions	6. Reconfigure IIS Settings 7. Reconfigure scheduled jobs.

Remediation Phase

Albertson Consulting will perform an extensive investigation to find the cause of any security breach or disaster, finding an explanation to any breach or disaster is critical to prevent the issue from reoccurring.

Appendix A: Disaster Recovery Contacts - Admin Contact List

The critical team members who would be involved in recovery procedures for feature sets are summarized below.

Feature Name	Contact Lists
DR Team	Derek Schaible – 7012607777 Dan Albertson – 7012402030 Doug Frazier – 7012145522 Tenelle Vetter - 7015093781

Appendix B: Glossary/Terms

Standard Operating State: Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

Presentation Layer: Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed and system requests are passed for processing and data retrieval to the appropriate layer.

Processing Layer: System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically this layer processes data from the other layers. Typically these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

Database Layer: The database layer is where data typically resides in an application stack. Typically data is stored in a relational database such as SQL Server, Microsoft Access, or Oracle, but it can be stored as XML, raw data, or tables. This layer typically is optimized for data querying, processing and retrieval.

Network Layer: The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

Storage Layer: This is typically an infrastructure layer and provides data storage and access. In most environments this is usually regarded as SAN or NAS storage.

Hardware/Host Layer: This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

Virtualization Layer: In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

Administrative Layer: The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.

Client Data Security

Client Data Security

1. Overview

All client data is securely stored on Amazon Web Services (AWS) cloud infrastructure. Our production data is housed in the US-WEST-2 (Oregon) region, with a disaster recovery system in US-EAST-1 (Virginia). AWS is tasked with the protection of the infrastructure that operates AWS services within the AWS Cloud. This infrastructure undergoes regular assessments and verifications by third-party auditors as part of the AWS compliance programs.

Our relational database services (RDS) employ AES-256 encryption, the industry standard, to secure data. Amazon RDS manages access authentication and data decryption with minimal performance impact. Data encryption applies both at rest and during transmission; it covers not only instance storage but also extends to read replicas, automated backups, and snapshots.

For data in transit, Oracle utilizes Oracle Native Network Encryption AES-256, while MySQL data is secured over SSL. Inbound web traffic is secured via SSL and, depending on the requirements, may also involve additional measures such as Web Application Firewall (WAF) authorization, IP whitelisting, Google 2-step Authenticator, or VPN access.

Access within our network to all client data is strictly controlled. Our staff at ACI must comply with internal security protocols that safeguard both data and physical equipment. These protocols include adherence to rigorous procedures and policies regarding the handling of confidential and sensitive information.

We strictly prohibit subcontractor access to production data. Employee access to sensitive data is contingent upon authentication at AAL2 level with a username and password, supplemented by Google 2-step Authenticator for network access. This comprehensive approach ensures robust security and integrity of client data across all our systems.

2. Perimeter Controls

ACCESS IS SCRUTINIZED

AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who have a need to be present at a data center must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

ENTRY IS CONTROLLED AND MONITORED

Entering the Perimeter Layer is a controlled process. We staff our entry gates with security officers and employ supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge that requires multi-factor authentication and limits access to pre-approved areas.

AWS DATA CENTER WORKERS ARE SCRUTINIZED, TOO

AWS employees who routinely need access to a data center are given permissions to relevant areas of the facility based on job function. But their access is regularly scrutinized, too. Staff lists are routinely reviewed by an area access manager to ensure each employee’s authorization is still necessary. If an employee doesn’t have an ongoing business need to be at a data center, they have to go through the visitor process.

MONITORING FOR UNAUTHORIZED ENTRY

We are continuously watching for unauthorized entry on our property, using video surveillance, intrusion detection, and access log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.

AWS SECURITY OPERATIONS CENTERS MONITORS GLOBAL SECURITY

AWS Security Operations Centers are located around the world and are responsible for monitoring, triaging, and executing security programs for our data centers. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data center security teams. In short, they support our security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyze a potential security incident.

2. Data Backups

Oracle and MySQL backups are governed by the automated backup feature of Amazon RDS, which facilitates point-in-time recovery of your DB instance. This feature captures both your database and its transaction logs, storing them for a retention period defined by the user. Consequently, it is possible to restore your DB instance to any specific second within your retention period, up to the last five minutes. The automatic backup retention period is set to thirty-five days, while monthly snapshots are preserved for one year.

Additionally, daily full Oracle and MySQL snapshots are securely stored in the disaster recovery environment located in Northern Virginia. All data backups are encrypted both at rest and during transit to ensure the utmost security and compliance with data protection standards.

3. File Backups

Files are backed up daily, with every version of these daily backups retained for a duration of two years. After this period, only the final version of each file is preserved indefinitely. All file backups are securely stored in S3 buckets, which are not publicly accessible and are protected with 256-bit AES encryption.

The backup client employs a 256-bit AES encryption key to safeguard data during transit, ensuring robust security measures are maintained.

Furthermore, production files are synchronized with the Disaster Recovery (DR) environment every 15 minutes, guaranteeing up-to-date redundancy and swift recovery capabilities in the event of an incident.

4. Instance Image & Volume Snapshots

Daily instance snapshots are captured and retained for 30 days, ensuring frequent and recent backups are available for operational recovery. Additionally, monthly snapshots are captured and preserved for a full year, providing a longer-term backup solution. This structured approach to snapshot management offers comprehensive data protection and facilitates effective disaster recovery planning.

5. Web Application Firewall

The Barracuda Web Application Firewall (WAF) offers robust protection for applications against a spectrum of external threats, including the OWASP Top 10 security risks, zero-day threats, data leakage, and application-layer denial of service (DoS) attacks. This is achieved through a dual approach that combines positive, signature-based policies with advanced anomaly detection capabilities, enabling the Barracuda WAF to counteract even the most sophisticated attacks aimed at your web applications. Additionally, the configuration of the web application firewall is securely backed up daily to the Barracuda cloud environment, ensuring that security settings and configurations are preserved and can be quickly restored if necessary.

6. Password Encryption

Passwords are secured using a salted-hash mechanism. In this context, "salt" refers to a random string of data that is added to a password before hashing. The primary purpose of salt is to enhance the security of password hashes by ensuring that each user's password remains unique, even if two users choose the same password. This uniqueness helps prevent hash collisions and thwarts attempts at unauthorized access. Furthermore, the addition of salt complicates efforts by attackers to use hash-matching strategies, such as dictionary attacks, across the system. By preventing the straightforward testing of known passwords on all user accounts simultaneously, salt significantly bolsters system security against various types of cyber threats.

7. Structured Application Security

All applications should include input and output validation, implement authentication, never store credit card numbers, generate logs for important security events, secure sensitive data by encrypting them using approved encryption algorithms. Applications should conform to client defined password policy, any other security requirement set for a specific client.

8. Data loss prevention methodology

Identify and classify sensitive data
Use data encryption
Harden systems
Implement a rigorous patch management strategy
Allocate roles
Automate as much as possible
Use anomaly detection
Establish metrics
Don’t save unnecessary data

9. Application-Level Protection

Our application employs robust mechanisms for role-based and user-based access controls, ensuring that personally identifiable information (PII) is accessible only to a minimal and necessary set of users or roles. During the implementation phase, we collaborate closely with your team to tailor these controls, guaranteeing that access to PII is tightly restricted. Additionally, our system includes functionality to mask search results, ensuring that sensitive information remains hidden from unauthorized users.

Amazon Web Services: Risk and Compliance

May 2017

We welcome your feedback. Please share your thoughts at this link.

This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance questions.

Table of Contents

Risk and Compliance Overview

AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS' part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:

- Obtaining industry certifications and independent third-party attestations described in this document
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

For a more detailed description of AWS security please see:
AWS Security Center: https://aws.amazon.com/security/

For a more detailed description of AWS Compliance please see
AWS Compliance page: https://aws.amazon.com/compliance/

Additionally, The AWS Overview of Security Processes Whitepaper covers AWS' general security controls and service-specific security.

Shared Responsibility Environment

Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them (described in the AWS Certifications and Third-party Attestations section of this document) to perform their control evaluation and verification procedures as required.

The next section provides an approach on how AWS customers can evaluate and validate their distributed control environment effectively.

Strong Compliance Governance

As always, AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help companies gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

Evaluating and Integrating AWS Controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This documentation assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated. This information also assists customers in their efforts to account for and to validate that controls in their extended IT environment are operating effectively.

Traditionally, the design and operating effectiveness of control objectives and controls are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation/verification, by the customer or customer's external auditor, is generally performed to validate controls. In the case where service providers, such as AWS, are used, companies request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objective and controls. As a result, although customer's key controls may be managed by AWS, the control environment can still be a unified framework where all controls are accounted for and are verified as operating effectively. Third-party attestations and certifications of AWS can not only provide a higher level of validation of the control environment, but may relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS cloud.

AWS IT Control Information

AWS provides IT control information to customers in the following two ways:

1. **Specific control definition.** AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment. AWS' controls can be considered designed and operating effectively for many compliance purposes, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies (e.g., ISO 27001 auditors may request a SOC 1 Type II report in order to complete their evaluations for customers).

Other specific control activities relate to AWS' Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. As discussed below, AWS is compliant with FISMA Moderate standards and with the PCI Data Security Standard. These PCI and FISMA standards are very prescriptive and require independent validation that AWS adheres to the published standard.

2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, evaluation of AWS' industry certifications may be performed. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to companies that handle credit card information. With AWS' compliance with the FISMA standards, AWS complies with a wide range of specific controls required by US government agencies. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

AWS Global Regions

Data centers are built in clusters in various global regions, including: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Frankfurt), EU (Ireland), Asia Pacific (Seoul) Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), China (Beijing), and South America (Sao Paulo).

For a complete list of regions, see the AWS Global Infrastructure page.

AWS Risk and Compliance Program

AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

Risk Management

AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

In addition, the AWS control environment is subject to various internal and external risk assessments. AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.2, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.

Control Environment

AWS manages a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS' service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS' control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures.

Information Security

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

AWS Certifications, Programs, Reports, and Third-Party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

CJIS

AWS complies with the FBI's Criminal Justice Information Services (CJIS) standard. We sign CJIS security agreements with our customers, including allowing or performing any required employee background checks according to the **CJIS Security Policy**.

Law enforcement customers (and partners who manage CJI) are taking advantage of AWS services to improve the security and protection of CJI data, using the advanced security services and features of AWS, such as activity logging (**AWS CloudTrail**), encryption of data in motion and at rest (S3's Server-Side Encryption with the option to bring your own key), comprehensive key management and protection (AWS **Key Management Service** and **CloudHSM**), and integrated permission management (IAM federated identity management, multi-factor authentication).

AWS has created a Criminal Justice Information Services (CJIS) **Workbook** in a security plan template format aligned to the CJIS Policy Areas. Additionally, a CJIS Whitepaper has been developed to help guide customers in their journey to cloud adoption.

Visit the CJIS Hub Page**: https://aws.amazon.com/compliance/cjis/**

CSA

In 2011, the Cloud Security Alliance (CSA) launched **STAR**, an initiative to encourage transparency of security practices within cloud providers. The **CSA Security, Trust & Assurance Registry** (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. **AWS is a CSA STAR registrant** and has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and document what security controls exist in AWS' Infrastructure as a Service offerings. The CAIQ provides 298 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

See: **Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1**

Cyber Essentials Plus

Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks.

It demonstrates the baseline controls AWS implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "**10 Steps to Cyber Security**". It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organizations that offer incentives for businesses holding this certification.

Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to EU (Ireland) region.

DoD SRG Levels 2 and 4

The Department of Defense (DoD) Cloud Security Model (SRG) provides a formalized assessment and authorization process for cloud service providers (CSPs) to gain a DoD Provisional Authorization, which can subsequently be leveraged by DoD customers. A Provisional Authorization under the SRG provides a reusable certification that attests to our compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation on AWS. AWS currently holds provisional authorizations at Levels 2 and 4 of the SRG.

Additional information of the security control baselines defined for **Levels 2, 4, 5, and 6 can be found at: http://iase.disa.mil/cloud_security/Pages/index.aspx**.

Visit the DoD Hub Page**: https://aws.amazon.com/compliance/dod/**

FedRAMP SM

AWS is a Federal Risk and Authorization Management Program (FedRAMPsm) Compliant Cloud Service Provider. AWS has completed the testing performed by a FedRAMPsm accredited Third-Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMPsm requirements at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMPsm repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment. The two FedRAMPsm Agency ATOs encompass all U.S. regions (the AWS GovCloud (US) region and the AWS US East/West regions).

For a complete list of the services that are in the accreditation boundary for the regions stated above, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

For more information on AWS FedRAMPsm compliance please see the AWS FedRAMPsm FAQs at:

https://aws.amazon.com/compliance/fedramp/

FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18, or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

AWS enables covered entities and their business associates subject to FERPA to leverage the secure AWS environment to process, maintain, and store protected education information.

AWS also offers a **FERPA-focused whitepaper** for customers interested in learning more about how they can leverage AWS for the processing and storage of educational data.

The "**FERPA Compliance on AWS Whitepaper**" outlines how companies can use AWS to process systems that facilitate FERPA compliance: https://d0.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, SSL terminations in **AWS GovCloud (US)** operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the **AWS GovCloud (US) environment**.

FISMA and DIACAP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (**FISMA**). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (**DIACAP**).

GxP

GxP is an acronym that refers to the regulations and guidelines applicable to life sciences organizations that make food and medical products such as drugs, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers and to ensure the integrity of data used to make product-related safety decisions.

AWS offers a **GxP whitepaper** which details a comprehensive approach for using AWS for GxP systems. This whitepaper provides guidance for using **AWS Products in the context of GxP** and the content has been developed in conjunction with AWS pharmaceutical and medical device customers, as well as software partners, who are currently using AWS Products in their validated GxP systems.

For more information on the GxP on AWS **please contact AWS Sales and Business Development**.

For additional information please see our GxP Compliance FAQs:
https://aws.amazon.com/compliance/gxp-part-11-annex-11/

HIPAA

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information and AWS will be signing business associate agreements with such customers. AWS also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of health information. The Architecting for HIPAA Security and Compliance on Amazon Web Services whitepaper outlines how companies can use AWS to process systems that facilitate HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) compliance.

Customers who execute an AWS BAA may use any AWS service in an account designated as a HIPAA Account, but they may only process, store and transmit PHI using the HIPAA-eligible services defined in the AWS BAA. For a complete list of these services, see the HIPAA Eligible Services Reference page (https://aws.amazon.com/compliance/hipaa-eligible-services-reference/).

AWS maintains a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the administrative, technical, and physical safeguards required under HIPAA. Using these services to store, process, and transmit PHI allows our customers and AWS to address the HIPAA requirements applicable to the AWS utility-based operating model.

For additional information please see our HIPAA Compliance FAQs and Architecting for HIPAA Security and Compliance on Amazon Web Services.

IRAP

The Information Security Registered Assessors Program (IRAP) enables Australian government customers to validate that appropriate controls are in place and determine the appropriate responsibility model for addressing the needs of the Australian Signals Directorate (ASD) Information Security Manual (ISM).

Amazon Web Services **has completed an independent assessment** that has determined all applicable ISM controls are in place relating to the processing, storage and transmission of Unclassified (DLM) for the AWS Sydney Region.

IRAP Compliance FAQs:
https://aws.amazon.com/compliance/irap/

For more information see: **Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations**

ISO 9001

AWS has achieved ISO 9001 certification, AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

The ISO 9001 certification covers the quality management system over a specified scope of AWS services and Regions of operations. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

ISO 9001:2008 is a global standard for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

The AWS ISO 9001 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_9001_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 9001 certification at:
https://aws.amazon.com/compliance/iso-9001-faqs/

ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing significant information regarding our security controls and practices.

The AWS ISO 27001 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27001 certification at:
https://aws.amazon.com/compliance/iso-27001-faqs/

ISO 27017

ISO 27017 is the newest code of practice released by the International Organization for Standardization (ISO). It provides implementation guidance on information security controls that specifically relate to cloud services.

AWS has achieved ISO 27017 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

The AWS ISO 27017 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27017_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27017 certification at:
https://aws.amazon.com/compliance/iso-27017-faqs/

ISO 27018

ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

AWS has achieved ISO 27018 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

The AWS ISO 27018 certification can be downloaded at:
https://d0.awsstatic.com/certifications/iso_27018_certification.pdf

AWS provides additional information and frequently asked questions about its ISO 27018 certification at:
https://aws.amazon.com/compliance/iso-27018-faqs/

ITAR

The **AWS GovCloud (US)** region supports US International Traffic in Arms Regulations (**ITAR**) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to the US. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party to validate the proper controls are in place to support customer export compliance programs for this requirement.

MPAA

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a “certification,” media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS.

See the AWS Compliance MPAA hub page for additional details:
https://aws.amazon.com/compliance/mpaa/

MTCS Tier 3 Certification

The **Multi-Tier Cloud Security (MTCS)** is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The certification assessment requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

View the MTCS Hub Page at:
https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/

NIST

In June 2015 The National Institute of Standards and Technology (NIST) released guidelines **800-171**, "Final Guidelines for Protecting Sensitive Government Information Held by Contractors". This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on nonfederal systems.

AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which AWS has already been audited under the FedRAMP program. The FedRAMP Moderate security control baseline is more rigorous than the recommended requirements established in Chapter 3 of 800-171, and includes a significant number of security controls above and beyond those required of FISMA Moderate systems that protect CUI data. A detailed mapping is available in the **NIST Special Publication 800-171**, starting on page D2 (which is page 37 in the PDF).

PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers. The AWS PCI Compliance Package includes the AWS PCI Attestation of Compliance (AoC), which shows that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 3.1, and the AWS PCI Responsibility Summary, which explains how compliance responsibilities are shared between AWS and our customers in the cloud.

For a complete list of services in scope for PCI DSS Level 1, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

The latest scope of services and regions for the AWS PCI DSS Level 1 certification can be found at:
https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

SOC 1/ISAE 3402

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with American Institute of Certified Public Accountants (AICPA): AT 801 (formerly SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This report is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

Objective Area	Objective Description
Security Organization	Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.
Employee User Access	Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.
Logical Security	Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
Secure Data Handling	Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.
Physical Security and Environmental Protection	Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.
Change Management	Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.
Data Integrity, Availability and Redundancy	Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.
Incident Handling	Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved.

The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS' customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS' commitment to the SOC 1 report is ongoing, and AWS will continue the process of periodic audits. For the current scope of the SOC 1 report, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security and availability principles set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting customer data. The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

SOC 3

AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically-available summary of the AWS SOC 2 report. The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process to request a SOC 2 report. The SOC 3 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services. View the AWS SOC 3 report here.

Key Compliance Questions and AWS

This section addresses generic cloud computing compliance questions specifically for AWS. These common compliance questions listed may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.

Ref	Cloud Computing Question	AWS Information
1	Control ownership. Who owns which controls for cloud-deployed infrastructure?	For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report.

Ref	Cloud Computing Question	AWS Information
2	Auditing IT. How can auditing of the cloud provider be accomplished?	Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.
3	Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment?	If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS' physical controls, they can reference the AWS SOC 1 Type II report which details the controls that AWS provides.
4	HIPAA compliance. Is it possible to meet HIPAA compliance requirements while deployed in the cloud provider environment?	HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers can use AWS services to maintain a security level that is equivalent or greater than those required to protect electronic health records. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic.
5	GLBA compliance. Is it possible to meet GLBA certification requirements while deployed in the cloud provider environment?	Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions, and build GLBA-compliant applications on AWS infrastructure. If the customer requires specific assurance that physical security controls are operating effectively, they can reference the AWS SOC 1 Type II report as relevant.
6	Federal regulation compliance. Is it possible for a US Government agency to be compliant with security and privacy regulations while deployed in the cloud provider environment?	US Federal agencies can be compliant under a number of compliance standards, including the Federal Information Security Management Act (FISMA) of 2002, Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Processing Standard (FIPS) Publication 140-2, and the International Traffic in Arms Regulations (ITAR). Compliance with other laws and statutes may also be accommodated depending on the requirements set forth in the applicable legislation.
7	Data location. Where does customer data reside?	AWS customers designate in which physical region their data and their servers will be located. Data replication for S3 data objects is done within the regional cluster in which the data is stored and is not replicated to other data center clusters in other regions. AWS customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.

Ref	Cloud Computing Question	AWS Information
8	E-Discovery. Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements?	AWS provides infrastructure, and customers manage everything else, including the operating system, the network configuration, and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
9	Data center tours. Are data center tours by customers allowed by the cloud provider?	No. Due to the fact that our data centers host multiple customers, AWS does not allow data center tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report. This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data center physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FedRAMPsm testing programs.
10	Third-party access. Are third parties allowed access to the cloud provider data centers?	AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS data center manager per the AWS access policy. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls.
11	Privileged actions. Are privileged actions monitored and controlled?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, ITAR, and FedRAMPsm audits.
12	Insider access. Does the cloud provider address the threat of inappropriate insider access to customer data and applications?	AWS provides specific SOC 1 controls to address the threat of inappropriate insider access, and the public certification and compliance initiatives covered in this document address insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.

Ref	Cloud Computing Question	AWS Information
13	Multi-tenancy. Is customer segregation implemented securely?	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 3.1 published in April 2015. Note that AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating your Amazon EC2 compute instances at the hardware level.
14	Hypervisor vulnerabilities. Has the cloud provider addressed known hypervisor vulnerabilities?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper for more information on the Xen hypervisor and instance isolation.
15	Vulnerability management. Are systems patched appropriately?	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems.
16	Encryption. Do the provided services support encryption?	Yes. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB, and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Refer to the AWS Security white paper for more information.
17	Data ownership. What are the cloud provider's rights over customer data?	AWS customers retain control and ownership of their data. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis.
18	Data isolation. Does the cloud provider adequately isolate customer data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Amazon S3 provides advanced data access controls. Please see the AWS security whitepaper for more information about specific data services' security.
19	Composite services. Does the cloud provider layer its service with other providers' cloud services?	AWS does not leverage any third-party cloud providers to deliver AWS services to customers.

Ref	Cloud Computing Question	AWS Information
20	Physical and environmental controls. Are these controls operated by the cloud provider specified?	Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FedRAMP^{sm} require best practice physical and environmental controls.
21	Client-side protection. Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices?	Yes. AWS allows customers to manage client and mobile applications to their own requirements.
22	Server security. Does the cloud provider allow customers to secure their virtual servers?	Yes. AWS allows customers to implement their own security architecture. See the AWS security whitepaper for more details on server and network security.
23	Identity and Access Management. Does the service include IAM capabilities?	AWS has a suite of identity and access management offerings, allowing customers to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way. Please see the AWS web site for more information.
24	Scheduled maintenance outages. Does the provider specify when systems will be brought down for maintenance?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
25	Capability to scale. Does the provider allow customers to scale beyond the original agreement?	The AWS cloud is distributed, highly secure and resilient, giving customers massive scale potential. Customers may scale up or down, paying for only what they use.
26	Service availability. Does the provider commit to a high level of availability?	AWS does commit to high levels of availability in its service level agreements (SLA). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.9%. Service credits are provided in the case these availability metrics are not met.
27	Distributed Denial Of Service (DDoS) attacks. How does the provider protect their service against DDoS attacks?	The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks.
28	Data portability. Can the data stored with a service provider be exported by customer request?	AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport.
29	Service provider business continuity. Does the service provider operate a business continuity program?	AWS does operate a business continuity program. Detailed information is provided in the AWS Security Whitepaper.

Ref	Cloud Computing Question	AWS Information
30	Customer business continuity. Does the service provider allow customers to implement a business continuity plan?	AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures.
31	Data durability. Does the service specify data durability?	Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.
32	Backups. Does the service provide backups to tapes?	AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS web site.
33	Price increases. Will the service provider raise prices unexpectedly?	AWS has a history of frequently reducing prices as the cost to provide these services reduces over time. AWS has reduced prices consistently over the past several years.
34	Sustainability. Does the service provider company have long term sustainability potential?	AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high long term sustainability potential.

AWS Contact

Customers can request the reports and certifications produced by our third-party auditors or can request more information about AWS Compliance by contacting AWS Sales and Business Development. The representative will route customers to the proper team depending on nature of the inquiry. For additional information on AWS Compliance, see the AWS Compliance site or send questions directly to awscompliance@amazon.com.

Appendix A: CSA Consensus Assessments Initiative Questionnaire v3.0.1

The Cloud Security Alliance (CSA) is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing." [Reference **https://cloudsecurityalliance.org/about/**] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security *Application Security*	AIS-01.1	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. AWS has in place procedures to manage new development of resources. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	
	AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	
	AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	
	AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Application & Interface Security *Customer Access Requirements*	AIS-02.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	AWS Customers retain responsibility to ensure their usage of AWS is in compliance with applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/compliance) and providing certifications, reports and other relevant documentation directly to AWS Customers.
	AIS-02.2	Are all requirements and trust levels for customers' access defined and documented?	
Application & Interface Security *Data Integrity*	AIS-03.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	AWS data integrity controls as described in AWS SOC reports illustrates the data integrity controls maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 14 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Application & Interface Security *Data Security / Integrity*	AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	AWS Data Security Architecture was designed to incorporate industry leading practices. Refer to AWS Certifications, reports and whitepapers for additional details on the various leading practices that AWS adheres to (available at http://aws.amazon.com/compliance).
Audit Assurance & Compliance *Audit Planning*	AAC-01.1	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	AWS obtains certain industry certifications and independent third-party attestations and provides certain certifications, reports and other relevant documentation directly to AWS Customers.
Audit Assurance & Compliance *Independent Audits*	AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	AWS provides third-party attestations, certifications, Service Organization Controls (SOC) reports and other relevant compliance reports directly to our customers under NDA. The AWS ISO 27001 certification can be downloaded here: http://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf. The AWS SOC 3 report can be downloaded here: https://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat
	AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	
	AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	AAC-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external audits and risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.
	AAC-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	
	AAC-02.6	Are the results of the penetration tests available to tenants at their request?	
	AAC-02.7	Are the results of internal and external audits available to tenants at their request?	
	AAC-02.8	Do you have an internal audit program that allows for cross-functional audit of assessments?	
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 and Glacier services are designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website.
	AAC-03.2	Do you have capability to recover data for a specific customer in the case of a failure or data loss?	
	AAC-03.3	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
	AAC-03.4	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	AWS monitors relevant legal and regulatory requirements. Refer to ISO 27001 standard Annex 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01.1	Do you provide tenants with geographically resilient hosting options?	Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Refer to AWS Overview of Cloud Security whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR-01.2	Do you provide tenants with infrastructure service failover capability to other providers?	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	AWS Customers designate in which physical region their data and servers will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. AWS SOC reports provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing.
	BCR-03.2	Can tenants define how their data is transported and through which legal jurisdictions?	
Business Continuity Management & Operational Resilience Documentation	BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security/. Refer to ISO 27001 Appendix A Domain 12.
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05.1	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11.

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR -07.1	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	BCR - 07.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	
	BCR - 07.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	
	BCR - 07.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	
	BCR -07.5	Does your cloud solution include software/provider independent restore and recovery capabilities?	
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR -08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	AWS equipment is protected from utility service outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. In addition, refer to the AWS Cloud Security Whitepaper - available at http://aws.amazon.com/security.
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR -09.1	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	AWS CloudWatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	BCR - 09.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	
	BCR - 09.3	Do you provide customers with ongoing visibility and reporting of your SLA performance?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Business Continuity Management & Operational Resilience *Policy*	BCR -10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/compliance.
Business Continuity Management & Operational Resilience *Retention Policy*	BCR -11.1	Do you have technical control capabilities to enforce tenant data retention policies?	AWS provide customers with the ability to delete their data. However, AWS Customers retain control and ownership of their data so it is the customer's responsibility to manage data retention to their own requirements. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. For additional information refer to https://aws.amazon.com/compliance/data-privacy-faq/.
	BCR -11.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	
	BCR -11.4	Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	AWS backup and redundancy mechanisms have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 12 and the AWS SOC 2 report for additional information on AWS backup and redundancy mechanisms.
	BCR -11.5	Do you test your backup or redundancy mechanisms at least annually?	
Change Control & Configuration Management *New Development / Acquisition*	CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	Policies and Procedures have been established through AWS Security framework based upon NIST 800-53, ISO 27001, ISO 27017, ISO 27018, ISO 9001 standard and the PCI DSS requirements. Whether a customer is new to AWS or an advanced user, useful information about the services, ranging from introductions to advanced features, can be found on the AWS Documentation section of our website at https://aws.amazon.com/documentation/.
	CCC-01.2	Is documentation available that describes the installation, configuration and use of products/services/features?	
Change Control & Configuration Management *Outsourced Development*	CCC-02.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes. Refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-02.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Change Control & Configuration *Management Quality Testing*	CCC-03.1	Do you provide your tenants with documentation that describes your quality assurance process?	AWS maintains an ISO 9001 certification. This is an independent validation of AWS quality system and determined that AWS activities comply with ISO 9001 requirements. AWS Security Bulletins notify customers of security and privacy events. Customers can subscribe to the AWS Security Bulletin RSS feed on our website. Refer to aws.amazon.com/security/security-bulletins/. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS system development lifecycle (SDLC) incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details. In addition, refer to ISO 27001 standard, Annex A, domain 14 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	CCC-03.2	Is documentation describing known issues with certain products/services available?	
	CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	
	CCC-03.4	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	
Change Control & Configuration Management *Unauthorized Software Installations*	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	AWS' program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Change Control & Configuration Management *Production Changes*	CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles / rights / responsibilities within it?	AWS SOC reports provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 12 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Data Security & Information Lifecycle Management *Classification*	DSI-01.1	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	DSI-01.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user-friendly names, enhance searchability, and improve coordination between multiple users. The AWS Management Console has also supports tagging.

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-01.3	Do you have a capability to use system geographic location as an authentication factor?	AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL.
	DSI-01.4	Can you provide the physical location/geography of storage of a tenant's data upon request?	AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the [AWS Global Infrastructure]() page.
	DSI-01.5	Can you provide the physical location/geography of storage of a tenant's data in advance?	
	DSI-01.6	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	AWS Customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements.
	DSI-01.7	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions. AWS Customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the [AWS Global Infrastructure]() page.
Data Security & Information Lifecycle Management *Data Inventory / Flows*	DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the [AWS Global Infrastructure]() page.
	DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	
Data Security & Information Lifecycle Management *eCommerce Transactions*	DSI-03.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	All of the AWS APIs are available via SSH-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Customers may also use third-party encryption technologies.

Control Group	CID	Consensus Assessment Questions	AWS Response
	DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy*	DSI-04.1	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	AWS Customers retain control and ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.
	DSI-04.2	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	
Data Security & Information Lifecycle Management *Nonproduction Data*	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Data Security & Information Lifecycle Management *Ownership / Stewardship*	DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	AWS Customers retain control and ownership of their own data. Refer to the AWS Customer Agreement for additional information.
Data Security & Information Lifecycle Management *Secure Disposal*	DSI-07.1	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. Encryption of sensitive data is generally a good security practice, and AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256. The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage. In order to be able to do this efficiently and
	DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	

Control Group	CID	Consensus Assessment Questions	AWS Response
			with low latency, the EBS encryption feature is only available on EC2's more powerful instance types (e.g., M3, C3, R3, G2).
Datacenter Security *Asset Management*	DCS -01.1	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS -01.2	Do you maintain a complete inventory of all of your critical supplier relationships?	
Datacenter Security *Controlled Access Points*	DCS -02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Equipment Identification*	DCS -03.1	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Offsite Authorization*	DCS -04.1	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	AWS Customers can designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.

Control Group	CID	Consensus Assessment Questions	AWS Response
Datacenter Security *Offsite equipment*	DCS-05.1	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Datacenter Security *Policy*	DCS-06.1	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC reports provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 and SOC 2 reports provides further information.
Datacenter Security *Secure Area Authorization*	DCS-07.1	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	AWS Customers designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. For a complete list of available regions, see the AWS Global Infrastructure page.
Datacenter Security *Unauthorized Persons Entry*	DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Datacenter Security *User Access*	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Encryption & Key Management *Entitlement*	EKM-01.1	Do you have key management policies binding keys to identifiable owners?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
Encryption & Key Management *Key Generation*	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
	EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	
	EKM-02.3	Do you maintain key management procedures?	
	EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	
	EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	
Encryption & Key Management *Encryption*	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. In addition, refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	
	EKM-03.3	Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	EKM-03.4	Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	
Encryption & Key Management *Storage and Access*	EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. In addition, customers can leverage AWS Key Management Systems (KMS) to create and control encryption keys (refer to https://aws.amazon.com/kms/). Refer to AWS SOC reports for more details on KMS. AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP.
	EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	
	EKM-04.3	Do you store encryption keys in the cloud?	
	EKM-04.4	Do you have separate key management and key usage duties?	
Governance and Risk Management *Baseline Requirements*	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standards, Annex A, domain 14 and 18 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances.
	GRM-01.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	
	GRM-01.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	
Governance and Risk Management *Risk Assessments*	GRM-02.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS Customers. Continuous Monitoring of logical controls can be executed by customers on their own systems.

Control Group	CID	Consensus Assessment Questions	AWS Response
	GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. For more information refer to the AWS Compliance ISO 27018 FAQ http://aws.amazon.com/compliance/iso-27018-faqs/.
Governance and Risk Management *Management Oversight*	GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/compliance.
Governance and Risk Management *Management Program*	GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	AWS provides our customers with our ISO 27001 certification. The ISO 27001 certification is specifically focused on the AWS ISMS and measures how AWS internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms they are operating in alignment with the ISO 27001 certification standard. For additional information refer to the AWS Compliance ISO 27001 FAQ website: http://aws.amazon.com/compliance/iso-27001-faqs/.
	GRM-04.2	Do you review your Information Security Management Program (ISMP) least once a year?	
Governance and Risk Management *Management Support / Involvement*	GRM-05.1	Do you ensure your providers adhere to your information security and privacy policies?	AWS has established information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance. Information about the AWS Compliance programs is published publicly on our website at http://aws.amazon.com/compliance/.
Governance and Risk Management *Policy*	GRM-06.1	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	
	GRM-06.2	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	
	GRM-06.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	
	GRM-06.4	Do you disclose which controls, standards,	

Control Group	CID	Consensus Assessment Questions	AWS Response
		certifications and/or regulations you comply with?	
Governance and Risk Management *Policy Enforcement*	GR M-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	AWS provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	GR M-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	
Governance and Risk Management *Business / Policy Change Impacts*	GR M-08.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
Governance and Risk Management *Policy Reviews*	GR M-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Our AWS Cloud Security Whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security and http://aws.amazon.com/compliance, are updated on a regular basis to reflect updates to the AWS policies.
	GR M-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	The AWS SOC reports provide details related to privacy and security policy review.
Governance and Risk Management *Assessments*	GR M-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Refer to AWS Risk and Compliance Whitepaper (available at aws.amazon.com/security) for additional details on AWS Risk Management Framework.
	GR M-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	
Governance and Risk	GR M-11.1	Do you have a documented, organization-wide program in place to manage risk?	In alignment with ISO 27001, AWS maintains a Risk Management program to mitigate and manage risk.

Control Group	CID	Consensus Assessment Questions	AWS Response
Management *Program*	GRM-11.2	Do you make available documentation of your organization-wide risk management program?	AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. AWS Risk Management program is reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Human Resources *Asset Returns*	HRS-01.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	AWS Customers retain the responsibility to monitor their own environment for privacy breaches. The AWS SOC reports provides an overview of the controls in place to monitor AWS managed environment.
	HRS-01.2	Is your Privacy Policy aligned with industry standards?	
Human Resources *Background Screening*	HRS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. The AWS SOC reports provides additional details regarding the controls in place for background verification.
Human Resources *Employment Agreements*	HRS-03.1	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	In alignment with ISO 27001 standard, all AWS employees complete periodic role based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details. All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.
	HRS-03.2	Do you document employee acknowledgment of training they have completed?	
	HRS-03.3	Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	
	HRS-03.4	Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	
	HRS-03.5	Are personnel trained and provided with awareness programs at least once a year?	
Human Resources *Employment Termination*	HRS-04.1	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. AWS SOC reports provide additional details.

Control Group	CID	Consensus Assessment Questions	AWS Response
	HRS - 04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provide further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Human Resources *Portable / Mobile Devices*	HRS -05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Human Resources *Nondisclosure Agreements*	HRS -06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs.
Human Resources *Roles / Responsibilities*	HRS -07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	The AWS Cloud Security Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security and http://aws.amazon.com/compliance.
Human Resources *Acceptable Use*	HRS -08.1	Do you provide documentation regarding how you may or access tenant data and metadata?	AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content. Refer to the ISO 27001 standard and 27018 code of practice for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 and ISO 27018.
	HRS - 08.2	Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	
	HRS - 08.3	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Human Resources *Training / Awareness*	HRS -09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. AWS roles and responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	HRS -09.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	
Human Resources *User Responsibility*	HRS -10.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 7 and 8. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition the AWS Cloud Security Whitepaper provides further details - available at http://aws.amazon.com/security.
	HRS -10.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?	
	HRS -10.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	
Human Resources *Workspace*	HRS -11.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8 and 9. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.
	HRS -11.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	
	HRS -11.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Identity & Access Management *Audit Tools Access*	IAM -01.1	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IAM -01.2	Do you monitor and log privileged access (administrator level) to information security management systems?	AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events. Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Identity & Access Management *User Access Policy*	IAM -02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM - 02.2	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	
Identity & Access Management *Diagnostic / Configuration Ports Access*	IAM -03.1	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored per the AWS access policy. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
Identity & Access Management *Policies and Procedures*	IAM -04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	
Identity & Access Management *Segregation of Duties*	IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Customers retain the ability to manage segregations of duties of their AWS resources. Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 6 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management *Source Code Access Restriction*	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	
Identity & Access Management *Third Party Access*	IAM-07.1	Do you provide multi-failure disaster recovery capability?	AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC reports provides further details. ISO 27001 standard Annex A, domain 15 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	IAM-07.2	Do you monitor service continuity with upstream providers in the event of provider failure?	
	IAM-07.3	Do you have more than one provider for each service you depend on?	
	IAM-07.4	Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	
	IAM-07.5	Do you provide the tenant the ability to declare a disaster?	
	IAM-07.6	Do you provided a tenant-triggered failover option?	
	IAM-07.7	Do you share your business continuity and redundancy plans with your tenants?	
Identity & Access Management	IAM-08.1	Do you document how you grant and approve access to tenant data?	AWS Customers retain control and ownership of their data. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data

Control Group	CID	Consensus Assessment Questions	AWS Response
User Access Restriction / Authorization	IAM - 08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	and server instances are logically isolated from other customers by default. Privileged user access controls are reviewed by an independent auditor during the AWS SOC, ISO 27001, PCI, ITAR, and FedRAMP audits.
Identity & Access Management *User Access Authorization*	IAM -09.1	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified.
	IAM - 09.2	Do you provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored.
Identity & Access Management *User Access Reviews*	IAM -10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	In alignment with ISO 27001 standard, all access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC reports. Exceptions in the User entitlement controls are documented in the SOC reports. Refer to ISO 27001 standards, Annex A, domain 9 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IAM -10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	
	IAM -10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	
Identity & Access Management *User Access Revocation*	IAM -11.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC reports provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information. Refer to ISO 27001 Annex A, domain 9 for additional details. AWS has

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM -11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Identity & Access Management *User ID Credentials*	IAM -12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa.
	IAM -12.2	Do you use open standards to delegate authentication capabilities to your tenants?	AWS Identity and Access Management (IAM) supports identity federation for delegated access to the AWS Management Console or AWS APIs. With identity federation, external identities (federated users) are granted secure access to resources in your AWS account without having to create IAM users. These external identities can come from your corporate identity provider (such as Microsoft Active Directory or from the AWS Directory Service) or from a web identity provider, such as Amazon Cognito, Login with Amazon, Facebook, Google or any OpenID Connect (OIDC) compatible provider.
	IAM -12.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	
	IAM -12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	
	IAM -12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	
	IAM -12.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	
	IAM -12.7	Do you allow tenants to use third-party identity assurance services?	
	IAM -12.8	Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on website at https://aws.amazon.com/iam/. AWS SOC reports provides details on the specific control activities executed by AWS.
	IAM -12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IAM - 12.10	Do you support the ability to force password changes upon first logon?	
	IAM - 12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	
Identity & Access Management *Utility Programs Access*	IAM -13.1	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides details on the specific control activities executed by AWS. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IAM -13.2	Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	
	IAM -13.3	Are attacks that target the virtual infrastructure prevented with technical controls?	
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	AWS Incident response program (detection, investigation and response to incidents) has been developed in alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC reports provides additional details on controls in place to restrict system access. Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.
	IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	
	IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	
	IVS-01.4	Are audit logs centrally stored and retained?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Infrastructure & Virtualization Security *Change Detection*	IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS website for additional details - http://aws.amazon.com.
	IVS-02.2	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	
Infrastructure & Virtualization Security *Clock Synchronization*	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security *Capacity / Resource Planning*	IVS-04.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Details regarding AWS Service Limits and how to request an increase for specific services is available on the AWS website at http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html. AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	
	IVS-04.3	Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	
Infrastructure & Virtualization Security *Management - Vulnerability Management*	IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security *Network Security*	IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website - http://aws.amazon.com/documentation/.
	IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are
	IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	
	IVS-06.4	Are all firewall access control lists documented with business justification?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Infrastructure & Virtualization Security *OS Hardening and Base Controls*	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected. Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP.
Infrastructure & Virtualization Security *Production / Nonproduction Environments*	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/.
	IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	
	IVS-08.3	Do you logically and physically segregate production and non-production environments?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 13 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Infrastructure & Virtualization Security *Segmentation*	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	
	IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	
	IVS-09.3	Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-09.4	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection*	IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.
	IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	AWS Customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments.
Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening*	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization. Refer to AWS SOC reports for more information on Access Controls.
Infrastructure & Virtualization Security *Wireless Security*	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Policies, procedures and mechanisms to protect AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
	IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	

Control Group	CID	Consensus Assessment Questions	AWS Response
	IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	
Infrastructure & Virtualization Security *Network Architecture*	IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	AWS Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements. Internally, AWS network segmentation is aligned with the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. AWS security controls are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP compliance.
Interoperability & Portability *APIs*	IPY-01	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Details regarding AWS APIs can be found on the AWS website at https://aws.amazon.com/documentation/. In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC reports outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
Interoperability & Portability *Data Request*	IPY-02	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	
Interoperability & Portability *Policy & Legal*	IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	
	IPY-03.2	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	Customer retain control and ownership of their content. Customers can choose how they migrate applications and content both on and off the AWS platform at their discretion.

Control Group	CID	Consensus Assessment Questions	AWS Response
Interoperability & Portability *Standardized Network Protocols*	IPY-04.1	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	AWS allows customers to move data as needed on and off AWS storage. Refer to http://aws.amazon.com/choosing-a-cloud-platform for more information on Storage options.
	IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	
Interoperability & Portability *Virtualization*	IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e,g., OVF) to help ensure interoperability?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. Refer to the AWS Cloud Security Whitepaper for additional details - available at http://aws.amazon.com/security.
	IPY-05.2	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	
Mobile Security *Anti-Malware*	MOS-01	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to ISO 27001 standard, Annex A, domain 12 for additional information.
Mobile Security *Application Stores*	MOS-02	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	AWS has established an information security framework and policies and has effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
Mobile Security *Approved Applications*	MOS-03	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	
Mobile Security *Approved Software for BYOD*	MOS-04	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Mobile Security *Awareness and Training*	MOS-05	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	
Mobile Security *Cloud Based Services*	MOS-06	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	
Mobile Security *Compatibility*	MOS-07	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	
Mobile Security *Device Eligibility*	MOS-08	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	
Mobile Security *Device Inventory*	MOS-09	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	
Mobile Security *Device Management*	MOS-10	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	
Mobile Security *Encryption*	MOS-11	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	
Mobile Security *Jailbreaking and Rooting*	MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Legal*	MOS -13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to manage mobile security devices and the access to the customer's content.
	MOS -13.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	
Mobile Security *Lockout Screen*	MOS -14	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	
Mobile Security *Operating Systems*	MOS -15	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	
Mobile Security *Passwords*	MOS -16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	
	MOS -16.2	Are your password policies enforced through technical controls (i.e. MDM)?	
	MOS -16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	
Mobile Security *Policy*	MOS -17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	
	MOS -17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	MOS -17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	
Mobile Security *Remote Wipe*	MOS -18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	
	MOS -18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	
Mobile Security *Security Patches*	MOS -19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	
	MOS -19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	
Mobile Security *Users*	MOS -20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	
	MOS - 20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management*	SEF-02.1	Do you have a documented security incident response plan?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. The AWS SOC reports provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
	SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?	
	SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	

Control Group	CID	Consensus Assessment Questions	AWS Response
	SEF-02.4	Have you tested your security incident response plans in the last year?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting*	SEF-03.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	
	SEF-03.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation*	SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	
	SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	
	SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	
	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics*	SEF-05.1	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard. Refer to ISO 27001 Annex A, domain 16 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?	
Supply Chain Management, Transparency and Accountability	STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	Customers retain control and ownership over the quality of their data and potential quality errors that may arise through their usage of AWS services. Refer to AWS SOC report for specific details in relation to Data Integrity and Access Management (including least privilege access)

Control Group	CID	Consensus Assessment Questions	AWS Response
Data Quality and Integrity	STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	
Supply Chain Management, Transparency and Accountability *Incident Reporting*	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC reports provides details on the specific control activities executed by AWS. The AWS Cloud Security Whitepaper (available at http://aws.amazon.com/security) provides additional details.
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services*	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	AWS manages capacity and utilization data in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	STA-03.2	Do you provide tenants with capacity planning and use reports?	
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments*	STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 15 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
Supply Chain Management, Transparency and Accountability *Third Party Agreements*	STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information. AWS does not generally outsource development of AWS services to subcontractors.
	STA-05.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	
	STA-05.3	Does legal counsel review all third-party agreements?	
	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	
	STA-05.5	Do you provide the client with a list and copies of all sub processing agreements and keep this updated?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews*	STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?	AWS maintains formal agreements with key third party suppliers and implements appropriate relationship management mechanisms in line with their relationship to the business. AWS' third party management processes are reviewed by independent auditors as part of AWS ongoing compliance with SOC and ISO 27001.
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics*	STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	
	STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	
	STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	
	STA-07.4	Do you review all agreements, policies and processes at least annually?	
Supply Chain Management, Transparency and Accountability *Third Party Assessment*	STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?	
	STA-8.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?	
Supply Chain Management, Transparency and Accountability *Third Party Audits*	STA-09.1	Do you permit tenants to perform independent vulnerability assessments?	Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC reports provides additional details on the specific control activities executed by AWS.
	STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	

Control Group	CID	Consensus Assessment Questions	AWS Response
Threat and Vulnerability Management *Antivirus / Malicious Software*	TVM -01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	AWS' program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC reports provides further details. In addition, refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM -01.2	Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	
Threat and Vulnerability Management *Vulnerability / Patch Management*	TVM -02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS' own maintenance and system patching generally do not impact customers. Refer to AWS Cloud Security Whitepaper for further information - available at http://aws.amazon.com/security. Refer to ISO 27001 standard, Annex A, domain 12 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	TVM - 02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM - 02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	
	TVM - 02.4	Will you make the results of vulnerability scans available to tenants at their request?	
	TVM - 02.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	
	TVM - 02.6	Will you provide your risk-based systems patching time frames to your tenants upon request?	
Threat and Vulnerability Management *Mobile Code*	TVM -03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	AWS allows customers to manage client and mobile applications to their own requirements.
	TVM - 03.2	Is all unauthorized mobile code prevented from executing?	

Appendix B: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations

The Cloud Computing Security Considerations was created to assist agencies in performing a risk assessment of services offered by Cloud Service Providers. The following provides AWS alignment to the Security Considerations, published on September 2012. For additional details refer to: http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

Key Area	Questions	AWS RESPONSE
Maintaining Availability and Business Functionality	a. Business criticality of data or functionality. Am I moving business critical data or functionality to the cloud?	AWS customers retain control and ownership of their content. Customers are responsible for the classification and use of their content.
	b. Vendor's business continuity and disaster recovery plan. Can I thoroughly review a copy of the vendor's business continuity and disaster recovery plan that covers the availability and restoration of both my data and the vendor's services that I use? How much time does it take for my data and the services that I use to be recovered after a disaster, and do the vendor's other customers that are larger and pay more money than me get prioritization?	AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/. AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9 and the AWS SOC 1 Type II report for additional information.

Key Area	Questions	AWS RESPONSE
	c. My data backup plan. Will I spend additional money to maintain an up to date backup copy of my data located either at my agency's premises, or stored with a second vendor that has no common points of failure with the first vendor?	AWS customers retain control and ownership of their content and it is the customer's responsibility to manage their data backup plans. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS website. AWS offers a range of cloud computing services to support Disaster Recovery. To learn more about Disaster Recovery on AWS visit https://aws.amazon.com/disaster-recovery/.
	d. My business continuity and disaster recovery plan. Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data center and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically "failover", so that if one vendor's services become unavailable, control is automatically and smoothly transitioned to the other vendor.	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11 provides additional details. AWS has been validated

Key Area	Questions	AWS RESPONSE
		and certified by an independent auditor to confirm alignment with ISO 27001 certification.
	e. My network connectivity to the cloud. Is the network connectivity between my agency’s users and the vendor’s network adequate in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss?	Customers can also choose their network path to AWS facilities, including multiple VPN endpoints in each AWS Region. In addition, AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	f. Vendor's guarantee of availability. Does the Service Level Agreement (SLA guarantee that the vendor will provide adequate system availability an quality of service, using their robust system architecture and business processes?	AWS does commit to high levels of availability in its service level agreements (SLAs). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.99% Service credits are provided in the case these availability metrics are not met. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel. AWS Network Management is regularly reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMPsm.
	g. Impact of outages. Can I tolerate the maximum possible downtime of the SLA? Are the scheduled outage windows acceptable both in duration and time of day, or will scheduled outages interfere with my critical business processes?	AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS' own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer.
	h. SLA inclusion of scheduled outages. Does the SLA guaranteed availability percentage include scheduled outages?	AWS does not operate an environment with scheduled outage as AWS provides customers the ability to architect their environment to take advantage of multiple Availability Zones and regions.
	i. SLA compensation. Does the SLA adequately reflect the actual damage caused by a breach of the SLA such as unscheduled downtime or data loss?	AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS' Service Level Agreement.

Key Area	Questions	AWS RESPONSE
	j. Data integrity and availability. How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data?	AWS data integrity controls as described in AWS SOC 1 Type II report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. In addition, refer to ISO 27001 standard, Annex A, domain 12 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. You choose where to store your data by specifying a region (for Amazon S3) or an availability zone within a region (for EBS). Data stored in Amazon Elastic Block Store (Amazon EBS) is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones. Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security
	k. Data restoration. If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA?	AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region.
	l. Scalability. How much available spare computing resources does the vendor provide to enable my usage of the vendor's services to scale at short notice?	The AWS cloud is distributed, highly secure and resilient, giving customers large scaling potential. Customers may scale up or down, paying for only what they use.

Key Area	Questions	AWS RESPONSE
	m. Changing vendor. If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business, how do I get access to my data in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? How do I ensure that my data is permanently deleted from the vendor's storage media? For Platform as a Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency?	Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS.
Protecting Data from Unauthorized Access by a Third Party	a. Choice of cloud deployment model. Am I considering using a potentially less secure public cloud, a potentially more secure hybrid cloud or community cloud, or a potentially most secure private cloud?	AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet. Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center

Key Area	Questions	AWS RESPONSE
	b. Sensitivity of my data. Is my data to be stored or processed in the cloud classified, sensitive, private, or data that is publicly available such as information from my public web site? Does the aggregation of my data make it more sensitive than any individual piece of data? For example, the sensitivity may increase if storing a significant amount of data, or storing a variety of data that if compromised would facilitate identity theft. If there is a data compromise, could I demonstrate my due diligence to senior management, government officials and the public?	AWS customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements.
	c. Legislative obligations. What obligations do I have to protect and manage my data under various legislation, for example the Privacy Act, the Archives Act, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government?	AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third-party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers. AWS has published a whitepaper on using AWS in the context of Australian privacy considerations, available here.

Key Area	Questions	AWS RESPONSE
	d. Countries with access to my data. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centers? Will the vendor notify me if the answers to these questions change?	AWS customers choose the AWS Region or regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location of their choice. AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) region and store their content onshore in Australia. If the customer makes this choice, their content will be located in Australia unless the customer chooses to move the data. Customers can replicate and back up content in more than one region, but AWS does not move or replicate customer content outside of the customer's chosen region or regions. AWS is vigilant about customers' security and does not disclose or move data in response to a request from the Australian, U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-U.S. governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prevented from doing so.

Key Area	Questions	AWS RESPONSE
	e. Data encryption technologies. Are hash algorithms, encryption algorithms and key lengths deemed appropriate by the DSD ISM used to protect my data when it is in transit over a network, and stored on both the vendor's computers and on backup media? The ability to encrypt data while it is being processed by the vendor's computers is still an emerging technology and is an area of current research by industry and academia. Is the encryption deemed strong enough to protect my data for the duration of time that my data is sensitive?	AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications. AWS cryptographic processes are reviewed by independent third-party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP^{sm}. The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance. The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSMs are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSMs near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive access to CloudHSMs, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your Amazon EC2 applications.
	f. Media sanitization. What processes are used to sanitize the storage media storing my data at its end of life, and are the processes deemed appropriate by the DSD ISM?	When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	g. Vendor's remote monitoring and management. Does the vendor monitor, administer or manage the computers that store or process my data? If yes, is this performed remotely from foreign countries or from Australia? Can the vendor provide patch compliance reports and other details about the security of workstations used to perform this work, and what controls prevent the vendor's employees from using untrustworthy personally owned laptops?	Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.
	h. My monitoring and management. Can I use my existing tools for integrity checking, compliance checking, security monitoring and network management, to obtain visibility of all my systems regardless of whether these systems are located locally or in the cloud? Do I have to learn to use additional tools provided by the vendor? Does the vendor even provide such a mechanism for me to perform monitoring?	AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. The AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system performance and reliability, or help close security gap.
	i. Data ownership. Do I retain legal ownership of my data, or does it belong to the vendor and may be considered an asset for sale by liquidators if the vendor declares bankruptcy?	AWS customers retain ownership and control of their data. AWS only uses each customer's content to provide the AWS services selected by each customer to that customer and does not use customer content for any secondary purposes. AWS treats all customer content the same and has no insight as to what type of content the customer chooses to store in AWS. AWS simply makes available the compute, storage, database and networking services selected by customer – AWS does not require access to customer content to provide its services.

Key Area	Questions	AWS RESPONSE
	j. Gateway technologies. What technologies does the vendor use to create a secure gateway environment? Examples include firewalls, traffic flow filters, content filters, and antivirus software and data diodes where appropriate.	The AWS network provides significant protection against traditional network security issues and customers can implement further protection. Refer to the AWS Overview of Security whitepaper (available at http://aws.amazon.com/security) for additional details. Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection. AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third-party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP^{sm}.
	k. Gateway certification. Is the vendor's gateway environment certified against government security standards and regulations?	AWS obtains certain industry certifications and independent third-party attestations which include the AWS Gateway environment.
	l. Email content filtering. For email Software as a Service, does the vendor provide customizable email content filtering that can enforce my agency's email content policy?	A Customer can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available.

Key Area	Questions	AWS RESPONSE
	m. Policies and processes supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by policies and processes including threat and risk assessments, ongoing vulnerability management, a change management process that incorporates security, penetration testing, logging and regular log analysis, use of security products endorsed by the Australian Government, and compliance with Australian government security standards and regulations?	Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security. AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and formerly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment.
	n. Technologies supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by direct technical controls including timely application of security patches, regularly updated antivirus software, defense in depth mechanisms to protect against unknown vulnerabilities, hardened operating systems and software applications configured with the strongest possible security settings, intrusion detection and prevention systems,	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment.

Key Area	Questions	AWS RESPONSE
	and data loss prevention mechanisms?	
	o. Auditing the vendor's IT security posture. Can I audit the vendor' implementation of security measures, including performing scans and other penetration testing of the environment provided to me? If there is justifiable reason why auditing is not possible, which reputable third party has performed audits and other vulnerability assessments? What sort of internal audits does the vendor perform, and which compliance standards and other recommended practices from organization's such as the Cloud Security Alliance are used for these assessments? Can I thoroughly review a copy of recent resulting reports?	AWS provides third-party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.

Key Area	Questions	AWS RESPONSE
	p. User authentication. What identity and access management systems does the vendor support for users to log in to use Software as a Service?	AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. AWS supports identity federation that makes it easier to manage users by maintaining their identities in a single place. AWS IAM includes support for the Security Assertion Markup Language (SAML) 2.0, an open standard used by many identity providers. This new feature enables federated single sign-on, or SSO, empowering users to log into the AWS Management Console or make programmatic calls to AWS APIs, by using assertions from a SAML-compliant identity provider, such as Shibboleth and Windows Active Directory Federation Services.
	q. Centralized control of data. What user training, policies and technical controls prevent my agency's users from using unapproved or insecure computing devices without a trusted operating environment to store or process sensitive data accessed using Software as a Service?	N/A

Key Area	Questions	AWS RESPONSE
	r. Vendor's physical security posture. Does the vendor use physical security products and devices that are endorsed by the Australian Government? How is the vendor's physical data center designed to prevent the tampering or theft of servers, infrastructure and the data stored thereon? Is the vendor's physical data center accredited by an authoritative third party?	The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report, and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations AWS provides data center physical access and information to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls. Refer to ISO 27001 standard, Annex A, domain 9 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
	s. Software and hardware procurement. What procurement process is used to ensure that cloud infrastructure software and hardware has been supplied by a legitimate source and has not been maliciously modified in transit?	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standard, Annex A, domain 7 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by the Vendor's Customers	a. Customer segregation. What assurance do I have that the virtualization and "multi-tenancy" mechanisms guarantee adequate logical and network segregation between multiple tenants, so that a malicious customer using the same physical computer as me cannot access my data?	Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.
	b. Weakening my security posture. How would using the vendor's cloud infrastructure weaken my agency's existing network security posture? Would the vendor advertise me as one of their customers without my explicit consent, thereby assisting an adversary that is specifically targeting me?	AWS customers are considered confidential and would not advertise customer details without explicit consent. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
	c. Dedicated servers. Do I have some control over which physical computer runs my virtual machines? Can I pay extra to ensure that no other customer can use the same physical computer as me e.g. dedicated servers or virtual private cloud?	VPC allows customers to launch Amazon EC2 instances that are physically isolated at the host hardware level; they will run on single tenant hardware. A VPC can be created with 'dedicated' tenancy, in which case all instances launched into the VPC will utilize this feature. Alternatively, a VPC may be created with 'default' tenancy, but customers may specify 'dedicated' tenancy for particular instances launched into the VPC.
	d. Media sanitization. When I delete portions of my data, what processes are used to sanitize the storage media before it is made available to another customer, and are the processes deemed appropriate by the DSD ISM?	Customers retain ownership and control of their content and provide customers with the ability to delete their data. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in or NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
Protecting Data from Unauthorized Access by Rogue Vendor Employees	a. Data encryption key management. Does the vendor know the password or key used to decrypt my data, or do I encrypt and decrypt the data on my computer so the vendor only ever has encrypted data?	AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.
	b. Vetting of vendor's employees. What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy?	AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities.
	c. Auditing vendor's employees. What robust identity and access management system do the vendor's employees use? What auditing process is used to log and review the actions performed by the vendor's employees?	In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources. Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security.
	d. Visitors to data center. Are visitors to data centers escorted at all times, and is the name and other personal details of every visitor verified and recorded?	All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is routinely logged and audited.
	e. Physical tampering by vendor's employees. Is network cabling professionally installed to Australian standards or internationally acceptable standards, to help avoid the vendor's employees from accidentally connecting cables to the wrong computers, and to help readily highlight any deliberate attempts by the vendor's employees to tamper with the cabling?	Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. This includes appropriate protection for network cables. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standard, Annex A, domain 9 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.

Key Area	Questions	AWS RESPONSE
	f. Vendor's subcontractors. Do the answers to these questions apply equally to all of the vendor's subcontractors?	Provisioning contractor / vendor access is managed the same for both employees and contractors, with responsibility shared across Human Resources (HR), Corporate Operations and Service Owners. Vendors are subject to the same access requirements as employees.
Handling Security Incidents	a. Timely vendor support. Is the vendor readily contactable and responsive to requests for support, and is the maximum acceptable response time captured in the SLA or simply a marketing claim that the vendor will try their best? Is the support provided locally, or from a foreign country, or from several foreign countries using an approach that follows the sun? What mechanism does the vendor use to obtain a real-time understanding of the security posture of my use of the vendor's services so that the vendor can provide support?	AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers. The service helps customers of all sizes and technical abilities to successfully utilize the products and features provided by Amazon Web Services. All AWS Support tiers offer customers of AWS Infrastructure Services an unlimited number of support cases with pay-by-the-month pricing and no long-term contracts. The four tiers provide developers and businesses the flexibility to choose the support tiers that meet their specific needs.
	b. Vendor's incident response plan. Does the vendor have a security incident response plan that specifies how to detect and respond to security incidents, in a way that is similar to incident handling procedures detailed in the DSD ISM? Can I thoroughly review a copy?	The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution. AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.
	c. Training of vendor's employees. What qualifications, certifications and regular information security awareness training do the vendor's employees require, to know how to use the vendor's systems in a secure manner and to identify potential security incidents?	In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.

Key Area	Questions	AWS RESPONSE
	d. Notification of security incidents. Will the vendor notify me via secure communications of security incidents that are more serious than an agreed threshold, especially in cases where the vendor might be liable? Will the vendor automatically notify law enforcement or other authorities, who may confiscate computing equipment used to store or process my data?	Notification of security incidents are handled on a case-by-case basis and as required by applicable law. Any notification is performed via secure communications.
	e. Extent of vendor support. How much assistance will the vendor provide me with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence?	AWS provides infrastructure and customers manage everything else, including the operating system, the network configuration and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings.
	f. My access to logs. How do I obtain access to time synchronized audit logs and other logs to perform a forensic investigation, and how are the logs created and stored to be suitable evidence for a court of law?	Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol). AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. Refer to aws.amazon.com/cloudtrail for additional details. AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com.
	g. Security incident compensation. How will the vendor adequately compensate me if the vendor's actions, faulty software or hardware contributed to a security breach?	AWS' incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS. The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details.

Key Area	Questions	AWS RESPONSE
	h. Data spills. If data that I consider is too sensitive to be stored in the cloud is accidentally placed into the cloud, referred to as a data spill, how can the spilled data be deleted using forensic sanitization techniques? Is the relevant portion of physical storage media zeroed whenever data is deleted? If not, how long does it take for deleted data to be overwritten by customers as part of normal operation, noting that clouds typically have significant spare unused storage capacity? Can the spilled data be forensically deleted from the vendor's backup media? Where else is the spilled data stored, and can it be forensically deleted?	Customers retain ownership and control of their content. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.

Appendix C: Glossary of Terms

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

DSS: The Payment Card Industry Data Security Standard (DSS) is a worldwide information security standard assembled and managed by the Payment Card Industry Security Standards Council.

EBS: Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

FedRAMP^{sm}: The Federal Risk and Authorization Management Program (FedRAMP^{sm}) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP^{sm} is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels.

FISMA: The Federal Information Security Management Act of 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FIPS 140-2: The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information.

GLBA: The Gramm–Leach–Bliley Act (GLB or GLBA), also known as the Financial Services Modernization Act of 1999, sets forth requirements for financial institutions with regard to, among other things, the disclosure of nonpublic customer information and the protection of threats in security and data integrity.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

IAM: AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

ITAR: International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Government agencies and contractors must comply with ITAR and restrict access to protected data.

ISAE 3402: The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

ISO 9001: AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

ISO 27001: ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

NIST: National Institute of Standards and Technology. This agency sets detailed security standards as needed by industry or government programs. Compliance with FISMA requires agencies to adhere to NIST standards.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

PCI: Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

QSA: The Payment Card Industry (PCI) Qualified Security Assessor (QSA) designation is conferred by the PCI Security Standards Council to those individuals that meet specific qualification requirements and are authorized to perform PCI compliance assessments.

SAS 70: Statement on Auditing Standards No. 70: Service Organizations is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization (such as AWS) and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. The SAS 70 report has been replaced by the Service Organization Controls 1 report.

Service: Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

Service Level Agreement (SLA): A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

SOC 1: Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (formerly referred to as the SSAE 16 report), is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

SSAE 16 [deprecated]: The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

SOC 2: Service Organization Controls 2 (SOC 2) reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.

SOC 3: Service Organization Controls 3 (SOC 3) reports are designed to meet the needs of uses who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 Reports can be freely distributed or posted on a website as a seal.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

Version History

October 2016

- Thirteenth and Fourteenth regions added (US East - Ohio and Asia Pacific - Mumbai)

January 2016

- Added GxP Compliance Program
- Twelfth region added (Asia Pacific - Seoul)

December 2015

- Updates to certifications and third-party attestations summaries
- Added ISO 27017 certification
- Added ISO 27018 certification
- Eleventh region added (China - Beijing)

November 2015

- Update to CSA v3.0.1

August 2015

- Updates to in-scope services for PCI 3.1
- Updates to regions in-scope for PCI 3.1

May 2015

- Tenth region added (EU - Frankfurt)
- Updates to in-scope services for SOC 3
- SSAE 16 language deprecated

Apr 2015

- Updates to in-scope services for: FedRAMP^{sm}, HIPAA, SOC 1, ISO 27001, ISO 9001

Feb 2015

- Updates to FIPS 140-2 VPN endpoints and SSL-terminating load balancers
- Updates to PCI DSS verbiage

Dec 2014

- Updates to certifications and third-party attestations summaries

Nov 2013 version

- Edits to IPsec tunnel encryption verbiage

Jun 2013 version

- Updates to certifications and third-party attestations summaries
- Updates to Appendix C: Glossary of Terms
- Minor changes to formatting

Jan 2013 version

- Edits to certifications and third-party attestations summaries

Nov 2012 version

- Edits to content and updated certification scope
- Added reference to the SOC 2 and MPAA

Jul 2012 version

- Edits to content and updated certification scope
- Addition of the CSA Consensus Assessments Initiative Questionnaire (Appendix A)

Jan 2012 version

- Minor edits to content based on updated certification scope
- Minor grammatical edits

Dec 2011 version

- Change to Certifications and Third-party Attestation section to reflect SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, and FIPS 140-2
- Addition of S3 Server Side Encryption
- Added additional cloud computing issue topics

May 2011 version

- Initial release

Notices

This document is provided for informational purposes only. It represents AWS' current product offerings as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS' products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

HOW TO OPEN THIS ARTIFACT

- **Please scroll through to next page to view the artifact downloaded**. To access any **supporting attachments, click the paperclip 📎 icon** in the left of this document and double click the file you would like to open.
  - If you do not see a paperclip icon, right click and select "Show Navigation Pane Buttons".
  - Use latest version of Adobe Acrobat Reader (Windows | Mac | Additional guidance)

TERMS AND CONDITIONS

You hereby agree that you will not distribute, display, or otherwise make this document available to an *individual or entity*, unless expressly permitted herein. This document is AWS Confidential Information (as defined in the AWS Customer Agreement), and you may not remove these terms and conditions from this document, nor take excerpts of this document, without Amazon's express written consent. You may not use this document for purposes competitive with Amazon. You may distribute this document, in its complete form, upon the commercially reasonable request by (1) an end user of your service, to the extent that your service functions on relevant AWS offerings provided that such distribution is accompanied by documentation that details the function of AWS offerings in your service, provided that you have entered into a confidentiality agreement with the end user that includes terms not less restrictive than those provided herein and have named Amazon as an intended beneficiary, or (2) a regulator, so long as you request confidential treatment of this document (each (1) and (2) is deemed a "Permitted Recipient"). You must keep comprehensive records of all Permitted Recipient requests, and make such records available to Amazon and its auditors, upon request.

You further (i) acknowledge and agree that you do not acquire any rights against Amazon's Service Auditors in connection with your receipt or use of this document, and (ii) release Amazon's Service Auditor from any and all claims or causes of action that you have now or in the future against Amazon's Service Auditor arising from this document. The foregoing sentence is meant for the benefit of Amazon's Service Auditors, who are entitled to enforce it. "Service Auditor" means the party that created this document for Amazon or assisted Amazon with creating this document.

System and Organization Controls 3 (SOC 3) Report

Report on the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy

For the Period October 1, 2022 – March 31, 2023

EY
Building a better
working world

Ernst & Young LLP
725 South Figueroa St
Los Angeles, CA
90017-5418

Tel: +1 213 977 3200
Fax: +1 213 977 3729

Report of Independent Accountants

To the Management of Amazon Web Services, Inc.,

Scope

We have examined management’s assertion, contained within the accompanying “Management’s Report of its Assertions on the Effectiveness of Its Controls Over the Amazon Web Services System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy” (Assertion), that Amazon Web Services, Inc.’s (AWS) controls over the Amazon Web Services System (System) were effective throughout the period October 1, 2022 to March 31, 2023 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy (applicable trust services criteria) set forth in the AICPA’s TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management’s Responsibilities

AWS’ management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Amazon Web Services System and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Amazon Web Services System to mitigate risks that threaten the achievement of the principal service commitments and system requirements

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion, which includes (1) obtaining an understanding of AWS’ relevant security, availability, confidentiality, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating AWS' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of AWS and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve AWS' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, AWS' controls over the system were effective throughout the period October 1, 2022 to March 31, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst + Young LLP

May 12, 2023

Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Amazon Web Services System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Privacy

We, as management of Amazon Web Services, Inc., are responsible for:

- Identifying the Amazon Web Services System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and system requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period October 1, 2022 to March 31, 2023 to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, and privacy set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Amazon Web Services Management

Attachment A – Amazon Web Services System Overview

Since 2006, Amazon Web Services (AWS) has provided flexible, scalable and secure IT infrastructure to businesses of all sizes around the world. With AWS, customers can deploy solutions in a cloud computing environment that provides compute power, storage, and other application services over the Internet as their business needs demand. AWS affords businesses the flexibility to employ the operating systems, application programs, and databases of their choice.

The scope of this system description includes the following services:

- AWS Amplify
- Amazon API Gateway
- Amazon AppFlow
- AWS Application Migration Service
- AWS App Mesh
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Audit Manager
- Amazon Augmented AI [Excludes Public Workforce and Vendor Workforce for all features]
- Amazon EC2 Auto Scaling
- AWS Backup
- AWS Batch
- Amazon Braket
- AWS Certificate Manager (ACM)
- AWS Chatbot
- Amazon Chime
- Amazon Chime SDK
- AWS Cloud9
- Amazon Cloud Directory
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudShell
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Cognito
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- Amazon Kendra
- AWS Key Management Service (KMS)
- Amazon Keyspaces (for Apache Cassandra)
- Amazon Kinesis Data Analytics
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lake Formation
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Location Service
- Amazon Macie
- Amazon Managed Grafana
- AWS Managed Services
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Service for Prometheus
- Amazon Managed Workflows for Apache Airflow
- Amazon MemoryDB for Redis
- Amazon MQ
- Amazon Neptune
- AWS Network Firewall
- Amazon OpenSearch Service
- AWS OpsWorks Stacks
- AWS OpsWorks [includes Chef Automate, Puppet Enterprise]
- AWS Organizations
- AWS Outposts
- Amazon Personalize

- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Config
- Amazon Connect
- AWS Control Tower
- AWS Data Exchange
- AWS Database Migration Service (DMS)
- AWS DataSync
- Amazon Detective
- Amazon DevOps Guru
- AWS Direct Connect
- AWS Directory Service [Excludes Simple AD]
- Amazon DocumentDB [with MongoDB compatibility]
- Amazon DynamoDB
- EC2 Image Builder
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Container Registry (ECR)
- Amazon Elastic Container Service – (both Fargate and EC2 launch types)
- AWS Elastic Disaster Recovery
- Amazon Elastic Kubernetes Service (EKS) [both Fargate and EC2 launch types]
- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Amazon ElastiCache
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert
- AWS Elemental MediaLive
- Amazon Elastic MapReduce (EMR)
- Amazon EventBridge
- Amazon FinSpace
- AWS Firewall Manager
- Amazon Forecast
- Amazon Fraud Detector
- FreeRTOS
- Amazon FSx
- Amazon S3 Glacier
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- Amazon GuardDuty
- AWS Health Dashboard
- Amazon Pinpoint
- Amazon Polly
- AWS Private Certificate Authority
- Amazon Quantum Ledger Database (QLDB)
- Amazon QuickSight
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (RDS)
- AWS Resource Access Manager (RAM)
- AWS Resource Groups
- AWS RoboMaker
- Amazon Route 53
- Amazon SageMaker [Excludes Studio Lab, Public Workforce and Vendor Workforce for all features]
- AWS Secrets Manager
- AWS Security Hub
- AWS Server Migration Service (SMS)
- AWS Serverless Application Repository
- AWS Service Catalog
- AWS Shield
- AWS Signer
- Amazon Simple Email Service (SES)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- AWS IAM Identity Center (successor to AWS Single Sign-On)
- AWS Snowball
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- AWS Transfer Family
- Amazon Translate
- Amazon Virtual Private Cloud (VPC)
- VM Import/Export

- Amazon HealthLake
- AWS Identity and Access Management (IAM)
- Amazon Inspector Classic
- AWS loT Core
- AWS IoT Device Management
- AWS WAF
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- Amazon WorkSpaces Web
- AWS X-Ray

More information about the in-scope services, can be found at https://aws.amazon.com/compliance/services-in-scope/

The scope of locations covered in this report includes the supporting data centers located in the following regions:

- **Australia:** Asia Pacific (Sydney) (`ap-southeast-2`), Asia Pacific (Melbourne) (`ap-southeast-4`)
- **Bahrain:** Middle East (Bahrain) (`me-south-1`)
- **Brazil:** South America (São Paulo) (`sa-east-1`)
- **Canada:** Canada (Central) (`ca-central-1`)
- **England:** Europe (London) (`eu-west-2`)
- **France:** Europe (Paris) (`eu-west-3`)
- **Germany:** Europe (Frankfurt) (`eu-central-1`)
- **Hong Kong:** Asia Pacific (`ap-east-1`)
- **India:** Asia Pacific (Mumbai) (`ap-south-1`), Asia Pacific (Hyderabad) (`ap-south-2`)
- **Ireland:** Europe (Ireland) (`eu-west-1`)
- **Italy:** Europe (Milan) (`eu-south-1`)
- **Indonesia:** Asia Pacific (Jakarta) (`ap-southwest-3`)
- **Japan:** Asia Pacific (Tokyo) (`ap-northeast-1`), Asia Pacific (Osaka) (`ap-northeast-3`)
- **Singapore:** Asia Pacific (Singapore) (`ap-southeast-1`)
- **South Africa:** Africa (Cape Town) (`af-south-1`)
- **South Korea:** Asia Pacific (Seoul) (`ap-northeast-2`)
- **Spain:** Europe (Spain) (`eu-south-2`)
- **Sweden:** Europe (Stockholm) (`eu-north-1`)
- **Switzerland:** Europe (Zurich) (`eu-central-2`)
- **United Arab Emirates:** Middle East (UAE) (`me-central-1`)
- **United States:** US East (Northern Virginia) (`us-east-1`), US East (Ohio) (`us-east-2`), US West (Oregon) (`us-west-2`), US West (Northern California) (`us-west-1`), AWS GovCloud (US-East) (`us-gov-east-1`), AWS GovCloud (`US-West`) (`us-gov-west-1`)

and the following AWS Edge locations in:

- Caba, Argentina
- General Pacheco, Argentina
- Koto City, Japan
- Osaka, Japan
- Shinagawa, Japan
- Wiltshire, United Kingdom
- Ashburn, United States
- Atlanta, United States

- Brisbane, Australia
- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Sydney, Australia
- Vienna, Austria
- Brussels, Belgium
- Fortaleza, Brazil
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Sofia, Bulgaria
- Montreal, Canada
- Toronto, Canada
- Vancouver, Canada
- Huechuraba, Chile
- Santiago de Chile, Chile
- Bogotá, Colombia
- Zagreb, Croatia
- Prague, Czech Republic
- Ballerup, Denmark
- Tallinn, Estonia
- Espoo, Finland
- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Dusseldorf, Germany
- Frankfurt, Germany
- Hamburg, Germany
- Munich, Germany
- Kropia, Greece
- Hong Kong, SAR
- Budapest, Hungary
- Bangalore, India
- Bhubaneswar, India
- Changodar, India
- Chennai, India
- Hyderabad, India
- Jaipur, India
- Kolkata, India
- Mumbai, India
- Navi Mumbai, India
- Delhi, India
- Patna, India
- Pune, India
- Nairobi, Kenya
- Anyang-si, Republic of Korea
- Seoul, Republic of Korea
- Kuala Lumpur, Malaysia
- Santiago de Querétaro, Mexico
- Amsterdam, Netherlands
- Schiphol-Rijk, Netherlands
- Auckland, New Zealand
- Christchurch, New Zealand
- Rosedale, New Zealand
- Oslo, Norway
- Barka, Oman
- Pueblo Nuevo, Panama
- Estación Terrena, Peru
- Santiago de Surco, Peru
- Manila, Philippines
- Warsaw, Poland
- Lisbon, Portugal
- Bucharest, Romania
- Singapore, Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Barcelona, Spain
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- Taipei, Taiwan
- New Taipei City, Taiwan
- Bangkok, Thailand
- Bannmai, Thailand
- Khlong Nueng, Thailand
- Pakkret, Thailand
- Tambon Klong Tamru, Thailand
- Thung Song Hong, Thailand
- Dubai, United Arab Emirates
- Fujairah, United Arab Emirates
- Birmingham, United Kingdom
- Brentford, United Kingdom
- Hull, United Kingdom
- Billerica, United States
- Boston, United States
- Chicago, United States
- Columbus, United States
- Dallas, United States
- Denver, United States
- Eden Prairie, United States
- El Segundo, United States
- Elk Grove Village, United States
- Franklin, United States
- Garland, United States
- Greenwood Village, United States
- Houston, United States
- Hillsboro, United States
- Irving, United States
- Itasca, United States
- Jacksonville, United States
- Jersey City, United States
- Kansas City, United States
- Las Vegas, United States
- Los Angeles, United States
- Memphis, United States
- Miami, United States
- Milpitas, United States
- Minneapolis, United States
- Nashville, United States
- New York City, United States
- Newark, United States
- Norfolk, United States
- North Las Vegas, United States
- Northlake, United States
- Portland, United States
- Palo Alto, United States
- Philadelphia, United States
- Phoenix, United States
- Piscataway, United States
- Pittsburgh, United States
- Rancho Cordova, United States
- Reston, United States
- Richardson, United States
- San Diego, United States
- San Jose, United States
- Seattle, United States
- Secaucus, United States

- Bekasi, Indonesia
- Jakarta, Indonesia
- Clonshaugh, Ireland
- Dublin, Ireland
- Haifa, Israel
- Milan, Italy
- Palermo, Italy
- Rome, Italy
- Inzai, Japan
- London, United Kingdom
- Manchester, United Kingdom
- Milton Keynes, United Kingdom
- Slough, United Kingdom
- Surrey, United Kingdom
- Swinton, United Kingdom
- Southfield, United States
- Tampa, United States
- Tempe, United States
- Tukwila, United States
- Vienna, United States
- West Valley City, United States
- HaNoi, Vietnam
- Ho Chi Minh, Vietnam

and the following Wavelength locations in:

- Toronto, Canada
- Berlin, Germany
- Dortmund, Germany
- Munich, Germany
- Osaka, Japan
- Tama, Japan
- Daejeon, South Korea
- Seoul, South Korea
- London, United Kingdom
- Salford, United Kingdom
- Alpharetta, United States
- Annapolis Junction, United States
- Aurora, United States
- Azusa, United States
- Charlotte, United States
- Euless, United States
- Houston, United States
- Knoxville, United States
- Las Vegas, United States
- Minneapolis, United States
- New Berlin, United States
- Pembroke Pines, United States
- Plant City, United States
- Redmond, United States
- Rocklin, United States
- Southfield, United States
- Tempe, United States
- Wall Township, United States
- Westborough, United States

as well as Local Zone locations in:

- Buenos Aires, Argentina
- Perth, Australia
- Santiago, Chile
- Copenhagen, Denmark
- Helsinki, Finland
- Hamburg, Germany
- Kolkata, India**
- Delhi, India**
- Queretaro, Mexico
- Muscat, Oman
- Lima, Peru
- Warsaw, Poland
- Taipei, Taiwan
- Bangkok, Thailand
- Atlanta, United States
- Boston, United States
- Chicago, United States
- El Segundo, United States
- Greenwood Village, United States
- Hillsboro, United States
- Houston, United States
- Irvine, United States
- Kansas City, United States**
- Las Vegas, United States
- Lee's Summit, United States*
- Miami, United States
- Minneapolis, United States
- Philadelphia, United States
- Phoenix, United States
- Piscataway, United States
- Richardson, United States
- Seattle, United States

* This Local Zone is a private Local Zone and may not be available to all customers.
** This location has a public and private Local Zone. Private Local Zones may not be available to all customers.

Infrastructure

AWS operates the cloud infrastructure that customers may use to provision computing resources such as processing and storage. The AWS infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. The AWS infrastructure is designed and managed in accordance with security compliance standards and AWS best practices.

Components of the System

AWS offers a series of Analytics; Application Integration; Business Productivity; Compute; Customer Engagement; Database; Desktop & App Streaming; Developer Tools; Internet of Things; Management Tools; Media Services; Migration; Mobile Services; Network & Content Delivery; Security, Identity, and Compliance; and Storage services. A description of the AWS services included within the scope of this report is listed below:

<u>AWS Amplify</u>
AWS Amplify is a set of tools and services that can be used together or on their own, to help front-end web and mobile developers build scalable full stack applications, powered by AWS. With Amplify, customers can configure app backend and connect applications in minutes, deploy static web apps in a few clicks and easily manage app content outside of AWS console. Amplify supports popular web frameworks including JavaScript, React, Angular, Vue, Next.js, and mobile platforms including Android, iOS, React Native, Ionic, and Flutter.

<u>AWS Application Migration Service</u>
AWS Application Migration Service is the primary service that AWS recommends for lift-and-shift applications to AWS. The service minimizes time-intensive, error-prone manual processes by automatically converting customers’ source servers from physical, virtual, or cloud infrastructure to run natively on AWS. Customers are able to use the same automated process to migrate a wide range of applications to AWS without making changes to applications, their architecture, or the migrated servers.

<u>Amazon API Gateway</u>
Amazon API Gateway is a service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With Amazon API Gateway, customers can create a custom API to code running in AWS Lambda, and then call the Lambda code from customers' API. Amazon API Gateway can execute AWS Lambda code in a customer’s account, start AWS Step Functions state machines, or make calls to AWS Elastic Beanstalk, Amazon EC2, or web services outside of AWS with publicly accessible HTTP endpoints. Using the Amazon API Gateway console, customers can define customers' REST API and its associated resources and methods, manage customers' API lifecycle, generate customers' client SDKs, and view API metrics.

<u>Amazon AppFlow</u>
Amazon AppFlow is an integration service that enables customers to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift. With AppFlow, customers can run data flows at enterprise scale at the frequency they choose - on a schedule, in response to a business event, or on demand. Customers are able to configure data transformation capabilities like filtering and validation to generate rich, ready-to-use data as part of the flow itself, without additional steps.

AWS App Mesh

AWS App Mesh is a service mesh that provides application-level networking which allows customer services to communicate with each other across multiple types of compute infrastructure. App Mesh gives customers end-to-end visibility and high availability for their applications. AWS App Mesh makes it easy to run services by providing consistent visibility and network traffic controls, which helps to deliver secure services. App Mesh removes the need to update application code to change how monitoring data is collected or traffic is routed between services. App Mesh configures each service to export monitoring data and implements consistent communications control logic across applications.

AWS App Runner

AWS App Runner is a service that makes it easy for developers to quickly deploy containerized web applications and APIs, at scale and with no prior infrastructure experience required. The service provides a simplified infrastructure-less abstraction for multi-concurrent web applications and API-based services. With App Runner, infrastructure components like build, load balancers, certificates and application replicas are managed by AWS. Customers simply provide their source-code (or a pre-built container image) and get a service endpoint URL in return against which requests can be made.

Amazon AppStream 2.0

Amazon AppStream 2.0 is an application streaming service that provides customers instant access to their desktop applications from anywhere. Amazon AppStream 2.0 simplifies application management, improves security, and reduces costs by moving a customer's applications from their users' physical devices to the AWS Cloud. The Amazon AppStream 2.0 streaming protocol provides customers a responsive, fluid performance that is almost indistinguishable from a natively installed application. With Amazon AppStream 2.0, customers can realize the agility to support a broad range of compute and storage requirements for their applications.

AWS AppSync

AWS AppSync is a service that allows customers to easily develop and manage GraphQL APIs. Once deployed, AWS AppSync automatically scales the API execution engine up and down to meet API request volumes. AWS AppSync offers GraphQL setup, administration, and maintenance, with high availability serverless infrastructure built in.

Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure for customers to manage. Athena is highly available; and executes queries using compute resources across multiple facilities and multiple devices in each facility. Amazon Athena uses Amazon S3 as its underlying data store, making customers' data highly available and durable.

AWS Audit Manager

AWS Audit Manager helps customers continuously audit AWS usage to simplify how customers manage risk and compliance with regulations and industry standards. AWS Audit Manager makes it easier to evaluate whether policies, procedures, and activities—also known as controls—are operating as intended. The service offers prebuilt frameworks with controls that are mapped to well-known industry standards and regulations, full customization of frameworks and controls, and automated collection and organization of evidence as designed by each control requirement.

Amazon Augmented AI (excludes Public Workforce and Vendor Workforce for all features)

Amazon Augmented AI is a machine learning service which makes it easy to build the workflows required for human review. Amazon A2I brings human review to all developers, removing the undifferentiated heavy lifting associated with building human review systems or managing large numbers of human reviewers whether it runs on AWS or not. The public and vendor workforce options of this service are not in scope for purposes of this report.

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling launches/terminates instances on a customer's behalf according to conditions customers define, such as schedule, changing metrics like average CPU utilization, or health of the instance as determined by EC2 or ELB health checks. It allows customers to have balanced compute across multiple availability zones and scale their fleet based on usage.

AWS Backup

AWS Backup is a backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway. Using AWS Backup, the customers can centrally configure backup policies and monitor backup activity for AWS resources, such as Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon EFS file systems, and AWS Storage Gateway volumes. AWS Backup automates and consolidates backup tasks previously performed service-by-service, removing the need to create custom scripts and manual processes.

AWS Batch

AWS Batch enables developers, scientists, and engineers to run batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. AWS Batch plans, schedules, and executes customers' batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances.

Amazon Braket

Amazon Braket, the quantum computing service of AWS, is designed to help accelerate scientific research and software development for quantum computing. Amazon Braket provides everything customers need to build, test, and run quantum programs on AWS, including access to different types of quantum computers and classical circuit simulators and a unified development environment for building and executing quantum circuits. Amazon Braket also manages the classical infrastructure required for the execution of hybrid quantum-classical algorithms. When customers choose to interact with quantum computers provided by third-parties, Amazon Braket anonymizes the content, so that only content necessary to process the quantum task is sent to the quantum hardware provider. No AWS account information is shared and customer data is not stored outside of AWS.

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) is a service that lets the customer provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and their internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the manual process of purchasing, uploading, and renewing SSL/TLS certificates.

AWS Chatbot

AWS Chatbot is an AWS service that enables DevOps and software development teams to use Slack or Amazon Chime chat rooms to monitor and respond to operational events in their AWS Cloud. AWS Chatbot processes AWS service notifications from Amazon Simple Notification Service (Amazon SNS), and forwards them to Slack or Amazon Chime chat rooms so teams can analyze and act on them. Teams can respond to AWS service events from a chat room where the entire team can collaborate, regardless of location.

Amazon Chime

Amazon Chime is a communications service that lets customers meet, chat, and place business calls inside and outside organizations, all using a single application. With Amazon Chime, customers can conduct and attend online meetings with HD video, audio, screen sharing, meeting chat, dial—in numbers, and in-room video conference support. Customer can use chat and chat rooms for persistent communications across desktop and mobile devices. Customers are also able to administer enterprise users, manage policies, and set up SSO or other advanced features in minutes using Amazon Chime management console.

Amazon Chime SDK

The Amazon Chime SDK is a set of real-time communications components that customers can use to quickly add messaging, audio, video, and screen sharing capabilities to their web or mobile applications. Customers can use the Amazon Chime SDK to build real-time media applications that can send and receive audio and video and allow content sharing. The Amazon Chime SDK works independently of any Amazon Chime administrator accounts and does not affect meetings hosted on Amazon Chime.

AWS Cloud9

AWS Cloud9 is an integrated development environment, or IDE. The AWS Cloud9 IDE offers a rich code-editing experience with support for several programming languages and runtime debuggers, and a built-in terminal. It contains a collection of tools that customers use to code, build, run, test, and debug software, and helps customers release software to the cloud. Customers access the AWS Cloud9 IDE through a web browser. Customers can configure the IDE to their preferences. Customers can switch color themes, bind shortcut keys, enable programming language-specific syntax coloring and code formatting, and more.

Amazon Cloud Directory

Amazon Cloud Directory enables customers to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions. Customers also can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries. For example, customers can create an organizational chart that can be navigated through separate hierarchies for reporting structure, location, and cost center.

AWS Cloud Map

AWS Cloud Map is a cloud resource discovery service which allows customers to define custom names for their application resources. Cloud Map maintains the location of these changing resources to increase application availability.

Customers can register any application resource, such as databases, queues, microservices, and other cloud resources, with custom names. Cloud Map then constantly checks the health of resources to make sure the location is up-to-date. The application can then query the registry for the location of the resources needed based on the application version and deployment environment.

AWS CloudFormation

AWS CloudFormation is a service to simplify provisioning of AWS resources such as Auto Scaling groups, ELBs, Amazon EC2, Amazon VPC, Amazon Route 53, and others. Customers author templates of the infrastructure and applications they want to run on AWS, and the AWS CloudFormation service automatically provisions the required AWS resources and their relationships as defined in these templates.

Amazon CloudFront

Amazon CloudFront is a fast content delivery network (CDN) web service that securely delivers data, videos, applications and APIs to customers globally with low latency and high-transfer speeds. CloudFront offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks. These services co-reside at edge networking locations – globally scaled and connected via the AWS network backbone – providing a more secure, performant, and available experience for the users.

CloudFront delivers customers' content through a worldwide network of Edge locations. When an end user requests content that customers serve with CloudFront, the user is routed to the Edge location that provides the lowest latency, so content is delivered with the best possible performance. If the content is already in that Edge location, CloudFront delivers it immediately.

In addition to Edge locations, CloudFront also uses Amazon Cloud Extension (ACE). ACE is a CloudFront infrastructure (single-rack version) deployed to a non-Amazon controlled facility, namely an internet service provider (ISP) or partner network. Qualifying Network Operators can deliver CloudFront content efficiently and cost effectively from within their network by deploying ACE in their data centers.

AWS CloudHSM

AWS CloudHSM is a service that allows customers to use dedicated hardware security module (HSM) appliances within the AWS cloud. AWS CloudHSM is designed for applications where the use of HSM appliances for encryption and key storage is mandatory.

AWS acquires these production HSM devices securely using the tamper evident authenticable bags from the vendors. These tamper evident authenticable bag serial numbers and production HSM serial numbers are verified against data provided out-of-band by the manufacturer and logged by approved individuals in tracking systems.

AWS CloudHSM allows customers to store and use encryption keys within HSM appliances in AWS data centers. With AWS CloudHSM, customers maintain full ownership, control, and access to keys and sensitive data while Amazon manages the HSM appliances in close proximity to customer applications and data. All HSM media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS Secure Zones.

AWS CloudShell

AWS CloudShell is a browser-based shell used to securely manage, explore, and interact with your AWS resources. CloudShell is pre-authenticated with customer console credentials. Common development and operations tools are pre-installed, so no local installation or configuration is required. With CloudShell, customers can run scripts with the AWS Command Line Interface (AWS CLI), experiment with AWS service APIs using the AWS SDKs, or use a range of other tools to be productive. Customers can use CloudShell right from their browser.

AWS CloudTrail

AWS CloudTrail is a web service that records AWS activity for customers and delivers log files to a specified Amazon S3 bucket. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

AWS CloudTrail provides a history of AWS API calls for customer accounts, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Amazon CloudWatch

Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides the customers with data and actionable insights to monitor their applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing the customers with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers.

Amazon CloudWatch Logs

Amazon CloudWatch Logs is a service used to monitor, store, and access log files from Amazon Elastic Compute Cloud (EC2) instances, AWS CloudTrail, Route 53 and other sources. CloudWatch Logs enables customers to centralize the logs from systems, applications and AWS services used in a single, highly scalable service. Customers can easily view them, search for patterns, filter on specific fields or archive them securely for future analysis. CloudWatch Logs enables customers to view logs, regardless of their source, as a single and consistent flow of events ordered by time, and to query them based on specific criteria.

AWS CodeBuild

AWS CodeBuild is a build service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild scales continuously and processes multiple builds concurrently, so that customers' builds are not left waiting in a queue. Customers can use prepackaged build environments or can create custom build environments that use their own build tools. AWS CodeBuild eliminates the need to set up, patch, update, and manage customers' build servers and software.

AWS CodeCommit

AWS CodeCommit is a source control service that hosts secure Git-based repositories. It allows teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need for customers to operate their own source control system or worry about scaling their infrastructure.

CodeCommit can be used to securely store anything from source code to binaries, and it works seamlessly with the existing Git tools.

AWS CodeDeploy

AWS CodeDeploy is a deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and the customer's on-premises servers. AWS CodeDeploy allows customers to rapidly release new features, helps avoid downtime during application deployment, and handles the complexity of updating the applications.

AWS CodePipeline

AWS CodePipeline is a continuous delivery service that helps customers automate release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of customers release process every time there is a code change, based on the release model defined by the customer. This enables customers to rapidly and reliably deliver features and updates. Customers can easily integrate AWS CodePipeline with third-party services such as GitHub or with their own custom plugin.

Amazon Cognito

Amazon Cognito lets customers add user sign-up, sign-in, and manage permissions for mobile and web applications. Customers can create their own user directory within Amazon Cognito. Customers can also choose to authenticate users through social identity providers such as Facebook, Twitter, or Amazon; with SAML identity solutions; or by using customers' own identity system. In addition, Amazon Cognito enables customers to save data locally on users' devices, allowing customers' applications to work even when the devices are offline. Customers can then synchronize data across users' devices so that their app experience remains consistent regardless of the device they use.

Amazon Comprehend

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. Amazon Comprehend uses machine learning to help the customers uncover insights and relationships in their unstructured data without machine learning experience. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech; and automatically organizes a collection of text files by topic.

Amazon Comprehend Medical

Amazon Comprehend Medical is a HIPAA-eligible natural language processing (NLP) service that facilitates the use of machine learning to extract relevant medical information from unstructured text. Using Amazon Comprehend Medical, customers can quickly and accurately gather information, such as medical condition, medication, dosage, strength, and frequency from a variety of sources like doctors' notes, clinical trial reports, and patient health records. Amazon Comprehend Medical uses advanced machine learning models to accurately and quickly identify medical information, such as medical conditions and medications, and determines their relationship to each other, for instance, medicine dosage and strength.

AWS Config

AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows customers to automate the evaluation of recorded configurations against desired configurations. With AWS Config, customers can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine overall compliance against the configurations specified within the customers' internal guidelines. This enables customers to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Amazon Connect

Amazon Connect is an easy-to-use omnichannel cloud contact center that helps customers provide superior customer service across voice, chat, and tasks at lower cost than traditional contact center systems. Amazon Connect simplifies contact center operations, improves agent efficiency and lowers costs. Customers can setup a contact center in minutes that can scale to support millions of customers from the office or as a virtual contact center.

AWS Control Tower

AWS Control Tower provides the easiest way to set up and govern a new, secure, multi-account AWS environment based on AWS' best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. With AWS Control Tower, builders can provision new AWS accounts that conform to customer policies. If customers are building a new AWS environment, starting out on the journey to AWS, starting a new cloud initiative, or are completely new to AWS, Control Tower will help customers get started quickly with governance and AWS' best practices built-in.

AWS Data Exchange

AWS Data Exchange makes it easy to find, subscribe to, and use third-party data in the cloud. Qualified data providers include category-leading brands. Once subscribed to a data product, customers can use the AWS Data Exchange API to load data directly into Amazon S3 and then analyze it with a wide variety of AWS analytics and machine learning services. For data providers, AWS Data Exchange makes it easy to reach the millions of AWS customers migrating to the cloud by removing the need to build and maintain infrastructure for data storage, delivery, billing, and entitling.

AWS Database Migration Service (DMS)

AWS Database Migration Service (DMS) is a cloud service that enables customers to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. AWS DMS can be used to migrate data into the AWS Cloud, between on-premises instances (through AWS Cloud setup), or between combinations of cloud and on-premises setups. The service supports homogenous migrations within one database platform, as well as heterogeneous migrations between different database platforms. AWS Database Migration Service can also be used for continuous data replication with high-availability.

AWS DataSync

AWS DataSync is an online data transfer service that simplifies, automates and accelerates moving data between on-premises storage and AWS Storage services, as well as between AWS Storage services. DataSync can copy data between Network File System (NFS), Server Message Block (SMB) file servers, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon EFS file systems and Amazon FSx for Windows File Server file systems. DataSync automatically handles many of the tasks related to data transfers that can slow down migrations or burden customers' IT operations, including running customers own instances, handling encryption, managing scripts, network optimization, and data integrity validation.

Amazon Detective

Amazon Detective allows customers to easily analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activity. Amazon Detective collects log data from customer's AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables customers to conduct faster and more efficient security investigations. AWS Security services can be used to identify potential security issues or findings.

Amazon Detective can analyze trillions of events from multiple data sources and automatically creates a unified, interactive view of the resources, users, and the interactions between them over time. With this unified view, customers can visualize all the details and context in one place to identify the underlying reasons for the findings, drill down into relevant historical activities, and quickly determine the root cause.

Amazon DevOps Guru

Amazon DevOps Guru is a service powered by machine learning (ML) that is designed to improve an application's operational performance and availability. DevOps Guru helps detect behaviors that deviate from normal operating patterns so customers can identify operational issues before they impact them.

DevOps Guru uses ML models informed by years of Amazon.com and AWS operational excellence to identify anomalous application behavior (for example, increased latency, error rates, resource constraints, and others) and helps surface critical issues that could cause potential outages or service disruptions. When DevOps Guru identifies a critical issue, it automatically sends an alert and provides a summary of related anomalies, the likely root cause, and context for when and where the issue occurred. When possible, DevOps Guru also helps provide recommendations on how to remediate the issue.

AWS Direct Connect

AWS Direct Connect enables customers to establish a dedicated network connection between their network and one of the AWS Direct Connect locations. Using AWS Direct Connect, customers can establish private connectivity between AWS and their data center, office, or colocation environment.

AWS Directory Service (excludes Simple AD)

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft Active Directory (AD), enables customers' directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD stores directory content in encrypted Amazon Elastic Block Store volumes using encryption keys. Data in transit to and from Active Directory clients is encrypted when it travels through Lightweight Directory Access Protocol (LDAP) over customers' Amazon Virtual Private Cloud (VPC) network. If an Active Directory client resides in an off-cloud network, the traffic travels to customers' VPC by a virtual private network link or an AWS Direct Connect link.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, and highly available document database service that supports MongoDB workloads. Amazon DocumentDB is designed from the ground-up to give customers the performance, scalability, and availability customers need when operating mission-critical MongoDB workloads at scale. Amazon DocumentDB implements the Apache 2.0 open source MongoDB 3.6 API by emulating the responses that a MongoDB client expects from a MongoDB server, allowing customers to use their existing MongoDB drivers and tools with Amazon DocumentDB.

Amazon DocumentDB uses a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64 TB per database cluster.

Amazon DynamoDB

Amazon DynamoDB is a managed NoSQL database service. Amazon DynamoDB enables customers to offload to AWS the administrative burdens of operating and scaling distributed databases such as hardware provisioning, setup and configuration, replication, software patching, and cluster scaling.

Customers can create a database table that can store and retrieve data and serve any requested traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified and the amount of data stored, while maintaining consistent, fast performance. All data items are stored on Solid State Drives (SSDs) and are automatically replicated across multiple availability zones in a region.

EC2 Image Builder

EC2 Image Builder makes it easier to automate the creation, management, and deployment of customized, secure, and up-to-date “golden” server images that are pre-installed and pre-configured with software and settings to meet specific IT standards.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an application container launch program for customers to launch and scale their applications on top of AWS. Customers can use AWS Elastic Beanstalk to create new environments using Elastic Beanstalk curated programs and their applications, deploy application versions, update application configurations, rebuild environments, update AWS configurations, monitor environment health and availability, and build on top of the scalable infrastructure provided by underlying services such as Auto Scaling, Elastic Load Balancing, Amazon EC2, Amazon VPC, Amazon Route 53, and others.

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect customers from component failure. Amazon EBS allows customers to create storage volumes from 1 GB to 16 TB that can be mounted as devices by Amazon EC2 instances. Storage volumes behave like raw, unformatted block devices, with user supplied device names and a block device interface. Customers can create a file system on top of Amazon EBS volumes, or use them in any other way one would use a block device (e.g., a hard drive).

Amazon EBS volumes are presented as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs before reuse. If customers have procedures requiring that all data be wiped via a specific method, customers can conduct a wipe procedure prior to deleting the volume for compliance with customer requirements. Amazon EBS includes Data Lifecycle Manager, which provides a simple, automated way to back up data stored on Amazon EBS volumes.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) is Amazon’s Infrastructure as a Service (IaaS) offering, which provides scalable computing capacity using server instances in AWS’ data centers. Amazon EC2 is designed to make web-scale computing easier by enabling customers to obtain and configure capacity with minimal friction. Customers create and launch instances, which are virtual machines that are available in a wide variety of hardware and software configurations.

Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host layer, the virtual instance OS or guest OS, a firewall, and signed API calls. Each of these items builds on the capabilities of the others. This helps prevent data contained within Amazon EC2 from being intercepted by unauthorized systems or users and to provide Amazon EC2 instances themselves security without sacrificing flexibility of configuration. The Amazon EC2 service utilizes a hypervisor to provide memory and CPU isolation between virtual machines and controls access to network, storage, and other devices, and maintains strong isolation between guest virtual machines. Independent auditors regularly assess the security of Amazon EC2 and penetration teams regularly search for new and existing vulnerabilities and attack vectors.

AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software**.**

Amazon EC2 provides a complete firewall solution, referred to as a Security Group; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic**.**

Amazon provides a Time Sync function for time synchronization in EC2 Linux instances with the Coordinated Universal Time (UTC). It is delivered over the Network Time Protocol (NTP) and uses a fleet of redundant satellite-connected and atomic clocks in each region to provide a highly accurate reference clock via the local 169.254.169.123 IP address. Irregularities in the Earth’s rate of rotation that cause UTC to drift with respect to the International Celestial Reference Frame (ICRF), by an extra second, are called leap second. Time Sync addresses this clock drift by smoothing out leap seconds over a period of time (commonly called leap smearing) which makes it easy for customer applications to deal with leap seconds**.**

Amazon Elastic Container Registry (ECR)
Amazon Elastic Container Registry is a Docker container image registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon Elastic Container Registry is integrated with Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

Amazon Elastic Container Service (both Fargate and EC2 launch types)
Amazon Elastic Container Service is a highly scalable, high performance container management service that supports Docker containers and allows customers to easily run applications on a managed cluster of Amazon EC2 instances. Amazon Elastic Container Service eliminates the need for customers to install, operate, and scale customers' own cluster management infrastructure. With simple API calls, customers can launch and stop Docker-enabled applications, query the complete state of customers' clusters, and access many familiar features like security groups, Elastic Load Balancing, EBS volumes, and IAM roles. Customers can use Amazon Elastic Container Service to schedule the placement of containers across customers' clusters based on customers' resource needs and availability requirements.

AWS Elastic Disaster Recovery
AWS Elastic Disaster Recovery minimizes downtime and data loss with the recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. Customers can set up AWS Elastic Disaster Recovery on their source servers to initiate secure data

replication. Customer content is replicated to a staging area subnet in their AWS account, in the AWS Region they select. The staging area design reduces costs by using affordable storage and minimal compute resources to maintain ongoing replication. Customers can perform non-disruptive tests to confirm that implementation is complete. During normal operation, customers can maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills. If customers need to recover applications, they can launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time.

Amazon Elastic Kubernetes Service (EKS) (both Fargate and EC2 launch types)

Amazon Elastic Kubernetes Service (EKS) makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS. Amazon EKS runs the Kubernetes management infrastructure for the customer across multiple AWS availability zones to eliminate a single point of failure. Amazon EKS is certified Kubernetes conformant so the customers can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be easily migrated to Amazon EKS.

Amazon Elastic File System (EFS)

Amazon Elastic File System (EFS) provides file storage for Amazon EC2 instances. EFS presents a network attached file system interface via the NFS v4 protocol. EFS file systems grow and shrink elastically as data is added and deleted by users. Amazon EFS spreads data across multiple Availability Zones; in the event that an Availability Zone is not reachable, the structure allows customers to still access their full set of data.

The customer is responsible for choosing which of their Virtual Private Clouds (VPCs) they want a file system to be accessed from by creating resources called mount targets. One mount target exists for each availability zone, which exposes an IP address and DNS name for mounting the customer's file system onto their EC2 instances. Customers then log into their EC2 instance and issue a 'mount' command, pointing at their mount target' IP address or DNS name. A mount target is assigned one or more VPC security groups to which it belongs. The VPC security groups define rules for what VPC traffic can reach the mount targets and in turn can reach the file system.

Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) provides customers with a load balancer that automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It allows customers to achieve greater levels of fault tolerance for their applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.

Amazon ElastiCache

Amazon ElastiCache automates management tasks for in-memory cache environments, such as patch management, failure detection, and recovery. It works in conjunction with other AWS services to provide a managed in-memory cache. For example, an application running in Amazon EC2 can securely access an Amazon ElastiCache Cluster in the same region with very slight latency.

Using the Amazon ElastiCache service, customers create a Cache Cluster, which is a collection of one or more Cache Nodes, each running an instance of the Memcached, Redis Engine, or DAX Engine. A Cache Node is a self-contained environment which provides a fixed-size chunk of secure, network-attached RAM. Each Cache Node runs an instance of the Memcached, Redis Engine, or DAX Engine, and has its own DNS name and port. Multiple types of Cache Nodes are supported, each with varying amounts of associated memory.

AWS Elemental MediaConnect

AWS Elemental MediaConnect is a high-quality transport service for live video. MediaConnect enables customers to build mission-critical live video workflows in a fraction of the time and cost of satellite or fiber services. Customers can use MediaConnect to ingest live video from a remote event site (like a stadium), share video with a partner (like a cable TV distributor), or replicate a video stream for processing (like an over-the-top service). MediaConnect combines reliable video transport, highly secure stream sharing, and real-time network traffic and video monitoring that allow customers to focus on their content, not their transport infrastructure.

AWS Elemental MediaConvert

AWS Elemental MediaConvert is a file-based video transcoding service with broadcast-grade features. It allows customers to create video-on-demand (VOD) content for broadcast and multiscreen delivery at scale. The service combines advanced video and audio capabilities with a simple web services interface. With AWS Elemental MediaConvert, customers can focus on delivering media experiences without having to worry about the complexity of building and operating video processing infrastructure.

AWS Elemental MediaLive

AWS Elemental MediaLive is a live video processing service. Customers can create high-quality video streams for delivery to broadcast televisions and internet-connected multiscreen devices, like connected TVs, tablets, smart phones, and set-top boxes. The service works by encoding live video streams in real-time, taking a larger-sized live video source and compressing it into smaller versions for distribution to viewers. AWS Elemental MediaLive enables customers to focus on creating live video experiences for viewers without the complexity of building and operating video processing infrastructure.

Amazon Elastic MapReduce (EMR)

Amazon Elastic MapReduce (EMR) is a web service that provides managed Hadoop clusters on Amazon EC2 instances running a Linux operating system. Amazon EMR uses Hadoop processing combined with several AWS products to do such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing. Amazon EMR actively manages clusters for customers, replacing failed nodes and adjusting capacity as requested. Amazon EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

Amazon EventBridge

Amazon EventBridge delivers a near real-time stream of events that describe changes in AWS resources. Customers can configure routing rules to determine where to send collected data to build application architectures that react in real time to the data sources. Amazon EventBridge becomes aware of operational changes as they occur and responds to these changes by taking corrective action as necessary by sending message to respond to the environment, activating functions, making changes and capturing state information

Amazon FinSpace

Amazon FinSpace is a data management and analytics service that makes it easy to store, catalog, and prepare financial industry data at scale. Amazon FinSpace reduces the time it takes for financial services industry (FSI) customers to find and access all types of financial data for analysis.

AWS Firewall Manager

AWS Firewall Manager is a security management service that makes it easier to centrally configure and manage AWS WAF rules across customer accounts and applications. Using Firewall Manager, customers can roll out AWS WAF rules for their Application Load Balancers and Amazon CloudFront distributions across accounts in AWS Organizations. As new applications are created, Firewall Manager also allows customers to bring new applications and resources into compliance with a common set of security rules from day one.

Amazon Forecast

Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. With Amazon Forecast, customers can import time series data and associated data into Amazon Forecast from their Amazon S3 database. From there, Amazon Forecast automatically loads the data, inspects it, and identifies the key attributes needed for forecasting. Amazon Forecast then trains and optimizes a customer's custom model and hosts them in a highly available environment where it can be used to generate business forecasts.

Amazon Forecast is protected by encryption. Any content processed by Amazon Forecast is encrypted with customer keys through Amazon Key Management Service and encrypted at rest in the AWS Region where a customer is using the service. Administrators can also control access to Amazon Forecast through an AWS Identity and Access Management (IAM) permissions policy – ensuring that sensitive information is kept secure and confidential.

Amazon Fraud Detector

Amazon Fraud Detector helps detect suspicious online activities such as the creation of fake accounts and online payment fraud. Amazon Fraud Detector uses machine learning (ML) and 20 years of fraud detection expertise from AWS and Amazon.com to automatically identify fraudulent activity to catch more fraud, faster. With Amazon Fraud Detector, customers can create a fraud detection ML model with just a few clicks and use it to evaluate online activities in milliseconds.

FreeRTOS

FreeRTOS is an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. FreeRTOS extends the FreeRTOS kernel, a popular open source operating system for microcontrollers, with software libraries that make it easy to securely connect the small, low-power devices to AWS cloud services like AWS IoT Core or to more powerful edge devices running AWS IoT Greengrass.

Amazon FSx

Amazon FSx provides third-party file systems. Amazon FSx provides the customers with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA). The customers don't have to worry about managing file servers and storage, as Amazon FSx automates the time-consuming administration tasks such as hardware provisioning, software configuration, patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.

Amazon S3 Glacier

Amazon S3 Glacier is an archival storage solution for data that is infrequently accessed for which retrieval times of several hours are suitable. Data in Amazon S3 Glacier is stored as an archive. Archives in Amazon S3 Glacier can be created or deleted, but archives cannot be modified. Amazon S3 Glacier archives are organized in vaults. All vaults created have a default permission policy that only permits access by the account creator or users that have been explicitly granted permission. Amazon S3 Glacier enables customers to set access policies on their vaults for users within their AWS Account. User policies can express access criteria for Amazon S3 Glacier on a per vault basis. Customers can enforce Write Once Read Many (WORM) semantics for users through user policies that forbid archive deletion.

AWS Global Accelerator

AWS Global Accelerator is a networking service that improves the availability and performance of the applications that customers offer to their global users. AWS Global Accelerator also makes it easier to manage customers' global applications by providing static IP addresses that act as a fixed entry point to customer applications hosted on AWS which eliminates the complexity of managing specific IP addresses for different AWS Regions and Availability Zones.

AWS Glue

AWS Glue is an extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. The customers can create and run an ETL job with a few clicks in the AWS Management Console.

AWS Glue DataBrew

AWS Glue DataBrew is a visual data preparation tool that makes it easy for data analysts and data scientists to clean and normalize data to prepare it for analytics and machine learning. Customers can choose from pre-built transformations to automate data preparation tasks, all without the need to write any code.

Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect the customers' AWS accounts and workloads. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, the customers now have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud.

Amazon HealthLake

Amazon HealthLake is a service offering healthcare and life sciences companies a complete view of individual or patient population health data for query and analytics at scale. Using the HealthLake APIs, health organizations can easily copy health data, such as imaging medical reports or patient notes, from on-premises systems to a secure data lake in the cloud. HealthLake uses machine learning (ML) models to automatically understand and extract meaningful medical information from the raw data, such as medications, procedures, and diagnoses. HealthLake organizes and indexes information and stores it in the Fast Healthcare Interoperability Resources (FHIR) industry standard format to provide a complete view of each patient's medical history.

AWS Identity and Access Management (IAM)

AWS Identity and Access Management is a web service that helps customers securely control access to AWS resources for their users. Customers use IAM to control who can use their AWS resources (authentication) and what resources they can use and in what ways (authorization). Customers can grant other people permission to administer and use resources in their AWS account without having to share their password or access key. Customers can grant different permissions to different people for different resources. Customers can use IAM features to. securely give applications that run on EC2 instances the credentials that they need in order to access other AWS resources, like S3 buckets and RDS or DynamoDB databases.

VM Import/Export

VM Import/Export is a service that enables customers to import virtual machine images from their existing environment to Amazon EC2 instances and export them back to their on premises environment. This offering allows customers to leverage their existing investments in the virtual machines that customers have built to meet their IT security, configuration management, and compliance requirements by bringing those virtual machines into Amazon EC2 as ready-to-use instances. Customers can also export imported instances back to their off-cloud virtualization infrastructure, allowing them to deploy workloads across their IT infrastructure.

Amazon Inspector Classic

Amazon Inspector Classic is an automated security assessment service for customers seeking to improve the security and compliance of applications deployed on AWS. Amazon Inspector Classic automatically assesses applications for vulnerabilities or deviations from leading practices. After performing an assessment, Amazon Inspector Classic produces a detailed list of security findings prioritized by level of severity.

AWS IoT Core

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core provides secure communication and data processing across different kinds of connected devices and locations so that customers can easily build IoT applications such as industrial solutions and connected home solutions.

AWS IoT Device Management

AWS IoT Device Management provides customers with the ability to securely onboard, organize, and remotely manage IoT devices at scale. With AWS IoT Device Management, customers can register their connected devices individually or in bulk and manage permissions so that devices remain secure.

Customers can also organize their devices, monitor and troubleshoot device functionality, query the state of any IoT device in the fleet, and send firmware updates over-the-air (OTA). AWS IoT Device Management is agnostic to device type and OS, so customers can manage devices from constrained microcontrollers to connected cars all with the same service. AWS IoT Device Management allows customers to scale their fleets and reduce the cost and effort of managing large and diverse IoT device deployments.

AWS IoT Events

AWS IoT Events is a service that detects events across thousands of IoT sensors sending different telemetry data, such as temperature from a freezer, humidity from respiratory equipment, and belt speed on a motor. Customers can select the relevant data sources to ingest, define the logic for each event using simple 'if-then-else' statements, and select the alert or custom action to trigger when an event occurs. IoT Events continuously monitors data from multiple IoT sensors and applications, and it integrates with other services, such as AWS IoT Core, to enable early detection and unique insights into events. IoT Events automatically triggers alerts and actions in response to events based on the logic defined to resolve issues quickly, reduce maintenance costs, and increase operational efficiency.

AWS IoT Greengrass

AWS IoT Greengrass seamlessly extends AWS to edge devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage. With AWS IoT Greengrass, connected devices can run AWS Lambda functions, execute predictions based on machine learning models, keep device data in sync, and communicate with other devices securely – even when not connected to the Internet.

AWS IoT SiteWise

AWS IoT SiteWise is a service that enables industrial enterprises to collect, store, organize, and visualize thousands of sensor data streams across multiple industrial facilities. AWS IoT SiteWise includes software that runs on a gateway device that sits onsite in a facility, continuously collects the data from a historian or a specialized industrial server, and sends it to the AWS Cloud. With the service, customers can skip months of developing undifferentiated data collection and cataloging solutions, and focus on using their data to detect and fix equipment issues, spot inefficiencies, and improve production output.

Amazon Kendra

Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for customer websites and applications so employees and customers can easily find content, even when it's scattered across multiple locations and content repositories.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) allows users to create and manage cryptographic keys. One class of keys, KMS keys, are designed to never be exposed in plaintext outside the service. KMS keys can be used to encrypt data directly submitted to the service. KMS keys can also be used to protect other types of keys, Data Encryption Keys (DEKs), which are created by the service and returned to the user's application for local use. AWS KMS only creates and returns DEKs to users; the service does not store or manage DEKs.

AWS KMS is integrated with several AWS services so that users can request that resources in those services are encrypted with unique DEKs provisioned by KMS that are protected by a KMS key the user chooses at the time the resource is created**.** See in-scope services integrated with KMS at https://aws.amazon.com/kms/. Integrated services use the plaintext DEK from AWS KMS in volatile memory of service-controlled endpoints; they do not store the plaintext DEK to persistent disk. An encrypted copy of the DEK is stored to persistent disk by the service and passed back to AWS KMS for decryption each time the DEK is needed to decrypt content the customer requests. DEKs provisioned by AWS KMS are encrypted with a 256-bit key unique to the customer's account under a defined mode of AES – Advanced Encryption Standard.

When a customer requests AWS KMS to create a KMS key, the service creates a key ID for the KMS key and (optionally) key material, referred to as a backing key, which is tied to the key ID of the KMS key. The 256-bit backing key can only be used for encrypt or decrypt operations by the service. Customers can choose to have a KMS key ID created and then securely import their own key material to associate with the key ID. If the customer chooses to enable key rotation for a KMS key with a backing key that the service generated, AWS KMS will create a new version of the backing key for each rotation event, but the key ID remains the same. All future encrypt operations under the key ID will use the newest backing key, while all previous versions of backing keys are retained to decrypt ciphertexts created under the previous version of the key. Backing keys and customer-imported keys are encrypted under AWS-controlled keys when created/imported and they are only ever stored on disk in encrypted form.

All requests to AWS KMS APIs are logged and available in the AWS CloudTrail of the requester and the owner of the key. The logged requests provide information about who made the request, under which KMS key, and describes information about the AWS resource that was protected through the use of the KMS key. These log events are visible to the customer after turning on AWS CloudTrail in their account .

AWS KMS creates and manages multiple distributed replicas of KMS keys and key metadata automatically to enable high availability and data durability. KMS keys themselves are regional objects; plaintext versions of the KMS keys can only be used in the AWS region in which they were created. KMS keys are only stored on persistent disk in encrypted form and in two separate storage systems to ensure durability. When a plaintext KMS key is needed to fulfill an authorized customer request, it is retrieved from storage, decrypted on one of many AWS KMS hardened security appliances in the region, then used only in memory to execute the cryptographic operation (e.g., encrypt or decrypt). The plaintext key is then marked for deletion so that it cannot be re-used. Future requests to use the KMS key each require the decryption of the KMS key in memory for another one-time use.

AWS KMS endpoints are only accessible via TLS using the following cipher suites that support forward secrecy:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-3DES-CBC3-SHA
- DHE-RSA-AES256-SHA256 (ParamSize: 2048)
- DHE-RSA-AES128-SHA256 (ParamSize: 2048)
- DHE-RSA-AES256-SHA (ParamSize: 2048)
- DHE-RSA-AES128-SHA (ParamSize: 2048)

By design, no one can gain access to the plaintext KMS key material. Plaintext KMS keys are only ever present on hardened security appliances for the amount of time needed to perform cryptographic operations under them. AWS employees have no tools to retrieve plaintext keys from these hardened security appliances. In addition, multi-party access controls are enforced for operations on these hardened security appliances that involve changing the software configuration or introducing new hardened security appliances into the service. These multi-party access controls minimize the possibility of an unauthorized change to the hardened security appliances, exposing plaintext key material outside the service, or allowing unauthorized use of customer keys. Additionally, key material used for disaster recovery processes by KMS are physically secured such that no AWS employee can gain access**.** Access attempts to recovery key materials are reviewed by authorized operators on a periodic basis**.** Roles and responsibilities for those cryptographic custodians with access to systems that store or use key material are formally documented and acknowledged**.**

Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) is a scalable, highly available Apache Cassandra–compatible database service. With Amazon Keyspaces, customers can run Cassandra workloads on AWS using the same Cassandra application code and developer tools that customers use today. Amazon Keyspaces is serverless and gives customers the performance, elasticity, and enterprise features customers need to operate business-critical Cassandra workloads at scale.

Amazon Kinesis Data Analytics

Amazon Kinesis Data Analytics is an easy way for customers to analyze streaming data, gain actionable insights, and respond to business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services. SQL users can easily query streaming data or build entire streaming applications using templates and an interactive SQL editor. Java developers can quickly build sophisticated streaming applications using open source Java libraries and AWS integrations to transform and analyze data in real-time.

Amazon Kinesis Data Firehose

Amazon Kinesis Data Firehose is a reliable way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, and Amazon OpenSearch Service enabling near real-time analytics with existing business intelligence tools and dashboards customers are already using today. The service automatically scales to match the throughput of the customers' data and requires no ongoing administration. It can also batch, compress, transform, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams is a massively scalable and durable real-time data streaming service. Kinesis Data Streams can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs and location-tracking events. The collected data is available in milliseconds to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing and more.

Amazon Kinesis Video Streams

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales the infrastructure needed to ingest streaming video data from millions of devices. It also durably stores, encrypts, and indexes video data in the streams, and allows the customers to access their data through easy-to-use APIs. Kinesis Video Streams enables the customers to playback video for live and on-demand viewing, and quickly build applications that take advantage of computer vision and video analytics.

Amazon Location Service

Amazon Location Service makes it easy for developers to add location functionality to applications without compromising data security and user privacy. With Amazon Location Service, customers can build applications that provide maps and points of interest, convert street addresses into geographic coordinates, calculate routes, track resources, and trigger actions based on location. Amazon Location Service uses high-quality geospatial data to provide maps, places, routes, tracking, and geofencing.

AWS Lake Formation

AWS Lake Formation is an integrated data lake service that makes it easy for customers to ingest, clean, catalog, transform, and secure their data and make it available for analysis and ML. AWS Lake Formation gives customers a central console where they can discover data sources, set up transformation jobs to move data to an Amazon Simple Storage Service (S3) data lake, remove duplicates and match records, catalog data for access by analytic tools, configure data access and security policies, and audit and control access from AWS analytic and ML services. Lake Formation automatically manages access to the registered data in Amazon S3 through services including AWS Glue, Amazon Athena, Amazon Redshift, Amazon QuickSight, and Amazon EMR to ensure compliance with customer defined policies. With AWS Lake Formation, customers can configure and manage their data lake without manually integrating multiple underlying AWS services.

AWS Lambda

AWS Lambda lets customers run code without provisioning or managing servers on their own. AWS Lambda uses a compute fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones in a region, which provides the high availability, security, performance, and scalability of the AWS infrastructure.

Amazon Lex

Amazon Lex is a service for building conversational interfaces into any application using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable customers to build applications with highly engaging user experiences and lifelike conversational interactions. Amazon Lex scales automatically, so customers do not need to worry about managing infrastructure.

AWS License Manager

AWS License Manager makes it easier to manage licenses in AWS and on-premises servers from software vendors. AWS License Manager allows customer's administrators to create customized licensing rules that emulate the terms of their licensing agreements, and then enforces these rules when an instance of EC2 gets launched. Customer administrators can use these rules to limit licensing violations, such as using more licenses than an agreement stipulates or reassigning licenses to different servers on a short-term basis. The rules in AWS License Manager also enable customers to limit a licensing breach by stopping the instance from launching or by notifying the customer administrators about the infringement. Customer administrators gain control and visibility of all their licenses with the AWS License Manager dashboard and reduce the risk of non-compliance, misreporting, and additional costs due to licensing overages.

AWS License Manager integrates with AWS services to simplify the management of licenses across multiple AWS accounts, IT catalogs, and on-premises, through a single AWS account.

Amazon Macie

Amazon Macie is a data security and data privacy service that uses machine learning and pattern matching to help customers discover, monitor, and protect their sensitive data in AWS.

Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial data, to provide customers with a better understanding of the data that organization stores in Amazon Simple Storage Service (Amazon S3). Macie also provides customers with an inventory of the S3 buckets, and it automatically evaluates and monitors those buckets for security and access control. Within minutes, Macie can identify and report overly permissive or unencrypted buckets for the organization.

If Macie detects sensitive data or potential issues with the security or privacy of customer content, it creates detailed findings for customers to review and remediate as necessary. Customers can review and analyze these findings directly in Macie, or monitor and process them by using other services, applications, and systems.

Amazon Managed Grafana

Amazon Managed Grafana is a service for open source Grafana, providing interactive data visualization for monitoring and operational data. Using Amazon Managed Grafana, customers can visualize, analyze, and alarm on their metrics, logs, and traces collected from multiple data sources in their observability system, including AWS, third-party ISVs, and other resources across their IT portfolio. Amazon Managed Grafana offloads the operational management of Grafana by automatically scaling compute and database infrastructure as usage demands increase, with automated version updates and security patching. Amazon Managed Grafana natively integrates with AWS services so customers can securely add, query, visualize, and analyze their AWS data across multiple accounts and regions with a few clicks in the AWS Console. Amazon Managed Grafana integrates with AWS IAM Identity Center (successor to AWS SSO) and supports Security Assertion Markup Language (SAML) 2.0, so customers can set up user access to specific dashboards and data sources for only certain users in their corporate directory.

AWS Managed Services

AWS Managed Services provides ongoing management of a customer's AWS infrastructure. AWS Managed Services automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support a customer's infrastructure.

Amazon Managed Service for Prometheus

Amazon Managed Service for Prometheus is a Prometheus-compatible monitoring and alerting service that facilitates monitoring of containerized applications and infrastructure at scale. The Cloud Native Computing Foundation's Prometheus project is an open source monitoring and alerting solution optimized for container environments. With Amazon Managed Service for Prometheus, customers can use the open source Prometheus query language (PromQL) to monitor and alert on the performance of containerized workloads, without having to scale and operate the underlying infrastructure. Amazon Managed Service for Prometheus automatically scales the ingestion, storage, alerting, and querying of operational metrics as workloads grow or shrink, and it is integrated with AWS security services to enable fast and secure access to data.

Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow is a service for Apache Airflow that lets customers use their current, familiar Apache Airflow platform to orchestrate their workflows. Customers gain improved scalability, availability, and security without the operational burden of managing underlying infrastructure. Amazon Managed Workflows for Apache Airflow orchestrates customer's workflows using Directed Acyclic Graphs (DAGs) written in Python. Customers provide Amazon Managed Workflows for Apache Airflow an Amazon Simple Storage Service (S3) bucket where customer's DAGs, plugins, and Python requirements reside. Then customers can run and monitor their DAGs from the AWS Management Console, a command line interface (CLI), a software development kit (SDK), or the Apache Airflow user interface (UI).

Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka is a service that makes it easy for customers to build and run applications that use Apache Kafka to process streaming data. Apache Kafka is an open-source platform for building real-time streaming data pipelines and applications. With Amazon MSK, customers can use Apache Kafka APIs to populate data lakes, stream changes to and from databases, and power machine learning and analytics applications.

Amazon MemoryDB for Redis

Amazon MemoryDB for Redis is a Redis-compatible, durable, in-memory database service. It is purpose-built for modern applications with microservices architectures.

Amazon MemoryDB for Redis is compatible with Redis, an open source data store, enabling customers to quickly build applications using the same flexible Redis data structures, APIs, and commands that they already use today. With Amazon MemoryDB for Redis, all of the customer's data is stored in memory, which enables the customer to achieve microsecond read and single-digit millisecond write latency and high throughput. Amazon MemoryDB for Redis also stores data durably across multiple Availability Zones (AZs) using a distributed transactional log to enable fast failover, database recovery, and node restarts. Delivering both in-memory performance and Multi-AZ durability, Amazon MemoryDB for Redis can be used as a high-performance primary database for microservices applications eliminating the need to separately manage both a cache and durable database.

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ that sets up and operates message brokers in the cloud. Message brokers allow different software systems – often using different programming languages, and on different platforms – to communicate and exchange information. Messaging is the communications backbone that connects and integrates the components of distributed applications, such as order processing, inventory management, and order fulfillment for e-commerce. Amazon MQ manages the administration and maintenance of ActiveMQ, a popular open-source message broker.

Amazon Neptune

Amazon Neptune is a fast and reliable graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying the graph with milliseconds latency. Amazon Neptune supports popular graph models, Property Graph, and W3C's RDF, and their respective query languages Apache, TinkerPop Gremlin, and SPARQL, allowing customers to easily build queries that efficiently navigate highly connected datasets. Neptune powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

AWS Network Firewall

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for customer virtual private cloud (VPC). With Network Firewall, customers can filter traffic at the perimeter of customer VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

Amazon OpenSearch Service

Amazon OpenSearch Service is a service that makes it easy for the customer to deploy, secure, and operate OpenSearch cost effectively at scale. Amazon OpenSearch Service lets the customers pay only for what they use – there are no upfront costs or usage requirements. With Amazon OpenSearch Service, the customers get the ELK stack they need, without the operational overhead.

AWS OpsWorks Stacks

AWS OpsWorks Stacks is an application and server management service. OpsWorks Stacks lets customers manage applications and servers on AWS and on-premises. With OpsWorks Stacks, customers can model their application as a stack containing different layers, such as load balancing, database, and application server. They can deploy and configure Amazon EC2 instances in each layer or connect other resources such as Amazon RDS databases. OpsWorks Stacks also lets customers set automatic scaling for their servers based on preset schedules or in response to changing traffic levels, and it uses lifecycle hooks to orchestrate changes as their environment scales.

AWS OpsWorks (includes Chef Automate, Puppet Enterprise)

AWS OpsWorks for Chef Automate is a configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks also maintains customers' Chef server by automatically patching, updating, and backing up customer servers. OpsWorks eliminates the need for customers to operate their own configuration management systems or worry about maintaining its infrastructure. OpsWorks gives customers access to all of the Chef Automate features, such as configuration and compliance management, which customers manage through the Chef console or command line tools like Knife. It also works seamlessly with customers' existing Chef cookbooks.

AWS OpsWorks for Puppet Enterprise is a configuration management service that hosts Puppet Enterprise, a set of automation tools from Puppet for infrastructure and application management. OpsWorks also maintains customers' Puppet master server by automatically patching, updating, and backing up customers' servers. OpsWorks eliminates the need for customers to operate their own configuration management systems or worry about maintaining its infrastructure. OpsWorks gives customers' access to all of the Puppet Enterprise features, which customers manage through the Puppet console. It also works seamlessly with customers' existing Puppet code.

AWS Organizations

AWS Organizations helps customers centrally govern their environment as customers grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps customers to centrally manage billing; control access, compliance, and security; and share resources across customer AWS accounts.

Using AWS Organizations, customers can automate account creation, create groups of accounts to reflect their business needs, and apply policies for these groups for governance. Customers can also simplify billing by setting up a single payment method for all of their AWS accounts. Through integrations with other AWS services, customers can use Organizations to define central configurations and resource sharing across accounts in their organization.

AWS Outposts

AWS Outposts is a service that extends AWS infrastructure, AWS services, APIs and tools to any data center, co-location space, or an on-premises facility for a consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing or local data storage. Outposts offer the same AWS hardware infrastructure, services, APIs and tools to build and run applications on premises and in the cloud. AWS compute, storage, database and other services run locally on Outposts and customers can access the full range of AWS services available in the Region to build, manage and scale on-premises applications. Service Link is established between Outposts and the AWS region by use of a secured VPN connection over the public internet or AWS Direct Connect.

AWS Outposts are configured with a Nitro Security Key (NSK) which is designed to encrypt customer content and give customers the ability to mechanically remove content from the device. Customer content is cryptographically shredded if a customer removes the NSK from an Outpost device.

Additional information about Security in AWS Outposts, including the shared responsibility model, can be found in the AWS Outposts User Guide.

AWS Health Dashboard

AWS Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact customers. While the AWS Health Dashboard displays the general status of AWS services, AWS Health Dashboard gives customers a personalized view into the performance and availability of the AWS services underlying customer's AWS resources.

The dashboard displays relevant and timely information to help customers manage events in progress and provides proactive notification to help customers plan for scheduled activities. With AWS Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving event visibility, and guidance to help quickly diagnose and resolve issues.

AWS Private Certificate Authority

AWS Private Certificate Authority (CA) is a managed private CA service enables customers to easily and securely manage the lifecycle of their private certificates. Private CA allows developers to be more agile by providing them APIs to create and deploy private certificates programmatically. Customers also have the flexibility to create private certificates for applications that require custom certificate lifetimes or resource names. With Private CA, customers can create and manage private certificates for their connected resources in one place with a secure, pay as you go, managed private CA service.

Amazon Personalize

Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking and customized direct marketing. Amazon Personalize goes beyond rigid static rule- based recommendation systems and trains, tunes, and deploys custom machine learning models to deliver highly customized recommendations to customers across industries such as retail, media and entertainment.

Amazon Pinpoint

Amazon Pinpoint helps customers engage with their customers by sending email, SMS, and mobile push messages. The customers can use Amazon Pinpoint to send targeted messages (such as promotional alerts and customer retention campaigns), as well as direct messages (such as order confirmations and password reset messages) to their customers.

Amazon Polly

Amazon Polly is a service that turns text into lifelike speech, allowing customers to create applications that talk, and build entirely new categories of speech-enabled products. Amazon Polly is a Text-to-Speech service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice.

Amazon Quantum Ledger Database (QLDB)

Amazon Quantum Ledger Database (QLDB) is a ledger database that provides a transparent, immutable and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB can be used to track each and every application data change and maintains a complete and verifiable history of changes over time.

Amazon QuickSight

Amazon QuickSight is a fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from customers' data. Using this cloud-based service customers can connect to their data, perform advanced analysis, and create visualizations and dashboards that can be accessed from any browser or mobile device.

Amazon Redshift

Amazon Redshift is a data warehouse service to analyze data using a customer's existing Business Intelligence (BI) tools. Amazon Redshift also includes Redshift Spectrum, allowing customers to directly run SQL queries against Exabytes of unstructured data in Amazon S3.

Amazon Rekognition

The easy-to-use Rekognition API allows customers to automatically identify objects, people, text, scenes, and activities, as well as detect any inappropriate content. Developers can quickly build a searchable content library to optimize media workflows, enrich recommendation engines by extracting text in images, or integrate secondary authentication into existing applications to enhance end-user security.

With a wide variety of use cases, Amazon Rekognition enables the customers to easily add the benefits of computer vision to the business.

Amazon Relational Database Service (RDS)

Amazon Relational Database Service (RDS) enables customers to set up, operate, and scale a relational database in the cloud. Amazon RDS manages backups, software patching, automatic failure detection, and recovery. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

AWS Resource Access Manager

AWS Resource Access Manager helps customers securely share their resources across AWS accounts, within their organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types. Customers are able to use AWS Resource Access Manager to share transit gateways, subnets, AWS License Manager license configurations, Amazon Route 53 Resolver rules, and more resource types.

AWS Resource Groups

AWS Resource Groups is a service that helps customers organize AWS resources into logical groupings. These groups can represent an application, a software component, or an environment. Resource groups can include more than fifty additional resource types, bringing the overall number of supported resource types to seventy-seven. Some of these new resource types include Amazon DynamoDB tables, AWS Lambda functions, AWS CloudTrail trails, and many more. Customers can now create resource groups that accurately reflect their applications, and take action against those groups, rather than against individual resources.

AWS RoboMaker

AWS RoboMaker is a service that makes it easy to develop, test, and deploy intelligent robotics applications at scale. RoboMaker extends the most widely used open-source robotics software framework, Robot Operating System (ROS), with connectivity to cloud services. This includes AWS machine learning services, monitoring services, and analytics services that enable a robot to stream data, navigate, communicate, comprehend, and learn. RoboMaker provides a robotics development environment for application development, a robotics simulation service to accelerate application testing, and a robotics fleet management service for remote application deployment, update, and management.

Amazon Route 53

Amazon Route 53 provides managed Domain Name System (DNS) web service. Amazon Route 53 connects user requests to infrastructure running both inside and outside of AWS. Customers can use Amazon Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of their application and its endpoints. Amazon Route 53 enables customers to manage traffic globally through a variety of routing types, including Latency Based Routing, Geo DNS, and Weighted Round Robin, all of these routing types can be combined with DNS Failover. Amazon Route 53 also offers Domain Name Registration; customers can purchase and manage domain names such as example.com and Amazon Route 53 will automatically configure DNS settings for their domains. Amazon Route 53 sends automated requests over the internet to a resource, such as a web server, to verify that it is reachable, available, and functional. Customers also can choose to receive notifications when a resource becomes unavailable and choose to route internet traffic away from unhealthy resources.

Amazon SageMaker (excludes Studio Lab, Public Workforce and Vendor Workforce for all features)
Amazon SageMaker is a platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes the barriers that typically "slow down" developers who want to use machine learning.

Amazon SageMaker removes the complexity that holds back developer success with the process of building, training, and deploying machine learning models at scale. Amazon SageMaker includes modules that can be used together or independently to build, train, and deploy a customer's machine learning models.

AWS Secrets Manager
AWS Secrets Manager helps customers protect secrets needed to access their applications, services, and IT resources. The service enables customers to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. The service is also extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager allows customers to control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the AWS Cloud, third-party services, and on-premises.

AWS Security Hub
AWS Security Hub gives customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. There are a range of powerful security tools at customers' disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. With Security Hub, customers can now have a single place that aggregates, organizes, and prioritizes their security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector Classic, and Amazon Macie, as well as from AWS Partner solutions. Findings are visually summarized on integrated dashboards with actionable graphs and tables.

AWS Server Migration Service (SMS)
AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for customers to migrate thousands of on-premises workloads to AWS. AWS SMS allows customers to automate, schedule, and track incremental replications of live server volumes, making it easier for customers to coordinate large-scale server migrations.

AWS Serverless Application Repository
The AWS Serverless Application Repository is a managed repository for serverless applications. It enables teams, organizations, and individual developers to store and share reusable applications, and easily assemble and deploy serverless architectures in powerful new ways. Using the Serverless Application Repository, customers do not need to clone, build, package, or publish source code to AWS before deploying it. Instead, customers can use pre-built applications from the Serverless Application Repository in their serverless architectures, helping customers reduce duplicated work, ensure organizational best practices, and get to market faster. Integration with AWS Identity and Access Management (IAM) provides resource-level control of each application, enabling customers to publicly share applications with everyone or privately share them with specific AWS accounts.

AWS Service Catalog

AWS Service Catalog allows customers to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, and helps customers achieve consistent governance and meet their compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

Amazon Simple Email Service (SES)

Amazon Simple Email Service (SES) is a cost-effective, flexible and scalable email service that enables developers to send mail from within any application. Customers can configure Amazon SES to support several email use cases including transactional, marketing, or mass email communications. Amazon SES' flexible IP deployment and email authentication options help drive higher deliverability and protect sender reputation, while sending analytics to measure impact of each email. With Amazon SES, customers can send email securely, globally and at scale.

Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (SNS) is a web service to set up, operate, and send notifications. It provides developers the capability to publish messages from an application and deliver them to subscribers or other applications. Amazon SNS follows the “publish-subscribe” (pub-sub) messaging paradigm, with notifications being delivered to clients using a “push” mechanism. Using SNS requires defining a "Topic", setting policies on access and delivery of the Topic, subscribing consumers and designating delivery endpoints, and publishing messages to a Topic. Administrators define a Topic as an access point for publishing messages and allowing customers to subscribe to notifications. Security policies are applied to Topics to determine who can publish, who can subscribe, and to designate protocols supported.

Amazon Simple Queue Service (SQS)

Amazon Simple Queue Service (SQS) is a message queuing service that offers a distributed hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can move data between distributed components of their applications that perform different tasks, without losing messages or requiring each component to be always available. Amazon SQS allows customers to build an automated workflow, working in close conjunction with Amazon EC2 and the other AWS infrastructure web services.

Amazon SQS’ main components consist of a frontend request-router fleet, a backend data-storage fleet, a metadata cache fleet, and a dynamic workload management fleet. User queues are mapped to one or more backend clusters. Requests to read, write, or delete messages come into the frontends. The frontends contact the metadata cache to find out which backend cluster hosts that queue and then connect to nodes in that cluster to service the request.

For authorization, Amazon SQS has its own resource-based permissions system that uses policies written in the same language used for AWS IAM policies. User permissions for any Amazon SQS resource can be given either through the Amazon SQS policy system or the AWS IAM policy system, which is authorized by AWS Identity and Access Management Service. Such policies with a queue are used to specify which AWS Accounts have access to the queue as well as the type of access and conditions.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (S3) provides a web services interface that can be used to store and retrieve data from anywhere on the web. To provide customers with the flexibility to determine how, when, and to whom they wish to expose the information they store in AWS, Amazon S3 APIs provide both bucket and object-level access controls, with defaults that only permit authenticated access by the bucket and/or object creator. Unless a customer grants anonymous access, the first step before a user can access Amazon S3 is to be authenticated with a request signed using the user's secret access key.

An authenticated user can read an object only if the user has been granted read permissions in an Access Control List (ACL) at the object level. An authenticated user can list the keys and create or overwrite objects in a bucket only if the user has been granted read and write permissions in an ACL at the bucket level. Bucket and object-level ACLs are independent; an object does not inherit ACLs from its bucket. Permissions to read or modify the bucket or object ACLs are themselves controlled by ACLs that default to creator-only access. Therefore, the customer maintains full control over who has access to its data. Customers can grant access to their Amazon S3 data to other AWS users by AWS Account ID or email, or DevPay Product ID. Customers can also grant access to their Amazon S3 data to all AWS users or to everyone (enabling anonymous access).

Network devices supporting Amazon S3 are configured to only allow access to specific ports on other Amazon S3 server systems**.** External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation.

Amazon Simple Workflow Service (SWF)

Amazon Simple Workflow Service (SWF) is an orchestration service for building scalable distributed applications. Often an application consists of several different tasks to be performed in a particular sequence driven by a set of dynamic conditions. Amazon SWF enables developers to architect and implement these tasks, run them in the cloud or on-premise and coordinate their flow. Amazon SWF manages the execution flow such that tasks are load balanced across the workers, inter-task dependencies are respected, concurrency is handled appropriately, and child workflows are executed.

Amazon SWF enables applications to be built by orchestrating tasks coordinated by a decider process. Tasks represent logical units of work and are performed by application components that can take any form, including executable code, scripts, web service calls, and human actions.

Developers implement workers to perform tasks. They run their workers either on cloud infrastructure, such as Amazon EC2, or off-cloud. Tasks can be long-running, may fail, may timeout and may complete with varying throughputs and latencies. Amazon SWF stores tasks for workers, assigns them when workers are ready, tracks their progress, and keeps their latest state, including details on their completion. To orchestrate tasks, developers write programs that get the latest state of tasks from Amazon SWF and use it to initiate subsequent tasks in an ongoing manner. Amazon SWF maintains an application's execution state durably so that the application can be resilient to failures in individual application components.

Amazon SWF provides auditability by giving customers visibility into the execution of each step in the application. The Management Console and APIs let customers monitor all running executions of the application. The customer can zoom in on any execution to see the status of each task and its input and output data. To facilitate troubleshooting and historical analysis, Amazon SWF retains the history of executions for any number of days that the customer can specify, up to a maximum of 90 days.

The actual processing of tasks happens on compute resources owned by the end customer. Customers are responsible for securing these compute resources, for example if a customer uses Amazon EC2 for workers then they can restrict access to their instances in Amazon EC2 to specific AWS IAM users. In addition, customers are responsible for encrypting sensitive data before it is passed to their workflows and decrypting it in their workers.

Amazon SimpleDB

Amazon SimpleDB is a non-relational data store that allows customers to store and query data items via web services requests. Amazon SimpleDB then creates and manages multiple geographically distributed replicas of data automatically to enable high availability and data durability.

Data in Amazon SimpleDB is stored in domains, which are similar to database tables except that functions cannot be performed across multiple domains. Amazon SimpleDB APIs provide domain-level controls that only permit authenticated access by the domain creator.

Data stored in Amazon SimpleDB is redundantly stored in multiple physical locations as part of normal operation of those services. Amazon SimpleDB provides object durability by protecting data across multiple availability zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

AWS IAM Identity Center (successor to AWS Single Sign-On)

AWS IAM Identity Center (successor to AWS Single Sign-On) is a cloud-based service that simplifies managing SSO access to AWS accounts and business applications. Customers can control SSO access and user permissions across all AWS accounts in AWS Organizations. Customers can also administer access to popular business applications and custom applications that support Security Assertion Markup Language (SAML) 2.0. In addition, AWS IAM Identity Center offers a user portal where users can find all their assigned AWS accounts, business applications, and custom applications in one place.

AWS Signer

AWS Signer is a managed code-signing service to ensure the trust and integrity of customer code. Customers validate code against a digital signature to confirm that the code is unaltered and from a trusted publisher. With AWS Signer, customer security administrators have a single place to define their signing environment, including what AWS Identity and Access Management (IAM) role can sign code and in what regions. AWS Signer manages the code-signing certificate public and private keys and enables central management of the code-signing lifecycle.

AWS Snowball

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple and secure.

AWS Snowball Edge

AWS Snowball Edge is a 100TB data transfer device with on-board storage and compute capabilities. Customers can use Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local datasets, or to support local workloads in remote or offline locations. Snowball Edge connects to customers' existing applications and infrastructure using standard storage interfaces, streamlining the data transfer process and minimizing setup and integration. Snowball Edge can cluster together to form a local storage tier and process customers' data on-premises, helping ensure their applications continue to run even when they are not able to access the cloud.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. Customers can transfer their Exabyte data via a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. After a customer's data is loaded, Snowmobile is driven back to AWS where their data is imported into Amazon S3 or Amazon Glacier.

AWS Step Functions

AWS Step Functions is a web service that enables customers to coordinate the components of distributed applications and microservices using visual workflows. Customers can build applications from individual components that each perform a discrete function, or task, allowing them to scale and change applications quickly. Step Functions provides a reliable way to coordinate components and step through the functions of a customer's application. Step Functions provides a graphical console to visualize the components of a customer's application as a series of steps. It automatically triggers and tracks each step, and retries when there are errors, so the customer's application executes in order and as expected, every time. Step Functions logs the state of each step, so when things do go wrong, customers can diagnose and debug problems quickly.

AWS Storage Gateway

The AWS Storage Gateway service connects customers' off-cloud software appliances with cloud-based storage. The service enables organizations to store data in AWS' highly durable cloud storage services: Amazon S3 and Amazon Glacier.

AWS Storage Gateway backs up data off-site to Amazon S3 in the form of Amazon EBS snapshots. AWS Storage Gateway transfers data to AWS and stores this data in either Amazon S3 or Amazon Glacier, depending on the use case and type of gateway used. There are three types of gateways: Tape, File, and Volume Gateways. The Tape Gateway allows customers to store more frequently accessed data in Amazon S3 and less frequently accessed data in Amazon Glacier.

The File Gateway allows customers to copy data to S3 and have those files appear as individual objects in S3. Volume gateways store data directly in Amazon S3 and allow customers to snapshot their data so that they can access previous versions of their data. These snapshots are captured as Amazon EBS Snapshots, which are also stored in Amazon S3. Both Amazon S3 and Amazon Glacier redundantly store these snapshots on multiple devices across multiple facilities, detecting and repairing any lost redundancy. The Amazon EBS snapshot provides a point-in-time backup that can be restored off-cloud or on a gateway running in Amazon EC2, or used to instantiate new Amazon EBS volumes. Data is stored within a single region that customers specify.

AWS Systems Manager

AWS Systems Manager gives customers the visibility and control to their infrastructure on AWS. AWS Systems Manager provides customers a unified user interface so that customers can view their operational data from multiple AWS services, and it allows customers to automate operational tasks across the AWS resources.

With AWS Systems manager, customers can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and take action on groups of resources.

Amazon Textract

Amazon Textract automatically extracts text and data from scanned documents. With Textract customers can quickly automate document workflows, enabling customers to process large volumes of document pages in a short period of time. Once the information is captured, customers can take action on it within their business applications to initiate next steps for a loan application or medical claims processing. Additionally, customers can create search indexes, build automated approval workflows, and better maintain compliance with document archival rules by flagging data that may require redaction.

Amazon Timestream

Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases. Amazon Timestream saves customers time and cost in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a cost optimized storage tier based upon user defined policies. Amazon Timestream's purpose-built query engine lets customers access and analyze recent and historical data together, without needing to specify explicitly in the query whether the data resides in the in-memory or cost-optimized tier. Amazon Timestream has built-in time series analytics functions, helping customers identify trends and patterns in data in real-time.

Amazon Transcribe

Amazon Transcribe makes it easy for customers to add speech-to-text capability to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, recorded speech needs to be converted to text before it can be used in applications.

Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets to create a fully searchable archive.

Amazon Transcribe automatically adds punctuation and formatting so that the output closely matches the quality of manual transcription at a fraction of the time and expense.

AWS Transfer Family

AWS Transfer Family enables the transfer of files directly into and out of Amazon S3. With the support for Secure File Transfer Protocol (SFTP)—also known as Secure Shell (SSH) File Transfer Protocol, the File Transfer Protocol over SSL (FTPS) and the File Transfer Protocol (FTP), the AWS Transfer Family helps the customers seamlessly migrate their file transfer workflows to AWS by integrating with existing authentication systems and providing DNS routing with Amazon Route 53.

Amazon Translate

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Neural machine translation is a form of language translation automation that uses deep learning models to deliver more accurate and more natural sounding translation than traditional statistical and rule- based translation algorithms. Amazon Translate allows customers to localize content - such as websites and applications - for international users, and to easily translate large volumes of text efficiently.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (VPC) enables customers to provision a logically isolated section of the AWS cloud where AWS resources can be launched in a virtual network defined by the customer. Customers can connect their existing infrastructure to the network isolated Amazon EC2 instances within their Amazon VPC, including extending their existing management capabilities, such as security services, firewalls and intrusion detection systems, to include their instances via a Virtual Private Network (VPN) connection. The VPN service provides end-to-end network isolation by using an IP address range of a customer's choice, and routing all of their network traffic between their Amazon VPC and another network designated by the customer via an encrypted Internet Protocol security (IPsec) VPN.

Customers can optionally connect their VPC to the Internet by adding an Internet Gateway (IGW) or a NAT Gateway. An IGW allows bi-directional access to and from the internet for some instances in the VPC based on the routes a customer defines, which specify which IP address traffic should be routable from the internet, Security Groups, and Network ACLs (NACLS) which limit which instances can accept or send this traffic. Customers can also optionally configure a NAT Gateway which allows egress-only traffic initiated from a VPC instance to reach the internet, but not allow traffic initiated from the internet to reach VPC instances. This is accomplished by mapping the private IP addresses to a public address on the way out, and then map the public IP address to the private address on the return trip.

The objective of this architecture is to isolate AWS resources and data in one Amazon VPC from another Amazon VPC, and to help prevent data transferred from outside the Amazon network except where the customer has specifically configured internet connectivity options or via an IPsec VPN connection to their off-cloud network.

Further details are provided below:

- **Virtual Private Cloud (VPC):** An Amazon VPC is an isolated portion of the AWS cloud within which customers can deploy Amazon EC2 instances into subnets that segment the VPC's IP address range (as designated by the customer) and isolate Amazon EC2 instances in one subnet from another. Amazon EC2 instances within an Amazon VPC are accessible to customers via Internal Gateway (IGW), Virtual Gateway (VGW), or VPC Peerings established to the Amazon VPC

- **IPsec VPN:** An IPsec VPN connection connects a customer's Amazon VPC to another network designated by the customer. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. Amazon VPC customers can create an IPsec VPN connection to their Amazon VPC by first establishing an Internet Key Exchange (IKE) security association between their Amazon VPC VPN gateway and another network gateway using a pre-shared key as the authenticator. Upon establishment, IKE negotiates an ephemeral key to secure future IKE messages. An IKE security association cannot be established unless there is complete agreement among the parameters. Next, using the IKE ephemeral key, two keys in total are established between the VPN gateway and customer gateway to form an IPsec security association. Traffic between gateways is encrypted and decrypted using this security association. IKE automatically rotates the ephemeral keys used to encrypt traffic within the IPsec security association on a regular basis to ensure confidentiality of communications.

AWS WAF

AWS WAF is a web application firewall that helps protect customer web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Customers can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for their specific application. New rules can be deployed within minutes, letting customers respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that customers can use to automate the creation, deployment, and maintenance of web security rules.

Amazon WorkDocs

Amazon WorkDocs is a secure content creation, storage and collaboration service. Users can share files, provide rich feedback, and access their files on WorkDocs from any device. WorkDocs encrypts data in transit and at rest, and offers powerful management controls, active directory integration, and near real-time visibility into file and user actions. The WorkDocs SDK allows users to use the same AWS tools they are already familiar with to integrate WorkDocs with AWS products and services, their existing solutions, third-party applications, or build their own.

Amazon WorkMail

Amazon WorkMail is a managed business email and calendaring service with support for existing desktop and mobile email clients. It allows access to email, contacts, and calendars using Microsoft Outlook, a browser, or native iOS and Android email applications. Amazon WorkMail can be integrated with a customer's existing corporate directory and the customer controls both the keys that encrypt the data and the location (AWS Region) under which the data is stored.

Customers can create an organization in Amazon WorkMail, select the Active Directory they wish to integrate with, and choose their encryption key to apply to all customer content. After setup and validation of their mail domain, users from the Active Directory are selected or added, enabled for Amazon WorkMail, and given an email address identity inside the customer owned mail domain.

Amazon WorkSpaces

Amazon WorkSpaces is a managed desktop computing service in the cloud. Amazon WorkSpaces enables customers to deliver a high-quality desktop experience to end-users as well as help meet compliance and security policy requirements. When using Amazon WorkSpaces, an organization's data is neither sent to nor stored on end-user devices. The PCoIP protocol used by Amazon WorkSpaces uses an interactive video stream to provide the desktop experience to the user while the data remains in the AWS cloud or in the organization's off-cloud environment.

When Amazon WorkSpaces is integrated with a corporate Active Directory, each WorkSpace joins the Active Directory domain, and can be managed like any other desktop in the organization. This means that customers can use Active Directory Group Policies to manage their Amazon WorkSpaces and can specify configuration options that control the desktop, including those that restrict users' abilities to use local storage on their devices. Amazon WorkSpaces also integrates with customers' existing RADIUS server to enable multi-factor authentication (MFA).

Amazon WorkSpaces Web

Amazon WorkSpaces Web is an on-demand, managed service designed to facilitate secure browser access to internal websites and software-as-a-service (SaaS) applications. Customers can access the service from existing web browsers without infrastructure management, specialized client software, or virtual private network (VPN) solutions.

AWS X-Ray

AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, customers or developers can understand how their application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through the customers' application and shows a map of the application's underlying components. Customers or developers can use X-Ray to analyze both applications in development and in production.

Attachment B – Principal Service Commitments and System Requirements

Overview

Amazon Web Services (AWS) designs its processes and procedures to meet its objectives for the AWS System. Those objectives are based on the service commitments that AWS makes to user entities (customers), the laws and regulations that govern the provision of the AWS System, and the financial, operational and compliance requirements that AWS has established for the services.

The AWS services are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which AWS operates.

Security, Availability and Confidentiality commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the AWS website. Security, Availability and Confidentiality commitments are standardized and include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the AWS System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- Security and confidentiality principles inherent to the fundamental design of the AWS System are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principles inherent to the fundamental design of the AWS System are designed to replicate critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication to meet the service commitments.
- Privacy principles inherent to the fundamental design of the AWS System are designed to protect the security and confidentiality of AWS customer content to meet the service commitments.

Amazon Web Services establishes operational requirements that support the achievement of security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in AWS' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Amazon Web Services System.

As an Infrastructure as a Service (IaaS) System, the AWS System is designed based on a shared responsibility model where both AWS and the customers are responsible for aspects of security, availability and confidentiality. Details of the responsibilities of customers can be found on the AWS website and in the Customer Agreement.

People

Amazon Web Services' organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing the Company's tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established points of authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, security practices, policies and procedures. Employees are provided with the Company's Code of Business Conduct and Ethics and additionally complete annual Security & Awareness training to educate them as to their responsibilities concerning information security. Compliance audits are performed so that employees understand and follow established policies.

Data

AWS customers retain control and ownership of their own data. Customers are responsible for the development, operation, maintenance, and use of their content. AWS prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent unauthorized access to assets. AWS uses techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. All production media is securely decommissioned in accordance with industry-standard practices. Production media is not removed from AWS control until it has been securely decommissioned.

Availability

The AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to and recovers from a major availability event or incident within the AWS services environment. This program builds upon the traditional approach of addressing contingency management which incorporates elements of business continuity and disaster recovery plans and expands this to consider critical elements of proactive risk mitigation strategies such as engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning.

AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Service team response plans are tested and updated through the due course of business, and the AWS Resiliency plan is tested, reviewed, and approved by senior leadership annually.

AWS has identified critical system components required to maintain the availability of the system and recover service in the event of outage. Critical system components (example: code bases) are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failure like generators and cooling equipment are not shared across Availability Zones. Additionally, Availability Zones are physically separate, and designed such that even extremely uncommon disasters such as fires, tornados or flooding should only affect a single Availability Zone. AWS replicates critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication.

AWS continuously monitors service usage to project infrastructure needs to support availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements

Confidentiality

AWS is committed to protecting the security and confidentiality of its customers' content, defined as "Your Content" at https://aws.amazon.com/agreement/. AWS' systems and services are designed to enable authenticated AWS customers to access and manage their content. AWS notifies customers of third-party access to a customer's content on the third-party access page located at https://aws.amazon.com/compliance/third-party-access. AWS may remove a customer's content when compelled to do so by a legal order, or where there is evidence of fraud or abuse as described in the Customer Agreement (https://aws.amazon.com/agreement/) and Acceptable Use Policy (https://aws.amazon.com/aup/). In executing the removal of a customer's content due to the reasons stated above, employees may render it inaccessible as the situation requires. For clarity, this capability to render customer content inaccessible extends to encrypted content as well.

In the course of AWS system and software design, build, and test of product features, a customer's content is not used and remains in the production environment. A customer's content is not required for the AWS software development life cycle. When content is required for the development or test of a service's software, AWS service teams have tools to generate mock, random data.

AWS knows customers care about privacy and data security. That is why AWS gives customers ownership and control over their content by design through tools that allow customers to determine where their content is stored, secure their content in transit or at rest, and manage access to AWS services and resources. AWS also implements technical and physical controls designed to prevent unauthorized access to or disclosure of a customer's content. As described in the Physical Security and Change Management areas in Section III of this report, AWS employs a number of controls to safeguard data from within and outside of the boundaries of environments which store a customer's content. As a result of these measures, access to a customer's content is restricted to authorized parties.

AWS contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and assess security incidents. These plans and playbooks include guidelines for responding to potential data breaches in accordance with contractual and regulatory requirements. AWS security engineers follow a protocol when responding to potential data security incidents. The protocol involves steps, which include validating the presence customer content within the AWS service (without actually viewing the data), determining the encryption status of a customer's content, and determining improper access to a customer's content to the extent possible.

During the course of their response, the security engineers document relevant findings in internal tools used to track the security issue. AWS Security Leadership is regularly apprised of all data security issue investigations. In the event there are positive indicators that customer content was potentially accessed by an unintended party, a security engineer engages AWS Security Leadership and the AWS Legal team to review the findings. AWS Security Leadership and the Legal team review the findings and determine if a notifiable data breach has occurred pursuant to contractual or regulatory obligations. If confirmed, affected customers are notified in accordance with the applicable reporting requirement.

Vendors and third parties with restricted access, that engage in business with Amazon, are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments are included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or renewal. AWS monitors the performance of third parties through periodic reviews on a risk-based approach, which evaluate performance against contractual obligations.

AWS communicates its confidentiality commitments to customers on its public website located at https://aws.amazon.com/compliance/third-party-access/ for contractors and https://aws.amazon.com/compliance/sub-processors/ for sub-processors. The effective date of the policy is communicated there and updated periodically. Before AWS authorizes and permits any new subcontractor to access any customer content, AWS will update this website to inform customers. Vendor confidentiality commitments are governed by the terms of the contract between AWS and the vendor.

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend Amazon Security Awareness (ASA) training, which includes policies and procedures related to protecting a customer's content. Confidentiality requirements are included in the Data Handling and Classification Policy. Policies are reviewed and updated at least annually.

Privacy

AWS classifies customer data into two categories: customer content and account information. AWS defines customer content as software (including machine images), data, text, audio, video, or images that a customer or any end user transfers to AWS for processing, storage, or hosting by AWS services in connection with that customer's account, and any computational results that a customer or any end user derives from the foregoing through their use of AWS services. For example, customer content includes content that a customer or any end user stores in Amazon Simple Storage Service (S3). The terms of the AWS Customer Agreement (https://aws.amazon.com/agreement/) and AWS Service Terms (https://aws.amazon.com/service-terms/) apply to customer content.

Account information is information about a customer that a customer provides to AWS in connection with the creation or administration of a customer account. For example, account information includes names, user names, phone numbers, email addresses, and billing information associated with a customer account. Any information submitted by the customer that AWS needs in order to provide services to the customer or in connection with the administration of customer accounts, is not in-scope for this report.

The AWS Privacy Notice is available from the AWS website at https://aws.amazon.com/privacy/. The AWS Privacy Notice is reviewed by the AWS Legal team, and is updated as required to reflect Amazon's current business practices and global regulatory requirements. The Privacy Notice describes how AWS collects and uses a customer's personal information in relation to AWS websites, applications, products, services, events, and experiences. The Privacy Notice does not apply to customer content.

As part of the AWS account creation and activation process, AWS customers are informed of the AWS Privacy Notice and are required to accept the Customer Agreement, including the terms and conditions related to the collection, use, retention, disclosure, and disposal of their data. Customers are responsible for determining what content to store within AWS, which may include personal information. Without the acceptance of the Customer Agreement, customers cannot sign up to use the AWS services.

The AWS Customer Agreement informs customers of the AWS data security and privacy commitments prior to activating an AWS account and is made available to customers to review at any time on the AWS website.

The customer determines what data is entered into AWS services and has the ability to configure the appropriate security and privacy settings for the data, including who can access and use the data. Further, the customer is able to choose not to provide certain data. Additionally, the customer manages notification or consent requirements, and maintains the accuracy of the data.

Additionally, the AWS Customer Agreement notes how AWS shares, secures, and retains customer content. AWS also informs customers of updates to the Customer Agreement by making it available on its website and providing the last updated date. Customers should check the Customer Agreement website frequently for any changes to the Customer Agreement**.**

AWS does not store any customer cardholder data obtained from customers. Rather, AWS passes the customer cardholder data and sends it immediately to the Amazon Payments Platform, the PCI-certified platform that Amazon uses for all payment processing. This platform returns a unique identifier that AWS stores and uses for all future processing. The Amazon Payments Platform sits completely outside of the AWS boundary and is run by the larger Amazon entity. It is not an AWS service, but it is utilized by the larger Amazon entity for payment processing. As such, the Amazon payment platform is not in-scope for this report.

AWS offers customers the ability to update their communication preferences through the AWS console or via the AWS Email Preference Center. When customers update their communication preferences using their email, their updated preferences are saved. Customers can unsubscribe from AWS marketing emails within the AWS console. AWS Customers will still receive important account-related notifications from AWS, such as monthly billing statements, or if there are significant changes to a service that customers use.

AWS provides authenticated customers the ability to access, update, and confirm their data. Denial of access will be communicated using the AWS console. Customers can sign into to their AWS accounts through the AWS console to view and update their data.

AWS (or Amazon) does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. AWS Legal reviews and maintains records of all the information requests, which lists information on the types and volume of information requested. Unless AWS is prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, AWS notifies customers before disclosing customer content so they can seek protection from disclosure. AWS shares customer content only as described in the AWS Customer Agreement.

AWS may produce non-content and/or content information in response to valid and binding law enforcement and governmental requests, such as subpoenas, court orders, and search warrants. “Non-content information” means customer information such as name, address, email address, billing information, date of account creation, and service usage information. Content information” includes the content that a customer transfers for processing, storage, or hosting in connection with AWS services and any computational results. AWS records customer information requests to maintain a complete, accurate, and timely record of such requests.

If required, customers are responsible for providing notice to the individuals whose data the customer collects and uses within AWS. AWS is not responsible for providing such notice to or obtaining consent from these individuals and is only responsible for communicating its privacy commitments to AWS customers, which is provided during the account creation and activation process.

AWS has documented an incident response policy and plan which outlines an organized approach for responding to security breaches and incidents. The AWS Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security breaches and incidents, which includes status information required for supporting forensic activities, trend analysis, and evaluation of incident details.

As part of the process, potential breaches of customer content are investigated and escalated to AWS Security and AWS Legal. Affected customers and regulators are notified of breaches and incidents where legally required. Customers can subscribe to the AWS Security Bulletins page, which provides information regarding identified security issues. AWS notifies affected customers and regulators of breaches and incidents as legally required in accordance with team processes.

AWS retains and disposes of customer content in accordance with the Customer Agreement and the AWS Data Classification and Handling Policy. When a customer terminates their account or contract with AWS, the account is put under isolation; after which within 90 days, customers can restore their accounts and related content. AWS services hosting customer content are designed to retain customer content until the contractual obligation to retain a customers’ content ends or a customer-initiated action to remove or delete the content is taken. When a customer requests data to be deleted, AWS utilizes automated processes to detect that request and make the content inaccessible. After the deletion is complete, automated actions are taken on deleted content to render the content unreadable.

AWS performs application security reviews for Third-Party systems that integrate with AWS, to ascertain security risks are identified and mitigated. A typical security review considers privacy components such as retention period, use, and collection of data as applicable. The review starts with a system owner initiating a review request to the dedicated AWS Vendor Security (AVS) team, and submitting detailed information about the artifacts being reviewed. A Security review is required if an AWS Team engages with a new external party for collecting data or modifications to existing systems.

During this process, the AVS team determines the granularity of review required based on the artifact’s design, threat model, and impact to AWS’ risk profile. They provide security guidance, validate security assurance material, and meet with external parties to discuss their penetration tests, Software Development Life Cycle, change management processes, and other operating security controls. They work with the system owner to identify, prioritize, and remediate security findings. The AVS team collaborates with AWS Legal as needed to validate that changes are in-line with AWS privacy policies. The AVS team provides their final approval after they have adequately assessed the risks and worked with the requester to implement security controls to mitigate identified risks.

MGMT. SYS.
RvA C 466

Certificate

CERTIFY
EY
POINT

Certificate number: 2013-009
Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: December 11, 2011
Re-issue date of certificate: December 3, 2018
Expiration date of certificate: November 7, 2019

EY CertifyPoint will, according to the certification agreement dated November 9, 2016, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2018.01 dated November 1, 2018 this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V, the Netherlands and is governed by the Dutch law. Any dispute relating to this certificate shall be subject to the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All right reserved. © Copyright

Amazon Web Services, Inc.

Scope for certificate 2013-009

The scope of this ISO/IEC 27001:2013 Certification is bounded by specified services of Amazon Web Services, Inc. and specified facilities. The ISMS is centrally managed out of Amazon Web Services, Inc. headquarters in Seattle, Washington, United States of America.

The in-scope applications, systems, people, and processes are globally implemented and operated by teams out of an explicit set of facilities that comprise Amazon Web Services, Inc. and are specifically defined in the scope and bounds.

The Information Security Management System mentioned in the below scope is restricted as defined in the "ISMS Manual" version 2018.03, signed on November 1, 2018 by the Vice President of AWS Security.

The Amazon Web Services, Inc. ISMS scope includes the services as mentioned on https://aws.amazon.com/compliance/iso-certified/ and locations as stated in the following section of this certificate.

This scope (edition: December 3, 2018) is only valid in connection with certificate 2013-009.

Amazon Web Services, Inc.

Scope for certificate 2013-009

Locations in scope:

AWS data centers, which house the hardware supporting the AWS Services listed above. AWS Data centers are located in US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US), Canada (Montréal), EU (London), EU (Paris), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Mumbai), Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo) Regions, as well as the following AWS Edge locations in:

- Canberra, Australia
- Melbourne, Australia
- Perth, Australia
- Sydney, Australia
- Vienna, Austria
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Montréal, Canada
- Toronto, Canada
- Vancouver, Canada
- Prague, Czech Republic
- Hong Kong, China
- London, England
- Manchester, England
- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Munich, Germany
- Bengaluru, India
- Chennai, India
- Mumbai, India
- New Delhi, India
- Dublin, Ireland
- Milan, Italy
- Osaka, Japan
- Tokyo, Japan
- Seoul, Korea
- Kuala Lumpur, Malaysia
- Amsterdam, Netherlands
- Manila, Philippines Warsaw, Poland
- Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- Taipei, Taiwan
- Dubai, United Arab Emirates
- Arizona, United States
- California, United States
- Colorado, United States
- Florida, United States
- Georgia, United States
- Illinois, United States
- Indiana, United States
- Massachusetts, United States
- Minnesota, United States
- Missouri, United States
- Nevada, United States
- New Jersey, United States
- New York, United States
- Ohio, United Sates
- Oregon, United States
- Pennsylvania, United States
- Texas, United States
- Virginia, United States
- Washington, United States

This scope (edition: December 3, 2018) is only valid in connection with certificate 2013-009.

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 11

Report from Legal Counsel

Henna Rasul, Board Counsel will provide the Board with a general update on legal activities as needed.

Action: None – Informational Only

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 12

Reports from Board Chair and Board Members

a. **Report from Board Chair and Board Members**

b. **2024 Proposed Meeting Schedule**
Next meeting proposed: Wednesday, July 24, 2024 at 4:30pm. Teleconference hosted via Zoom and in-person at the Reno Board Office

c. **Future Agenda Items**
1) Welcome New Board Member Appointments
2) Election of Board Chair/Vice Chair (as needed)
3) Comprehensive Review of Proposed Revisions to NRS 637B to Pursue in 2025 Legislative Session
4) Update on Progress of Proposed Regulations LCB File R108-23
5) Update and Report Out from Strategies 360 on Legislative and Lobbying Activities for 2024 Interim and 2025 Legislative Session
6) Other Items As Proposed

Action: Approve, Table, or Take No Action on the Matter

AGENDA ITEM 13

Public Comment

No vote may be taken upon a matter raised during a period devoted to public comment until the matter itself has been specifically included on an agenda as an item upon which action may be taken. (NRS 241.020)

Action: None – Informational Only

State of Nevada
Speech-Language Pathology, Audiology & Hearing Aid Dispensing Board

AGENDA ITEM 14

Adjournment

Action: Meeting Adjourned