WISCONSIN

UNIVERSITY OF WISCONSIN–MADISON

University of Wisconsin–Madison
Campus Information Security Program
&
2018–2021 Cybersecurity Strategy

Volume I – Information Security Program

Volume II – Cybersecurity Strategy

Volume III – Helpful Information

December 31, 2018

Final

Table of Contents

Record of Updates

Update Number	Change Information	Entered By	Date Entered
Draft v1	Consolidated input from Cybersecurity Strategy teams.	Bob Turner	**12-10-2017**
Draft v1.1	Edits and additions to the pre-release version for Office of Cybersecurity Internal Review	Bob Turner	**12-29-2017**
Draft v2	Edits and incorporating feedback from Cybersecurity Team.	Stefan Wahe	**01-23-2018**
Draft v2.1	Made ready for MIST review	Bob Turner	**01-28-2018**
Draft v2.2	Adding MIST feedback	Bob Turner	**02-16-2018**
Draft v2.3	Additional MIST Feedback	Stefan Wahe	**02-22-2016**
Draft v3.0	Made ready for DoIT Director and Divisional CIO review	Bob Turner	**02-24-2018**
Draft v4.0	Made ready for IT Governance Review	Bob Turner	**04-01-2018**
Draft v5.0	Complete overhaul to create Information Security Program and Cybersecurity Strategy document for IT Governance approval in advance of new CIO arrival on August 1, 2018	Bob Turner	**06-01-2018**
Draft v5.1	Final edits before technical writer review	Stefan Wahe	**06-29-2018**
Draft v5.2	Final Edits post Technical Edit	Bob Turner	**07-28-2018**
Draft v5.3	Final Edits for Cross TAG Review	Bob Turner	**08-12-2018**
Final Draft	Final Draft following DTAG and CIO Feedback. Per DTAG recommendation, document is now in three volumes with short Executive Summary Vol I - Information Security Program and Organization Vol II - Cybersecurity Strategy and the Challenges & Opportunities (including strategy maintenance) Vol III - Helpful Information	Bob Turner and Stefan Wahe	**11-23-2018**
Released Final Version	Original document separated into a separate Executive Summary with this document containing detail of the Information Security Program and Cybersecurity Strategy.	Bob Turner	**12-31-2018**

Executive Sponsor Review and Approval

Name	Role	Date
Lois Brooks	**Vice Provost for IT and CIO**	**11/30/2018**

Related Documents

Document Name	Date
UW System Regent Policy Document 25-5, Information Security	**2/5/2016**
UW System Information Security Program v 1.0	**4/30/2018**

Introduction

The University of Wisconsin–Madison (UW-Madison) Information Security Program and Cybersecurity Strategy provides university executives and staff with a broad view of activities designed to protect information through collaboration, education, and innovation. UW-Madison seeks to optimize risk management by refining current useful strategies and goals and by defining new information security and cybersecurity strategies. The Program and Strategy is focused on protecting information in electronic, print and other formats with the scope being University-wide.

The Threat

As detailed later in the Information Security Program, during one week of 2018, the University encountered 121,499 vulnerability exploits to include brute-force and malicious code-execution. Of those reported, 73 percent were of CRITICAL or HIGH severity. Cybersecurity risk management is complex as changes in security infrastructure, global criminal and nation-state threats, and the sophistication of exploits and vulnerabilities continually increase. Also relevant are the continuing threats posed by criminal elements, nation-state actors and the volumes of data we hold.

The cybersecurity threat to UW-Madison information and technology are real and increase or change monthly. Those threats include, but are not limited to:

- increasing compromise of campus credentials, likely as the result of phishing;
- user mistakes and errors;
- denial of service attacks;
- insider threats; and
- our inability to detect malicious code within encrypted communications paths.

The sophistication of phishing or other social engineering threats can easily lead to compromise of personal data or allow access to key information technology resources. Threat actors have increased the complexity of attacks directed at higher education. Cybersecurity industry reporting suggests increasing sophistication and changes to attack patterns in the categories of hacking, social engineering, and malware may target faculty and senior university leaders. Ransomware attacks carried out through website exploitation increase the likelihood that a major system or network outage could stop the business of the university with increased cost to recover.

Purpose and Use

Information Security Program provides a framework for greater protection of data; management of the University's networks, information systems and applications; and the continued improvement to the people, processes, and technology that collectively execute the Program and enable continued success with the Strategy. The framework supports improving UW–Madison's cybersecurity posture.

For central and distributed information technology (IT) staff and security professionals, this Program and Strategy is an important guide to help them improve and maintain cybersecurity at UW-Madison. The document provides the readers with direction to sustain information systems in alignment with and in support of the university's mission. This strategy incorporates feedback from the UW–Madison community based on lessons learned during implementation of the original 2015 Strategy. Information Security community representation in both the development and drafting teams along with IT and Faculty governance review confirms this document has the support of the UW community, reflecting greater cybersecurity maturity and evolving best practices that are easily integrated across the campus and transferrable to the University of Wisconsin System and other UW Institutions.

This document is the official description of the UW-Madison Information Security Program. Changes or exceptions to the program are to be submitted to the Office of Cybersecurity for processing, update, and subsequent approval by the Chief Information Officer. Deviations which cannot be effectively aligned to the UW System's information security program and supporting policies and standards will be submitted for review by the UW System Vice President for Information Security for review and concurrence.

All changes will be recorded on the Record of Changes page with an updated document posted and announced per current communications policy and standards.

Any exceptions to the UW System Information Security policies and associated standards should be evaluated based on the application to UW-Madison and the risk associated with the particular situation. This should include factors related to data classification, institutional objectives, regulatory and compliance matters, systems and processing criteria, and technology.

Document Organization

This document complements the University of Wisconsin (UW) System Information Security Program published in April 2018 and includes a complete revision of the previous 2015 – 2019 UW–Madison Cybersecurity Strategy published in July 2015, updated in 2016 and which started revision in 2017. This Program and Strategy will be effective on approval in the Fall of 2018 with annual updates.

- Volume I contains the description and components of the Information Security Program. Appendix A is part of that volume and describes the recommended cybersecurity organization.
- Volume II contains the Cybersecurity Strategy and Goals for managing the people, process and technology components of the Information Security Program. The challenges and opportunities of executing this Program and Strategy are detailed in Appendix B within that volume. The details on how the Cybersecurity Team and the campus community developed the strategy (along with the maintenance of the strategy once approved) is provided in Appendix C.
- Volume III contains additional acronyms, abbreviations terms, and definitions related to information security and cybersecurity operations.

Intended Outcomes

By adhering to the Information Security Program and executing the strategies above, we will measurably improve institutional user competence, more effectively manage risk, and provide a return on the investments made over the last three years and into the future.

Contact

The point of contact for information or questions regarding the UW-Madison Information Security Program and Cybersecurity Strategy is the Chief Information Security Officer. Additional information is on the Office of Cybersecurity website at https://it.wisc.edu/about/office-of-the-cio/cybersecurity/

Volume I – The Information Security Program and Cybersecurity Organization

> "We are at a crossroads in the area of information security. Nationally, data losses, ransomware attacks, threats to privacy, theft of intellectual property, credit card breaches, identity theft and denial of service attacks have become a way of life."
>
> Raymond Cross
> UW System President; April 4, 2018

1.0 The Information Security Program

This program exists to ensure the availability, integrity, and confidentiality of institutionally developed and UW System owned data and to protect information assets from unauthorized access, loss, alteration, or damage. The challenge is in supporting the open information sharing needs of the academic and research environment. A robust information security ecosystem is critical to enabling the UW–Madison mission of teaching, research, and outreach while simultaneously supporting the UW System mission of developing human resources, discovering and disseminating knowledge, and extending knowledge and its application beyond the boundaries of its institutions.

The UW–Madison IT community, the Office of Cybersecurity and the Chief Information Security Officer must work collaboratively to establish, develop, and maintain this Program. They are guided by the standards set forth in the UW System Information Security Program and Policies and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a technical approach and a policy framework for cybersecurity risk management, including asset identification, systems protection, threat detection, incident response and recovery. NIST CSF is widely adopted across both public and private sector organizations, throughout the United States.

1.1 Scope of the Program

The concepts, policies, standards, and initiatives within this Program apply to *all* UW–Madison schools, colleges, institutions, and divisions. Third party affiliates will be required to adhere to this program as UW-Madison ratifies contracts. Compliance with the components of the UW–Madison and UW System enterprise information security programs, policies, and standards is expected and encouraged as part of daily operations of the university.

As stated in the UW System Information Security Program, "Each member of the UW System community is responsible for the security and protection of information assets over which he or she has control. The UW System community is defined as students, faculty, staff, third-party vendors, visiting scholars/lecturers and/or units and other persons who are acting on, for, or on behalf of the UW System and its institutions."

We further define the UW-Madison community as the group of people working together to achieve common goals toward the mission of teaching, research, and outreach. However, there may be smaller, focused communities working towards specific teaching, research, or outreach objectives.

We must protect our resources, which include (but are not limited to) all electronic equipment, facilities, access/control systems, technologies, and data used for information processing, transfer, storage, display, printing and communications, as well as services that are owned, leased, operated, provided by, or otherwise connected to UW–Madison and UW System resources. We must protect community members from harm due to data exposure and loss; guard against the physical and logical integrity of these resources against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise; and preserve the integrity of institutional information systems and data.

1.2 Mission

The Office of Cybersecurity[1] leads the implementation of this Program to enable the primary institutional mission of teaching, research, and outreach. Working closely with the distributed IT community and security experts, they provide innovative and creative IT security services and protect vital information and research data by developing, refining, and continually delivering comprehensive information security and privacy programs for the UW–Madison. The community of security experts serve university leadership by presenting risk assessment and management data while protecting the physical and logical integrity of these resources against threats, such as unauthorized intrusions, malicious misuse, or inadvertent compromise of institutional information systems and data.

1.3 Vision

Embodying the Wisconsin Idea, the Office of Cybersecurity embraces the revolution of cybersecurity in higher education, becoming a leading provider of cybersecurity services to the university community. This work should make a noticeable impact in securing important information and research data to the benefit of the University of Wisconsin System, Wisconsin communities, and beyond.

UW-Madison will effectively secure information and manage cybersecurity-related risk to information technology assets to meet these over-arching UW System Information Security Program goals:

- prevent data loss or compromise that could otherwise result in significant risk to highly sensitive/personal or institutional data or reputation;
- improve the security of critical system and network services through enterprise focused and defense-in-depth approaches to reduce risks commonly associated with disaggregated computing environments;
- proactively assess, reduce and manage risk in a manner that enables data/system owners, administrators and the larger UW System community to be more aware of the risks that their information assets are vulnerable to, identify controls to reduce those risks, and understand what risks remain after any identified controls have been implemented; and
- enhance crisis and information security incident response/management to enable the UW System to quickly recover its information assets in the event of a catastrophic event and to manage information security events more efficiently and effectively, thereby reducing or minimizing the damages to the UW System community[2].

[1] The Office of Cybersecurity is directly aligned under the Vice Provost for Information Technology and Chief Information Officer. This group was created in 2014 by consolidating the former Division of Information Technology (DoIT) IT Security Team and the Office of Campus Information Security and renamed the UW-Madison IT Security Team. The name change to Office of Cybersecurity was made in 2015 to better reflect the full scope of the office's mission.

[2] From the UW System Information Security Program Version 1.0 of April 30, 2018. Available online at https://www.wisconsin.edu/information-security/download/UW_Information-Security-Program_Final_30April2018.pdf

1.4 Cybersecurity Guiding Principles

The Office of Cybersecurity aligns its work to support the mission of the University. The Cybersecurity Team has a significant and key role in protecting the reputation of the institution and the privacy and academic freedom of the faculty, staff, and students. The Cybersecurity Team cannot do it alone. Every person who uses data and IT services on campus has a role.

As members of the UW-Madison community, relationships are founded on mutual respect and common goals. Collectively, the Office of Cybersecurity, the Madison Information Security Team (MIST), CIOs and IT Directors, understand the UW-Madison community want their information and programs as secure as necessary and their people to be safe and successful. Collectively, everyone needs to work on digital safety knowing that research, teaching and learning data and information are vital to the University's mission. The inadvertent exposure of personal data and other confidential data entrusted to the UW-Madison community will cause harm if exposed to the wrong audiences. The information systems and university services that house that data need to be intact and available to support the work that leads to success. Effective and efficient protection requires the wise use of resources, investment in well-supported tools, and teamwork as they are used.

The Guiding Principles of Cybersecurity at UW–Madison are not just for the Office of Cybersecurity, they are for the whole university community working together to enhance privacy, academic freedom, safety, and success. The following Principles have evolved since July 2015 and, as established here, the Cybersecurity Team, IT managers, and distributed IT staff will continually monitor and propagate them to all UW-Madison communities. These Principles will also be incorporated within policy and process statements issued throughout the life of this Cybersecurity Strategic Plan:

- Teamwork: Working together with all having a role in using and protecting data and IT services.
- Prudence: Content, regulations, and use of the data and services determine the appropriate level of protection.
- Integration: Protection is built in from start to finish. It is not efficient to add it later.
- Comprehensive: Protecting data and resources requires an effective combination of training, policy, and services.
- Judiciousness: Encourage the wise use of resources while protecting the University's reputation and its ability to accomplish its mission.
- Reliability: The community trusts the IT security community to invest in well-supported tools and practice teamwork while in use.
- Communication: Timely and targeted information about data protection is shared among the various communities of the University and UW System.
- Respect: Be good digital citizens. Respect and protect each other by following civil, safe, and secure practices.
- Privacy: Enhance the privacy and academic freedom of the university community through prudent and confidential protection of data and resources.

Guiding Principles applicability to faculty, staff and students: Everyone has a role in protecting data. Everyone is on the same team. As members of the same team, we treat each other with mutual respect and encouragement. Everyone has to step up to the challenges of securing personal data and place a high priority on protecting Social Security Numbers, bank accounts, credit card numbers, health care data, and other personal information that may be exploited to commit crimes or hurt people's reputation. By following safe and secure practices on personal and university devices, everyone remains good digital citizens. Personal privacy is important to everyone, and privacy helps support academic freedom. Training, policy, and secure practices all work together to enhance privacy.

Guiding Principles applicability to managers: Protecting data and university assets involves everyone throughout an organization. We must design protections that reduce financial and reputational risk to acceptable levels. Effective protection requires the right mix of training, teamwork, and technical solutions. Partnership with the Office of Cybersecurity leverages local resources to create protections that are both effective and efficient. Training and adherence to policy complement technical solutions so the total package accomplishes the goal. Wise use of resources to reduce risk enhances the overall success of an organization (e.g. management can ensure that everyone receives security training appropriate to that individual's role).

Guiding Principles applicability to IT professionals: IT professionals have an important role in assuring that training, teamwork, and technical solutions are adequate to protect data and systems. We gain efficiency by partnering from the start of a project and continuing throughout the project's life cycle to determine the necessary level of security and require the correct security controls when purchasing, designing, implementing, or maintaining information systems and services.

IT staff are on the front lines in defending the networks and securing data and fully understand that data and system security is necessary in all their actions and processes. Additionally, they understand that security is not just an IT function. End users and management are part of the team that makes it possible. IT professionals are partners with the Cybersecurity Team in making the best use of the unique capabilities found across the university. Timely and omni-directional sharing of information are the most useful byproduct of the partnership.

Guiding principles applicable to leaders: Leaders must assure that they understand the risks associated with cyber threats and the impacts of data loss and business interruption. They must promote and support cybersecurity actions and investments, and ensure the organizations under their direction follow policy and practice.

2.0 The Need for Security

The world of cybersecurity in 2018 is very different from 2015, and will be very different still in 2023 and beyond. Changes in technology, business requirements, legal and regulatory requirements, cybersecurity threats, and people themselves create a shifting landscape that requires timeliness and agility. This changing landscape, in conjunction with an ever-present cybersecurity risk, creates the need for a mature organization that considers cybersecurity and technical depth throughout the course of the various change management lifecycles used on campus. This includes project development, planning, developing, testing, implementation, and Continuous Diagnostics and Mitigation (CDM). Also included is the decommissioning of information systems that have reached the end of their life. Cybersecurity is a partner with the campus community in each step. These partnerships will reduce cybersecurity risk, protect data, and address current and emerging threats. Risk is always present. How the University addresses risk, however, reveals the cybersecurity maturity at the University of Wisconsin-Madison.

2.1 Reducing Cybersecurity Risk and Protecting Institutional Data

Reducing cybersecurity risk while preserving information security is a shared goal and one of the primary areas of improvement for the university. Risk reduction strategies must evolve to address current threats with the support of various university advisory groups and governance bodies[3]. Collaboratively, the focus must be on continued identification of risk and the appropriate classification, handling, and protection of data. This focus prevents inappropriate access to or loss of restricted or sensitive data. Risk reduction also includes performance of continual monitoring and diagnostics that ensure visibility of IT assets and the vulnerabilities associated with specific technology. This activity includes processes and procedures for managing personally identifiable data, intellectual property and other important and protected information. The Office of Cybersecurity leads and advises the UW-Madison community on both the necessary risk response measures to protect information systems and the controls that reduce the cost of operations. The Cybersecurity Team seeks to enable faculty and researchers as they carry out the missions of the University in teaching, research, and outreach. Likewise, risk tolerant strategies make the University vulnerable to cyber-attack, data loss or mismanagement, and increased cost to operate from additional system administrative and maintenance expense.

2.2 The Threat

UW-Madison executives, faculty, researchers, administrators and IT staff understand that higher education engages in open dialogue and prolific sharing of information to stimulate research, facilitate teaching and learning, and promote outreach. It is a business imperative that the data generated, managed, and employed as part of daily work be protected. Collaboration drives operations at UW-Madison, while the necessary exchanges of information, data, and ideas leaves the information technology environment vulnerable to a wide variety of threats. The user community is a broad mix of skills and levels of experience. Users connect with many government and non-government organizations and vendors to access services or connect other enterprises within the security envelope. Often with limited resources, the University continues to face threat vectors that include malware attacks (where more than 90 percent originate through e-mail or web servers),[4] theft of credentials through social engineering attacks like e-mail phishing[5], and malicious code or malware designed to exploit existing system vulnerabilities or popular applications.

3.0 Data Governance – Understanding Data and Risk

All users have a responsibility to maintain integrity and confidentiality of the UW-Madison data with which they work. Users who have a role that requires the handling of data should understand the risk associated with using those data. Some of the institutional data is public by nature and the ability to share that data freely assists us in conducting business for UW-Madison. Other institutional data is more sensitive in nature and the risk associated with interacting with it is commensurately greater.

[3] This includes the Information Technology Committee, IT Governance and Advisory Groups, Madison Information Security Team.

[4] Integration Partners article *Top 6 Higher Education Security Risks and Issues* published 11-Sep-2017

[5] A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person (NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, dated May 2013).

Users should know not to share restricted data with others and not increase risk to the institution.

A key outcome of establishing risk categories for data is the ability to assign security controls based on characteristics of availability, integrity, and confidentiality for both data and the information systems where the data is at rest or in transit. Key terms to understand include[6]:

Availability controls ensure information is accessible and useable upon demand by an authorized entity. Cybersecurity events that impact availability include denial of service attacks, prolonged maintenance activity, or partial loss of access to specific data or services.

Integrity controls guard against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Integrity means sensitive data has not been modified or deleted in an unauthorized and undetected manner. Cybersecurity events that impact integrity include data breaches, including those that go undetected for significant periods; ability to ensure the authenticity and accuracy of agreements and transactions; and presence of malicious code within specific fields in a database.

Confidentiality controls provide authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Restricted or Sensitive information is not disclosed to individuals, entities, devices, or processes unless they have been authorized by the appropriate data steward to access the information. Cybersecurity events impacting confidentiality could include evidence of SQL injection attacks, session hijacking, or data loss events.

Table 1 provides an example of broad information categories based on the required confidentiality. The level of integrity and availability will vary among applications with notional risk of exposure of the system or data increasing based on the value of the data or the potential for damage should the data be compromised.

Table 1: UW-Madison Information Security Classification and Risk Detail

Category	Availability	Integrity	Confidentiality	Risk of Exposure
Restricted	(varies)*	High	High	High
Sensitive	(varies)*	(varies)*	Moderate	Medium
Internal	(varies)*	(varies)*	Low	Low
Published/Public	(varies)*	(varies)*	N/A	Low

4.0 Cybersecurity Operations

The Cybersecurity Operations Center (CSOC) continually monitors for indicators of compromise. During one week of 2018, the CSOC observed 121,499 vulnerability exploits to include brute-force and malicious code-execution. Of those reported, 2,928 exploits were of CRITICAL severity, 86,090 exploits were HIGH, and 30,822 exploits listed as MEDIUM. Cybersecurity risk management grows more complex as definitions and processes are refined to address changes in security infrastructure, global criminal and nation-state threats, and the sophistication of exploits and vulnerabilities. Based on the ongoing success in cybersecurity operations since early 2017, the CSOC is able to accurately assess ongoing threats to the University.

The Top Five threats are:

1. **Increasing compromise of campus credentials, likely as the result of phishing**. These

[6] Definitions from NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, dated May 2013

credentials could allow an attacker to access many campus IT services, e.g. email, VPN, cloud file storage, ERPs, etc. Historically, attackers have focused on using these credentials for spam and phishing attacks. Still, increased use of the same credentials to access other IT services, like Qualtrics surveys, continues to create opportunities for compromise.

2. **Denial of service attacks**. Typically, denial-of-service attacks seen by the CSOC are short-lived and are directed at devices on the student network (ResNet). However, a targeted, prolonged attack would consume many IT staff resources and lead to temporary service outages, as Rutgers University experienced between 2014 and 2016[7].
3. **User mistakes and errors**. This includes misdirected communications, misconfiguration of servers, inappropriate elevation of privilege, etc.
4. **Insider threats**. The frequency of insider threats is low, but the impact could potentially be large. An example of this threat could be a student breaking into faculty offices to install key loggers on their computers. The stolen information could then be used to change grades[8].
5. **Encrypted communications**. It is estimated that half of campus network traffic is encrypted. The inability to inspect encrypted data channels for malicious activity greatly reduces the opportunity to detect attacks without deploying additional security controls. Not having visibility into all traffic impacts the ability to secure University-managed devices. The impact is partially mitigated when IT staff deploy host-based security controls.

The sophistication of phishing events, which are socially engineered attempts to entice compromise of personal data or access control features, has steadily increased against higher education targets since 2014. The standard elements of a phishing email are more realistic in nature, and threat actors have increased phishing events directed at higher education. Cybersecurity industry reporting suggests an increase of attack patterns in the categories of hacking, social engineering, and malware in the Education sector. Social Engineers target faculty and senior university leaders and are increasing the level of sophistication in the messages. The recent increases in e-mail based ransomware attacks carried out through website exploitation increase the likelihood that a major system or network outage could result in impact that stops the business of the university with increased cost to recover. Knowing about and employing backup and recovery tools can mitigate the damage of these attacks. Within a security controls structure based largely on user-based enforcement, cybersecurity and IT professionals must help users pay attention to security training and increase their situational awareness in order to counter accidental or intentional insider threat scenarios.

5.0 Roles and Responsibilities

According to Regent Policy Document 25-5[9], the Board of Regents delegates to the President of the UW System the authority to implement and maintain an information security program. Each UW System institution shall consistently apply the program and related processes.

In order for chancellors to consistently apply the UW System Information Security Program, on April 4, 2018, the UW System President specified via memo that, "…all information technology (IT) environments at each institution shall be under the oversight of a single person designated by the

[7] http://www.dailytargum.com/article/2017/01/cybersecurity-expert-identifies-rutgers-student-as-ddos-perpetrator

[8] Similar to events reported at Kansas State University as shown in Oct 28, 2017 Weekly Cybersecurity Report.

[9] https://www.wisconsin.edu/regents/policies/information-technology-information-security/

chancellor. The designee shall have the authority to ensure all IT operations at the institution are conducted in a secure fashion."

At UW–Madison, the Chancellor designated the Vice Provost for Information Technology and Chief Information Officer to be responsible for ensuring that appropriate security controls are available and enforced. The Division of Information Technology (DoIT) and Distributed IT organizations and teams have joined with the Cybersecurity Team to provide appropriate guidance and assistance to the greater UW–Madison community to ensure all members of the community understand and employ the required controls to protect the information assets within their purview in accordance with this program and supporting UW–Madison and UW System information security policies.

While respecting the unique mission and requirements of individual schools, colleges, institutions and divisions, promoting the similarities between institution information security organizations can facilitate inter-institutional lines of communication and form a foundational organization and structure that supports the overall goal of improving information security. Accountability is constant throughout the organization. Each role described in Table 2 has specific responsibilities which must be carried out to make the university secure. Distributed organizations may combine or add responsibilities based on local needs.

Table 2: UW-Madison Information Security Roles and Responsibilities

Role	Job Functions	Responsibilities
Chancellor	Assumes high level accountability and responsibility for UW–Madison's compliance with the timely adoption and implementation of the UW System Information Security Program.	• Conveys priority of information security work to CIO or other designee and other institution leadership • Maintains accountability to the UW System Board of Regents
Provost	Delegated accountability from the Chancellor for UW–Madison's compliance with the timely adoption and implementation of the UW System Information Security Program.	• Facilitates CIO or other designee influence over institution information systems • Resolves high level conflict regarding information security issues
Vice Chancellor for Finance and Administration (VCFA)	Delegated accountability from the Chancellor for UW–Madison's compliance with the timely adoption and implementation of the UW System Information Security Program.	• Facilitates CIO or other designee influence over institution information systems • Resolves high level conflict regarding information security issues
Risk Executives	An executive or director 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 who will ultimately be responsible for paying for a breach.	• Provides leadership of the academic / functional unit by emphasizing the importance of cybersecurity. • Reviews Risk Assessments and recommendations provided by the Office of Cybersecurity to: (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. • Provides resources to reduce risk as agreed to from the Risk Assessment.

Role	Job Functions	Responsibilities
Vice-Provost for Technology and CIO	Leads a customer-focused organization that delivers innovative, efficient, and effective technology solutions to support the teaching, research, and service missions of the UW System and institutions Serves as the institution's single responsible executive for oversight of the information technology environment.	• Advances the technology aspects of important institution initiatives • Manages IT strategic planning and decision-making • Supports the research, teaching and outreach mission of UW System and institutions • Maintains data governance, architecture, and management • Ensures all IT operations at the institution are conducted in a secure fashion
UW-Madison Chief Information Security Officer (CISO)	The CISO ensures the development, adoption, implementation, and executive direction of operations within the UW-Madison Information Security Program, providing leadership and management of the Cybersecurity Team, technical consultative direction to campus and Distributed IT units necessary to achieve continuous compliance with the UW System Security Program, as well as managing large scale IT security and cybersecurity initiatives, incident response activities, and other related cybersecurity events.	• Develops policy and supporting standards for UW-Madison and in support of the UW System Information Security Program • Evaluates and recommends appropriate technical, physical and administrative controls, in support of the UW-Madison Information Security Program • Communicates expectations to the UW-Madison Information Security community • Provides direction to campus stakeholders on the appropriate implementation of UW-Madison and UW System policies and standards • Evaluates and recommends UW-Madison CIO approval and forwarding of mitigating control exception requests for UW System Information Security Policy and Standards • Communicates appropriate matters to the UW System Vice President of Information Security
Divisional Chief Information Officers and IT Directors	Divisional IT Leaders act as an information security conduit and liaison for their division by providing guidance and support to, and representing the perspective of, their division's leadership and departments.	• Collaborate with other divisional IT leaders and departmental staff on all aspects of information security that affect their departments. • Disseminate information, providing how-to instructions, awareness campaigns, and informational support to their departments • Act as a liaison between the departments and the Office of Cybersecurity, advocate on behalf of departments.
IT Operations Manager(s)	Manages the operation of an information technology unit or area including computer hardware, software, networking and telecommunications equipment. Plans, organizes, and controls all aspects of the operation including; supervision and scheduling of professional and technical staff, prioritizing and assigning of the work, and coordinating activities with other UW System or institution units.	• Plans, organizes and controls the operation of complex information technology units • Provides technical support for all hardware and systems software sets standards • Establishes procedures, oversees the acquisition of supplies and equipment schedules • Installs and de-installs computer hardware; plans and establishes security systems; recommends hardware acquisitions and the maintenance of support equipment; • Ensures the contracting and procurement of new equipment and software

Role	Job Functions	Responsibilities
IT Security Specialists	Performs security operations, information security threat analysis, and tools maintenance.	• Gathers and analyzes materials about information systems to provide recommendations to improve compliance and achieve greater levels of data and information systems security • By supporting academic / functional unit leadership, ensures security program operations and controls are being consistently applied • Assesses requirements for updates to security plans based on changes to business functions, technical vulnerabilities, and emerging threats
Research IT	Manages and secures the information technology components of research projects and centers, with specific emphasis on data integrity and security. Works with and enables researchers in the IT space.	• Plans, organizes and controls the operation of research information technology • Installs and de-installs computer hardware; plans and establishes security systems; recommends hardware acquisitions and the acquisition and maintenance of support equipment • Provides technical support for all hardware and software • Acts as a technical resource and provides consultation to researchers and their projects
Academic / Teaching and Learning IT	A DoIT Department and professionals across campus who apply technology to current and future academic environments and as a partner with faculty for numerous technological initiatives in the teaching and learning ecosystem. These professionals design, develop and evaluate technology-enhanced learning experiences for today's learners.	• Plans, organizes and controls the operation of academic and teaching and learning related information technology • Installs and de-installs computer hardware; plans and establishes security systems; recommends acquisition of hardware and maintenance of support equipment • Provides technical support for teaching and learning related hardware and software • Acts as a technical resource and provides consultation to researchers and their projects
Distributed IT Staff	Manages the information technology aspects of one or more specific departments or centers. Responsibilities may include desktop, laptop, and server computer hardware, software, networking and telecommunications equipment. Works with department faculty, staff, and leadership to plan, organize, and control local information technology and meet campus information security requirements.	• Implement policies in their department, work with divisional and cybersecurity requirements. • Plans, organizes and controls the operation of their local information technology • Provides technical support for all hardware and systems software sets standards • Establishes procedures, oversees the acquisition of supplies and equipment schedules • Installs and de-installs computer hardware; plans and establishes security systems; recommends hardware acquisitions and the acquisition and maintenance of support equipment; • Works on the contracting and procurement of new equipment and software

Role	Job Functions	Responsibilities
Risk Manager	At the institution level, manages, develops, and implements System and Institutional risk management programs, policies, and procedures appropriate to the organization. Ensures continuity of Cyber Liability Insurance program effort with CISO, ISO, Records Manager, and other information security resources. ** Requires system-driven training for the institution risk managers.	• Analyzes risks and communicates appropriate responses • Reviews and negotiates contracts as they relate to insurance, indemnification, and liability issues in consultation with Legal Counsel, or UW System Office or Risk Management • Administers and manages university programs: ○ Liability and automobile claims ○ Property insurance claims ○ Loss control programs ○ International safety and security programs • Maintains key statistics related to risk management processes, and uses those statistics to continuously improve processes
Records Manager (Designated as the Records Officer per Wisconsin Statute Wis. Stat. 15.04(1)(j) and Regents Policy 3-2 Public Records Management)	Provides consultation on research records and data management issues. Consults system-wide with all office levels in managing all information assets, regardless of format or medium, in accordance with Records Management Best Practices.	• Develops and maintains a public records management program that fulfills state and federal legal requirements • Provides records management training and assistance to institution employees • Provides special assistance to UW System institution: legal counsel, legal custodians for public records requests, auditors, and archivists • Collaborates with technology professionals in developing and maintaining information and digitization systems that create, receive, store, destroy, and archive electronic public records in compliance with state and federal requirements
Data Governance / Data Custodian	Facilitates data-driven decision-making and enables users from all departments of the institution to be able to make informed decisions, a culture of information literacy and sharing should be established at the institution level.	• Develops the risk management strategies and compliance with record retention policies for differing record types • Aligns and coordinates with records management to ensure compliance. • Ensures there are common data definitions, and those definitions are made available across multiple to enable informed decision-making
Data Steward(s)	Management and oversight of UW System and institution data assets to provide business users with high-quality data that is easily accessible in a consistent manner. Allow for and facilitate data-driven decision making.	• Evaluates and classifies data according to UW System policy and procedure • Facilitates the communication of institutional data-related policies across the institution • Promotes data governance across the institution • Implements major data-related projects • Recommends the need for resources and budget for the implementation of major data-related projects • Monitors key metrics related to the ongoing program operations

Role	Job Functions	Responsibilities
Information System Owners	Individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST SP 800-37r1, Appendix B). The System Owner is accountable to the risk executive to ensure that a through risk assessment is completed in a timely and collaborative manner. They are accountable for validating the categorization of the system and for agreeing to the level of security controls that should be applied.	• Plans, organizes and controls the development and delivery of designated information systems. • Provides technical and financial support for all hardware and systems software within the system's development life cycle. • Establishes procedures, oversees the acquisition of supplies and equipment schedules • Coordinates the contracting, procurement, installation and de-installation of computer hardware and software; plans and establishes security systems; manages hardware acquisitions and the acquisition and maintenance of support equipment; • Provides technical support for all hardware and software • Acts as a technical resource and provides consultation to researchers and their projects; confers with local security teams and Office of Cybersecurity staff to coordinate Risk Management Framework and cybersecurity operational issues
Functional Managers / Business Process Owners	Individuals using information systems to conduct the institution's business. They are management and subject matter experts on the availability, integrity, and confidentiality needs of business processes, and the usage of data in the system. They aid in determining the system category and participate in risk scoring.	• Coordinate exchange of information on business operations issues with technical staff, System Owners, developers and IT staff • Provide information and data security information used to categorize the system • Provide feedback on efficacy of security controls and their impact on the business process • Participate in system security audits as necessary.

7.0 Strategic Relationships

Information Security Programs are successful when leaders give support and the communities that the strategy serves are actively involved. This Program is developed with input from many areas of the UW-Madison Campus and through partnerships across UW System and the Big Ten Academic Alliance. To enable a culture that values cybersecurity and reduces risk, UW-Madison leadership and the Office of Cybersecurity must maintain a trusting relationship with the campus and UW-System. This includes functions spanning academic, research, technology and business, compliance, and outreach functions. By building these relationships, the Office of Cybersecurity confirms a shared understanding of the strategies, promoting a unified response by applying appropriate controls that reduce risks to university data and systems.

To maintain trust, the Cybersecurity Team will collaboratively develop sustainable security services that are respectful to academic freedom and personal privacy. The Office will use well-defined frameworks and processes that allow close collaboration with campus and UW-System stakeholders. The Office pledges to continue to develop strategic relationships that identify the various needs of the communities under its support. In addition, it will work with these communities to build out distributed operations and ownership in securing local systems, data, and networks.

Appendix B: Cybersecurity Organization, Governance and Communication identifies how the Office of Cybersecurity manages strategic relationships in the roles of governance, collaboration, advising, operations, and communications. Examples of engaged groups include, but are not limited to:

UW-Madison:

Information Technology Committee
IT Governance (IT Steering Committee)
UW-Madison Information Security Team (UW-MIST)
Data Stewardship Council
Research and Sponsored Programs
The Biosafety Task Force
The Office of Compliance
The HIPAA Compliance Program
Payment Card Industry Compliance Team
Distributed CIOs and IT Directors
DoIT Directors and Management

UW System:

UW System Chief Information Officer Council
Technical Information Security Committee
Human Resource System Service Center
Shared Financials Services

Outreach:

Big Ten Academic Alliance (BTAA)
EDUCAUSE - Higher Education Information Security Council
State of Wisconsin Division of Enterprise Technology
Research and Education Networks – Information Sharing and Analysis Center (REN-ISAC)

8.0 Implementation, Enforcement, and Monitoring

UW-Madison will implement this Campus Information Security Program through institutional delivery of enterprise security services to include assessment of risk and associated costs or resources.

UW-Madison Risk Executives have overall responsibility to comply with this program and related information security policies. The Office of Cybersecurity supports and evaluates compliance with the Program through the following activities: designing and developing processes and controls to manage risks; defining measures of success; and assisting with escalating critical issues and emerging risks.

To ensure the information security program is applied consistently and benefits the UW System as a whole, the Chief information Security Officer and the Cybersecurity Team shall consolidate relevant UW-Madison information security and cybersecurity data and report quarterly to the UW System Associate Vice President of Information Security.

8.1 Violation Reporting and Escalation

Failure to adhere to provisions of this program and supporting information security policies and standards may result in the suspension or loss of access to UW-Madison and UW System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of information assets, there may be circumstances where Risk Executives may immediately suspend or deny access to their IT resources.

8.2 Periodic Review

This program will be periodically updated to maintain alignment with relevant developments regarding cybersecurity threats, risks, and compliance matters facing UW-Madison, the UW System, or higher education.

The information security program is reviewed during the yearly strategy review or as required, and will be revised based on (but not limited to): updated industry regulations or standards; organizational changes; or newly identified risks and threats.

9.0 Legal or Regulatory and Contractual Requirements

UW-Madison continuously endeavors to comply with implications of any applicable laws and regulations. Examples of some of the requirements include the following: 20 U.S.C. § 1232g, Family Educational Rights and Privacy Act (FERPA); Pub.L. 104-191, Health Insurance Portability and Accountability Act (HIPAA); Pub.L. 106-102, Gramm-Leach-Bliley Act (GLBA); Section 134.98, Wisconsin Statutes, Notice of unauthorized acquisition of personal information; and Payment Card Industry (PCI) Data Security Standards.

The Office of Cybersecurity supports a stronger baseline on procurement by reviewing contracts for purchase of IT hardware, software and services to include cloud systems, infrastructure, platforms and software. The Cybersecurity Team also conducts targeted risk assessments and maintains data on vendors which may be required by the applicable requirements (e.g., PCI-DSS) to provide third party risk assessment certificates.

10.0 Information Security Policies

The baseline policies, standards and procedures regarding information security are numbered within the 1000 series of system-wide policies that are available on the UW System Administrative Policies and Procedures website.

10.1 Information Security Policies, Standards and Procedures

An information security policy is a document that outlines principles that must be met and are specific to a particular topic or area. Standards and procedures contain specific requirements that must be met by institutions. Guidelines are adopted based on specific technologies or unique work processes.

10.2 Information Security Policy Development

UW-Madison IT Policy is considered University policy. Implementation plans govern the efficient and effective development of IT resources and meet the needs of research, instruction, and administration; comply with applicable laws or regulations, UW System policies; and meet other external mandates.

UW-Madison IT policy development is a collaborative process that is integrated with UW-Madison shared governance and IT governance. IT policies are reviewed and approved by governance bodies with institution-wide representation. The authority of shared governance and IT governance gives IT policies institution-wide scope and authority.

Appendix A: Cybersecurity Organization, Governance and Communication

This appendix describes organizational relationships and describes actions of the different governance bodies at UW–Madison and within the UW System with a direct focus on information security and cybersecurity. Under the general direction of the Vice Provost for Information Technology/Chief Information Officer (CIO), the Chief Information Security Officer (CISO) supports the vision and mission of the university through development and delivery of an innovative and comprehensive information security and privacy program for the University of Wisconsin-Madison (UW-Madison). The scope of this program is university-wide and should drive information protection through collaboration, education, and innovation with advice focused on protecting information in electronic, print, and other formats. This strategy ensures that information created, acquired, or maintained by UW and authorized users is handled and used in accordance with its intended purposes[10].

Introduction

Information security at UW-Madison is driven mainly by the Office of Cybersecurity at the direction of campus leadership. However, campus IT security is ultimately a product of collaboration primarily with distributed IT staff but includes faculty, staff, and students.

It is important to understand the role of governance and its influence on the Office of Cybersecurity but it must be examined in the context of the other relationships of Cybersecurity to both campus and off-campus groups. The following section covers those relationships and their influence on the Office of Cybersecurity.

This section also addresses the role of Cybersecurity in regulatory compliance. For example, the Deputy CISO is the designated HIPAA Security Officer (as required under the HIPAA Security Rule).

Evolving IT environments

How Cybersecurity interacts with the rest of campus is affected by a campus environment that is evolving. Since formulation of the previous strategic plan there have been several developments at UW-Madison related to IT and data governance, including:

- development of a formal IT governance process including an IT Steering Committee that will have a direct line to the Office of Cybersecurity;
- creation of an IT Center of Excellence that will provide a focal point for the strategic and effective definition and delivery of IT services across the University; and
- formation of a Data Governance Council chaired by the Chief Data Officer which will define enterprise data types and determine safeguard requirements.

Internal and external relationships

To meet its stated mission, the Cybersecurity Team must function at several levels:

- Strategically: Develop long term security strategies to address evolving technology and increasing threats.
- Operationally: Responsible for security controls and procedures to be developed, deployed, and executed at both campus and system levels.

[10] From the Chief Information Security Officer (CISO) Position Description dated August 2014.

- Collaboratively: Work closely with data governance and security groups at several levels, including campus (UW-MIST, UWIAC), UW System (TISC), and cross-institutional (BTAA Security working group)
- Cooperatively: Provide communication needed to support its role in education, awareness, and training.

The UW–Madison Office of Cybersecurity organization and descriptions shown in this appendix provides a single touch-point for all cybersecurity related groups and organizations. The Cybersecurity Team is a unified team that addresses the full spectrum of cybersecurity related policy, processes, and technology services supported by or provided for the UW–Madison campus. With an eye toward standardization and economy of scale, this team is charged to work within the Mission, Vision, and Guiding Principles described in the main body of this document, performing the role described in the succeeding sections.

Role of the Office of Cybersecurity

The University-wide cybersecurity program protects information in electronic, print, and other formats to assure that information created, acquired, or maintained by the University and its authorized users meets its intended purpose. The program also protects information and its infrastructure from external or internal threats and ensures that UW complies with statutory and regulatory requirements regarding information access, security, and privacy.

Under the leadership of the Chief Information Security Officer (CISO), the Cybersecurity Team is responsible, as an office supporting the Vice Provost for Information Technology and Chief Information Officer, for focus on these six areas:

1. identification and management of IT security risk through governance, risk management and compliance programs;
2. on behalf of the CIO, development of IT and cybersecurity policy, providing leadership for related program planning and documentation;
3. monitoring of the UW–Madison campus and UW-System IT Enterprise and response to cybersecurity incidents;
4. support of IT security engineering actions and active management of applied security controls to reduce risk as part of active cybersecurity defense;
5. promotion of campus leadership and operational entities awareness of cybersecurity threat vectors, attack surfaces, threat actors, IT Security solutions and industry trends; and
6. provision of security education, training and awareness by engaging DoIT Academic Technology and DoIT User Services to elevate the level of understanding among UW–Madison constituents.

The Office of Cybersecurity

The Office of Cybersecurity is established as an office under the Vice Provost for Information Technology and Chief Information Officer. The office is headed by the Director, Office of Cybersecurity, and Chief Information Security Officer, with two assigned Assistant Directors and two Special Assistants. The remaining staff are aligned to four cybersecurity domains as shown in Figure A-1.

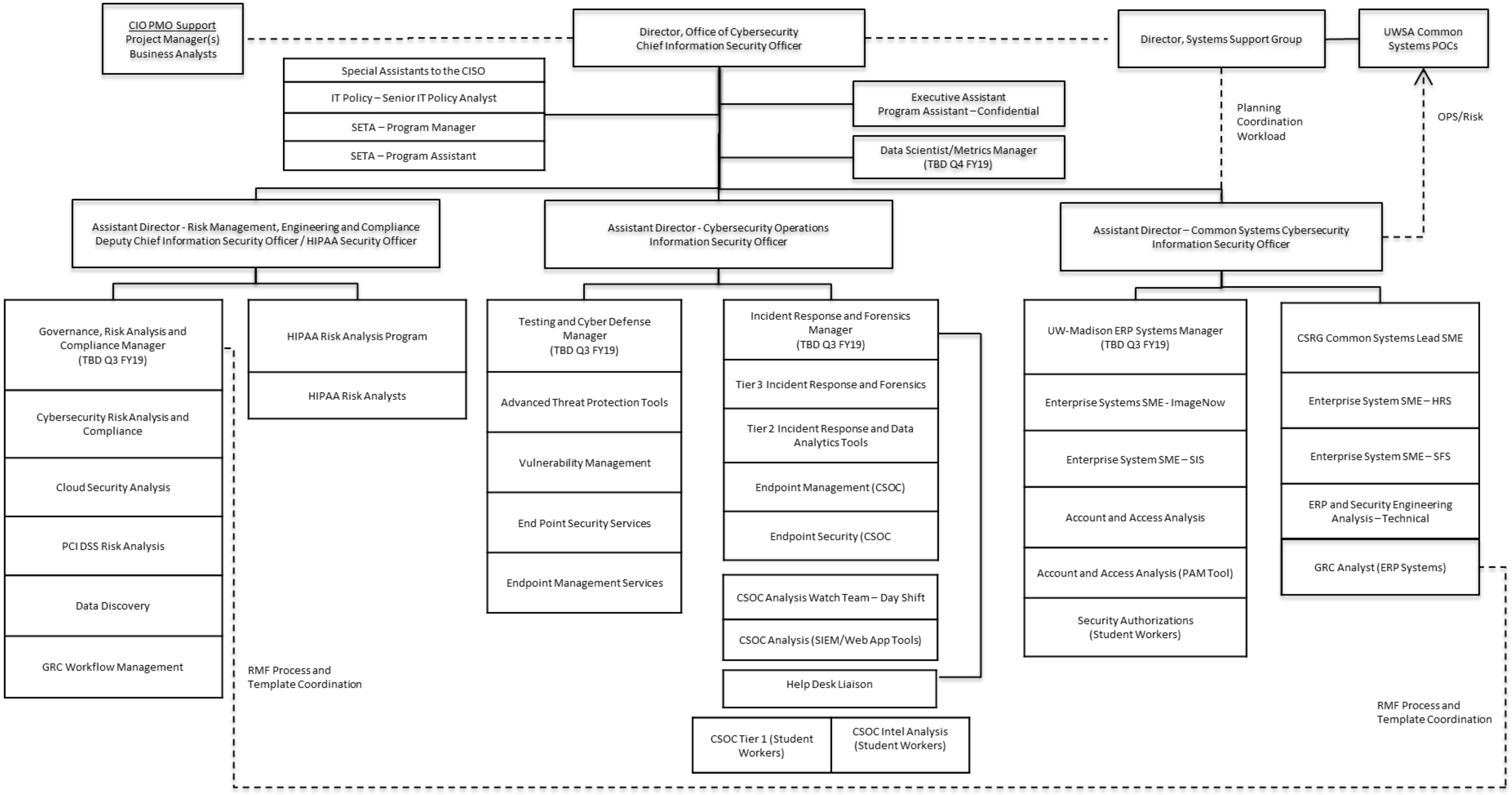
CIO PMO Support
Project Manager(s)
Business Analysts
Director, Office of Cybersecurity
Chief Information Security Officer
Director, Systems Support Group
UWSA Common Systems POCs
Special Assistants to the CISO
IT Policy – Senior IT Policy Analyst
SETA – Program Manager
SETA – Program Assistant
Executive Assistant
Program Assistant – Confidential
Data Scientist/Metrics Manager
(TBD Q4 FY19)
Planning
Coordination
Workload
OPS/Risk
Assistant Director - Risk Management, Engineering and Compliance
Deputy Chief Information Security Officer / HIPAA Security Officer
Assistant Director - Cybersecurity Operations
Information Security Officer
Assistant Director – Common Systems Cybersecurity
Information Security Officer
Governance, Risk Analysis and Compliance Manager
(TBD Q3 FY19)
Cybersecurity Risk Analysis and Compliance
Cloud Security Analysis
PCI DSS Risk Analysis
Data Discovery
GRC Workflow Management
HIPAA Risk Analysis Program
HIPAA Risk Analysts
RMF Process and
Template Coordination
Testing and Cyber Defense Manager
(TBD Q3 FY19)
Advanced Threat Protection Tools
Vulnerability Management
End Point Security Services
Endpoint Management Services
Incident Response and Forensics Manager
(TBD Q3 FY19)
Tier 3 Incident Response and Forensics
Tier 2 Incident Response and Data Analytics Tools
Endpoint Management (CSOC)
Endpoint Security (CSOC
CSOC Analysis Watch Team – Day Shift
CSOC Analysis (SIEM/Web App Tools)
Help Desk Liaison
CSOC Tier 1 (Student Workers)
CSOC Intel Analysis (Student Workers)
UW-Madison ERP Systems Manager
(TBD Q3 FY19)
Enterprise Systems SME - ImageNow
Enterprise System SME – SIS
Account and Access Analysis
Account and Access Analysis (PAM Tool)
Security Authorizations
(Student Workers)
CSRG Common Systems Lead SME
Enterprise System SME – HRS
Enterprise System SME – SFS
ERP and Security Engineering Analysis – Technical
GRC Analyst (ERP Systems)
RMF Process and
Template Coordination

Figure A-1: UW–Madison Office of Cybersecurity Organization (as of December 2018)

Governance, Risk Management and Compliance

This team focuses on governance and methods to accurately identify and assess IT security risks. Through implementation of a Risk Management Framework, they design and architect security strategy and advise system owners and developers on methods to implement security controls for applications and infrastructure. On behalf of the UW–Madison VP-CIO, this team also establishes, monitors, and maintains IT policies and security standards, including the appropriate cybersecurity baselines and plans across campus and in coordination with the various advisory groups.

Common Systems Cybersecurity Team

Although currently focused on Enterprise Resource Planning systems, this team performs security assessments and manages account and role access authorizations across the spectrum of systems managed by DoIT on behalf of the University and UW System Administration.

This team is also responsible for implementing, supporting, operating and monitoring security controls to protect enterprise business applications for UW System in the Common Systems Review Group (CSRG) portfolio.

Over the next few years the Common Systems Cybersecurity Team will adjust focus to secure Systems as a Service (SaaS) environments in the cloud. This includes UW-Madison owned ERP systems to include Student Information Systems and learning management or document imaging systems.

Security Testing and Cyber Defense

This team supports implementation of frameworks and processes that pro-actively identify, assess, and manage vulnerabilities by testing systems throughout the systems' development life cycles. This includes guiding system administration and engineering staff in implementing an appropriate set of IT risk mitigation controls.

Monitoring and Incident Response

Monitor the network and systems for attacks, respond to incidents, and recommend or perform incident remediation.

Special Assistants to the CISO

Security Education, Training and Awareness - This Special Assistant creates and maintains a portfolio of security awareness efforts for students, staff, faculty and other community groups.

IT Policy - This Special Assistant manages the IT Policy portfolio and facilitates the policy planning processes to include communications outreach to UW–Madison communities.

IT and Cybersecurity Staff external to the Office of Cybersecurity

IT Security staff supporting the CIOs, IT Directors, and IT teams in the individual Schools, Institutions, Colleges, and Departments (SCIDs) interact with the Office of Cybersecurity on an individual basis or as part of the Madison Information Security Team (MIST). Functional relationships among the various campus and off-campus groups and how they interact with the Cybersecurity Team based on the various relationships are shown in Figure A-2.

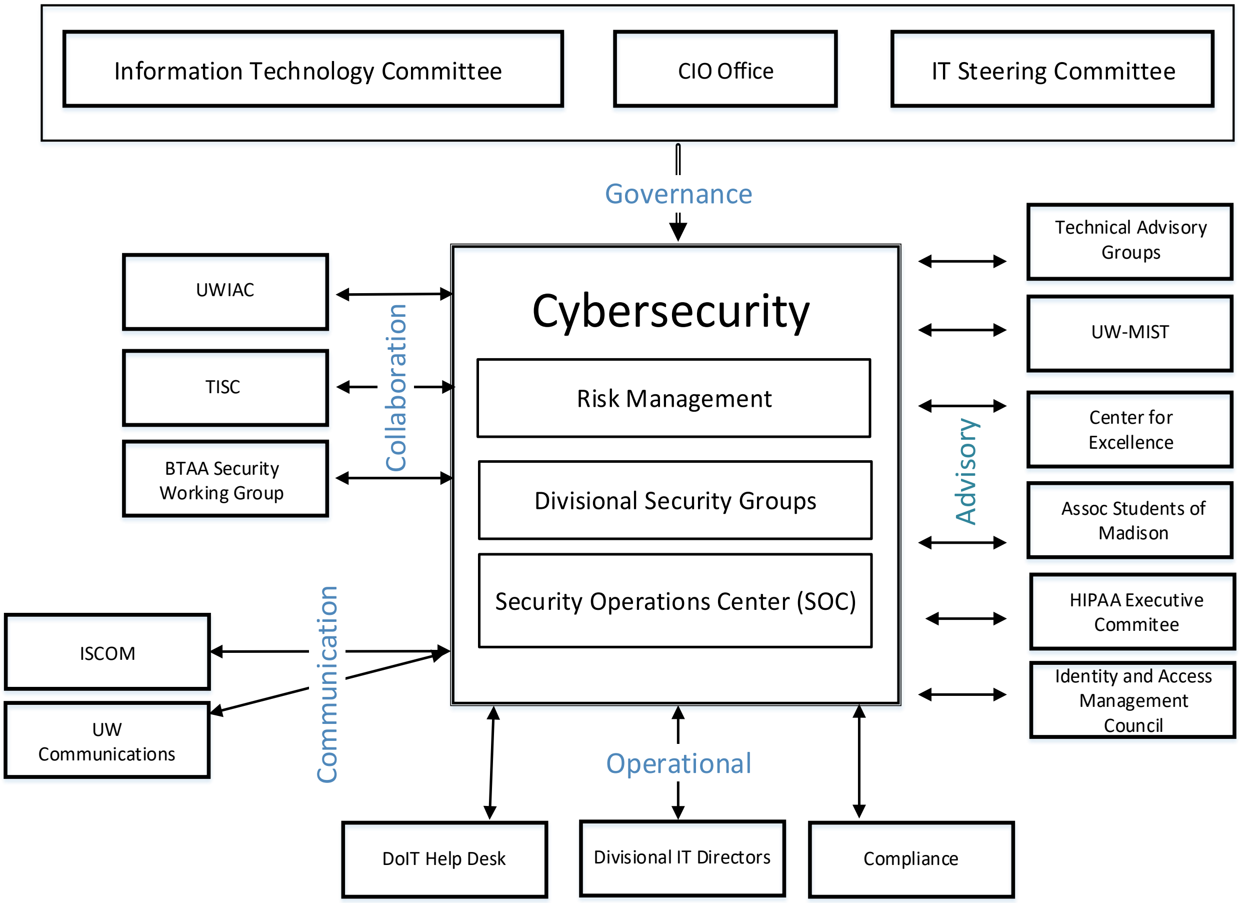

Figure A-2: Cybersecurity Governance, Advisory, and Operational Relationships

External to UW-Madison, the Chief Information Security Officer is the UW-Madison voting member of the University of Wisconsin Technical Information Security Committee (UW TISC) and works directly with University of Wisconsin System Administration (UWSA) information security leadership. The UWSA Associate Vice President for Information Security and the UWSA CISO have a direct interface with the UW-Madison CISO and may occasionally seek services and advice from the staff, with particular emphasis on UW Common Systems.

Governance Bodies and Committees

The organizational charts and descriptions that follow define the various governance structures and alignments that are significant to the UW–Madison and UW System's distributed governance structure.

Lines of Authority

Reporting relationships vary widely among schools, colleges and divisions at UW–Madison. And from a practical perspective, there are approximately seven tiers.

1. Board of Regents of the University of Wisconsin System.
2. President, University of Wisconsin System.
3. UW–Madison Chancellor.

4. UW–Madison Provost, UW–Madison Vice Chancellor for Finance and Administration (VCFA), Vice Chancellor for Legal Affairs, and Vice Chancellor for Research and Graduate Education.
    a. These executives support the Chancellor as members of the Chancellor's cabinet.
5. Deans and Directors of Schools, Colleges, Institutions, and Divisions.
6. UW–Madison Vice Provost for Information Technology and Chief Information Officer.

Official UW System Cybersecurity Advisory Relationships

Within the UW System, there are two tiers of advisory relationships for cybersecurity at the UW System level which align to campus leadership through interaction with the Information Technology Management Council and the UW System Technical Information Security Council as well as the organizations responsible for components of Common Systems (e.g. HRS, SFS, Learn@UW).

1. The Information Technology Management Council (ITMC) consists of the CIO of each UW system campuses and is led by the CIO of UW System Administration. The "CIO Council" meets monthly. There is also a semi-annual ITMC conference. The CIO council is advisory to UW System leadership and each other.
2. The group focused on information security is called the UW Technical Information Security Council (UW TISC). UW TISC consists of the CISO, Information Security Officer (ISO), or other designated security representatives from each institution. Additional people from some institutions also attend the council's meeting at the ITMC conferences. UW TISC reports to the UWSA Assistant Vice President for Information Security and is advisory to the CIO council and each other.

Other Governance Arrangements

Not included in this document are other data domains that have their own governance arrangements. These are important areas of cybersecurity governance, but the list is too long and too detailed for an overview in this strategic plan.

Volume II – The Cybersecurity Strategy, Challenges and Opportunities

> "A strategy is multi-dimensional planning, multi-team collaboration, and multitasking action."
>
> — Pearl Zhu
> Digital Valley: Five Pearls of Wisdom to Make Profound Influence

Cybersecurity Strategies, Goals, and Metrics

The 2015 Cybersecurity Strategy introduced seven strategic elements that started with defining how data is governed and classified, and how risk could be effectively managed within a framework based on NIST principles and adaptation of the guidelines normally assigned for federal information systems. After two years operating within the 2015 strategy, several of those seven strategic elements were completed or significantly accomplished; the remaining needed performance improvement as the state of the UW-Madison Cybersecurity Program evolved. In this next iteration of the Strategy, the existing goals that establish a sense of community were modified or restated and will improve the levels of competence within the cybersecurity team and the distributed IT community. There are additional changes to strategic elements seeking to better manage security through consolidation of tools, tactics, techniques, and procedures. The Office of Cybersecurity remains the driving force in continuing to implement those strategies and goals that focus on optimizing information security and delivery of cybersecurity services by measuring actions and effects through CDM.

This integration of the Strategy establishes new approaches and goals that support appropriate classification of information and protection of data; those establishing trust that information security services will be respectful of academic freedom; those which address risk detection and enable operations that detect and mitigate threats; and those that promote research and outreach in partnership with key stakeholders. The Office of Cybersecurity is committed to presenting a coherent Strategy embodied in the elements listed in this appendix that clearly define the strategy, list the goals, and include metrics that will be tracked to determine goal status and achievement. Each strategic element will have a clear linkage to the UW-Madison Strategic Framework *for Wisconsin and the World*[11].

Strategy #1 – Community

Build a community of experts to improve institutional user competence through Security Education, Training, and Awareness.

The UW-Madison community is defined as group of people working together to achieve common goals. At a high level, the goal is the mission of teaching, research, and outreach. However, there may be smaller, focused communities working towards specific objectives. UW-Madison information system users are well-educated and considered to be the strongest non-technical security control available. Accounting for the human factor - not technology - is key to establishing an adequate and appropriate level of security. If people are the key, more attention must be paid to preparing and maintaining this "asset." A robust and enterprise-wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them. An effective IT security awareness and training program instills proper rules

[11] The UW-Madison Strategic Plan can be found at https://chancellor.wisc.edu/strategicplan2/

of behavior for the use of IT systems and information as well as empower the community to align with secure computing habits. The program communicates IT security policies and procedures that need to be followed. This must precede and support any impacts due to noncompliance. A successful program is measured, assessed, and modified over time.

Goals and Metrics

The following goals have been established to address these strategic elements over the next five years:

1. Goal: The Security Education, Training, and Awareness (SETA) Lead will include all relevant and interested people in campus community cybersecurity awareness efforts. The Office of Cybersecurity will establish a program to survey UW–Madison communities and identify relevant and interested security-related needs, which may include basic security skills, advanced security tools instruction, or advanced cybersecurity assessment and audit techniques. The program should begin January 2019.

2. Goal: The SETA Lead will work with the campus community to define specific security awareness programs (e.g. security staff, developers, people who are in charge of securing applications and data, students, administrators, faculty, or researchers).

   a. Create and conduct an annual survey to measure Cybersecurity Awareness in the campus communities (faculty, staff, and students), with the first survey to occur during October 2018 and results evaluated by December 2018. This survey will become an annual event with results and updates posted on the Office of Cybersecurity website during the following Winter/Spring academic term.

   b. Prior to January 2019: In alignment with UW System Administration Policy 1032, refine and further develop annual training and awareness for all employees appropriate to their role.

   c. Prior to Summer 2019: Develop risk management training programs based on input from groups who were involved with assessments under the Risk Management Framework.

3. Goal: In coordination with MIST, the CISO and Deputy CISO will take positive steps to improve awareness of cybersecurity initiatives by:

   a. Developing a set of venues (webpage, bulletin boards, and handouts) for the campus community to view helpful cybersecurity information on learn about cybersecurity initiatives, and provide a process to accept and process feedback.

   b. Creating a link on the Office of Cybersecurity site (https://it.wisc.edu/about/office-of-the-cio/cybersecurity/) to a form that allows community members to submit feedback.

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
6.3	Institutions collaborate with key stakeholders for the relevant data (e.g. consult with the registrar about student data) to assess and identify sensitive information that requires encryption and integrity controls. Review data residing in relational databases, file shares and large-scale storage, E-mail systems, user workstations, mobile devices (PDAs, smartphones and removable media) and backup media.	12/31/2018	12/31/2018
8.2	Conduct UW System-wide RFP for privileged account escalation software.	10/31/2018	2/28/2019
8.3	Work with institutions to implement a process or technological solution that allows for the temporary, on-demand escalation of privileges.	1/31/2019	1/31/2019
9.2	Assign an individual to develop and lead a UW system wide IS Risk Management program.	7/31/2018	Completed
9.2a	Create a proposed information security (IS) risk management program to	11/1/2018	Completed

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
	properly identify and manage data risk.		
10.2	Perform an exercise, in collaboration with key stakeholders from all UW institutions to identify the strengths and weaknesses of the current products. Document the results of this exercise.	6/1/2019	6/1/2019
10.3	Conduct UW System wide RFP for training and awareness materials that satisfy the identified gaps and weaknesses in the current products.	8/1/2019	8/1/2019
10.4	Make training / awareness materials available to all UW institutions.	8/15/2019	8/15/2019
10.6	Verify and validate that institution training materials encompass key IS topics delineated in the Security Awareness & Training Standards document including but not limited to social engineering, sensitive data protection, password security, ransomware, and email security.	10/15/2019	10/1/2019
11.1	Create a framework for institutions to request and help select tools that best fit their needs.	11/1/2019	11/1/2019
11.2	In addition, to the "Compensating Controls Form", develop a process by which institutions with limited budgets can request approval for lower cost/ open source tools (that meet or exceed applicable standards documents).	1/1/2019	1/1/2019
12.2	Once SME's have been identified, create an easily accessible internal document with the names, areas of expertise and contact information for each SME. Establish a requirement to review these selections periodically.	12/1/2019	12/1/2019
12.5	Implement a professional development training plan UW system-wide to meet IT/IS requirements.	3/1/2020	3/1/2020
14.3	Assist any institutions that do not have a patch testing and deployment processes with development and implementation.	11/30/2019	11/30/2019

Links to Campus Strategy

- create the best possible environment in which people can carry out their responsibilities to the university;
- promote resource stewardship, improve service delivery and efficiency, and ensure administrative capacity; and
- sponsor a comprehensive campaign to invest in the future of the university and the students, faculty, and staff who will shape the future of Wisconsin and the world.

Strategy #2 – Service Alignment

Build and align cybersecurity services used by the Office of Cybersecurity and distributed IT service providers to gain efficiencies for UW–Madison and UW System by utilizing common best practices.

UW–Madison has the responsibility to support campus cybersecurity and computing including those associated with UW System. Making campus best practices in security operations available to all UW campuses at scale saves considerable cost and resources. There needs to be greater engagement between the Cybersecurity Team, IT service providers, and distributed IT organizations to create relationships that lead to sustainable security services that are respectful to academic freedom and personal privacy, with well-defined frameworks and processes. Services will need to be adequately resourced to meet metrics for success, which must include response time to cybersecurity incidents and events.

1. Goal: Establish an annual review of campus Cybersecurity services and operations to ensure alignment with Cybersecurity strategies. This requires engagement with the community to address their unique cybersecurity related requirements. Also included are cybersecurity consulting during software selection and cybersecurity expertise embedded in an implementation team. On the same schedule, provide governance groups with data that enables decisions on the creation, retention, or discontinuation of services based on utilization, risk reduction, costs, and alignment with strategy. This goal includes ensuring retained services are provided with the level of resources needed for

success. The following are tactical steps to meet this goal:

a. the CISO will encourage MIST members to confer with their Divisional CIOs or IT Directors to define criteria that describes security service operations by January 31, 2018;

b. the CISO will create a governance oversight process by November 1, 2018;

c. the CISO will provide yearly metrics on service adjustments or service creations to IT governance, including all TAGs beginning May 30, 2019.

2. Goal: The CISO is accountable for ensuring that best practices respect UW–Madison faculty, staff, and student values, norms, and privacy regarding research equipment and data. Every three years, the CISO will engage the distributed IT community to identify common best practice approaches for existing services and identify gaps or redundancies in service operations. This will include collaboration with local and national experts on processes to merge best practices into existing services to achieve holistic solutions throughout UW System. By July 2018, the CISO will identify a designee to engage the Big Ten Academic Alliance and UW System (duties will include attending breakout security group meetings and collecting key documents).

3. Goal: The Deputy CISO and Assistant Director of Cybersecurity Operations will identify all service operations from each Cybersecurity domain that should be transitioned to the Cybersecurity Operations Center (CSOC). Each Cybersecurity domain will evaluate and publish goals to operationalize functions from their domain into CSOC capabilities by November 2018.

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
3.2	Establish a process for institutions to conduct a review of locally owned IT-related assets and define categories under which these assets will fall (capital, data center, network, end-user, etc.).	8/31/2018	10/31/2018
3.2a	Institutions begin conducting inventory, with categorization, of IT-related assets.	10/1/2018	10/31/2018
3.2b	Institutions complete inventory of IT-related assets.	12/31/2018	12/31/2018
3.3	Conduct RFP for UW System-wide asset management solution, for IT-related assets.	12/31/2018	12/31/2018
3.3a	For institutions with decentralized IT management, help design and implement a tool that all IT departments can leverage to manage their own assets but provide the central IT function with ongoing visibility into tracked assets. UW System should explore viability of engaging consultants to accelerate asset management.	1/31/2019	1/31/2019
3.6	Establish a requirement and process to audit the inventory database annually, with all departments participating and verifying the presence of each asset and all associated information.	7/1/2019	7/1/2019
4.1a	Conduct cost analysis of network protection solutions for potential UW Common System purchase.	8/31/2018	Complete
4.2a	Conduct cost analysis of security monitoring solutions for potential UW Common System purchase.	8/31/2018	TBD
4.3	Institutions create an inventory of systems that produce security related logging data. Potential sources include (but are not limited to): operating systems, application servers, databases, cloud services, firewalls, security sensors, workstations, and network switching/routing appliances.	12/31/2018	12/31/2018
4.3a	All inventoried system logs must be collected in central logging repository.	2/28/2019	4/30/2019
4.4	Establish a requirement for the log source inventory to be reviewed at least annually at the institution-level.	3/1/2019	3/1/2019
4.5	Institutions verify that all logging requirements as prescribed in the Security Monitoring Standard have been achieved.	4/1/2019	10/1/2019
6.2	Conduct cost analysis of data encryption solutions for potential UW Common System purchase.	11/1/2018	TBD

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
6.3	Institutions collaborate with key stakeholders for the relevant data (e.g. consult with the registrar about student data) to assess and identify sensitive information that requires encryption and integrity controls. Review data residing in relational databases, file shares and large-scale storage, E-mail systems, user workstations, mobile devices (PDAs, smartphones and removable media) and backup media.	12/31/2018	TBD
6.4	Verify and validate that the requirements as prescribed in the Endpoint Protection Standard have been achieved at each institution.	4/1/2019	TBD
13.2	Assist any institutions that do not have a user entitlement review process with the implementation, planning and logistics of a user entitlement review process.	7/1/2019	TBD
13.3	Institutions submit their user entitlement review process and UW System ensures that all requirements listed in the Entitlement Review section of the Identity and Access Management Standard have been addressed.	12/1/2019	TBD
14.3	Assist any institutions that do not have a patch testing and deployment processes with development and implementation.	11/30/2019	TBD
14.4	Ensure that institutions have developed schedules and maintenance windows for patch management, software and virus definition updates.	1/1/2019	TBD
14.5	Verify that all institutions have established processes and procedures that meet or exceed the requirements regarding patch application, as described in the Endpoint Protection Standard and Threat and Vulnerability Management Standard.	2/1/2019	TBD

Links to Campus Strategy

- promote resource stewardship, improve service delivery and efficiency, and ensure administrative capacity;
- create a stable and sustainable financial structure through the implementation of a transformed budget model;
- identify and pursue new revenue sources aligned with the institution's mission and goals;
- promote environmental sustainability through campus operations, integrated with research and education; and
- transform library structures and technologies to best support research and learning, and to attain campus efficiencies.

Strategy #3 – Measure

Establish security metrics, optimize services, promote compliance, achieve Continuous Diagnostics and Mitigation.

Security metrics are collected and analyzed to communicate the security posture at UW–Madison. By collecting and communicating security metrics, cybersecurity professionals may:

- validate security controls are working as designed and address inadequate controls;
- identify emerging threats and trends;
- ensure successful compliance with required policies, regulatory requirements, and standards; and
- ensure that repeatable funding is being allocated. The measurement of security control status is completed at intervals sufficient to support the goals.

The Cybersecurity Team, distributed IT managers, and distributed security staff must work together to successfully address the network's ability to produce and report cybersecurity metrics that reflect the status and trends associated with key security functions.

To develop a service model that supports Continuous Diagnostics and Mitigation (CDM) (which deploys tools and services that provide ongoing measurement of the risk profile of the Information Technology enterprise), CDM informs responses to events and strengthens the cybersecurity posture of networks and information. CDM is an integral part of a Risk Management Framework that supports the Systems Development Life Cycle.

To effect accomplishment of this strategy, the CISO will establish a Data Scientist and Metrics Manager position in the Office of Cybersecurity. This position will report directly to the CISO and will have authority to work with Assistant Directors in the Office of Cybersecurity and divisional IT organizations in order to develop processes and tools to harvest data from existing or future systems, tools, processes and people and create a Cybersecurity Metrics Management program. Other duties will include maturing the metrics and goals for all of the strategies in this volume and to provide a user friendly reporting interface for organizations and researchers to use cybersecurity data to improve operations within the UW-Madison Information Security Program.

Goals and Metrics

1. Goal: By July 2019, the Deputy CISO and Assistant Director of Cybersecurity Operations are responsible for establishing and implementing a framework for CDM. Considerations for developing this model should include the identification of gaps in the existing set of tools and operational capabilities based on the US-CERT CDM Framework by January 2019.

2. Goal: By July 2019, the CISO will develop and implement a process to determine if tools and service operations are being used and are adequately supported. The process should include a decision-making process for discontinuing a service and should align to support campus policies. Considerations for completing this goal include:

   a. By December 2018, document the portfolio of existing tools, including capabilities and operational support.

   b. By December 2018, identify how each existing tool aligns with cybersecurity strategy.

   c. By February 2019, gather metrics and report on usage and Total Cost of Ownership (TCO) of each tool.

3. Goal: By January 2019, the Deputy CISO and the Governance, Risk Management, and Compliance Lead are responsible for creating and implementing a method to track engagements of the Risk Management Process. They will then determine effectiveness of the program, track recurring risks to provide common mitigation solutions, and optimize services or to training it staff for effectiveness. A method to monitor how to service the process at scale will be included. They will publish quarterly reports to the CISO and CIO.

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
4.1a	Conduct cost analysis of network protection solutions for potential UW Common System purchase.	8/31/2018	Complete
4.2a	Conduct cost analysis of security monitoring solutions for potential UW Common System purchase.	8/31/2018	TBD
4.3	Institutions create an inventory of systems that produce security related logging data. Potential sources include (but are not limited to): operating systems, application servers, databases, cloud services, firewalls, security sensors, workstations, and network switching/routing appliances.	12/31/2018	12/31/2018
4.3a	All inventoried system logs must be collected in central logging repository.	2/28/2019	4/30/2019
4.5	Institutions verify that all logging requirements as prescribed in the	4/1/2019	10/1/2019

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
	Security Monitoring Standard have been achieved.		
5.3a	Institutional Record Custodians verify that data retention schedules are properly implemented at each UW institution to meet regulatory, contractual and compliance requirements.	1/15/2019	Complete
5.6	Verify and validate that the requirements regarding the encryption, prevention of loss, data leakage, and integrity have been achieved at each institution as prescribed in the Data Protection Standard.	4/1/2019	4/1/2019
6.4	Verify and validate that the requirements have been achieved at each institution as prescribed in the Endpoint Protection Standard.	4/1/2019	12/15/2019
7.7	Conduct cost analysis of annualized spending for system-wide Multifactor Authentication to determine if cost efficiencies can be realized.	7/15/2019	7/15/2019
7.8	Verify and validate that institutions have developed and implemented configurations for Multifactor Authentication that meet or exceed the requirements prescribed in the Identify and Access Management Standard.	7/15/2019	6/30/2019
8.4	Verify and validate that institutions have a process in place for the setup and maintenance of all Privileged Accounts that meets or exceeds the requirements prescribed in the Identity and Access Management Standard.	1/1/2020	8/1/2019
9.4	Determine costs associated with UW system-wide comprehensive risk management training, and relevant risk management training solutions.	2/28/2019	08/15/2019
9.7a	Verify and validate that the each institution's risk register meets or exceeds the requirements delineated in the Risk Management Standards document.	9/15/2019	03/15/2020
9.8	Verify and validate that each institution's Risk Management programs meet or exceed the minimum standards prescribed in the assessment, analysis, and remediation phases of the Risk Management Standards document.	10/1/2019	03/15/2020
14.7	Verify and validate that institutions are ensuring that missing patches can be identified and patch level for software, systems and network are being reported.	4/1/2019	4/1/2019

Links to Campus Strategy

- Promote resource stewardship, improve service delivery and efficiency, and ensure administrative capacity.

Strategy #4 – Data

Develop processes that aid end-users and organizations in managing data throughout its lifecycle, including provision of services that support data inventory, classification, and protection as defined in Risk Management Framework.

For the past few years, data protection at UW–Madison has been rightly focused on policy, standards, and governance. Now, as significant progress has been made within these focus areas, it is important that all campus units are fully included in the execution of the data protection program and processes in a deep, meaningful, and participatory way.

It is critical that all campus units have the proper information regarding University data handling and security practices. The Office should provide educational materials to campus units to aid in their understanding of data classification, handling, and security controls. This may include developing alternative ways for research, clinical, academic, and administration units to store restricted data.

Goals and Metrics

1. Goal: Prior to the 2019-2020 Academic Year, develop templates of ready-to-implement *security controls* - safeguards or countermeasures to avoid, detect,[12] counteract, or minimize security risks - appropriate for each data classification, and make them widely available and well-promoted.
    - Metric: *% compliance (via scans or self-reporting); template for each of 4 data classifications; # of shares.*
2. Goal: Ongoing through FY-19, promote and encourage the development of cost-effective restricted data[13] storage services.
    - Metric: *Is there a restricted data storage service; % utilization of restricted data storage as function of time; # of units making use of services.*
3. Goal: In January 2019 assess User awareness and the use of educational materials. Develop and execute a project to increase by 50 percent the number of campus stakeholders that make use of materials or attend data protection educational events, and offer pathways to credentialing and certifications.
    - Metric: *# number attendees at events; # events per year, # of credentials or certifications earned per year.*

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
5.2	Institutions appoint Data Stewards for specific types of data (e.g. the Registrar for student data). It is the responsibility of the Data Steward to work with Security, Privacy and/or Data Officers to assure that the data is classified appropriately.	10/31/2018	12/31/2018
5.3	Each UW institution identifies and assigns a Record Custodian to meet the Record Custodian responsibilities.	11/30/2018	Complete
5.3a	Institutional Record Custodians verify that data retention schedules are properly implemented at each UW institution to meet regulatory, contractual and compliance requirements.	1/15/2019	6/30/2018
5.4	Ensure that Data Stewards are enforcing compliance of data retention and destruction policies.	2/1/2019	2/1/2019
5.5	Establish a requirement for Data Stewards to review data classifications at least annually.	3/1/2019	3/1/2019
5.6	Verify and validate that the requirements regarding the encryption, prevention of loss, data leakage and integrity have been achieved at each institution as prescribed in the Data Protection Standard.	4/1/2019	4/1/2019
6.3	Institutions collaborate with key stakeholders for the relevant data (e.g. consult with the registrar about student data) to assess and identify sensitive information that requires encryption and integrity controls. Review data residing in relational databases, file shares and large-scale storage, E-mail systems, user workstations, mobile devices (PDAs, smartphones and removable media), and backup media.	12/31/2018	2/1/2019
8.1	Ensure that institutions have established a requirement for the periodic review of existing privileged accounts to verify continuing need.	8/1/2018	12/31/2018
8.3	Work with institutions to implement a process or technological solution that allows for the temporary, on-demand escalation of privileges.	1/31/2019	3/15/2019

[12] United States., Joint Task Force Transformation Initiative. (2013). Security and privacy controls for federal information systems and organizations (pp. B-21). Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved September 14, 2017, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[13] Restricted Data Security Standards. (2017, May 19). Retrieved September 11, 2017, from https://it.wisc.edu/about/office-of-the-cio/cybersecurity/security-tools-software/restricted-data-security-standards/

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
8.4	Verify and validate that institutions have a process in place for the setup and maintenance of all Privileged Accounts that meets or exceeds the requirements prescribed in the Identity and Access Management Standard.	1/1/2020	1/1/2020
13.1	Verify that all institutions have a user entitlement review process and ensure everyone has what they need to meet minimum stanadards.	6/1/2019	TBD
13.3	Institutions submit their user entitlement review process and UW System ensures that all requirements listed in the Entitlement Review section of the Identity and Access Management Standard have been addressed.	12/1/2019	TBD
13.4	Institutions establish a schedule for when each access type will be reviewed, based on the varying degrees of access.	2/1/2020	TBD
14.2	Review of each institution's processes for the testing and deployment of patches.	8/15/2019	TBD
14.3	Assist any institutions that do not have a patch testing and deployment processes with development and implementation.	11/30/2019	TBD
14.4	Ensure that institutions have developed schedules and maintenance windows for patch management, software and virus definition updates.	1/1/2019	TBD
14.5	Verify that all institutions have established processes and procedures that meet or exceed the requirements regarding patch application, as described in the Endpoint Protection Standard and Threat and Vulnerability Management Standard.	2/1/2019	TBD

Links to Campus Strategy

- Optimize the research and scholarship infrastructure on the university;
- nurture growth of people through professional development and performance excellence;
- create the best possible environment in which people can carry out their responsibilities to the university;
- promote resource stewardship, improve service delivery and efficiency, and ensure administrative capacity; and
- commit to being responsible stewards of human, intellectual, cultural, financial, and environmental resources.

Strategy #5 – Trust

Improve relationships that advance trust through understanding among local and distributed IT organizations, service providers, and the Office of Cybersecurity. This includes jointly developing sustainable security services that are respectful to academic freedom and personal privacy, with well-defined frameworks and processes that allow close collaboration between campus stakeholders and the Office of Cybersecurity.

Maximum effectiveness requires a high level of trust between Office of Cybersecurity and stakeholders such as Risk Executives, researchers and research centers, faculty, students, IT staff, and administrators. The Office must be trustworthy in order to facilitate access to equipment and information while encouraging open discussions of data practices. Acknowledging the expertise that resides in the distributed IT organizations and in larger service providing organizations like the Administrative Information Management Services (AIMS) and the Division of Information Technology (DoIT) offers opportunities to increase trust through technical exchanges that are respectful of the intellectual capital and technology investments made by all parties. Furthermore, trust will encourage higher rates of adoption of best practices and policies.

Developing trustworthiness requires open and regular communication with stakeholder communities. Increased interaction with stakeholders will also lead to more usable systems, policies, and practices as developers gain a richer understanding of user values, requirements, and constraints.

Increasing trust between Office of Cybersecurity and stakeholders reflects University of Wisconsin–Madison traditions of shared governance and decision making. Trust promotes the exchange of ideas and viewpoints consistent with the sifting and winnowing ideals of campus. While trust is often intangible and difficult to measure, the Office will use these provisional metrics. Understanding their inadequacy, additional survey methods including third party reviews will be pursued. The goals below are considered ongoing and are not bound by time related metrics.

Goals and Metrics

1. Goal: Enhance positive work relationships through fielding advanced cybersecurity services offerings, socializing and vetting services, and processes via face-to-face stakeholder meetings, with a specific emphasis on frequent, low-effort, high-impact interactions.
    - Metric: *number of campus stakeholders served by Cybersecurity-provided services based on the number of campus stakeholders reached.*
2. Goal: Provide a diverse group of input mechanisms for campus stakeholders, with a particular emphasis on decisions impacting intellectual freedom and personal privacy.
    - Metric: *describe number and type of input mechanisms.*
3. Goal: Clearly demonstrate to campus stakeholders an enduring respect for academic freedom and personal privacy in cybersecurity operations by leveraging internal and external marketing expertise. Where necessary, develop messages specific to diverse communities which address unique community issues (e.g., cybersecurity requirements should enable research progress and not hinder the research community).
    - Metric: *# of communication messages, evidence of use of constructive feedback to improve messaging, # of adverse comments showing lack of respect for constituents or communities.*

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
2.1	Create an avenue for institutions to leverage UW System legal function for compliance identification and collaboration (through TISC, CIO Council, etc.) on a plan for addressing compliance obligations.	5/31/2018	TBD
2.1b	Establish initial communications between UW System Legal and collaborative groups (TISC, IAC, CIO Council, etc.)	5/31/2018	TBD
2.2	Create a compliance liaison position who will serve as the champion of compliance awareness at the System level and function as the point of contact and subject matter expert for institutions regarding compliance-related matters.	7/1/2018	TBD
7.4	Assist any institutions that have not yet begun Multifactor Authentication implementation with planning and logistics.	12/15/2018	12/15/2018
8.3	Work with institutions to implement a process or technological solution that allows for the temporary, on-demand escalation of privileges.	1/31/2019	1/31/2019
9.4a	Train all relevant personnel on risk management.	5/1/2019	08/15/2020
9.6	Establish a process and materials to help raise awareness among senior institution members (e.g. Chancellors, Provosts) of the importance of information systems risk management within a general risk management program.	7/1/2019	3/27/2019
10.2	Perform an exercise, in collaboration with key stakeholders from all UW institutions, to identify the strengths and weaknesses of the current products. Document the results of this exercise.	6/1/2019	6/1/2019
10.4	Make training and awareness materials available to all UW institutions.	8/15/2019	8/15/2019
11.1	Create a framework for institutions to request and help select tools that best fit their needs.	11/1/2019	11/1/2019
13.2	Assist any institutions that do not have a user entitlement review process	7/1/2019	7/1/2019

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
	with the implementation, planning and logistics of a user entitlement review process.		
14.3	Assist any institutions that do not have a patch testing and deployment processes with development and implementation.	11/30/2019	11/30/2019

Links to Campus Strategy

- Create the best possible environment in which people can carry out their responsibilities to the university.
  - There is a belief in the importance of working with and learning from those of differing backgrounds and views.

Strategy #6 – Operational Risk

Establish a centralized process to detect and mitigate threats, disseminate threat intelligence, and to improve those capabilities for stakeholders.

It is important that UW–Madison maintain a Cybersecurity Operations Center (CSOC) to improve its security posture, as well as work on preventing, analyzing, and responding to cybersecurity incidents. Further, the CSOC should also partner with campus academic units to offer educational experiences, student jobs, internships, research, and public activities in the areas of cybersecurity and society, cybersecurity management and analysis, privacy, and identity management.

In order to accomplish this strategy, the CSOC will need to continue developing or refining:

- Executive sponsorship and governance
- Useful Cybersecurity metrics
- Access to campus data and system information
- Partnerships with campus academic units
- A long-term funding model that supports staffing and tools
- Repeatable processes where possible
- Effective communication with campus units
- Collaboration across distributed campus information technology units
- Connections to external threat sharing organizations

Goals

1. Goal: Continue to evolve the cybersecurity operations center (CSOC) to be leveraged by the UW–Madison and UW System to detect and analyze threats with due consideration to expansion of service to 24-hour operations by July 1, 2019. The CSOC staff will assist with analysis, infrastructure support, vulnerability management, forensics and threat reporting.
   - Metric: *# of CSOC security event "plays" that are developed and tracked over time. # of tickets processed by the CSOC, other actions as required or evolving from the 2018 UW System Administration Information Security Program.*
2. Goal: Implement and maintain a resource that connects security contact(s) to users, groups of users (e.g. UDDS), and network assets (e.g. IP addresses, vLANs, Firewalls). Access and contact assignment should be role-based whenever possible.
   - Metric: *% of contacts; % of campus claimed by contacts; does the system exist; % of contacts verified in the last year.*

3. Goal: Develop and implement CSOC service levels beginning with the default service level - which all devices on the campus network receive - and progressing to other levels of additional service based on individual unit needs.
   - Metric: *# of units and/or # devices on boarded to service levels beyond "default."*
   - Metric: *Onboard the SIS, SFS and HRS as the first environments to enjoy a higher service level.*

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
3.2	Establish a process for institutions to conduct a review of locally owned IT-related assets and define categories under which these assets will fall (capital, data center, network, end-user, etc.).	8/31/2018	10/31/2018
3.2a	Institutions begin conducting inventory, with categorization, of IT-related assets.	10/1/2018	10/31/2018
3.3a	For institutions with decentralized IT management, help design and implement a tool that all IT departments can leverage to manage their own assets, but provide the central IT function with ongoing visibility into tracked assets. UW System should explore the viability of engaging consultants to accelerate asset management.	1/31/2019	1/31/2019
3.3b	If an enterprise inventory system for IT assets has not been implemented at institutions, assist those institutions with data collection for future integration into a UW System-wide asset management solution.	1/31/2019	1/31/2019
3.4	Institutions populate a UW System-wide asset management solution with current IT assets.	4/31/19	1/31/2019
3.5	Assist institutions in performing a risk analysis exercise on all critical IT-related assets to determine the potential effects of the asset experiencing a loss of service as a result of a cyberattack, accident, disaster, or emergency. UW Incident Response Policy and Standards documents [1033 and 1033.A] inform the risk analysis.	6/30/2019	6/30/2019
4.3	Institutions create an inventory of systems that produce security-related logging data. Potential sources include (but are not limited to): operating systems, application servers, databases, cloud services, firewalls, security sensors, workstations, and network switching/routing appliances.	12/31/2018	12/31/2018
4.3a	All inventoried system logs must be collected in central logging repository.	2/28/2019	4/30/2019
4.4	Establish a requirement for the log source inventory to be reviewed at least annually at the institution level.	3/1/2019	3/1/2019
4.5	Institutions verify that all logging requirements have been achieved as prescribed in the Security Monitoring Standard.	4/1/2019	10/1/2019
9.7	Institutions create or purchase a risk register solution that serves as a central repository for all risks identified via vulnerability assessments, external and internal pen tests, leadership discussions, third party assessments, and other data points. Additionally, the chosen solution must include a mechanism by which residual risks can be tracked and decisions documented.	9/1/2019	02/28/2019
9.8	Verify and validate that each institution's Risk Management programs meet or exceed the minimum standards prescribed in the assessment, analysis, and remediation phases of the Risk Management Standards document.	10/1/2019	03/15/2020
9.9	Create an exception management or risk acceptance program to track situations in which UW institutions are unable to precisely follow the UW Risk Management policy [1039].	10/15/2019	03/15/2020

Links to Campus Strategy

- Improve access and affordability through need-based financial aid, scholarships, and fellowships to ensure socioeconomic diversity and timely completion.
- Scale Wisconsin Experience opportunities through innovative classroom environments and active learning, locally and globally, to prepare students for successful careers and lives.

- Promote resource stewardship, improve service delivery and efficiency, and ensure administrative capacity.
- Commit to being responsible stewards of human, intellectual, cultural, financial, and environmental resources.

Strategy #7 – Research and Outreach

Partner with stakeholders at the University to be the champion for educational experiences, student jobs, internships, research and public activities, risk management and analysis, privacy, and identity management, thereby becoming a model organization for other cybersecurity teams throughout Wisconsin.

UW–Madison has a unique collection of human, technical, and cultural resources, making it an ideal candidate to become a world leader in cybersecurity research and outreach. At the University's core is the Wisconsin Idea. First articulated in 1905, the Wisconsin Idea says that education and research should not be confined to a campus, classroom or laboratory, but should extend out to the entire state and beyond.[14] Since then, the University has defined itself with a long and deep history of public service and research for the public good. As the world's cybersecurity crisis deepens, UW–Madison should carry on the Wisconsin Idea by bringing the best and brightest ideas and discoveries to improve the security of all digital citizens.

A full embrace of the Wisconsin Idea through research collaborations and outreach also benefits campus by making the University's data more secure. As cybersecurity research is conducted, the Cybersecurity Team can leverage and participate in that research, providing immediate value to all campus users. In addition, a close working relationship between the Office and cybersecurity researchers has the potential to spread to other research projects, making it easier to protect and be protected. Outreach programs reduce potential attack vectors (e.g. a local computer participating in a botnet), and recruit new generations of cybersecurity professionals from diverse backgrounds who can bring new ideas and new ways of looking at old problems.

Goals

1. Goal: Prior to the end of Academic Year 2019-2020, partner with at least two UW–Madison academic units to develop classroom, hands-on educational, and research experiences for students in cybersecurity, risk, privacy, identity management, and data protection.
   - Metric: *# of educational events, results from user surveys, reduction in the number of incidents or events in a partner academic unit.*
2. Goal: As an ongoing goal, encourage, partner with, and support students, faculty, and multi-disciplinary teams in conducting and obtaining funding for research in the areas of cybersecurity, privacy, and related topics. This could include collaboration with research proposal developers, consultation with research teams, or assistance in recruiting specific researchers to join the staff.
   - Metric: *# number partnerships, published documents with specific cybersecurity staff contributions, # hours contributed to supporting specific research projects.*

[14] The Wisconsin Idea. (n.d.). Retrieved September 13, 2017, from http://www.wisc.edu/wisconsin-idea/

3. Goal: Starting in June 2020, work with human behavior experts to study the effect of behaviors and circumstance on risk, support research and develop security controls that modify circumstance to mitigate or reduce risk-inducing behaviors and tendencies.
   - Metric: *# of behavioral security controls developed and tested.*

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
2.2	Create a compliance liaison position who will serve as the champion of compliance awareness at the System level and function as the point of contact and subject matter expert for institutions regarding compliance-related matters.	7/1/2018	TBD
3.3a	For institutions with decentralized IT management, help design and implement a tool that all IT departments can leverage to manage their own assets, but provide the central IT function with ongoing visibility into tracked assets. UW System should explore the viability of engaging consultants to accelerate asset management.	1/31/2019	1/31/2019
3.3b	If an enterprise inventory system for IT assets has not been implemented at institutions, assist those institutions with data collection/gathering for future integration into a UW System-wide asset management solution.	1/31/2019	12/31/2018
10.4	Make training and awareness materials available to all UW institutions.	8/15/2019	8/15/2019
14.3	Assist any institutions that do not have a patch testing and deployment processes with development and implementation.	11/30/2019	11/30/2019

Links to Campus Strategy/Goals

- nurture excellence in research, scholarship, and creative activity across all divisions;
- engage the interdisciplinary strength to generate creative solutions;
- partner with UW System schools, corporations, communities, and government to bring value to Wisconsin citizens;
- promote economic development and job creation through campus technology-transfer ecosystem, in partnership with the business and entrepreneurial communities;
- extend the educational mission to Wisconsin and the world with new technology and partnerships;
- leverage distinctive interdisciplinary strength to address complex problems in the state and world;
- believe in the importance of working with and learning from those of differing backgrounds and views; and
- promote the application of research and teaching to issues of importance for the state, the nation, and the world, and place learning and discovery in the service of political, economic, social, and cultural progress.

Appendix B: Challenges and Opportunities

In an organization as large, diverse, and complex as UW-Madison there will inevitably be challenges to accomplishing the Cybersecurity Strategy. As a foundation for successful realization of the long-term strategy, this volume identifies challenges and defines opportunities for success and innovation that will further enable the strategic elements and goals. These opportunities are expressed as definitive statements modeled on past successes. For example, the implementation of the PCI Compliance Assistance team's approach to campus PCI compliance. These opportunities are governed in the same successful ways as those achieved by the UW–Madison technology and security committees and forums. These challenges and opportunities will evolve with time as the Strategy is followed and the needs of the University evolve. As additional challenges are presented, this document will be reviewed and updated to provide understanding that promotes opportunity in meeting the challenges head-on.

In general, challenges to executing the Cybersecurity Strategy and addressing the cybersecurity threats to the university include:

- the distributed nature of communities and the inconsistencies in IT and cybersecurity standards, practices, and guidelines presents many opportunities;
- diverse and changing technology, business processes, use cases, and cybersecurity skill levels;
- the need for defined and consistent cybersecurity services that establish responsibilities for managing and leveraging the centralized and distributed IT and cybersecurity professionals;
- different and competing priorities compounded by the ever-changing nature of security laws, policies, and procedures; and
- the need for consistent sources of renewable funding and alignment of funding to the needs of central, distributed, and UW System IT service providers, system owners, and data stewards.

Primary areas for improvement are risk reduction, including threat detection and mitigation and accurate classification and protection of data. Improvements must include establishing an adequate inventory of hardware, software, and networking assets, along with standardizing configurations for common components. In addition, there is a growing need for transparency and higher awareness of issues of academic freedom and privacy. Efforts for improvement must consider the changing nature of policies, procedures, and communications involved in Cybersecurity architecture and operations.

Success for addressing these challenges and improvements involves the Cybersecurity Team engaging with the various stakeholders, distributed IT, and other communities to increase opportunities for cybersecurity-oriented research and outreach.

Challenge 1: Identifying and securing University data

Manage the security of University data through the initiative to "Find it. Assess it. Secure it."

This opportunity involves working closely with the Data Stewardship Committee and using current descriptions and definitions of data classifications, consistent processes, and state of the art tools to regularly evaluate the places where restricted and sensitive data are stored. Areas that lack the appropriate information security controls and are not appropriate for Restricted and Sensitive information and data to be stored are also monitored. Key elements of this objective include:

- Find all restricted data across campus that is required to be stored for business purposes, centralize the data storage and protect usage according to the currently applicable standards for high risk data (e.g. PCI, data security standards).
- Cybersecurity and data protection leadership will collaborate to identify data owners, stewards

and custodians[15], establish governance (awareness, responsibility and accountability) and begin data classification.

- Move all restricted data to a centrally managed and monitored location segregated from other data with well-controlled inbound and outbound access controls.

An ongoing measure for adhering to this objective is to obtain and curate an inventory of all assets (including applications, endpoints, servers, and people contacts such as data owners and security personnel) for all units that handle restricted data. Ensuring all campus IT and computing assets are registered in or linked to a central Configuration Management Database is a significant activity to support this objective.

This Challenge aligns to the UW System Administration (UWSA) 2-year work plan as follows:

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
1.1 & 3.1	UW Asset Management Policy and Standards documents [1035 and 1035.A] are ratified and published.	8/31/2018	TBD
3.2	Establish a process for institutions to conduct a review of locally owned IT-related assets and define categories under which these assets will fall (capital, data center, network, end-user, etc.).	8/31/2018	10/31/2018
3.3	Conduct RFP for UW System-wide asset management solution, for IT-related assets.	12/31/2018	12/31/2018
3.4	Institutions populate UW-System wide asset management solution with current IT assets.	4/30/19	4/30/2019
3.5	Assist institutions in performing a risk analysis exercise on all critical IT-related assets to determine the potential effects of the asset experiencing a loss of service as a result of a cyberattack, accident, disaster, or emergency. UW Incident Response Policy and Standards documents [1033 and 1033.A] inform the risk analysis.	6/30/2019	6/30/2019
3.6	Establish a requirement and process to audit the inventory database annually, with all departments participating and verifying the presence of each asset and all associated information.	7/1/2019	7/1/2019

This challenge would most likely be moderate cost to address and provide opportunity to achieve high impact to the UW-Madison cybersecurity efforts.

Challenge 2: Enabling a culture that values cybersecurity and reduced risk

Seek to enable, support and nourish a culture that collaboratively works to reduce risk to a level where the remaining potential consequences are acceptable to both management of the local unit and University leadership.

The opportunity is in centrally measuring the attributes of compliance according to generally accepted best practices, legal requirements, campus policies, and UW System policies. Efforts to enable a culture that values cybersecurity would include the following components:

[15] Data Steward is the main role that ensures the integrity of UW-Madison’s data. The Data Steward manages the critical data elements of the institution.

There are two types of Data Custodians: Business Custodians and Technical Custodians. Business Data Custodians are university officials having direct operational-level responsibility for the management of one or more types of data. They are charged with providing authorization for access to institutional data.

- coordinating and delivering cybersecurity training and certification opportunities across campus units and facilitating staff participation;
- offering and delivering consultative services to enable effective and secure project development;
- collaborating with campus units to facilitate use of existing cybersecurity services to leverage the use of cybersecurity tools across the institution;
- facilitating continued improvements as systems built using the Risk Management Framework (RMF) are assessed and deployed in order to ensure that all projects going forward have an understood and accepted risk; and
- developing an understanding of risk reduction controls that must be managed locally.

This Challenge aligns to the UWSA 2-year work plan as follows

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
1.6	Conduct regular, ongoing training for IT and Information Security leadership at various UW institutions on established policies/standards.	10/15/2018	Ongoing
9.4	Determine costs associated with UW system-wide comprehensive risk management training, and relevant risk management training solutions.	2/28/2019	08/15/2020
10.1	UW Security Awareness and Training Policy and Standards documents [1032 and 1032.A] are updated and published.	5/1/2019	TBD
10.2	Perform an exercise, in collaboration with key stakeholders from all UW institutions to identify the strengths and weaknesses of the current products. Document the results of this exercise.	6/1/2019	6/1/2019
10.4	Make training and awareness materials available to all UW institutions.	8/15/2019	8/15/2019
10.5	Institutions implement a tracking system to monitor compliance and effectiveness of mandatory employee training.	10/1/2019	10/1/2019
10.6	Verify and validate that institution training materials encompass key information systems topics delineated in the Security Awareness and Training Standards document, including (but not limited) to social engineering, sensitive data protection, password security, ransomware, and email security.	10/15/2019	1/15/2019
12.5	Implement a professional development training plan UW system-wide to meet IT/IS requirements.	3/1/2020	3/1/2020

This challenge would most likely be medium cost to address and provide opportunity to achieve moderate impact to the UW-Madison cybersecurity efforts.

Challenge 3: Secure data environments must meet constituents' needs

Based on established Data Governance Program requirements, ensure that secured data environments are appropriately based on the needs of faculty, researchers, and administrators and meet the objectives within IT project requirement documents.

The opportunity here is to work closely with IT staff, engineers, and architects to interpret data governance and stewardship tenets and create IT and procedural ecosystems that inherently protect data availability, integrity, and confidentiality. This will be achieved through:

- using the lessons learned from a continually evolving spectrum of data security projects to apply to all data environments which house or manipulate sensitive data elements as defined in the Data Governance Framework;

- identifying, classifying and securing restricted data to ensure that it is being used and stored in a secure manner, or eliminate data which has outlived its usefulness or cannot be stored securely; and
- developing or retrofitting environments to meet applicable data storage standards and the needs of faculty, researchers, administrators, and IT projects.

This Challenge aligns to the UWSA 2-year work plan as follows:

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
6.2	Conduct cost analysis of data encryption solutions for potential UW Common System purchase.	11/1/2018	11/1/2018
6.3	Institutions collaborate with key stakeholders for the relevant data (e.g. consult with the registrar about student data) to assess and identify sensitive information that requires encryption and integrity controls. Review data residing in relational databases, file shares and large scale storage, E-mail systems, user workstations, mobile devices (PDAs, smartphones and removable media) and backup media.	12/31/2018	12/31/2018

This challenge would most likely be <u>high cost</u> to address and provide opportunity to achieve <u>high impact</u> to the UW-Madison cybersecurity efforts.

Challenge 4: Effective tools and processes

When working as a community to provide tools and processes to promote data collection for the analysis of security related events, there is facilitation of unified measurement of cybersecurity attributes.

Within the available resources, effective tools and processes are needed to promote improved analysis of security events across the enterprise. Although tools of this nature are of higher cost to acquire, the offset in risk identification and timely mitigation presents a return on investment which significantly offsets the cost associated with recovery from data breach or loss of availability. To capitalize on this opportunity, the Cybersecurity team will need to continually collect and centrally manage operational data using existing Advanced Threat Protection tools and processes that support effective security monitoring, incident response, and the development of security metrics. The main body of work should include:

- implementation of a robust event logging infrastructure that collects operational events from units across campus;
- implementation and management of an enhanced network security monitoring system for increased network visibility;
- making cybersecurity metrics available to those organizations who need them;
- collaboration with Madison Information Security Team (MIST) to identify options for improving system inventory, such as a centralized configuration management database;
- implementation and management of enhanced vulnerability scanning processes to identify systems at risk; and
- evolving and managing the current cybersecurity operations center.

This Challenge aligns to the UWSA 2-year work plan as follows:

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
5.6	Verify and validate that the requirements regarding the encryption, prevention of loss, data leakage and integrity, as prescribed in the Data Protection Standard have	4/1/2019	4/1/2019

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
	been achieved at each institution.		
9.5	Develop a long-term roadmap to address audit/assessment events.	6/1/2019	5/15/2019
9.7	Institutions create or purchase a risk register solution that serves as a central repository for all risks identified via vulnerability assessments, external and internal pen tests, leadership discussions, third party assessments and other data points. Additionally, the chosen solution must include a mechanism by which residual risks can be tracked and decisions documented.	9/1/2019	2/28/2019
14.1	UW Threat and Vulnerability Management Policy and Standards documents [1043 and 1043.A] are ratified and published.	8/1/2019	8/1/2019
14.5	Verify that all institutions have established processes and procedures that meet or exceed the requirements regarding patch application, as described in the Endpoint Protection Standard and Threat and Vulnerability Management Standard.	2/1/2019	2/1/2019

This challenge would most likely be high cost to address and provide opportunity to achieve high impact to the UW-Madison cybersecurity efforts.

Challenge 5: Stabilized funding to support cybersecurity services

The Office of Cybersecurity will work with leaders across campus to identify and stabilize sources of sustainable funding to enable accomplishment of technical or staffing related strategic goals.

Stabilized funding is needed to support cybersecurity services that achieve and maintain strategic goals. The CISO will support the Director of Finance to correct structural anomalies in the current budget model. With a goal to control cost, the cybersecurity related budget streams will consolidated to support all cybersecurity domains. The budget should accurately forecast funding from all sources and its alignment to the cybersecurity domains. Cybersecurity, the CIO, and UW-Madison leadership will then work with other campus leaders to define and document one-time and repeatable funding models. In addition, Cybersecurity and DoIT leadership will work with university communities to explore methods to increase funding through grants and scholarships provided by various granting bodies.

This Challenge aligns to the UWSA 2-year work plan as follows:

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
4.1a	Conduct cost analysis of network protection solutions for potential UW Common System purchase.	8/31/2018	3/31/2019
4.2a	Conduct cost analysis of security monitoring solutions for potential UW Common System purchase.	8/31/2018	3/31/2019
6.2	Conduct cost analysis of data encryption solutions for potential UW Common System purchase.	11/1/2018	3/31/2019
7.7	Conduct cost analysis of annualized spending for system-wide MFA to determine if cost efficiencies can be realized.	7/15/2019	7/15/2019
11.2	In addition, to the "Compensating Controls Form", develop a process by which institutions with limited budgets can request approval for lower cost or open source tools (that meet or exceed applicable standards documents).	1/1/2019	1/1/2019

This challenge would most likely be moderate cost to address and provide opportunity to achieve high impact to the UW-Madison cybersecurity efforts.

Challenge 6: Sustaining security operations, risk management, and compliance

Working with communities like the Madison Information Security Team (MIST) and UW System Administration's Information Assurance Council, continually refined to ensure security operations,

compliance program security requirements (FERPA, HIPAA, PCI-DSS, etc.), and risk assessments are conducted in a sustainable and repeatable manner that ensures standards for timeliness and measurable response are achieved and maintained.

Procedures to ensure sustainable security operations and compliance and risk management must be continually refined and improved. This opportunity offers the Cybersecurity Team a chance to lead efforts to develop training routines and processes to standardize cybersecurity risk assessments through innovative use of technology and proven development approaches. Assessments must incorporate special security requirements mandated based on information type, compliance program standards, or aligned security guidance and be tailored to allow completion in a reasonable timeframe with the least intrusion or interference with teaching, research, and university administrative and business processes.

This Challenge aligns to the UWSA 2-year work plan as follows:

Work Plan Section	Line Item	UWSA Due By	UW Madison Due By
1.7	Institutions develop an action plan to meet or exceed established policies and standards and submit to UWSA for review and compliance monitoring.	10/23/2018	TBD
2.1	Create an avenue for institutions to leverage UW System legal function for compliance identification and collaboration (through TISC, CIO Council, etc.) on a plan for addressing compliance obligations.	5/31/2018	TBD
2.2	Create a compliance liaison position who will serve as the champion of compliance awareness at the System level and function as the point of contact and subject matter expert for institutions regarding compliance-related matters.	7/1/2018	TBD
5.3a	Institutional Record Custodians verify that data retention schedules are properly implemented at each UW Institution to meet regulatory, contractual, and compliance requirements.	1/15/2019	Complete
5.4	Ensure that Data Stewards are enforcing compliance of data retention and destruction policies.	2/1/2019	2/1/2019
9.5	Develop a long-term roadmap to address audit/assessment events.	6/1/2019	05/15/2019
9.7	Institutions create or purchase a risk register solution that serves as a central repository for all risks identified via vulnerability assessments, external and internal pen tests, leadership discussions, third party assessments, and other data points. Additionally, the chosen solution must include a mechanism by which residual risks can be tracked and decisions documented.	9/1/2019	02/28/2019
9.8	Verify and validate that each institution’s Risk Management programs meet or exceed the minimum standards prescribed in the assessment, analysis, and remediation phases of the Risk Management Standards document.	10/1/2019	03/15/2020

This challenge would most likely be high cost to address and provide opportunity to achieve high impact to the UW-Madison cybersecurity efforts.

Challenge 7: Security awareness plans and community engagement

Cybersecurity leadership will work with DoIT and UW Communications, as well as partnering with the School of Business to develop materials that will promote the deliverables of the strategic goals and objectives.

Security awareness, marketing, and communications plans need to promote community engagement. The opportunity is to gain community wide acceptance of the messaging and marketing to ensure maximum reach of the cybersecurity messages. Suggested materials will include brochures, reports, presentations, web presence, social presence, and awareness material. This plan will include teambranding efforts and may include biographies of team members with formal headshots and team identity logo wear. Efforts will be carried out with the assistance of a dedicated Cybersecurity Communications liaison and various campus advisory committees.

This Challenge does not align with any UWSA 2-year work plan items.

This objective would be medium cost and medium impact to the UW-Madison cybersecurity efforts.

Challenge 8: Continual managing and measuring the cybersecurity program

The Office of Cybersecurity will continually measure the security program, using automation wherever possible, and identify appropriate metrics for managing Cybersecurity activities and services

The cybersecurity program must be continually measured in order to manage outcomes. This is an opportunity to apply the Factor Analysis of Information Risk (FAIR) methodology as a framework for understanding, measuring, and analyzing those factors that influence cybersecurity risk[16] to improve UW-Madison's cybersecurity risk management program. This methodology will allow central and distributed IT organizations to:

- evaluate existing methodologies for creation and distribution of surveys and polls to campus user groups and other appropriate audiences that captures the perceived merits and drawbacks of cybersecurity services;
- continually evaluate best internal practices and modify as needed based on feedback received;
- once feedback is received, review and revise cybersecurity awareness efforts targeted at certain campus user groups including, but not limited to, students, faculty, staff, and researchers; and
- establish, maintain, and revise as needed, a cybersecurity metrics cycle that supports the strategic objectives and CDM program.

This Challenge does not align with any UWSA 2-year work Plan items.

This challenge would most likely be high cost to address and provide opportunity to achieve high impact to the UW-Madison cybersecurity efforts.

[16] Freund, J. and Jones, J. (2014). *Measuring and Managing Information Risk: a FAIR approach*. This text provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, helping managers make better business decisions by understanding their organizational risk.

Appendix C: Strategy Development and Maintenance

This appendix provides information on how this strategy was developed and details the process for the on-going management of the strategy.

Improving the Strategy – Security is everyone's responsibility

This document articulates elements of strategy to include specific goals with enabling objectives, including those completed near term. Also included are the description of the cybersecurity organization, the mission, vision, and guiding principles, and the stated roles of the Office of Cybersecurity. Expanded discussion on the strategy and objectives are contained within Appendix A. The recommended cybersecurity organization is detailed in Appendix B, with Appendices C through F containing additional information in support of cybersecurity operations aligned to the strategy, goals, and objectives.

Goals that align to the strategic elements of this plan were developed using SMART techniques with each goal containing these five elements:

1. Specific – describing a defined aspect of the cybersecurity program for improvement.
2. Measurable – establish a quantifiable metric or a specific indicator of progress.
3. Assignable – of sufficient scope to be assigned to a specific individual or group.
4. Realistic – state what results can realistically be achieved within available resources.
5. Time-related – the specific date or defined period of time to deliver the results.

The continued success of this strategy and these goals rely on the ability of the Cybersecurity team, DoIT, and the distributed campus IT staff, faculty, university administrators, and other members of the governance community to effectively communicate and actively collaborate. Collectively, all groups must allow a respectful and agreed upon decision-making process.

The Strategy Development Team

This strategy was developed through an iterative approach with colleagues across UW-Madison and with those who support common IT services. Staff within the Office of Cybersecurity joined with these participants in the development and maintenance of this strategy:

- *Brenda Spychalla, CIO, School of Education*
- *Eric Giefer, CIO, Law School*
- *Dorothea Salo, Faculty Associate, The Information School*
- *Nicholas Davis, CISO, UW System Administration*
- *Philip Romero-Masters, Student Representative, The Information School*
- *Amanda Reese, HIPAA Privacy Officer, The Office of Compliance*
- *Rick Konopacki, Director, Networking and Security, School of Medicine and Public Health*
- *Bill Zimmerman, Assistant Director, DoIT User Services*
- *Kristin Eschenfelder, Professor and Director, The Information School*
- *George Watson, Consultant, Office of Quality Improvement*
- *Bruce Harville, Consultant, Office of Quality Improvement*
- *Daniel Simanek, IT Administrator, Research and Graduate Education*
- *Kristy Rogers, IT Security Analyst, UW System HRS Service Center*
- *Louann Gilbertson, CISO, UW-Platteville/UW-Whitewater*

Maintaining the Cybersecurity Strategic Plan

This Strategic Plan is sponsored by the Vice Provost for Information Technology and Chief Information Officer. While the initial plan was developed within the Cybersecurity Team, all updates or changes to this document are under the purview of the IT Policy Analysis Committee. Governance for updates or changes will conform to the UW-Madison adaptation of the Cornell Model[17] for policy development with the following deviations:

1. Updates and changes will originate from the UW–Madison Chief Information Security Officer and the Office of Cybersecurity after consulting with MIST and will be submitted as requirements to the IT Governance processes and advisory groups.
2. The information security program is reviewed during the yearly strategy review or as required and will be revised based on (but not limited to): updated industry regulations or standards; organizational changes; or newly identified risks and threats.
3. Prior to signature, all changes will be coordinated and reviewed through the Madison Information Security Team (MIST), then briefed to the IT Steering Committee (ITSC) and Advisory Groups, and the Information Technology Committee (ITC).
4. Following incorporation of any revisions, the document will be forwarded to the University of Wisconsin Systems Administration (UWSA) Information Assurance Council (UWIAC) and the Technology and Information Security Council (TISC) for information and potential adoption by the UW System Administration and campuses.
5. Final authority to implement changes rests with the UW–Madison Chief Information Officer (CIO) with endorsement by UWSA CIO if the change applies to the UW System.
6. UW–Madison CISO provides annual reports to the community for review. Any recommended changes will be reviewed and approved by the UW–Madison CIO until fully implemented.
7. Within the calendar year 2022 and every fourth year afterwards or upon transition between UW–Madison CIOs, this strategic plan will be reviewed and updated then extended for an additional five years.

[17] Use of the Cornell Model for developing policy was adopted at the January 2015 Policy Planning Team Meeting with details at https://wiki.doit.wisc.edu/confluence/display/POLICY/PPT+Meeting+2015-01-14. The new Policy Analysis Team was formed under Faculty Governance as a subcommittee of the Information Technology Committee in September 2017

Volume III – Helpful Information

This Appendix provides specific acronyms and abbreviations along with terms and definitions unique to UW-Madison's Information Security Program and Cybersecurity Strategy. It serves to amplify information provided in the UW System Information Security Program's exhaustive Glossary. It should be used as a reference when studying this document and is useful for other administrative programs and processes that come out of the program and strategy.

Acronyms and Abbreviations

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

Table D-1: Acronyms and Abbreviations

Acronym or Abbreviation	Long Title
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoIT	Division of Information Technology
D-CISO	Deputy Chief Information Security Officer
FERPA	Family Educational Rights and Privacy Act of 1974
HCC	Health Care Component
HERD	Higher Education Research and Development Survey
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HRS	Human Resource System
IRB	Institutional Review Boards
ITC	Information Technology Committee
ITMC	Information Technology Management Council
MIST	Madison Information Security Team
NIST	National Institute for Standards and Technology
NIST SP	NIST Special Publication
PCI CAT	PCI Compliance Assistance Team
PCI-DSS	Payment Card Industry Data Security Standard
PHI	Personal Healthcare Information
PII	Personally Identifiable Information
PPT	people, process, technology
PAT	Policy Planning Analysis Team
PTE	Professional Technical Education
RMF	Risk Management Framework
SDLC	Systems Development Life Cycle
SETA	Security Education, Training & Awareness

Acronym or Abbreviation	Long Title
SFS	Shared Financial System
TISC	Technology and Information Security Council (UW System)
UDDS	Unit, Division, Department, Sub-department
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

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.

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

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)

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)

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)

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)

Unit, Division, Department, Sub-department – Known as the UDDS, this data field is used to correlate financial, human resources and other unit level data fields to denote specific work organizations within the UW System.