Implementation Plan
for the University of Wisconsin-Madison Cybersecurity Risk Management Policy

January 15, 2018

as approved by the Information Technology Committee on January 19, 2018.

Implementation Plan for the University of Wisconsin-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, Information Technology (IT) governance, and the IT Committee.

IMPLEMENTATION

For each information system, 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. The Office of Cybersecurity will assist distributed Information Technology groups with developing implementation plans tailored to their group's needs.

Data Classifications [1]

The University 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 • The University is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed or disclosed
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 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 University of Wisconsin-Madison Cybersecurity Risk Management Policy

Risk Levels

Risk is attributed to assets based on the analysis of multiple factors which influence the Availability, Integrity or Confidentiality (AIC) of the asset.

Factors include:

- threats posed to that asset
- the vulnerabilities that expose the asset
- the impact to any of the UW-Madison mission, values or guiding principles and
- the likelihood that the availability, integrity or confidentiality of the asset will be compromised through a given vulnerability by a threat actor.

In a quasi-equation format:

[Risk(to AIC of an asset), (from a threat-vulnerability pairing)] = [the Likelihood of exploitation in a given time frame] X [the impact of such exploitation]

Incidents are categorized based on the severity of potential or actual impact to the university. The graphic below shows the color code as used in the Weekly IT Security Report provided to the University CIO and interested University leadership. Color codes are supported by a short narrative statement that summarizes the major impact of the incident.

Risk Rating Color Code

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

Please consult the Office of Cybersecurity if a more detailed discussion is needed or for assistance in the development of a tailored impact score matrix, as well as the building of a Risk Register (not shown) from the resulting scoring.

Risk Registration

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.

Timeline

With the volume of systems and networks at the University, a full implementation of the Risk Management Framework will take approximately 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.

PRIORITY	CATEGORY	TIMEFRAME

1	Systems with Restricted Data (PII/SSN's, Financial Accounts, HIPAA)	2017 through 2018
2	Research systems where grant funding is tied to security requirements	2017 through 2019 and ongoing
3	New or significantly updated systems with Sensitive Data	2019 - 2020
4	Remaining systems with Sensitive Data	2020 - 2021 and ongoing
5	Systems that only handle Internal Data	2021 - 2022 and ongoing
6	Systems that only handle Public Data	2022 and ongoing

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 by the Security Education, Training and Awareness Lead 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/).

Training for Risk Executives will be provided by the Chief Information Security Officer on an individual or group basis depending on the need and executive schedules. Training is tailored to the Risk Executive's needs and will include the items in the Step 5 Accept Risk section, including review of RMF packages aligned with the Risk Executive areas of responsibility.

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 Appendix A to this Implementation Plan.

Preparation for Risk Assessment

The first three steps of the Risk Management Framework (RMF) prepare the information system for a certifiable risk assessment. As shown in Appendix A, an information system is categorized according to the potential impact should the availability, integrity or confidentially of the system or data be compromised, (RMF Step 1.) Security controls are selected to reduce the likelihood and impact of a compromise, (RMF Step 2.) The security controls are implemented, then tested to measure how well they are functioning, (RMF Step 3.) At this point the information system is ready for a certifiable risk assessment.

Assessing, Accepting and Monitoring Risk

The Cybersecurity Risk Management Policy focuses on the final three steps of the RMF. The following describes the process which is mandated by the policy.

Implementation Plan for the University of Wisconsin-Madison Cybersecurity Risk Management Policy

A. Assess Risk (RMF Step 4)

The academic / functional unit and the Office of Cybersecurity cooperatively assess the cybersecurity risk associated with a system and if needed, consultation with other experts on campus.

B. Certify Risk (RMF Step 5)

The University 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.

C. Accept Risk (RMF Step 5)

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:

1. Assessed risk and impact to the University should a system be compromised or data lost.
2. Recommended remediation to include consideration for cost to implement.
3. 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.
4. The Risk Executive role is guided by the following:
    a. Risk Executives will be named within 60 days of the Cybersecurity Risk Management Policy being finalized. The initial list of Risk Executives will be the executives who reported IT spending for their unit as part of the second “IT Spend” report. The units reporting are listed in Appendix B to this implementation plan.
    b. 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.)
    c. Delegation of the Risk Executive role is not encouraged. If delegation of the work is made under the Risk Executive’s authority, the Risk Executive remains accountable for the outcomes .
    d. 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.
    e. The Risk Executive must be afforded a sufficient understanding of the information system through the technical experts and managers associated with the system.
    f. 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.
    g. After reviewing the Risk Assessment and recommendations of the Office of Cybersecurity, the Risk Executive will:
        1) accept the risk as certified, or
        2) assure that recommended action is taken to reduce the risk to an acceptable level, or

3) decline to authorize the system to operate.

h. Training for Risk Executives will be provided by the Chief Information Security Officer on an individual or group basis depending on the need and executive schedules. Training is tailored to the Risk Executive's needs and will include the items in 4.a. through g. above and will include review of a representative RMF package.

D. **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:

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

1. 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.
2. Issues that elevate the risk to High should be corrected or mitigated to Moderate within 15 calendar days.
3. Issues that elevate the risk to Moderate should be corrected or mitigated to Low within 90 calendar days.
4. 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.

E. **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 *C. Accept Risk*.

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

F. Re-evaluate Risk (RMF Step 6)

Risk evaluation occurs throughout the system life cycle as follows:

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

Special cases

Non-University-owned devices and services used for university business may be treated as part of a University 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.

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 A – University of Wisconsin-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. Risk ratings are driven by the Risk Assessment Tool which assigns values to threats, vulnerabilities, and likelihood of exploitation to determine risk.

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.

INTERNAL AND EXTERNAL THREAT, VULNERABILITY, AND LIKELIHOOD

Threat, vulnerability and likelihood of exploitation are complex and unique to specific business processes and technology. Cybersecurity risk is measurable depending on quantified or classified aspects of the data; characteristics of the information system; the definitions and characteristics of internal or external threat, system or environmental vulnerabilities; and the likelihood that the event or situation may manifest itself within a given application, information system or architecture. Internal threats can be accidental or intentional. Vulnerabilities are normally discovered outside of the information environment and reported by trusted sources and characterized against industry norms. The likelihood an event may take place is dependent

[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.

on the broader spectrum of people, technology and procedures in place to counter the threat and address the vulnerability.

The table below shows broad definitions of cybersecurity issues and the potential risk level that may be assigned to information systems using the Risk Management Framework.

DESCRIPTION	RISK LEVEL
ROOT-LEVEL INTRUSION: AN UNAUTHORIZED PERSON GAINED ROOT-LEVEL ACCESS/PRIVILEGES ON A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK DEVICE.	**High**
USER-LEVEL INTRUSION: AN UNAUTHORIZED PERSON GAINED USER-LEVEL PRIVILEGES ON A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK DEVICE.	**High**
ATTEMPTED ACCESS: AN UNAUTHORIZED PERSON SPECIFICALLY TARGETED A SERVICE/VULNERABILITY ON A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK DEVICE IN AN ATTEMPT TO GAIN UNAUTHORIZED OR INCREASED ACCESS/PRIVILEGES, BUT WAS DENIED ACCESS.	**Moderate**
DENIAL OF SERVICE (DOS): USE OF A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK WAS DENIED DUE TO AN OVERWHELMING VOLUME OF UNAUTHORIZED NETWORK TRAFFIC. DOS ACTIVITY MAY BE REPORTED AS HIGH RISK IF A SIGNIFICANT SEGMENT OF THE UNIVERSITY'S NETWORKS ARE DISABLED OR IF DESIGNATED CRITICAL INFRASTRUCTURE / KEY RESOURCES ARE TAKEN OFF-LINE.	**Moderate**
POOR SECURITY PRACTICE: A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK WAS INCORRECTLY CONFIGURED OR A USER DID NOT FOLLOW ESTABLISHED POLICY. THIS ACTIVITY MAY BE RATED AS MODERATE OR HIGH IF THE PRACTICE RESULTED IN SIGNIFICANT LOSS OF DATA OR DENIAL OF SERVICE.	**Low**
SCAN/PROBE: OPEN PORTS ON A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK DEVICE WERE SCANNED WITH NO DOS OR MISSION IMPACT.	**Low**
MALICIOUS CODE (MALWARE): HOSTILE CODE SUCCESSFULLY INFECTED A UNIVERSITY COMPUTER/INFORMATION SYSTEM/NETWORK DEVICE. UNLESS OTHERWISE DIRECTED, ONLY THOSE COMPUTERS THAT WERE INFECTED WILL BE REPORTED AS A MODERATE RISK INCIDENT UNLESS THE MALWARE HAS DISABLED A COMPLETE INFORMATION SYSTEM OR SIGNIFICANT SEGMENT OF THE UNIVERSITY'S NETWORK.	**Moderate**
SUSPICIOUS ACTIVITY (INVESTIGATION): ANY IDENTIFIED SUSPICIOUS ACTIVITY. THE EVENT WILL BE INVESTIGATED AS LOW RISK, AND EITHER DISMISSED OR CATEGORIZED AS ONE OF THE ABOVE TYPES OF ACTIVITY.	**Low**
EXPLAINED ANOMALY: AUTHORIZED NETWORK ACTIVITY.	**None**

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 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.

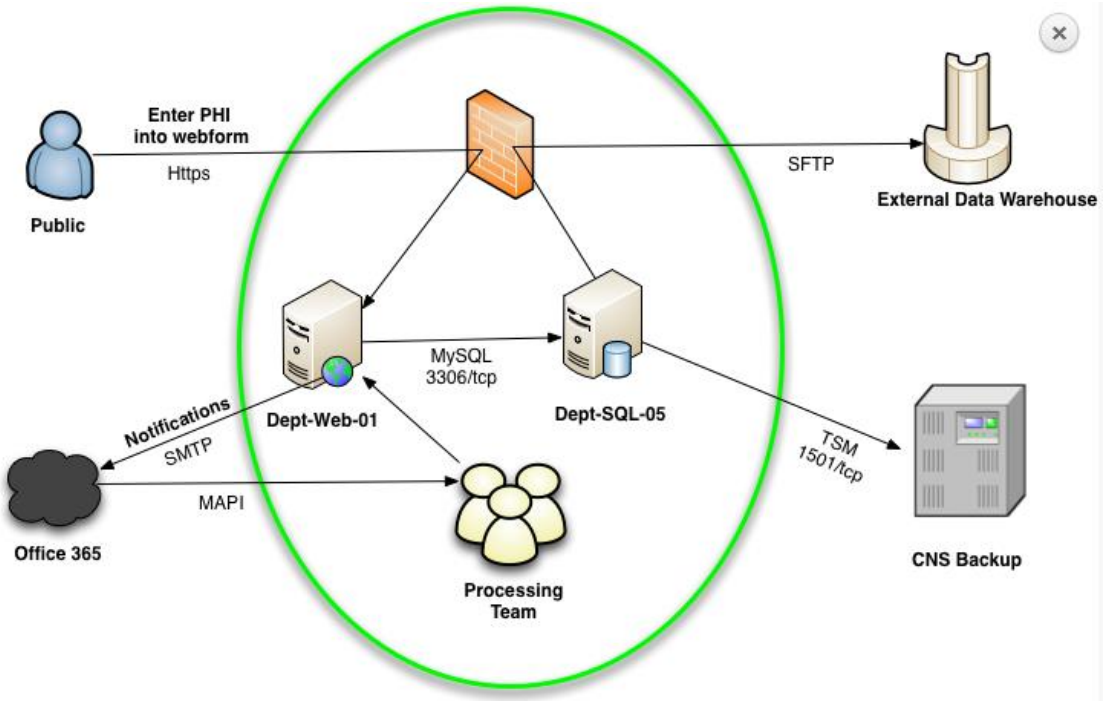

Figure 1: The System Security Boundary

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 University of Wisconsin-Madison Cybersecurity Risk Management Framework is designed to provide departmental directors and managers, 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 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 the University. This section describes the RMF

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

[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/

processes and implementation details and serves as a guide to determining cybersecurity risk to information systems and network architectures. 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 assessment and continued operating checks ensure maintenance of defined risk levels. The tables and graphic below describe the steps:

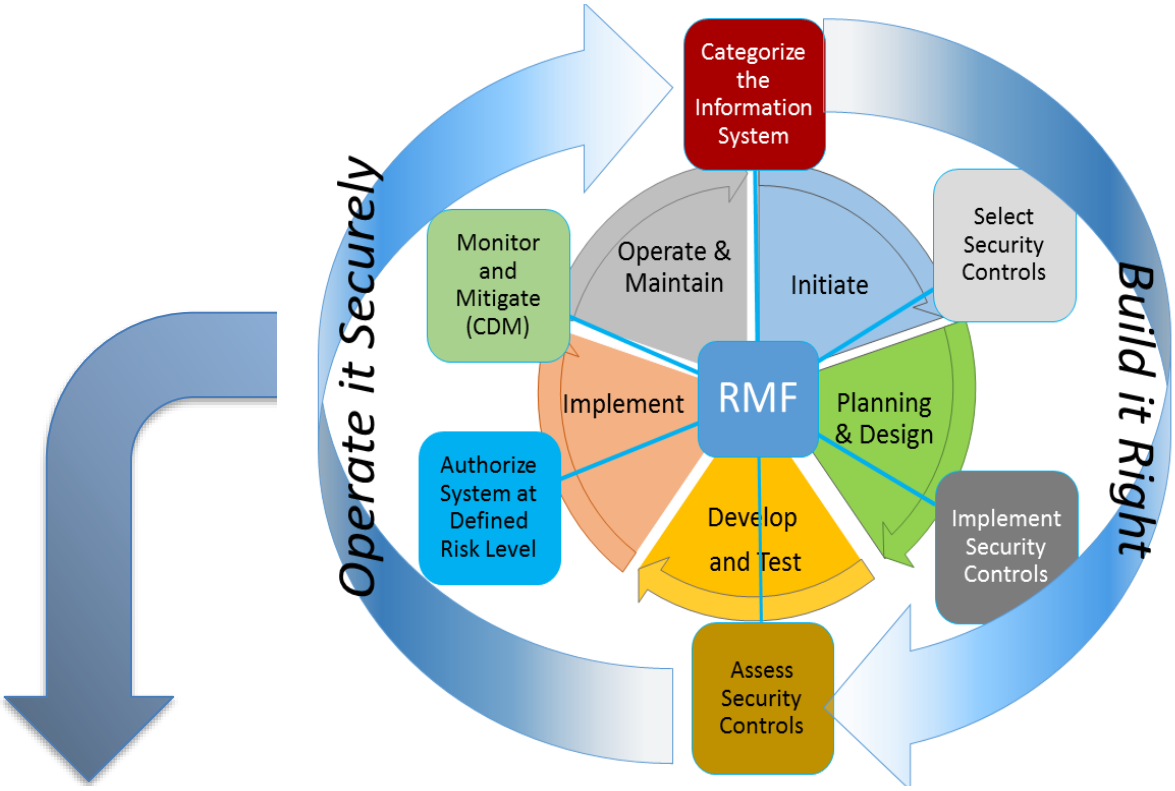

Figure 2: The Risk Management Framework

Steps within 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 estimated level of effort, schedule and resources occurs here.
1	Categorize the System	A data driven and collaborative 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. 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 required to protect the data are drawn from an agreed security controls framework (e.g., NIST 800-53). Alignment with specific compliance programs (i.e., HIPAA, FERPA, EU GDPR, GLBA, etc.) is necessary to ensure accuracy. The

Appendix A – University of Wisconsin-Madison Cybersecurity Risk Management Framework

STEP	ACTIVITY TITLE	DESCRIPTION
		proper controls are selected by the Risk Analyst in consultation with the System Owner. Controls that are not attainable will be accompanied by a suitable mitigation or explanation from the System Owner will be recorded.
3	Implement and Validate Controls	During design and development, the System Owner and Developers ensure the selected controls are incorporated in the system design, validated to provide the desired protections, and verified as operational. Consulting services from the Office of Cybersecurity are available as resources allow.
4	Risk Assessment	Independent of the development team, the Office of Cybersecurity conducts a documented assessment 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 by the CISO 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	The System Owner or the Cybersecurity Operations Center should 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 (CDM).

As shown in the table below, 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

Appendix A – University of Wisconsin-Madison Cybersecurity Risk Management Framework

STEP	ACTIVITY TITLE	PROJECT PHASE	INPUT DOCUMENTS AND ACTIVITIES	OUTPUT DOCUMENTS AND ACTIVITIES
				• 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

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

STEP	ACTIVITY TITLE	PROJECT PHASE	INPUT DOCUMENTS AND ACTIVITIES	OUTPUT DOCUMENTS AND ACTIVITIES
		PROJECT HANDOFF TO OPERATIONS		
6	Mitigate and Monitor (CDM)	Operate	• Approved scanning tool • Control Validation Plan • Step Five deliverables	• Provide Monthly Risk Reports & POAM updates • Security Control Validation Report

LEVEL OF EFFORT

The time to complete each step within the RMF depends on the data classification, information system size, and technical complexity. Each system will be assigned a Risk Analyst from the Office of Cybersecurity who will consult with and assist the technical teams, developers, system owners, business process owners, IT managers and Risk Executives in navigating the process. The tables below show a rough estimate of the level of effort for the assigned Risk Analyst for the overall risk assessment effort including all steps in the RMF. Level of effort and time to complete the process should be determined collaboratively at the onset of the project and is the responsibility of the system owner.

The Office of Cybersecurity has limited resources to assist and each engagement would be determined on when assets are available using a "best effort" approach. The table below shows an estimated level of effort based on the type of service needed and the relative size of the information system. This level of effort is contact time with the project only, not calendar hours or days necessary to gather all information, delays due to scheduling challenges, hand off time between reviews, or holiday and weekend hold time. The term "assets" encompasses host terminals, servers, switches, routers, firewalls, intrusion detection or protection systems or peripherals. When defining a system, including all active components that primarily security related is required to properly set the scope of the effort.

SERVICE	SYSTEM SIZE	# ASSETS	LABOR REQUIRED	LOE HOURS
CONSULTING SUPPORT	Small	1 – 5	1 Consultant	40
	Medium	6 – 15	1 Consultant	60
	Large	16 – 50	1 Consultant	60 - 80
	Extra Large	50+	1 Consultant 1 Specialist	120+
CONSULTING AND ASSISTANCE IN DEVELOPING SYSTEM SECURITY PLAN AND ARTIFACTS	Small	1 – 5	1 Consultant	60
	Medium	6-15	1 Consultant	80
	Large	16 – 30	1 Consultant	160
	Extra Large	30+	1 Consultant 1 Specialist	200+
CONSULTANT SUPPORT LABOR WITH SSP ARTIFACTS AND FULL TESTING SUPPORT	Small	1 – 5	1 Consultant 1 Specialist	120
	Medium	6-15	2 Consultants	200
	Large	16 – 50	2 Consultants 1 Specialist	300
	Extra Large	50+	2 Consultant	500+

Appendix A – University of Wisconsin-Madison Cybersecurity Risk Management Framework

SERVICE	SYSTEM SIZE	# ASSETS	LABOR REQUIRED	LOE HOURS
			2-3 Specialists	
CYBERSECURITY ARCHITECTURE AND ENGINEERING	Small	1 – 5	1 Consultant 1 Specialist	Project Dependent
	Medium	6-15	2 Consultants	
	Large	16 – 30	2 Consultants 1 Specialist	
	Extra Large	30+	1 Consultant 2+ Specialists	

The time estimated within each step of the RMF is shown in the table below and reflects a rough estimate of calendar days, weeks or months to process through each step given information is available and testing windows can be scheduled. Time to obtain a Risk Executive Signature is wholly dependent on the organization and the System Owner communications with the Risk Executive.

STEP WITHIN RMF	SYSTEM SIZE	ESTIMATED HOURS OR DAYS WITHIN EACH STEP
PLANNING	Small	2 weeks
	Medium	2 weeks
	Large	2 – 3 weeks
	Extra Large	2 – 3 weeks
STEP 1: CATEGORIZE THE SYSTEM	Small	1 day
	Medium	1 day
	Large	1 day
	Extra Large	2 days
STEP 2: SELECT SECURITY CONTROLS	Small	1 day
	Medium	1 day
	Large	2 days
	Extra Large	1 week
STEP 3: IMPLEMENT AND VALIDATE CONTROLS	Small	System Owner and Project Team dependent
	Medium	
	Large	
	Extra Large	
STEP 4: RISK ASSESSMENT	Small	2 days (depending on test duration needed)
	Medium	<5 days (depending on test duration needed)
	Large	1.5-2 weeks (depending on test duration needed)
	Extra Large	>2 weeks (depending on test duration needed)

Appendix A – University of Wisconsin-Madison Cybersecurity Risk Management Framework

STEP WITHIN RMF	SYSTEM SIZE	ESTIMATED HOURS OR DAYS WITHIN EACH STEP
STEP 5: AUTHORIZE THE SYSTEM (PRESENTATION AND CISO SIGNATURE	Small	<1 day
	Medium	1 day
	Large	<2 days
	Extra Large	2 days
STEP 5: AUTHORIZE THE SYSTEM (RISK EXECUTIVE SIGNATURE)	Small	<1 day
	Medium	1 day
	Large	<2 days
	Extra Large	2 days

A full description of each service and activities that take place in each step of the RMF along with information on the related cost is available upon request from the Office of Cybersecurity.

SECURITY CONTROL INHERITANCE

For most information systems and applications, there are security controls that can be inherited from the surrounding infrastructure or adjacent business processes or systems within the architecture. System Owners and Risk Executives should consider a security control as "inheritable" if it is a verified security asset. Much like an inheritance receive from the death of a relative, it's not real until it has been verified to exist and is functioning.

Information Systems "**inherit**" controls **from** an architecture or program like a child inherits heirlooms, property or money from a parent. **System owners can allow "inheritance**" of a security control **to** another architecture much as the deceased addressed the disposition of their earthly items in their Last Will and Testament. When an information system allows a control to be "inherited" and used by another system or architecture, the "parent" System Owner is responsible for keeping the control functioning – including making available to the "child" System Owner a record of periodic verification of that control.

Finally, the inherited control has to be appropriate for the system or architecture. For example, inheriting multi-factor authenticator management from the current UW System Human Resources System (HRS) which is using Symantec Multi-factor Authentication (MFA) and applying that control to a research data warehouse system where we want to have Duo MFA in place is, by rote, a control you cannot inherit where inheriting the availability of backup power supplied to a data center can cover a broad group of systems if housed within that data center.

Inherited security controls should be clearly marked within the Risk Assessment Tool and the Plan of Action and Milestones for the information system.

Appendix B – Initial List of Risk Executives

The following is the initial list of University units that should appoint Risk Executives for the Implementation Plan for the University of Wisconsin-Madison Cybersecurity Risk Management Policy. This includes Deans, Directors, and other leaders of high level university divisions and institutes.

A01 General Education Admin

A02 General Services, AIMS

A03 Business Services

A04 Division of Student Life

A05 Enrollment Management

A06 Division of Information Technology (DoIT)

A07 College of Agriculture and Life Sciences

A10 International Division

A12 Wisconsin School of Business

A17 School of Education

A18 Arts Institute

A19 College of Engineering

A27 School of Human Ecology

A34 Vice Chancellor for Research & Graduate Education

A40 Nelson Institute for Environmental Studies

A42 Division of Intercollegiate Athletics

A45 Law School

A48 College of Letters & Sciences

A49 General Library System

A52 Wisconsin State Lab of Hygiene

A53 School of Medicine and Public Health

A54 School of Nursing

A56 School of Pharmacy

A57 University Health Services

A71 Facilities Planning & Management

A77 University of Wisconsin Police

A80 Recreational Sports

A85 University Housing

A87 School of Veterinary Medicine

A88 Wisconsin Veterinary Diagnostic Lab

A93 Division of Continuing Studies

A96 Wisconsin Union

Appendix C – Terms, Definitions and Acronyms

TERMS AND DEFINITIONS

The terms and definitions shown below are provided to clarify specific characteristics of cybersecurity articulated within this document. Reference to source documents are provided as necessary to ensure complete understanding.

Application - A software program hosted by an information system. (NIST SP 800-37r1, Appendix B)

Availability - Ensuring timely and reliable access to and use of information. (44 U.S.C., Sec. 3542)

Authorization (to operate) – The official management decision given by the Risk Executive to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security controls. (NIST SP 800-37r1, Appendix B, Adapted)

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U.S.C., Sec. 3542)

Cybersecurity - The ability to protect or defend the use of cyberspace from cyber attacks (CNSS 4009). Derived from the term "cybernetics" which is the scientific study of communication and control processes in biological, mechanical, and electronic systems and originated from Greek *kubernan* meaning to steer or control (OED).

Data Governance – defined by the implementation of the UW–Madison data management framework, (in progress). For more information contact policy@cio.wisc.edu. For the current presentation on the topic, see: https://www.cio.wisc.edu/wp-content/uploads/2014/12/DataGovernanceFramework.pptx.

Information Category – As defined in National Institute of Standards and Technology Special Publication 800-60 (NIST SP 800-60 rev 1), *Guide for Mapping Types of Information and Information Systems to Security Categories*; Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation. UW–Madison information categories are represented on Page 6 of the *Introduction* to this document.

Information Classification – in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for that data.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (See 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III)

Appendix C – Terms, Definitions and Acronyms

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (44 U.S.C., Sec. 3542)

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (44 U.S.C., Sec. 3542)

Plan of Actions and Milestones (POAM) – A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (OMB Memorandum 02-01)

Risk – A 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. (FIPS 200, Adapted)

Risk Analyst – Individual from the Office of Cybersecurity assigned to help capture and refine information security requirements and ensure their integration into information technology component products and information systems through purposeful security design or configuration. (NIST SP 800-37r1, Appendix B, Adapted)

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system. (NIST SP 800-37r1, Appendix B, Adapted)

Risk Executive – 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.) (Cybersecurity Risk Management Implementation Plan)

Risk Executive (Function) – An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

Risk Management - The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (FIPS 200, Adapted)

Risk Register – A database managed by the Office of Cybersecurity that contains records for each Information System to which the Risk Management Framework is applied.

Appendix C – Terms, Definitions and Acronyms

Security Category – "The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals." (FIPS 199, Appendix A, p.8)

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (FIPS 199)

Security Control Inheritance – A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. (NIST SP 800-37r1, Appendix B)

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST SP 800-37r1, Appendix B)

System Security Plan – Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (NIST SP 800-37r1, Appendix B; See: NIST SP 800-18)

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-37r1, Appendix B, Adapted)

Threat Source – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent. (NIST SP 800-37r1, Appendix B)

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST SP 800-37r1, Appendix B)

ACRONYMS AND ABBREVIATIONS

The table below provides the long title associated with acronyms or abbreviations used in this document.

Acronym or Abbreviation	Long Title
D-CISO	Deputy Chief Information Security Officer
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoIT	Division of Information Technology

Appendix C – Terms, Definitions and Acronyms

Acronym or Abbreviation	Long Title
FERPA	Family Educational Rights and Privacy Act of 1974
HCC	Health Care Component
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HRS	Human Resource System
IRB	Institutional Review Boards
ITC	Information Technology Council
MIST	Madison Information Security Team
NIST	National Institute for Standards and Technology
NIST SP	NIST Special Publication
PCI-DSS	Payment Card Industry Data Security Standard
PHI	Personal Healthcare Information
PII	Personally Identifiable Information
PAT	Policy Analysis Team
POAM	Plan of Actions and Milestones
RMF	Risk Management Framework
SDLC	Systems Development Life Cycle
SETA	Security Education, Training & Awareness
SFS	Shared Financial System
UW–Madison	University of Wisconsin–Madison
UWSA	University of Wisconsin System Administration
VCFA	Vice Chancellor for Finance and Administration
VP IT	Vice Provost for Information Technology