Policy Proposal

for the

UW-Madison Cybersecurity Risk Management Policy

Revised: April 7, 2016

Submitted by

Bruce Maas, Chief Information Officer (CIO)
Bob Turner, Chief Information Security Officer (CISO)
Stefan Wahe, Associate Chief Information Security Officer (ACISO)

Other Contributors

Siggi Eckhardt, Cybersecurity Governance, Risk and Compliance
Gary De Clute, IT Policy Consultant

Contents

Review

- √ Office of Cybersecurity
- √ UW-Madison Information Security Team (UW-MIST)
- Madison Technical Advisory Group (MTAG)
- HIPAA Operations Committee
- Legal Services, including the Director of Compliance
- Information Technology Committee (ITC)
- Data Governance Executive Committee
- University Committee
- Executive Leadership

Proposal

There is a continual need to balance:

- the cost of adverse events that result from risk, and
- the cost of reducing risk to a more acceptable level.

The Cybersecurity Risk Management Framework (RMF) focuses on information system security from a technology and process perspective. The RMF does not address user behavior beyond the concept of User Based Enforcement of Security Controls.[1]

The RMF is a process for arriving at an understanding of risk and impact to information systems. The remediation of risk must seek to balance between the impact of adverse events and the cost to reduce risk.

1. **Goals**

   The Cybersecurity Risk Management Policy establishes the essential features of the RMF.[2] These need to be established up front and at a high level so that the whole UW-Madison community understands that:

   A. UW-Madison is determined to effectively manage the Institution's cybersecurity risk. Not doing so is likely to have unacceptable consequences to the institution and individuals.

   B. The essential features of the RMF described in the Cybersecurity Risk Management Policy will be the Institution's basic approach to managing cybersecurity risk. That basic approach is mandatory.

   C. The details will be worked out in a collaborative manner as we learn what works well at UW-Madison.

2. **Scope**

   All electronic systems of any kind that store or process data used for UW-Madison instruction, research, administration, or public service would be included. Exceptions would be possible but limited. An exception process will be part of the policy implementation.

3. **Process**

   a) **Assess Risk**

      The risk associated with a system is cooperatively assessed by the functional unit and the Office of Cybersecurity.

[1] CISO to provide…
[2] The RMF is a six step cyclical process. This proposal focuses on essential features of steps 4 thru 6.

b) Certify Risk

The CISO signs off to certify that the risk assessment is accurate.

c) Accept Risk

The responsible decision-maker should be an executive or director within the functional unit with the authority to accept the risk of operating the system at the certified risk level, (subject to regulatory requirements and review by senior executives.)

d) Reduce Risk

If the level of risk is initially too high, the functional unit makes plans and identifies resources to mitigate or reduce the risk. The assessment is revised following confirmation of corrective actions. The reduced level of risk is then accepted.

e) Monitor Risk

The system is monitored to assure that risk is managed at or below the accepted level. Monitoring will be designed to detect security vulnerabilities and threats, such as gaps in the security controls and detection of compromised systems. There will be policy and procedural safeguards to assure that monitoring respects personal privacy and academic freedom.

f) Re-evaluate Risk

Full evaluation will be conducted throughout the system life cycle with formal review every three years and informal review annually. Changes may increase risk and require more immediate risk evaluation.

4. Priorities

The process will be applied to declared higher risk systems first. Work on higher risk systems will begin immediately.[3] Moderate risk systems will follow. Low risk systems will eventually be included. The level of activity will be appropriate to the level of risk, with lower activity levels for lower risk systems.

5. Follow up

Details of the RMF at UW-Madison need to be worked out in follow-on policy and procedures. Follow-on development will use a collaborative approach and work with the campus community in order to tune the steps of the RMF to meet UW-Madison's needs.

[3] Work has already begun in time-critical situations or with volunteers.

Consistency with campus culture and values

- Risk is managed within the functional unit. The cost of information security, or lack thereof, is a cost of doing business.
- The appropriate decision-maker in the functional unit decides what level of risk is acceptable, subject to regulatory requirements and review by senior executives.
- The Office of Cybersecurity provides advice, assistance, and support. The office does not enforce security, it enables security. Enforcement is the responsibility and at the discretion of management.

Impact on campus

- As the RMF is implemented, beginning with the essential features proposed above, the overall cybersecurity risk to the institution will be gradually reduced. There will be a corresponding statistical reduction in the expected future cost of cybersecurity breaches. It is important to consider that the damage due to loss of reputation can have short- or long-term economic consequences far in excess of the direct out-of-pocket expenses and changes in programmatic cost that results from a breach.
- There are costs for assessing risk, reducing risk to an acceptable level, and maintaining risk at or below that level. That cost depends upon the regulatory environment, the level of risk that is acceptable, and the efficiencies gained by implementing “common controls” that are shared across campus. Each functional unit’s willingness to support the common controls reduces effort and reduces cost.
- The RMF provides a process for managing risk and the associated costs. Total cost of ownership associated with this policy should consider the cost of recovery if the system is breached or disabled during a cybersecurity event. Decisions made within that framework will determine the actual cost. The goal is to reduce the net cost to the Institution, averaged over time.