Process Steps

Title:	ODHS|OHA 090-006-01 Information Security Risk Assessment Process
Related to:	ODHS|OHA 090-006 Information Risk Assessment Policy
Effective date:	11/02/2020

Purpose

This document describes the process to identify and assess the information security risk to protected information within the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA).

Applicability

This process applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, as well as partners and contractors.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rules, and state and federal laws. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Process Steps

1. The Chief Information Risk Officer (CIRO) or information system owner may initiate an information security risk assessment in response to one of the following:
   a. Regulatory requirements.
   b. Specific events including but not limited to:
      A. Major modifications to the information system's environment.
      B. An information security incident.
      C. An internal or external audit.
   c. In support of the ODHS|OHA Information Security Risk Assessment program.
2. The Information Security Risk Coordinator engages the information system owner to understand the purpose and identify the scope of the assessment.
3. The information system owner or their designee designates a contract administrator. The contract administrator is responsible for ensuring information security risk assessment services are procured in accordance with the State of Oregon's contracting code and all applicable agency, state, and federal rules.
4. The Information Security Risk Coordinator assists the contract administrator to develop solicitation requirements, minimum qualifications, and evaluation criteria to comply with DAS 107-004-052.

5. The Information Security Risk Coordinator may assist the risk assessor by facilitating the testing of administrative, management, physical, and technical information security controls.
6. When the information security risk assessment is completed, the risk assessor prepares a draft report and sends it to the Information Security Risk Coordinator.
7. The Information Security Risk Coordinator send the draft report to the risk assessment participants for review and validation along with an information security risk assessment feedback log.
8. Using the provided information security risk assessment feedback log, risk assessment participants record comments, questions, and requested changes to the draft report and submit them to the Information Security Risk Coordinator.
9. The Information Security Risk Coordinator consolidates the information security risk assessment feedback logs and submits to the risk assessor for consideration.
10. The risk assessor responds to all comments and requested changes in the information security risk assessment feedback logs, and returns them with the updated draft report.
11. The review process represented in steps 8 through10 above are repeated until agreement is reached that the information contained in the draft report is an accurate depiction of the information collected during the assessment process.
12. The risk assessor makes the final determination as to whether assigned risk ratings in the final report are revised based on corrections of omissions, errors, or inaccuracies.
13. The risk assessor finalizes the information security risk assessment report. At a minimum, the information security risk assessment final report format contains the following elements:
    a. Vulnerability name and description.
    b. Threat name and description.
    c. Risk rating (likelihood and impact) with summary of reasoning.
    d. Remediation recommendations.
    e. Information security risks scored and sorted in priority order (highest to lowest).
    f. A profile based on the Agency standards and guidelines, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
14. The final information security risk assessment report is submitted to the contract administrator, the information system owners, and the Information Security Risk Coordinator for formal approval and acceptance.
15. Upon acceptance of the information security risk assessment report, the Information Security Risk Coordinator facilitates the risk triage process with the Office of Information Services Executive staff and the information system owner or their designee resulting in:
    a. A remediation owner identified for each risk.
    b. A plan of action and milestones (POA&M) developed by the remediation owner for each identified risk.
    c. Initial findings entered in the information security risk register.
16. The Information Security Risk Analyst documents the remediation updates in the information security risk register.
17. The Information Security Risk Coordinator communicates the results of the risk assessment to ODHS|OHA leadership for their review.

References

Center for Internet Security Top Twenty Critical Security Controls

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1
NIST SP 800-37 Rev. 2
NIST SP 800-39
NIST Cybersecurity Framework Version 1.1
45 CFR 160
45 CFR 164
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
Social Security Administration Information Exchange Security Requirements and Procedures
ODHS|OHA 090-005-01 Information Security Incident Reporting Process
ODHS|OHA 090-005-02 Information Security Incident Reporting Process Map
ODHS|OHA 090-006-02 Information Security Risk Assessment Process Map
Oregon Revised Statute 276.300 Information Systems Security in Executive Department; Rules
Oregon Revised Statute 279A-Public Contracting-General Provisions
DAS Procurement Training Law
Statewide Information and Cyber Security Standards 2019

Forms
MSC 0118s Solicitation Request Form

Related Policies
ODHS|OHA 090-006 Information Security Risk Assessment Policy
DAS 107-004-052 Information Security
DAS 107-004-120 Information Security Incident Response
ODHS|OHA 090-005 Information Security Incident Management Policy
OHA 100-014 Report and Response to Privacy and Security Incidents
ODHS 020-005 Contract Administration

Contact
Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
Email: ispo.inforisk@dhsoha.state.or.us

Process History
Version 1 DHS|OHA established 10/28/15
Version 1 DHS|OHA reviewed annually 09/20/16
Version 3 DHS|OHA revised 09/12/2018
Version 3 ODHS|OHA reviewed 11/02/2020

Keywords
Contract, contract administrator, information security, information security risk assessment, ISRA, Information Security Risk Coordinator, risk assessment, risk assessment log, vulnerabilities, threats, analysis

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.