Implementation Plan

for the UW-Madison

Cybersecurity Risk Management Policy

August 10, 2017 version

Implementation Plan for the UW-Madison Cybersecurity Risk Management Policy

This working document is the implementation plan for the Cybersecurity Risk Management Policy. The plan will be reviewed by the community, IT governance, and the ITC.

IMPLEMENTATION

The Office of Cybersecurity will maintain a separate and detailed implementation plan that is jointly developed with the System Owner, also known as a System Security Plan, for each information system. The Office of Cybersecurity will assist distributed Information Technology groups with developing implementation plans tailored to their group's needs.

Data Classifications [1]

UW-Madison has classified its institutional data assets into risk based categories for determining who is allowed to access institutional data and what security precautions must be taken to protect it against unauthorized access and use.

Restricted	Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause a significant level of risk to the University, affiliates or research projects. Data should be classified as Restricted if: • protection of the data is required by law or regulation or • UW-Madison is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed
Sensitive	Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause a moderate level of risk to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets or individuals.
Internal	Data should be classified as Internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in some risk to the University, affiliates, or research projects. By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive or Public data should be treated as Internal data.
Public	Data should be classified as Public prior to display on web-sites or once published without access restrictions; and when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates.

[1] From https://data.wisc.edu/data-governance/data-classifications/

Implementation Plan for the UW-Madison Cybersecurity Risk Management Policy

Timeline

With the volume of systems and networks at UW-Madison, a full implementation of the Risk Management Framework will take five years to complete. Implementation will initially focus on systems handling or storing data classified as Restricted, then Sensitive. Since exposure or loss of Internal or Public data does not pose an immediate operational impact or significant financial risk, those information systems will be reviewed as resources allow.

1. Systems with Restricted Data (SSN's, Financial Accounts, HIPAA, …)	2017 +
2. Research systems where grant funding is tied to security requirements	2017 +
3. New or significantly updated systems with Sensitive Data	2019 +
4. Remaining systems with Sensitive Data	2020 +
5. Systems that only handle Internal Data	2021 +
6. Systems that only handle Public Data	2022 +

Throughout the implementation period, systems of all kinds will benefit from advanced firewalls and network protections as those capabilities are further deployed. Public facing web servers will be monitored on a monthly basis for unwanted traffic, evidence of cyber-attack or potentially harmful data loss activity to ensure openly accessible data is protected.

Training

Training on the processes, tools and use of or completion of artifacts will be provided by the Office of Cybersecurity with the details considered to be out of scope for this document. Ongoing security awareness training will be provided and access to training tools will be widely publicized on the Office of Cybersecurity web pages (https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/).

PROCESS FOR MANAGING CYBERSECURITY RISK

This section describes process specific activities necessary to carry out the Cybersecurity Risk Management Policy. The process steps summarized below are required by the policy. Amplification of process steps and a helpful background on the Risk Management Framework (RMF) are in the Appendix to this Implementation Plan.

Risk Register

Information systems proposed to undergo Risk Assessment are entered into the Risk Register managed by the Office of Cybersecurity. A Risk Analyst will be assigned as resources become available. Organizations desiring to accelerate the process can contact the Chief Information Security Officer for guidance and options for meeting Risk Analyst resource requirements.

1. **Assess Risk** (RMF Step 4)

The academic / functional unit and the Office of Cybersecurity cooperatively assess the cybersecurity risk associated with a system.

2. **Certify Risk** (RMF Step 5)

The UW-Madison Chief Information Security Officer (CISO) signs the Risk Assessment to certify that the represented risk is accurate. The CISO may include recommended risk reduction strategies.

3. **Accept Risk** (RMF Step 5)

The risk of operating the system is accepted by the Risk Executive on behalf of UW-Madison. This is a leadership decision and should be based on the following:

a. Assessed risk and impact to the University should a system be compromised or data lost
b. Recommended remediation to include consideration for cost to implement
c. 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.
d. The Risk Executive role is guided by the following:
   (1) Risk Executives will be named within 60 days of the Cybersecurity Risk Management Policy being finalized.
   (2) The Risk Executive should be an executive or director (e.g., Dean or their appointee, department chair, director of a research lab, etc.) within the academic / 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 should be in the unit who will ultimately be responsible for paying for a breech (i.e., Dean or their appointee, department, research lab, etc.).
   (3) The Risk Executive balances the business needs, the potential financial and reputational cost of adverse events, and the cost of reducing the likelihood and severity of those events.
   (4) Delegation of the Risk Executive role is not encouraged. If delegation of the work is made under the Risk Executive's authority, the responsibility will not.
   (5) Risk Executives may access the expertise, training and support available from the Office of Cybersecurity for advice in making their risk determination or for additional guidance.
   (6) The Risk Executive must be afforded a sufficient understanding of the information system through the technical experts and managers associated with the system. After reviewing the Risk Assessment and recommendations of the Office of Cybersecurity, the Risk Executive will:
      a) accept the risk as certified, or
      b) assure that recommended action is taken to reduce the risk to an acceptable level, or
      c) decline to authorize the system to operate.

4. **Reduce Risk** (RMF Step 5 and 6)

The acceptable level of risk may be constrained by legal, regulatory or contractual requirements, and is subject to review by university leadership.

If the certified level of risk is unacceptable:

a. The Risk Executive assures that changes are made to the system that reduce the risk to an acceptable level.
b. The assessment and certification described in *Assess Risk* and *Certify Risk* are revised following confirmation of corrective actions. The reduced level of risk is then accepted as described in *Accept Risk*.

Following the Risk Assessment and subsequent acceptance by the Risk Executive, information systems with vulnerability, threat and impact changes that elevate the level of risk will have to be corrected or mitigated back to the assessed level (or lower) within the following time limits:

a. Issues that elevate the risk level to Critical should be corrected or mitigated to no greater than High within 72 – 96 hours or the system should be disconnected.
b. Issues that elevate the risk to High should be corrected or mitigated to Moderate within 15 calendar days.
c. Issues that elevate the risk to Moderate should be corrected or mitigated to Low within 90 calendar days.
d. If the issue occurs on a system evaluated at Low risk, but does not elevate the risk to Medium, it should be corrected within one year.

In all cases, the Risk Register maintained by the office of Cybersecurity should be updated along with adjusting the existing risk assessment and plan of action and milestones.

5. **Monitor Risk** (RMF Step 6)

The academic / functional unit and the Office of Cybersecurity continually monitor the system to assure that the level of risk remains at or below the level accepted in *Accept Risk*.

a. There must be policy and procedural safeguards to assure that monitoring activity respects privacy and academic freedom.
b. The design and implementation of monitoring is included in the assessment and certification described in *Assess Risk* and *Certify Risk*. Monitoring must be designed and implemented to, at a minimum:
    (1) detect known security vulnerabilities and threats, and
    (2) detect known indications that the system may be compromised;
c. Where the identified problems are individually or collectively significant enough to increase the level of risk above the level accepted in *Accept Risk*. Identified problems must be sufficiently mitigated to return the level of risk to the level accepted in *Accept Risk*.

6. **Re-evaluate Risk** (RMF Step 6)

Risk evaluation occurs throughout the system life cycle as follows:

a. The schedule for risk evaluation is part of the assessment and certification described in *Assess Risk* and *Certify Risk*. A typical schedule includes a formal evaluation every three years and an informal evaluation annually.
b. Change management is part of the assessment and certification described in *Assess Risk* and *Certify Risk*. Changes to the system that increase risk may require more immediate evaluation.
c. Following an evaluation, the assessment and certification described in *Assess Risk* and *Certify Risk* are revised, the risk is accepted or reduced as described in *Accept Risk* and *Reduce Risk*, and monitoring continues as described in *Monitor Risk*.

Special cases

Non-UW-Madison-owned devices and services used for university business may be treated as part of a UW-Madison information system, and if so, are subject to this policy. There must be policy and procedural controls in place to assure respect for property and privacy.

CONTACT

Questions and comments to this document can be directed to the Office of Cybersecurity at cybersecurity@cio.wisc.edu.

HELPFUL REFERENCES

UW-Madison Cybersecurity Risk Management Procedures website [under development], https://it.wisc.edu/about/office-of-the-cio/cybersecurity/risk-management-framework/]

National Institute for Standards and Technology Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

National Institute for Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems, and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute for Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Controlled Unclassified Information (32 CFR Part 2002), https://www.gpo.gov/fdsys/pkg/FR-2015-05-08/pdf/2015-10260.pdf

Appendix - UW-Madison Cybersecurity Risk Management Framework

BACKGROUND

Risk is defined as the measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence[2].

Cybersecurity risk may be presented from external sources or by individual actions of those working inside the network or information systems. The concept of cybersecurity risk includes operational risk to information and technology assets that have consequences affecting the availability, integrity or confidentiality, of information or information systems. This includes the resulting impact from physical or technical threats and vulnerabilities in networks, computers, programs and data. The data focus includes information flowing from or enabled by connections to digital infrastructure, information systems, or industrial control systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance[3]. The process described in this policy is a tool used to arrive at an understanding of risk involving information systems. Risk can be modeled as the likelihood of adverse events over a period of time, multiplied by the potential impact of those events. Risk is never reduced to zero. There is always a level of risk that must be accepted as a cost of doing business. Reducing the risk to an acceptable level is also a cost of doing business.

Systems are monitored to assure that the level of cybersecurity risk is maintained at or below an acceptable level. There are policy and procedural safeguards to assure that personal privacy and academic freedom are respected. The content or use of the data is only of interest to the extent that it indicates the presence of a vulnerability or threat, such as incoming data that is part of an attack on university systems, or outgoing data that indicates a system has already been compromised. University or personal data that is stolen by an attacker is no longer private. Scrupulous monitoring helps protect data from unscrupulous use.

THE INFORMATION SYSTEM

An information system can be defined as 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.[4] Each information system should include a security boundary which clearly defines the perimeter of the system and the extent of applicable security controls

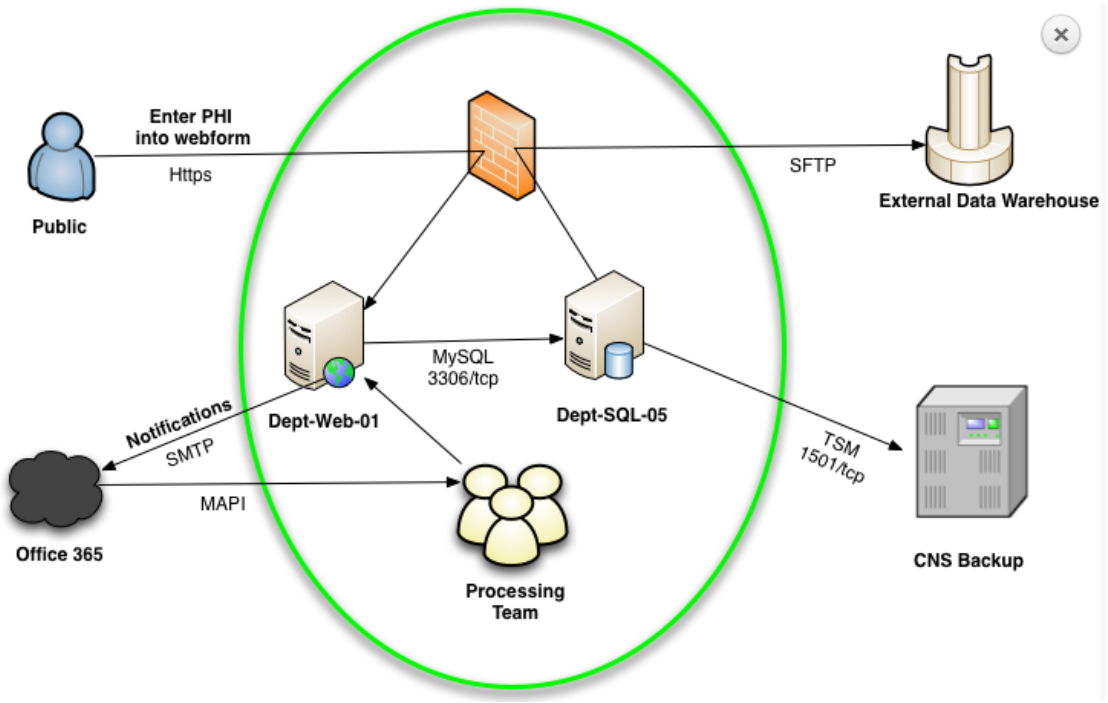
[2] From NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*, dated May 2013

[3] From *A Taxonomy of Operational Cyber Security Risks* by James Cebula and Lisa Young, Carnegie-Mellon University Software Engineering Institute, dated December 2010.

[4] From NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*, dated May 2013

to be defined and built in to the system. Figure 1 below[5] shows a simple client-server based system with the security boundary shown in green.

Figure 1: The System Security Boundary



The System Security Plan should address the hardware, software, security controls, and administrative or configuration issues associated with security the system and the data within that boundary. The plan should also describe the interactions with adjacent systems and networks and, where necessary, describe the security controls that protect access and secure the data.

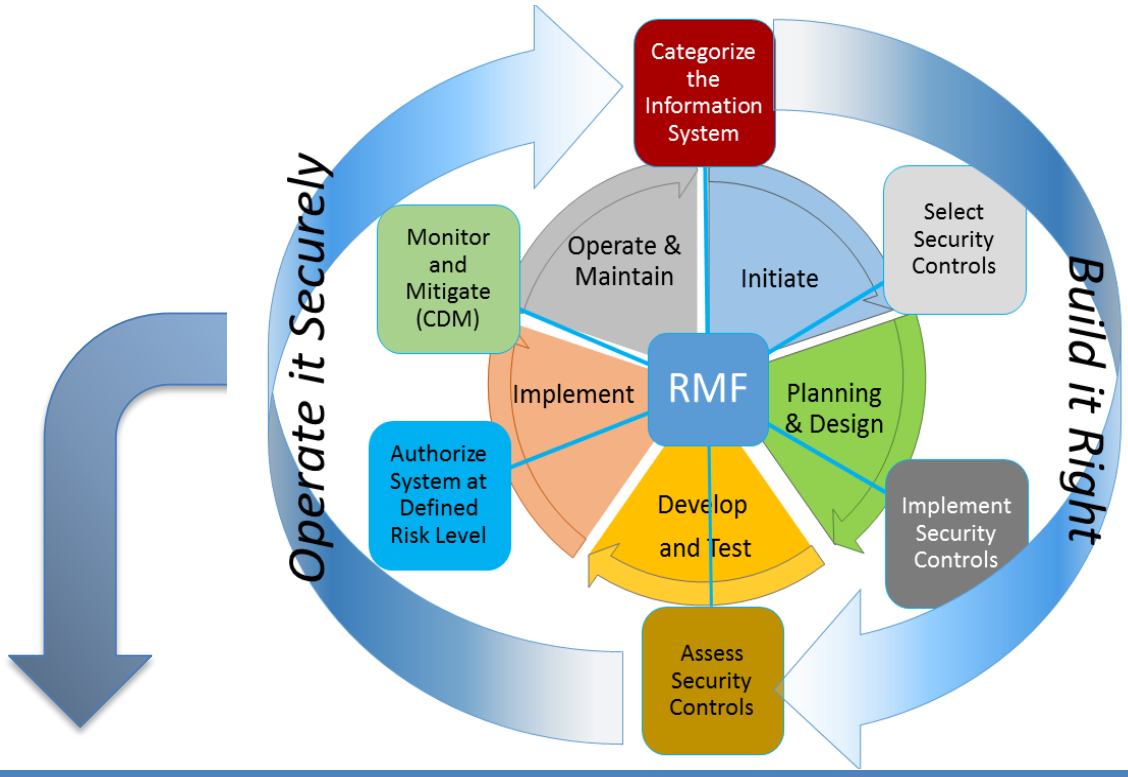
RISK MANAGEMENT FRAMEWORK

The Risk Management Framework, also called the RMF, is derived from the National Institute for Standards and Technology Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and specifically tailored to meet the requirements and culture at UW-Madison. This document describes the RMF processes and implementation details and serves as a guide to determining cybersecurity risk to information systems and network architectures. The UW-Madison Cybersecurity Risk Management Framework is designed to provide departmental directors, researchers, and information technologists with a tool to determine risk to data and operations of each network or system connected to or serviced by the campus information technology architecture. The RMF consists of six steps that guide the development of a system with information security controls built in. Once development is completed, a formal risk

[5] From University of Florida article *Creating an Information System/Data Flow Diagram* found at https://security.ufl.edu/it-workers/risk-assessment/creating-an-information-systemdata-flow-diagram/

assessment and continued operating checks ensure maintenance of defined risk levels. The tables and graphic below describe the steps:

Figure 2: The Risk Management Framework



Step	Activity Title	Description
Pre	Planning	Conducting discovery with the System Owner to aid in their understanding of the RMF and associated tools and processes. Identification of time and resources occurs here.
1	Categorize the System	A data driven process where the security requirements of the system are defined by the highest classification of data handled by, or stored within, the system or processes
2	Select Security Controls	Assignment of the administrative, physical and technical controls required to protect the data are drawn from an agreed security controls framework (e.g., NIST 800-53)
3	Implement and Validate Controls	During design and development, the selected controls are incorporated in the system design, validated to provide the desired protections, and verified as operational.

Appendix - UW-Madison Cybersecurity Risk Management Framework

Step	Activity Title	Description
4	Risk Assessment	Independent to the development team, a documented assessment is performed to test the selected controls. Residual risk is determined with mitigating factors applied. This stage leads to a formal declaration of risk for the system or network.
5	Authorize the System	A final risk review is conducted with a formal declaration of risk provided to the responsible Risk Executive who makes the determination whether to (1) operate the system at the defined risk level; (2) further mitigate risk; or (3) decline to allow continued operation.
System is Operational		
6	Monitor and Mitigate	Continually assess the operational controls against evolving vulnerability, threat and impact factors. Disruption to operations or loss of data occurs when controls fail, system upgrades occur without proper testing or external factors dictate, determine and implement mitigating controls or return the system to an earlier RMF step. This step is also known as Continuous Diagnostics and Mitigation.

The RMF aligns with the system development life cycle and requires input documentation and information for each step. Output artifacts are produced that are used in planning, development and testing, and certification of risk leading to implementation as shown in the table below.

Step	Activity Title	Project Phase	Input Documents and Activities	Output Documents and Activities
1	Categorize the System	Planning and Design	• Data definition including Classification • FISMA determination from Contract • Data description • System description from SDLC • CIS Benchmarks	• Cybersecurity Project Charter • System Security Plan (SSP) Questionnaire checklist • Data Security Triage Form • IT Security Baseline for Research and Academic Computing Template • Interview Checklist(s): e.g., FISMA Controls, HIPPA Test Plan, SA Checklist
2	Select Security Controls		• Complete and Validated SSP Questionnaire checklist	• Security Controls Inventory

Appendix - UW-Madison Cybersecurity Risk Management Framework

Step	Activity Title	Project Phase	Input Documents and Activities	Output Documents and Activities

3	Implement and Validate Controls	Develop and Test	• Configure Security Controls as determined.	• Completed Package Artifacts
				  ○ SSP
				  ○ Topology, Data Flow, System Security Boundary
				  ○ Ports & Protocols Table
				• Security Controls Workbook (Pre-Assessment)
				• Submitted Cybersecurity Risk Acceptance Request Form

4	Risk Assessment		• Provide All Audit Scan (host based scans & application based testing) • Completed Security Controls Checklist validated by scanning and manual review • Develop and Execute Testing Plans (Artifacts not provided will be created by the Office of Cybersecurity) • Step Three Deliverables	• Scanning tool (i.e., Qualys) generated Risk Assessment Report plus Analyst notes • Executed CCI and NIST checklists • Updated systems POAM • Validated Step Three Artifacts • Residual Risk Report
5	Authorize System	Implement	• Residual Risk Report • Step Four deliverables	• Chief Information Security Officer signed Risk Letter plus Risk Executive's Endorsement/Approval to Operate
Project Handoff to Operations				
6	Mitigate and Monitor	Operate	• Approved scanning tool • Control Validation Plan • Step Five deliverables	• Provide Monthly Risk Reports & POAM updates • Security Control Validation Report