Information Technology Services

WSU Guidelines:
Developing a Security Assessment Plan

Author(s): Michael Walters
Steven Conover

Date: 06/26/2020

WASHINGTON STATE UNIVERSITY

Revision History

Version No.	Date	Description	Author
1.0	06/26/2020	Initial Release	Michael Walters Steven Conover

Contents

1. Purpose:

Information assurance policies are created to set universal standards for organizations to facilitate data protection. They also align business goals and strategies with appropriate methods for technically or operationally protecting data. As business owners determine their requirements for protecting data, policies define the control standards this organization will follow to meet those requirements. Pursuant to Business Policies and Procedures Manual (BPPM) 87.20, Security Assessment and Authorization, information system owners shall prepare a security assessment plan for information systems/services under their care that describes the scope of the assessment and includes:

- The assessment environment, assessment team, and assessment roles and responsibilities,
- the information security and privacy controls under assessment,
- the assessment procedures to be used to determine security control effectiveness,
- an assessment of the information security controls of the information system and its environment of operation at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

2. Scope:

This plan applies to all Washington State University (WSU) information assets owned and/or managed by WSU Business Units.

3. Security Assessment Plan

University business units are to prepare System Assessment Plans for information systems and services for which they are responsible. If additional assessments are required by policy, standard, law, regulation, contract,or data sharing agreement (e.g., risk assessments, data protection impact assessments, penetration tests), they should be included as part of the Security Assessment Plan.

3.1.Phase 1: Define Scope

3.2. Objective

3.2.1. Purpose

- To determine the effectiveness of the implemented security controls in the information system environment being assessed.

3.2.2. Methodology

- Quantitative Analysis and/or Qualitative Analysis. (we will need to develop these methods and processes)

3.2.3. Information Assets

- Identify the information assets that are within the scope of the assessment.

Key Concepts	Definition
Assets	Information system and service resources, data, or other items of value to the organization.
Asset Enumeration	A listing or grouping of assets under assessment. Asset enumeration helps to scope the information security assessment.

3.2.4. Controls

- Determine the required set of information security controls that are within the scope of the assessment. The selected set of security controls are to be based on the classification of the particular systems/data being assessed and applicable policies, standards, laws, regulations, contracts, and data sharing agreements (e.g., EP 8, EP 37, WA State OCIO Standards)

3.2.5. Boundaries

- Identify Physical Boundaries (i.e., Workstations, Servers, Networking Equipment, etc.)
- Identify Logical Boundaries (e.g., Operational, , Production, Test, Development, Data stores etc.

4. Phase 2: Project Preparation

4.1.1. Team Preparation

- Select the assessment team
  - Assessment Team Lead – responsible for leading and coordinating the assessment, producing and distributing the assessment report. THisshould be someone other than the Information System Owner
  - Business Unit Team Lead - Information System Owner or other designated person from the responsible ITS Business Unit to act as a single point of contact for all phases of the assessment.
  - Other designated workforce members as required. Workforce members can be from within the business unit or external to the business unit.

- Request authorization for conducting Security Assessment from a designated Authorizing Official, to include the appropriate permissions and access. (See Authorizing Official in BPPM 87.01, Roles, Responsibilities, and Definitions)

4.1.2. Security Assessment Preparation

- Obtain required authorizations
- Review stated purpose and function of information system and/or service
- Identify systems and data to be assessed
- Map information assets
- Identify set of controls to be assessed

5. Phase 3: Data Gathering

5.1.1. Administrative Data Gathering

- Policies
- Procedures
- Training Processes
- Regulatory/compliance documentation
- Organization
  - Interviews
  - Observations

5.1.2. Technical Data Gathering

- System/network design and architecture documentation
- Configuration management & control baseline documentation
- Security control testing and evidence gathering

6. Phase 4: Data Review and Analysis

Review and analysis of the information collected in the Data Gathering phase (Phase 3).

7. Phase 5: Security Assessment Report

7.1.1. Security Assessment Report

- Executive Summary
- Introduction
  - Scope of the assessment
  - Selection of information security controls
- Assessment Results
  - Assessment methodology
  - Effectiveness of security controls
- Recommendations
- Appendices

7.1.2. Report Distribution

- The security assessment report is to be provided to the Information System Owner, the responsible Business Unit Data Custodian, and the responsible Business Unit Head.

8. Review Cycle:

This guideline is to be reviewed every three years or on an as-needed basis due to changes in information technology environment, business unit operations, policies, standards, or regulatory environments.

Appendix A: Glossary

Acronyms

Acronym	Definition
BPPM	Business Policies and Procedures Man
WSU	Washington State University

Terms

Term	Definition
Quantitative Analysis	An approach for determining the security risk decision variables such as value of an asset, likelihood that a vulnerability will be exploited, the severity of an impact, etc. through a complex computation.
Qualitative Analysis	An approach for determining the security risk decision variables such as value of an asset, likelihood that a vulnerability will be exploited, the severity of an impact, etc. through subjective judgement.
Countermeasures	Also known as safeguards, countermeasures are put in place to reduce the security risk.

Appendix B: Works Cited

The Security Risk Assessment Handbook, 2nd Edition
A Complete Guide for Performing Security Risk Assessments
Douglas J. Landoll