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:	12/12/2022

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 and 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 Information Security and Privacy Office (ISPO) Information Security Risk Assessment Policy.

2. The Information Security Risk Coordinator (ISRC) engages the information system owner to understand the purpose and identify the scope of the assessment. The information system owner is the person accountable for the information created, transmitted, received, or processed by a specific system.
3. The information system owner or their designee procures third-party risk assessment services with the contract administrator in accordance with the State of Oregon's contracting code and all applicable agency, state, and federal rules.
4. The ISRC assists the contract administrator to develop solicitation requirements, minimum qualifications, and evaluation criteria to comply with DAS 107-004-052 Cyber and Information Security Policy.
5. The ISRC 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 complete, the risk assessor prepares a security assessment report (SAR) and sends to the ISRC. The SAR:
    a. Contains a gap analysis of the National Institute of Standards and Technology (NIST) security controls for agency systems.
    b. Contains a gap analysis of the Center for Internet Security (CIS) Controls.
7. The ISRC sends the SAR to the risk assessment information system owners for review.
8. The information system owners can provide comments and questions regarding the SAR.
9. The ISRC consolidates the feedback of the SAR and submits to the risk assessor.
10. The risk assessor finalizes the SAR.
11. The ISRC generates the risk assessment report (RAR) which is a report that captures the security gap analysis from the security assessment report and rates the risks associated with the analysis.
12. The RAR includes:
    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 and the Center for Internet Security Controls.
13. The ISRC in collaboration with the CIO, CIRO, and information system owners, reviews, accepts, and addresses the risks in a variety of ways which include:
    a. Risk acceptance;

b. Risk avoidance;
c. Risk mitigation;
d. Risk sharing;
e. Risk transfer; or
f. Combination of any of the above.

14. The CIRO or designee communicates the results of the risk assessments to the following staff:
    a. Chief Information Officer
    b. Privacy Compliance Officer
    c. Program manager
    d. Information system owner
    e. ODHS|OHA Chief Audit Officer Executive
15. The ISRC facilitates the risk triage process with the information system owner or their designee resulting in:
    a. The identification of a risk owner identified for each risk.
    b. Initial findings entered in the information security risk register.
    c. Monitoring of the risk every 90 days until the risk is either remediated or a compensating control is put in place to mitigate the risk.
16. If the information system owners have exhausted all efforts to remediate or mitigate the risk and instead decide to accept, the information system owners submit a request for an exception using the MSC 3489 Risk Exception Request Form to the CIRO.

References

Center for Internet Security Critical Controls

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I Harmonized Security and Privacy Framework Version 2.2

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev. 1 Guide for Conducting Risk Assessments

NIST SP 800-37 Rev. 2 Risk Management Framework

NIST SP 800-39 Managing Information Security Risk : Organization, Mission, and Information System View

NIST Cybersecurity Framework Version 1.1

45 CFR 160 General Administrative Requirements

45 CFR 164 Security and Privacy

Federal Bureau of Investigation (FBI) Criminal Justice Information Systems Security Standards (CJIS)

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
ODHS|OHA Agency Information Security Plan

Related Policies

ODHS|OHA 090-006 Information Security Risk Assessment Policy
DAS 107-004-052 Cyber and 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

Forms

MSC 3483 Risk Exception Request Form

Contact

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
Email: ispo.inforisk@dhsoha.oregon.gov

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 2 ODHS|OHA reviewed 11/02/2020
Version 3 ODHS|OHA revised 10/04/2021
Version 4 ODHS|OHA revised 12/12/2022

Keywords
Contract, contract administrator, information security, information security risk assessment, ISRA, Information Security Risk Coordinator, ISRC, risk assessment, risk assessment report, RAR, risk assessor, security assessment report, SAR, threats, vulnerabilities

---

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.