
Department: UW Medicine Information Technology Services

Policy Number: SEC-09.01 –Risk Assessment Guideline

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

This guideline establishes a common terminology and methodology to use when conducting information security risk assessments which identify potential security risks to UW Medicine Information Systems.

Definitions

- See UW Medicine Information Security policy: SEC-REF UW Medicine Information Security Program Glossary of Terms.

Standard

The Information Risk Assessment includes the following components:

I. Evaluation of Risk to Confidentiality, Integrity, and Availability

The evaluation of the risk to confidentiality, integrity, and availability includes:

- A. The description of the Information System including, documentation of the physical and technical boundaries;
- B. The classification for the System (Please see UW Medicine Information Security Policy; *SEC-02 - Information and Information System Classification*); and
- C. Documentation of other Information Systems, if any, that are dependent on the information in the System being assessed.

II. Threat and Vulnerability Identification and Analysis

- A. **Threat Identification**
System Owners must evaluate and document sources of danger that could significantly impact system or data confidentiality, integrity, and/or availability.

Threat identification requires identifying threat sources as well as associated threat actions. These threats may include internal and external, manual and/or automated attacks.

Likelihood can also be based on University of Washington statistics, industry information, past UW Medicine¹ experience, and/or subject matter expertise.

B. Vulnerability Identification

Technical vulnerabilities are identified either by comparing systems with publicly available lists of vulnerabilities, through vulnerability scanning or a combination of both. Vulnerabilities associated with a process or practices are identified through comparison with industry best practices or through evaluation by subject matter experts. To fully evaluate a threat, associated vulnerabilities must be identified.

System Owners must have a process in place to assess known and relevant vulnerabilities to their Information System(s). System Owners must document known information on patches, updates, reconfiguration, and/or general process improvements.

Publicly available sources for technical vulnerability information:

- Databases, such as the National Institute of Standards and Technology (NIST) I-CAT vulnerability database (<http://icat.nist.gov>) and CERT (<http://www.cert.org/>)
- Vendor advisories (e.g. Microsoft's Security Site)
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)

Internal sources for vulnerability information:

- Utilizing the expertise of UW Medicine Technical User Groups (e.g., TUG), SIT notifications, and/or IT Services Help Desk Notifications

UW Medicine IT Services also conducts vulnerability scanning which assesses a system's ability to withstand intentional attempts to circumvent its security. Its objective is to test the system from the viewpoint of a threat, and to identify potential failures or deficiencies in system security controls.

¹ For the purpose of HIPAA, UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; Hall Health Primary Care Center; UW Medicine Eastside Specialty Center, University of Washington Physicians; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine and the University of Washington Health Care Components are subject to the UW Medicine Information Security Program.

C. Analysis

The analysis is the process by which System Owners use identified threats and vulnerabilities to evaluate the effectiveness of their information system’s controls. This process should assess potential consequences of adverse impact to the information systems resulting from a successful exploitation of vulnerabilities. The analysis should consider the qualitative impact on confidentiality, integrity, and availability. Existence and effectiveness of current controls should be taken into account. When this analysis produces gaps in the controls, the System Owner must take steps to reduce the risk.

The steps to control the risk are classified as either preventive or active and defined as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, filtering and firewall use, implementation to protect against malicious software, and authentication.
- Active controls warn of violations or attempted violations of security policy, and include such controls as audit trails, intrusion detection methods, and integrity checking.

III. Results Documentation

The System Owner must maintain a report describing the outcome of the Risk Assessment Process. Use the Risk Assessment worksheet below to document your threat and vulnerability identification, analysis, and remediation plan for your system.

1. For each threat:
 - a. Document the Potential Impact using the Potential Impact definition table,
 - b. Document the Likelihood using the Likelihood definition table.
2. Use the Risk table to assess the Risk Level for each threat from your assignment of Potential Impact and Likelihood.
3. Any threats with High Risk should be reported to the Security Infrastructure Team via the IT Services Help Desk.
4. The System Owner must document the remediation plan in the Remediation column for each threat that has a Moderate (M) or High (H) Risk level.

Potential Impact Level Definitions		
Low	Moderate	High

Potential Impact Level Definitions		
Low	Moderate	High
The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a limited adverse effect on operations, assets or public image.	The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a serious adverse effect on operations, assets or public image.	The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a severe adverse effect on operations, assets or public image.

Likelihood Level Definitions		
Low	Moderate	High
No one in the community has experienced the threat; existing controls will greatly deter or prevent success of a threat	Threat has been identified in the community, existing controls may impede threat	Confirmed vulnerabilities exploited in the community, existing controls may not be effective

Risk Table			
	Impact		
Likelihood	High	Moderate	Low
High	H	H	M
Moderate	H	M	L
Low	M	L	L

Risk Assessment Worksheet:

Information System Name:			
Information System Classification:			
Examples of threats include, but are not limited to:	Evaluation criteria of the threats include:		Remediation Plan
	Potential impact	Likelihood	Risk
External Individual w/ Malicious Intent <i>Consider the potential for</i>			

<i>unauthorized access, data theft, data destruction, identity theft, financial fraud, impersonation, etc.</i>				
External Individual w/out Malicious Intent <i>Consider the threat potential of unauthorized access, intrusion, resource use, nuisance activity, etc.</i>				
US Competitor or Professional External Individual <i>Consider the potential for authorized use or abuse of confidential information, sabotage, etc.</i>				
Internal Individual w/ Malicious Intent <i>Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.</i>				
Internal Individual w/out Malicious Intent <i>Consider the potential for inadvertent or accidental actions, unintentional errors and omissions (e.g., data entry error, programming error)</i>				
Terminated or Former Internal Individual <i>Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.</i>				
Foreign Entity or				

<p>Terrorist <i>Consider the potential for data loss or corruption, denial/disruption of service, damage to personnel, systems and hardware, etc.</i></p>				
<p>Malicious code or Cyber Incident <i>Consider the potential for data loss or corruption, denial/disruption of service, damage to systems and hardware, etc.</i></p>				
<p>Natural disaster (avalanches, earthquake, fire, flood, land slides, power outage, snow/cold, tornado, tsunami, volcano, wind and other such events) <i>Consider the potential for denial/disruption of service, loss or corruption of data, harm or inconvenience to staff, damage to hardware/facilities, lack of access to facilities, etc.</i></p>				
<p>Epidemic / Hazardous Materials / Weapons of Mass Destruction / Bioterrorism / Mass Casualties Incident <i>Consider the potential for mass injuries and casualties to staff as well as the public)</i></p>				
<p>Environmental <i>Consider the potential for long-term power failure, pollution, chemicals, and liquid leakage)</i></p>				
<p>Other</p>				

References:

- I.** 45 CFR Part 164; Section 164.308(a) (1) (ii) Risk Analysis
- II.** NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems
- III.** National Infrastructure Protection Center; Risk Management: An Essential Guide to Protecting Critical Assets

UW Medicine IT Services: _____ Date: _____
James S. Fine M.D., CIO, ISO
