Process Steps

Title:	DHS|OHA 090-006-01 Information Security Risk Assessment Process
Related to:	DHS|OHA 090-006 Information Risk Assessment Policy
Effective date:	09/12/2018

Purpose

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

Process Steps

1. The Chief Information Risk Officer (CIRO) or information owner may initiate an information security risk assessment in response to one of the following:
    a. Regulatory requirements
    b. Specific events including:
        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 DHS|OHA Information Security Risk Assessment program
2. The Information Security Risk Coordinator shall engage the information owner to understand the purpose and identify the scope of the assessment.
3. The information owner or their designee shall designate a contract administrator. The contract administrator shall be 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 shall assist 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 shall prepare a draft report and send it to the Information Security Risk Coordinator.
7. The draft report shall be sent by the Information Security Risk Coordinator 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 shall 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 shall consolidate the information security risk assessment feedback logs and submit to the risk assessor for consideration.
10. The risk assessor shall respond to all comments and requested changes in the information security risk assessment feedback logs, and return them with the updated draft report.
11. The review process represented in steps 8 through10 above shall be 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. The risk assessor shall make the final determination as to whether assigned risk ratings in the final report are revised based on corrections of omissions, errors, or inaccuracies.
12. The risk assessor shall finalize the information security risk assessment report. At a minimum, the information security risk assessment final report format shall contain 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.
13. The final information security risk assessment report shall be submitted to the contract administrator and the information security risk coordinator for formal approval and acceptance.
14. Upon acceptance of the information security risk assessment report, the Information Security Risk Coordinator shall facilitate the risk triage process with the Office of Information Services Executive staff and the information 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.
15. The Information Security Risk Analyst shall document the remediation updates in the information security risk register.
16. The Information Security Risk Coordinator shall communicate the results of the risk assessment to DHS|OHA leadership for their review.

References

Center for Internet Security Top Twenty Critical Security Controls

National Institute of Standards and Technology (NIST) SP800-30 Rev. 1 Guide for Conducting Risk Assessments

NIST SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

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

NIST Cybersecurity Framework

United States Computer Emergency Readiness Team (US-CERT), Assessing Security Risk in Legacy Systems

45 CFR 160 & 164

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
Social Security Administration Information Exchange Security Requirements and Procedures
2017 Statewide Information Security Standards
DHS|OHA 090-005-01 Information Security Incident Reporting Process
DHS|OHA 090-005-02 Information Security Incident Reporting Process Map
DHS|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

Forms

MSC 0118s Solicitation Request Form

Related Policies

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

Contact

Information Security and Privacy Office (ISPO)
Phone: 503-945-6812 (Security)
Fax: 503-947-5396
ispo.inforisk@dhsoha.state.or.us

Process History

Version 1 DHS|OHA established 10/28/15
Version 2 DHS|OHA reviewed annually 09/20/16
Version 3 DHS|OHA revised 09/12/2018

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.