Cybersecurity Risk Management – Risk Executive Responsibilities

Office of Cybersecurity
CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY
UNIVERSITY OF WISCONSIN-MADISON

I. Know your data…

a. **Classification**: What is the data's assigned classification? What reference is the classification attained from (e.g., derivative or contract means or when additional data sets are introduced to the project or information system)?
b. **Location**: Where is the data normally located (at rest), when moving to or returning from storage to work (in transit), or during work (manipulation or joining with other data).
c. **Access Requirements**: Who is allowed to see or manipulate the data and what are the requirements to access that data.

Data Classification	
UW-Madison	**UWSA**
Restricted	High
Sensitive	High/Moderate
Internal	Moderate/Low
Public	Low

II. What is your Risk Approach?

a. **Risk Averse** – where maintaining systems without risk is the key performance parameter. This approach is costly and labor intensive while ensuring low impact to data and information systems, to include reputational impact to the University.
b. **Risk Managed** – where managing risk as a business process with scale and scope to match the need for availability, integrity, and confidentiality[1]. This approach ensures cost and level of effort are commensurate with the value of the information and IT systems.
c. **Risk Tolerant** – where risk is seen as a natural by-product of work. This approach affords ease of use with initial cost considered lower. Cost will be determined based on the type and quantity of the damage resulting from a data breach or loss of the information system or data.

III. Risk Ratings

All risk is assessed and rated based on the impact to the University. The rating is a function of the likelihood the event will result in damage or loss to an information system and the impact to the availability of the information system or data, loss of integrity to a research project or research data or manipulation of academic or administrative information, or a breach of confidentiality related to; 1) staff or student identity, personal or financial information; 2) healthcare information; 3) research data; or 4) sensitive academic information. Risk ratings are shown in the table to the right.

RISK LEVEL	DESCRIPTION
CRITICAL	Event in progress or significant loss of data and damage to university networks
HIGH	Realized impact to the university
MODERATE	Potential significant impact to the university
LOW	No significant events
NONE	No evidence of risk

IV. The Risk Management Framework

The "Framework" or "RMF" is detailed in the Cybersecurity Risk Management Policy's Implementation Plan and is derived from NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. The RMF consists of the steps shown in the table below.

STEP	ACTIVITY TITLE	DESCRIPTION
0	**Preparation and Planning**	Conducting discovery with the System Owner. Identification of estimated level of effort, schedule and resources.
1	**Categorize the System**	Define the security requirements of the system using the highest classification of data handled. The System Owner must agree with the System Category to move on to the next step.
2	**Select Security Controls**	Assignment of the administrative, physical and technical controls (e.g., NIST 800-53). Alignment with specific compliance programs (i.e., HIPAA, FERPA, EU GDPR, GLBA, etc.)
3	**Implement and Validate Controls**	System Owner and Developers ensure the selected controls are incorporated in the system design, validated to provide the desired protections, and verified as operational.
4	**Risk Assessment**	Independent and documented assessment by the Office of Cybersecurity. Residual risk is determined with mitigating factors applied.
5	**Authorize the System**	A final risk review is conducted with a formal declaration of risk provided by the CISO to the responsible Risk Executive who makes the operational determination.
	SYSTEM IS OPERATIONAL	
6	**Monitor and Mitigate**	The System Owner or the Cybersecurity Operations Center should continually assess the operational controls against evolving vulnerability, threat and impact factors. This step is also known as Continuous Diagnostics and Mitigation (CDM).

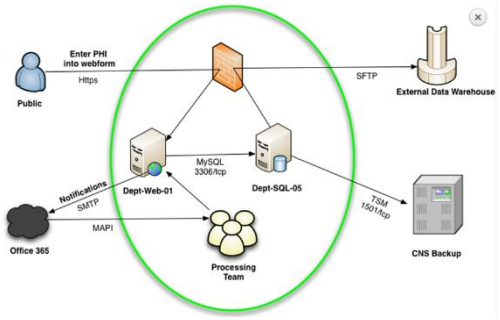
[1] **Availability** - Ensuring timely and reliable access to and use of information; **Integrity** - Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity; **Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U.S.C., Sec. 3542).

This paper is developed by the Office of Cybersecurity and is based on the UW-Madison Cybersecurity Risk Management Policy and Implementation Plan dated March 6, 2018 and approved by the Information Technology Committee of the University Committee of the Faculty Senate.

Cybersecurity Risk Management – Risk Executive Responsibilities

V. The Information System

An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.[i]



Each information system should have a System Security Plan and a security boundary which clearly defines the perimeter of the system and the extent of applicable security controls to be defined and built into the system. The figure to the right shows a simple client-server-based system with the security boundary shown in green.

VI. The Risk Executive

a. **Who**: An executive or director within the campus school, college, division, or functional unit, or in the line of authority above that unit. The Risk Executive must have the authority to accept the risk of operating the system on behalf of the institution and whose school, college, division, or functional unit will be responsible for paying for a breach.
b. **What**: After reviewing the Risk Assessment and recommendations of the Office of Cybersecurity, the Risk Executive will:
   i. accept the risk as certified, or
   ii. assure that recommended action is taken to reduce the risk to an acceptable level, or
   iii. decline to authorize the system to operate.
c. **When**: Risk Executives will be named within 60 days of the Cybersecurity Risk Management Policy being finalized.
d. **Why**: The Risk Executive balances the business needs, the potential financial and reputational cost of adverse events, and the cost to the school, college, division, or functional unit for reducing the likelihood and severity of those events.
e. **How**: The risk of operating the system is accepted by the Risk Executive on behalf of The University. This is a leadership decision and should be based on the following:
   i. Assessed risk and impact to the University should a system be compromised, or data lost.
   ii. Recommended remediation to include consideration for cost to implement.
   iii. Impact on the business process should the system, while in operation, lose availability of the system or data, encounter data integrity issues, or breach confidentiality of Restricted or Sensitive data.

VII. Mitigating Risk – How long should it take?

Critical and High risk must be corrected or mitigated to Moderate within timelines shown. The goal is to drive risk to the lowest level possible as soon as practical.

Assessed Risk Level	Mean Time to Remediate or Mitigate
Critical	As soon as possible - <96 hours
High	As soon as possible <15 calendar days
Moderate	<90 calendar days
Low	Within one year

VIII. Where do you go for help?

TYPE OF HELP NEEDED	CONTACT	PHONE	E-MAIL
Questions specific to your IT system	Your Local IT Support Team		
Challenges and opportunities, access to Risk Register, current RMF package status	Patti Havlicek– Assoc Dir Cybersecurity Risk Management & Compliance	O-262-0039	patti.havlicek@wisc.edu
Operational Cybersecurity issues (vulnerabilities, patching advice, etc.)	Allen Monette – Assoc Director Cybersecurity Operations & Interim CISO	O- 262-8369	allen.monette@wisc.edu
General risk management, security testing, and RMF questions	Risk Management and Compliance (RMC) Team		rmc-cybersecurity@cio.wisc.edu
Data Discovery	Testing and Cyber Defense (TCD) Team	O-262-2337	cybersecurity@cio.wisc.edu
Running vulnerability scans / technical projects	Testing and Cyber Defense (TCD) Team	O-262-2337	cybersecurity@cio.wisc.edu
Cybersecurity engineering assistance	RMC Team		rmc-cybersecurity@cio.wisc.edu
Firewall rule assistance	Cybersecurity Operations Center (CSOC)	O-264-1357	cybersecurity@cio.wisc.edu
Security Education, Training and Awareness	Tim Bohn – SETA Program Manager & Assoc Dir of Business Systems Security	O-262-6272	tim.bohn@wisc.edu
Anything else not covered above…	Jeff Savoy – Chief Information Security Officer	O-262-8369	jeffrey.savoy@wisc.edu

This paper is developed by the Office of Cybersecurity and is based on the UW-Madison Cybersecurity Risk Management Policy and Implementation Plan dated March 6, 2018 and approved by the Information Technology Committee of the University Committee of the Faculty Senate.

Cybersecurity Risk Management – Risk Executive Responsibilities

What information does the Risk Executive receive?

The Office of Cybersecurity will prepare a risk report to summarize the project, software or service requested and the overall risk of us of the data used with this service. This report is a collaboration with the distributed IT team that supports the IT needs of the requestor. This risk report will summarize the request, document the steps taken to review the potential risks and detail the vulnerabilities discovered. The report is presented to the risk executive via one of two channels:

1) Reports which present an overall Low, Low-Moderate or Moderate risk, will be sent via e-mail from Cybersecurity to the Risk Executive for review and acceptance of the risk.
2) Reports which present an overall Moderate-High or High risk will be presented by the Office of Cybersecurity to the Risk Executive in a collaborative meeting to ensure the Risk Executive can consult with their IT team and develop a plan for reducing the overall risk.

The Office of Cybersecurity will request confirmation of the risk acceptance by the Risk Executive via a signature on this report.