



3000 Landerholm Circle SE • Bellevue, WA 98007-6484 • www.bellevuecollege.edu

IT Security Standard:

Risk Assessment

Introduction

This standard defines the steps needed to implement the Bellevue College IT Security Policy for performing risk assessments on computer systems and application. The standard will be reviewed on an annual basis or when changes are implemented.

Scope

This standard defines specific procedures and requirements for performing risk assessments on computer systems and application. These systems and applications include:

1. Bellevue College network and computing infrastructure: Often these are addressed within the context of the security standard for the specific component. There are also times (for example when introducing some specific new technology into the existing architecture) when a detailed, standalone risk assessment will be performed.
2. Bellevue College procedures and methods: These will be addressed within the context of the procedure for the specific task or in a detailed standalone risk assessment document.
3. Bellevue College developed application and modules: These should be documented in a detailed, standalone risk assessment document, but will, if it is appropriate in the context of the project, be documented within the design document.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat, and Vulnerability Analysis

The impact of not understanding risk is either spending resources where they are not needed or not adequately addressing vulnerabilities and threats to a system. Ultimately, risk assessment provides the analysis necessary to spend precious resources wisely, and consciously accept risks when necessary.

Standard

The Goal

To understand:

1. What we need to protect (the assets).
2. What the likely attack vectors might be (the vulnerability).

3. What or who we must protect them against (the threat).
4. What losses are we likely to incur or willing to accept if an asset is "compromised" (the risk).
5. What can we do to protect the assets from the threat (mitigation) thereby reducing our risk.

This allows us to focus our efforts on implementing security in the most cost-effective fashion.

Requirements

As stated above in the goals, risk assessments are a critical part of the systems analysis phase of any significant project. They are important during the initial design to aid in evaluating the system's security context, as well as during ongoing system use to aid in assuring an appropriate mix of applications and procedures with a networked environment.

The Washington Department of Information Systems (DIS) has also recognized this, and has required risk assessments be formally performed in the following situations:

1. All significant fiscal or mission critical applications and systems.
2. All systems that contain confidential or sensitive information.
3. All Web-based applications. Risk assessments for these applications will identify appropriate authentication, access control, and encryption requirements.

The risk assessment must be filed electronically with the Bellevue College IT Security Administrator or an authorized designee.

Components of a Risk Assessment

Assets

The asset is what we are attempting to protect. A partial list of 'high-level' assets might include:

1. A person's confidential information (identification, health, financial, academic...)
2. A registration
3. A payment receipt
4. A transcript or degree
5. The organization's funds (cash or cash equivalent)
6. Network bandwidth or connectivity
7. Disk and CPU resources
8. The organization's good name

As all assets are not "created equal", the risk assessment will attempt to provide some general ranking to each asset identified. Bellevue College will use the following rating: critical, important, normal.

Vulnerabilities

Vulnerabilities are issues or weaknesses within the application or system architecture that provide an opportunity for someone to attack the system. A partial list of 'high-level' vulnerabilities might include:

1. Flawed human procedures
2. Less than optimal network interface practices
3. Insufficient control on computer access
4. Weak and/or abused version control/ software configuration management procedures
5. Flawed application or database design
6. Weak, missing, and/or incorrectly used audit controls

As all vulnerabilities are not "created equal", the risk assessment will attempt to provide some general ranking to each. Bellevue College will use the following rating: substantial, significant, nominal.

Threat

The threat is the person or condition (e.g., natural disaster) that might cause loss, damage, or compromise of the asset. A partial list of threats might include:

1. Careless administrative staff
2. Unscrupulous contractor
3. Careless students
4. Malicious users of public access terminals (e.g., in the college library)
5. Malicious Internet users
6. Fire, flood, earthquake

Note: It often makes sense to consider the vulnerability and the threat in combination.

As all threats are not "created equal", the risk assessment will attempt to provide some general ranking to each. Bellevue College will use the following rating: substantial, significant, nominal.

Risk

Risk in many ways is the intersection, or product, of the vulnerability and the threat against an asset. It, at its best, is a quantifiable measure of potential loss. It is used to prioritize where to focus resources for protecting assets and considering mitigation, or reduction, of risk. In non-trivial situations, risk will never go away but it can be both understood and managed.

Also, some risks vary over time. That is, after some time passes, the value of the asset decreases or the risk is diminished. For example: The encryption used to protect a password will be sufficient to protect it until the next scheduled change. This is referred to as Time Based Security, and applies in some cases.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Dean of Student Services (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. Bellevue College IT Security Policy
2. Department of Information Services, *Information Technology Standards*, March 2003, Section I.C.1
3. CIS Security Standard—Risk Assessment draft, April 2003.

Effective Date: July 2003
Date Last Modified: July 10, 2009