University of Wisconsin-Madison Cybersecurity Strategy (2015 – 2019)

A guide for protecting information through effective data governance and implementing cybersecurity controls in a risk management framework

Updated

July 10, 2017

Table of Contents

Record of Updates

Update Number	Date Entered	Change Information	Entered By
Interim	Oct 1, 2015	Changed WSRC titles throughout to read Consortium vice Corporation	Bob Turner
1.0	August 1, 2016	Added Appendix H – Year One Update, made appropriate modifications to existing goals and strategic elements, added new goals, simplified RACI chart, made minor editorial changes throughout	Bob Turner
1.1	October 22, 2016	Minor change to cover removing version number to avoid future confusion.	Bob Turner
2.0	July 10, 2017	Added Appendix I – Year Two Update. Made appropriate modifications to existing components – strategic elements, goals, and enabling objectives. Updated Appendix E to adjust the Office of Cybersecurity Organization Chart Minor editorial changes throughout.	Bob Turner

University of Wisconsin-Madison Cybersecurity Strategy

(Calendar Years 2015 – 2019)

Executive Summary

This document was updated in July 2017 following the second yearly assessment of progress. The updated strategy continues along the path to optimize risk management by defining information security strategies that will result in greater protection of data with measurable improvement to the University of Wisconsin-Madison cybersecurity posture, incrementally and over time. Where elements of risk have been inaccurately or inadequately defined or managed in the past, this strategy will seek feedback ahead of implementation. For those areas with greater cybersecurity maturity, the strategy will quickly evolve to best practices that are transferrable across the campus and the University of Wisconsin System.

Cybersecurity threats and threat actors are becoming more sophisticated. They are also increasing in volume, causing risk management strategies to become more complex. Since the original strategy was published in July 2015, the threat actors have increased in number, sophistication and targeting strategies. Higher Education is on the criminal's radar and we are frequently sought for the valuable research information and marketable data with healthcare and personal information for criminal elements to exploit. Ransomware is an ever increasing threat that UW-Madison cannot ignore. The threat actors have increased targeted Phishing events directed at higher education[1] that includes faculty and senior leaders as well as increased realism and threat impact in e-mail (phishing), SMS Texting (smishing) and voice calls or voice messages (vishing)[2] Ransomeware and attacks on Internet of Things components like buidlign access and camera systems, laboratory equipment, heqting, ventilation and air conditioning systems using advanced systems controls (SCADA) technology are now prominent threats to the UW-Madison information and networked systems infraastructures.

Optimized risk management requires approaches that center on the data the University requires for daily operations. Among the major categories of information requiring enhanced protection are research data, medical data and student information. Considering the widespread teaching and research centered on healthcare and personal health information, leaders and risk managers must also consider the impact of multiple and simultaneous incidents involving breach of data regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent legislation. This Cybersecurity Strategy provides a platform to validate effective practices, supported with automated real-time monitoring for accountability and eventually a set of decision metrics for estimating risk and security control effectiveness.

> *"It's all about the data."*
>
> *Jason Fishbain*
> *Chief Data Officer*
> *UW-Madison*

Directly supporting the Chief Information Officer and Vice Provost for Information Technology (CIO), the Chief Information Security Officer and dedicated CIO staff focusing on data management and enterprise IT decision management are charged to lead and manage campus cybersecurity to reduce risk. Risk reduction strategies must also be embraced by the various campus advisory groups and governance bodies (e.g., Information Technology Committee, Madison Technical Advisory Group, Madison Information Security

[1] SOURCE: *Advisory: University Payroll Theft Scheme*, Research and Education Information Security Analysis Center (REN-ISAC), dated November 12, 2014

[2] SOURCE: Keyworth, M. (January 1, 2016). *Vishing and smishing: The rise of social engineering fraud*. BBC World Service (Online).

Team) who's focus on continued identification of risk and appropriate handling of data will prevent inappropriate access to or loss of sensitive or restricted data. This focus must also include continued diagnostics to ensure visibility of IT assets and the vulnerabilities associated with their specific technology. These are followed by refining the processes and procedures for managing our intellectual property and other sensitive information. The Office of Cybersecurity leads and advises to provide both the necessary risk response measures to adequately protect information systems. Tools and processes that seek to avoid risk increase the cost of operations and may impact the ability of faculty and researchers to carry out the university-wide missions of teaching, research and outreach. Likewise, risk tolerant strategies place the university at risk for cyber-attack, data loss or mismanagement, and increased cost to operate through additional system administrative and maintenance cost.

This document outlines seven strategic principles, supporting goals to enable those principles, and eight enabling objectives that, if realized near term, will help sustain the strategy over the next five years. The elements and objectives shown below and articulated in greater detail later in this document are a collective work of the Office of Cybersecurity[3] and the UW-Madison Information Security Team[4] who enthusiastically support the immediate approval, adoption and implementation.

Elements of UW-Madison Cybersecurity Strategy

- *Strategy 1: Complete Data Governance and Information Classification Plan* ***(Completed 2017!)***
- *Strategy 2: Establish the UW-Madison Risk Management Framework to materially reduce cybersecurity risk* ***(Completed 2017!)***
- *Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness*
- *Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services*
- *Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination and Remediation*
- *Strategy 6: Optimize Services, Establish Security Metrics, , Promote Compliance, Achieve Continuous Diagnostics and Mitigation*
- *Strategy 7: Establish Collaborative Partnerships to assure teaching and research computing resources and results are available to fulfill the Wisconsin Idea and return value to the state and its citizens*

Near Term (Enabling) Objectives toward Cybersecurity Strategy Development

- *Objective 1: Consider retention of previous strategy's actionable items ("find it," "delete it," and "protect it").*
- *Objective 2: Enable and support a culture that values information security and works to reduce risk to a level where the remaining potential consequences are acceptable to management of the local unit and University leadership.*
- *Objective 3: Establish Restricted Data Environments based on the needs of Faculty, Researchers or IT project requirement documents.*

---

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

[4] The UW-Madison Information Security Team (MIST) is sponsored by the CIO and was created as a collaborative group of campus IT staff, management, and others with a common interest in promoting information security at UW Madison. This group provides communication, guidance and leadership for campus-wide security issues and initiatives along with serving as an advisory group to the UW-Madison Chief Information Security Officer.

- *Objective 4: Centralize data collection and aggregation for analysis of security related events to promote unified measurement of cybersecurity attributes.*
- *Objective 5: Identify and seek sources of repeatable funding to enable accomplishment of technical or staffing related strategic goals.*
- *Objective 6: Requirements are imposed upon UW-Madison by other agencies. Identify UW-Madison compliance (FERPA, HIPAA, PCI-DSS, Red Flags Rule, etc.) and then map the IT security components of each to applicable campus units.*
- *Objective 7: Develop and refine procedures to ensure security operations and risk assessments are conducted in a sustainable manner that ensures standards for timeliness and measurable response are achieved and maintained.*
- *Objective 8: Develop and implement a marketing and communications plan.*

"Strategy without tactics is the slowest route to victory, tactics without strategy is the noise before defeat."

- Sun Tzu (Ancient Chinese Military Strategist)

Introduction – The Threat

Cybersecurity threats and information system vulnerabilities will continue to attract those seeking to exploit University of Wisconsin information systems and capture important intellectual capital, personal or financial data for use in criminal enterprises. Threats include compromise of research information that can be exploited causing damage to the University's reputation, or revenue loss through theft of patent data and disruption of services. The risk and threat picture will continue to become more complex. This calls for continuous improvement in systems and applied security controls to ensure confidentiality of sensitive data, integrity of instructional and learning management systems, along with availability of computing and information processing systems and data. Effective cybersecurity occurs deliberately as a life cycle within an ecosystem based in processes, people and technology and should never be considered a one-time project with an end point.

Since 2015 cybersecurity risk management continues to grow in complexity as the definitions and processes are refined to address changes in security infrastructure, global criminal and nation-state threats, and the sophistication of exploits and vulnerabilities. As a single example among many, the sophistication of so-called Phishing events, which are socially engineered attempts to entice compromise of personal data or access control features, has increased between late-Fall of 2014 to the Spring of 2017. Every six to eight months, the standard elements of a phishing email become more realistic in nature and threat actors increase targeted Phishing events directed at higher education that includes faculty and senior leaders as well as increased sophistication in the messages. Quality of the Phishing attempts have also improved using more appropriate language and familiar phrases and key words. The recent increases in ransomware attacks carried out through e-mail and website exploitation increase the likelihood and impact that a major system or network outage could result that stops the business of the university and results in elevated cost to recover. Within a security controls structure that is based largely on user-based enforcement, additional attention must be paid to security training and awareness to counter accidental or intentional insider threat scenarios.

Approach to Developing the Strategy – It's all about the Data

The University of Wisconsin-Madison (UW-Madison) Cybersecurity Strategy will help to achieve goals of data protection and optimized risk management. This strategy outlines measures to continue the UW-Madison journey to properly classify the university's diverse data resources, then apply controls to optimize security of the data. This is done while promoting and continuously assessing key attributes of cybersecurity and information technology risk management. The significant feature of this strategy is the development and implementation of a tailored UW System Risk Management Framework (RMF) that enables full discovery of data with a tiered classification system based on attributes, volume and location. Defining data attributes and handling informs the proper classification of systems processing that data to enable selection, application and maintenance of appropriate security controls. Formal assessment of security controls implementation based on cybersecurity threat and likelihood of exploitation derives the level of residual risk to an information system and data. This discovery includes a formal authorization process to ensure awareness of the system's impact on the overall risk. It includes continuous monitoring, diagnostics,

Classifying the data drives the proper classification of the information system or network that drives the application of the right security controls.

review and mitigation of risk throughout the security life cycle to complete the framework.

Practicing Risk Management vs. Risk Avoidance

Information technology significantly influences the UW-Madison mission of teaching, research and outreach. Faculty, researchers and staff depend on the systems and services within the campus information enterprise to carry out their daily routine and to record the accomplishments and achievements and help account for the revenue levels which place the University near the top of educational and research institutions[5].

Fear, uncertainty and doubt is not a sound cybersecurity strategy as it can easily be turned against the organization's security program and erode confidence in the implementation of controls.

Kees Leune
Chief Information Security Officer, Adelphi University
In remarks before the EDUCAUSE Security Professional's Conference 2015

As discussed in NIST Special Publication 800-39[6], within an organization as diverse and complex as UW-Madison, organizational risk consists of program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk. Security risk related to the operation and senior university leaders, as part of their ongoing risk management responsibilities, should address use of information systems. Effective security risk management requires that UW-Madison departments, colleges and organizations operating in highly complex, interconnected environments using state-of-the-art and legacy information systems must recognize that explicit, well-informed risk-based decisions help balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. Managing information security risk, like risk management in general, is not an exact science. While based in the best collective judgments of individuals and groups, the concepts of risk avoidance, risk management and risk tolerance are not consistently understood or practiced. As the UW-Madison organization responsible for cybersecurity; and in most of the information enterprise, day-to-day operations; the Office of Cybersecurity takes a leading and advisory role in providing both the necessary and sufficient risk response measures to adequately protect the information systems. Tools and processes that seek to avoid risk increase the cost of operations and may impact the ability of faculty and researchers to carry out the university wide mission. Likewise, risk-tolerant strategies place the university at risk for cyber-attack, data loss or mismanagement, and increased cost through additional system administrative and maintenance.

Optimized risk management is applied to data identified as Personally Identifiable Information (PII) or Personal Healthcare Information (PHI) that the University requires for daily operations to include handling research, student information, and academic records. With the widespread teaching and research involving healthcare and personal health information, we must consider the impact of multiple and simultaneous incidents involving breach of data regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent legislation. Attention must also be directed toward restricted data under the Family Educational Rights and Privacy Act (FERPA) and to financial and credit card

[5] SOURCE: Higher Education Research and Development Survey (HERD), FY2013

[6] SOURCE: NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View, Joint Task Force Transformation Initiative, dated March 2011

or account information with handling regulated under the Purchase Card Industry Data Security Standard (PCI-DSS).

The Cybersecurity Strategy outlined in this document supports validation of effective practices, with automated real-time monitoring for accountability. Eventually, a set of decision metrics for estimating risk and security controls effectiveness will be developed. The entire UW Community will benefit from being proactively involved and supportive of continuous improvement offered within this strategy. For critical processes and systems, independent reviews should be planned and implemented to provide assurance that the spectrum of security controls are at the desired level of maturity and working as planned.

Our efforts will provide direction and, through the establishment of cybersecurity measures of effectiveness, emphasize continued identification of sensitive or restricted information. Efforts will include a management strategy including processes that prevent inappropriate access to or loss of sensitive or restricted data. This focus must also include continued diagnostics using the right tools and access to all IT assets that ensure visibility of vulnerabilities and risk associated with their specific technology. Refining the processes and procedures to manage our intellectual property and other sensitive data will follow it.

Measuring Effectiveness of	***People*** / ***Process***	***+***	***Compliance*** / ***Technology***	***=***	***Mature Cybersecurity***

Operational Relationships within the Office of the CIO

The recent standup of data governance and enterprise IT decision management strategies establish important relationships within the Office of the CIO. As shown in the figure below, cybersecurity functions and processes are informed by the work of Data Governance lead by the Chief Data Officer (CDO). Establishing detailed data classification will lead to appropriate system classification that drives selection of security controls and testing criteria. Ensuring all new or modified systems are controlled within the Enterprise IT Decision Management (EITDM) program ensures complete discovery of architectures and interfaces, along with the key players and relationships to improve cybersecurity.

The active relationship between the Office of Cybersecurity and the Division of Information Technology (DoIT) includes the coordination of functions within Governance, Risk Management and Compliance as well as Security Testing and Cyber Defense and the Security Operations teams and DoIT Service Teams. By ensuring a shared understanding of the strategies within this document, a more unified response and proactive customer focus can be achieved.

Figure 1: Operational Relationships

Developing the Strategy

The IT Security program at UW-Madison currently employs national and UW-Madison best practices for continual assessment. Cybersecurity risk assessment is supported with automated real-time monitoring for accountability and metrics. Employees who are proactively involved with prevention and management of systems, application of processes, promotion of continuous improvements will be able to analyze and consume real-time cyber threat intelligence. The overall goal for this strategic plan is for university enclaves to be able to set a benchmark using internal and external best practices for cybersecurity controls. For critical processes and systems, independent reviews will take place to ensure that controls mature and work as planned.

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 G 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[7] with each goal containing these five elements:

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

The 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, collaborate and actively. Collectively, we must allow a respectful and accepted decision-making process.

Cybersecurity Strategic Planning Governance

This Strategic Plan is sponsored by the Chief Information Officer and Vice Provost for Information Technology. While the initial plan was developed within the Office of Cybersecurity, all updates or changes to this document are under the purview of the IT Policy Planning Committee. Governance for updates or changes will conform to the Cornell Model[8] for policy development with the following deviations:

- *Updates and changes will originate from the UW-Madison Chief Information Security Officer and the Office of Cybersecurity and submitted as requirements to the IT Policy Planning Team*
- *Prior to signature, all changes will be coordinated and reviewed through the Madison Information Security Team (MIST), then briefed to the Information Technology Council (ITC) and the Madison Technical Advisory Group, then forwarded to the University of Wisconsin Systems Administration (UWSA) CISO and the Technology and Information Security Council (TISC) for information and potential adoption by the UW System Administration and campuses*

---

[7] From "There's a S.M.A.R.T. way to write management's goals and objectives" by George T. Doran as published in Management Review (AMA FORUM) 70 (11): 35–36. (1981)

[8] Using the Cornell Model for developing policy was discussed and approved at the January 2015 Policy Planning Team Meeting with details at https://wiki.doit.wisc.edu/confluence/display/POLICY/PPT+Meeting+2015-01-14.

- *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*
- *UW-Madison CISO provides quarterly reports to the community for review, recommended changes will be reviewed and approved by the UW-Madison CIO until fully implemented*
- *Within the calendar year 2018 and every fourth year afterwards, this plan will be reviewed and updated to refine and extend the strategic plan for an additional five years.*

The Strategy

Elements of UW-Madison Cybersecurity Strategy

The elements below form the strategy to prevent losses of restricted data while ensuring availability of systems, networks and services, ensure integrity of data and transactions. This strategy provides includes sub-strategies to refine processes and procedures to manage university-owned or developed intellectual property and other sensitive information. Each strategy element is further defined in Appendix A.

- *Strategy 1: Complete Data Governance and Information Classification Plan* ***(Completed 2017!)***
- *Strategy 2: Establish the UW-Madison Risk Management Framework to materially reduce cybersecurity risk* ***(Completed 2017!)***
- *Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness*
- *Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services*
- *Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination and Remediation*
- *Strategy 6: Optimize Services, Establish Security Metrics, Promote Compliance, Achieve Continuous Diagnostics and Mitigation*
- *Strategy 7: Establish Collaborative Partnerships to share resources and results to fulfill the Wisconsin Idea and return value to the state and its citizens*

Near Term (Enabling) Objectives toward Cybersecurity Strategy Development

The near term operational objectives presented below can be included in the strategies above with each objective detailed in Appendix A. They are modeled on past successes in projects like implementation of the PCI Compliance Assistance Team's approach to campus PCI compliance. The Objectives will be governed in the same successful ways as the UW-Madison technology and security committees and forums.

- *Objective 1: Consider retention of previous strategy's actionable items ("find it", "delete it", and "protect it").*
- *Objective 2: Enable, support and nourish a culture that values information security and actively works to reduce risk to a level acceptable to both management of the local unit and University leadership.*
- *Objective 3: Establish Restricted Data Environments based on the needs of Faculty, Researchers or IT project requirement documents.*
- *Objective 4: Centralize data collection and aggregation for analysis of security related events to promote unified cybersecurity measures.*
- *Objective 5: Identify and stabilize sources of repeatable funding to enable accomplishment of technical- or staffing-related strategic goals.*
- *Objective 6: Requirements are imposed upon UW-Madison by other agencies. Identify UW-*

Madison compliance (FERPA, HIPAA, PCI-DSS, etc.) and then map the IT security components of each to applicable campus units.

- *Objective 7: Develop and refine procedures to ensure security operations and risk assessments are conducted in a sustainable and repeatable manner that ensures standards for timeliness and measurable response are achieved and maintained.*
- *Objective 8: Develop and implement a marketing and communications plans.*

Expanded discussion on the strategy and objectives are contained within Appendix A. The recommended cybersecurity organization is detailed in Appendix B. Appendices C through G contain additional information in support of cybersecurity operations to be conducted to meet the strategy, goals and objectives.

Data Governance – Understanding Data and Risk

Through partnerships and with many units, UW-Madison has embarked on a significant effort to develop a common understanding of controls used to secure and manage data. These include elements such as research that has copyrights, proprietary information related to patents from inventions developed through UW-Madison sponsored research, and personally identifiable information (PII). Restricted Data sets could include Social Security Number, birth date, address, phone number, gender, etc.; private student data requiring protection the Family Educational Rights and Privacy Act of 1974 (FERPA); personal health information (PHI) and data covered under privacy and security legislation found in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Management of security controls articulated within research projects as they are stipulated during the individual colleges and department level Institutional Review Boards (IRB) will provide a framework that can be leveraged across campus to effect improvements in cybersecurity and enhance protection for important information in order to reduce risk to the university. We want to measure the activity in and status of systems and operations within UW-Madison computing and information technology environments. We then compare it to industry standards to provide valuable information to improve cybersecurity services, contribute to more effective governance and achieve the long term UW objectives for Internal Controls Maturity in an incremental and actionable fashion.

A key outcome of establishing data definitions is the ability to assign security controls based on characteristics of confidentiality, integrity and availability for both data and the information systems where the data is at rest or in transit. The table below provides an example of broad information categories based primarily 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.

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

Appendix A: Cybersecurity Strategies

- *Strategy 1: Complete Data Governance and Information Classification Plan* ***(Completed 2017!)***

This strategic element is complete as of July 2017 – See Appendix I

Federal Information Processing Standards Publication 199[9] provides objective standards to align a system's data sensitivity with security control measures used to protect the data and information that is handled by, stored within, or exchanged between IT systems. The guidelines can be tailored for the UW-Madison environment and provide standards to:

- Categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and *information systems in each such category*

The result will be a data governance plan that provides guidance on the classification of systems based on information that is stored, handled, or manipulated within the system. This will then lead to specific system risk determination and potential mitigations. Data is an essential currency of the UW-Madison. With the definition of "data," the concept of data governance spans these authoritative sources:

- FERPA records or data including UW student information whether marked for release or excluded
- Course and Learning Management System data including grades, portfolio entries or lesson plans
- Research data and intellectual property
- PHI, HIPAA and HITECH accountable information
- Special programs like Select Agent, Software Assurance Marketplace (SWAMP), Wisconsin Security Research Consortium (WSRC), etc.
- Other situations with information protected as directed by Grant or Sponsor

Components of effective data governance including accountability and a clear structure for oversight include the actions of responsible stewards who manage the integrity of the data, control over access, and security. Data stewards and IT systems administrators and technicians should receive consistent, repeatable training in all aspects of campus data management and retrieval. Proper System Classification stems from data governance and classification guidelines that are well understood and continually updated.

Data Governance informs system owners and security staff what to secure, where Cybersecurity controls informs on how to secure the data,

Successful achievement of the goals within this strategy are supplemented by campus wide procedures for capturing, classifying, labeling, retrieving and managing all types of data: research, institutional, and academic. Procedures should also include a commonly understood definition of what secure environments and acceptable risks mean for institutional data.

Goals:

1. With leadership and coordination provided by the CIO office and the Chief Data Officer, form a data

[9] SOURCE: FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, National Institute of Standards and Technology, dated February 2004

stewards group with representatives of major data stewards. Create a generally agreed upon data classification system is a well-defined process with a known end point. The stewards group should be formed by December 2015 and the Data Classification System completed by June 2016. Success is measured by the existence of a charter, meeting schedule, engagement procedures, and documented deliverables.

Status Update (Year One): Established Data Stewardship Council and Data Governance Executive Committee. Approved four tier data classification system. **GOAL COMPLETE**

2. With initial reports due by December 2015, validate compliance with the required portions of the restricted data management policy. Success is measured by compliance by all units actively represented on UW-MIST. All UW-MIST representatives are to advocate for compliance for their unit. Many units are represented on UW-MIST, which is a forum that can actively encourage compliance among those units. In addition, success is the identification reduction or documented justification for "shadow" systems that persists data originated for a source system.

3. (New Goal – Year One) Assist with developing the Restricted Administrative Data Authorization policy & procedures. Ensure that the policy is consistent with anticipated implementation of the Risk Management Framework.

Link to Campus Strategy/Goals:

1. We are committed to being responsible stewards of our human, intellectual, cultural, financial, and environmental resources.

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

   - *Strategy 2: Establish the UW-Madison Risk Management Framework to reduce cybersecurity risk* ***(Completed 2017!)***

This strategic element is complete as of July 2017 – See Appendix I

This strategic element is dependent upon establishment of a UW-Madison Data Governance Program that establishes definitions of general systems, restricted or sensitive data and an accompanying definition or description of levels of security that must be applied. A complete UW- Madison Risk Management Framework (RMF) consists of the component stages depicted in Figure A-1 described in Table A-1 and serves to educate various levels of management to measure and understand the value of their assets (data, systems and people). The potential loss of value to technology components and data resources is balanced against potential threats to those assets in a consistent and repeatable manner with the goal to determine if and what remediation should be planned and implemented. The RMF provides benefits to UW-Madison system owners and leadership within the different Colleges and Departments by serving as both the strategic basis and the operational framework for managing cybersecurity risk across the campus and provides a source for policy discussions throughout the UW System and System Campuses.

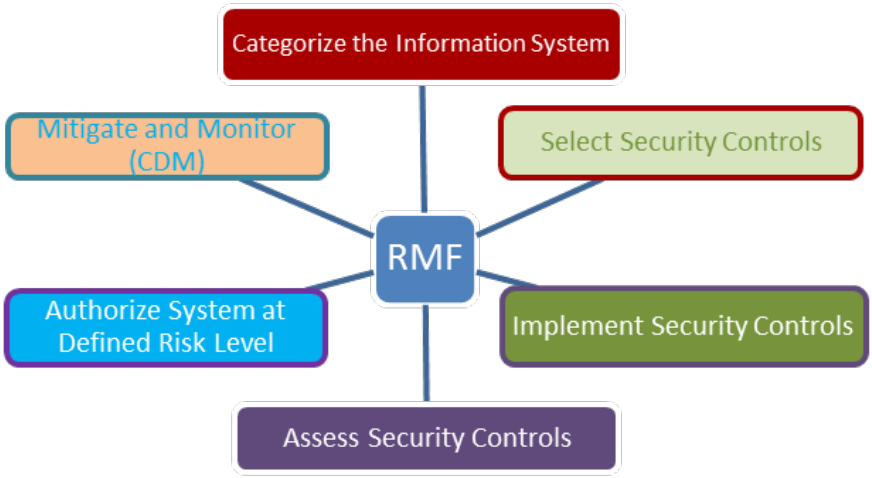

Figure A-1: Risk Management Framework Components

Table A-1: Stages of a Risk Management Framework (RMF)

RMF Stage	Description
Categorize System	A data driven process where the security requirements of the system are defined by the highest classification of data handled by or stored within the system or processes.
Select Security Controls	Assignment of the administrative, physical and technical controls required to protect the data are drawn from an agreed security controls framework.
Implement and Verify Controls	During design and development, the selected controls are incorporated into the system design and verified to adequately protect data.
Assess and Authorize	Assess the implementation of selected controls and determine the residual risk with mitigating factors applied. This stage leads to a formal declaration that the system operates at a defined level of risk.
Mitigate and Monitor	Continually assess the operational controls against the evolving vulnerability, threat and impact factors. When controls fail or external influencers dictate, determine and impose mitigating controls and review risk.

Goals:

1. Within 60 days of publication of this document, UW-Madison CISO and CIO will achieve agreement with UW System on business rules for adapting and applying the National Institute for Standards and Technology (NIST) approach to Risk Management using the Four Phase Process model[10] and employing other appropriate NIST, ISO 27001 and 27002, or other relevant industry or higher education community best practices and guidance.

[10] SOURCE: NIST SP 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, Joint Task Force Transformation Initiative, dated March 2011

Status Update (Year One): Team determined the National Institute for Standards and Technology (NIST) model will scale best for UW-Madison. Briefed at UW Technical Information Security Committee (TISC) Summer Meeting (July 2015) with no dissenting opinions. Standard was included in Regent Policy Directive 25-5 Information Security published in February 2016. **GOAL COMPLETE**

2. Within four months of completing Goal #1 for this Strategic Element, the UW-Madison CISO and Associate CISO will determine and present staffing needs to complete a new assessment for UW-Madison as the follow up to the original baseline. The presentation will include suggested timelines for the project and designated resources.
3. Prior to December 2015, a small group (no more than 4 people) of experienced security professionals from UW Madison and/or UW System, will define and present to groups yet to be determined, the "Organizational Parameters" for all items in NIST SP 800-53[11] Low and Moderate, and a direct mapping of 800-53 Low to the existing UW-Madison IT Security Baseline. Output will include notation of differences in the final choices for controls for the campus baseline going forward, vs. the original campus baseline.
4. Concurrent with Goal #3 above, the Governance, Risk and Compliance team will develop an implementation plan for conducting assessment and approval (steps 3 and 4 of the RMF) including training and guidance for system owners and distributed IT and cybersecurity staff. This implementation plan will include training for executive management, business unit, College or Department management and functional staff, system owners and distributed IT administrators and security staff.
5. (New Goal Year One) Develop supporting policy for Risk Management Framework.

Link to Campus Strategy/Goals:

1. Be responsible stewards of our resources by developing a solid understanding of the total cost of ownership for security tools and processes used to secure the information infrastructure.

Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness

It is generally understood that people are one of the weakest links in attempts to secure systems and networks. The "people factor" - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better 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[12]. An effective IT security awareness and training program explains proper rules of behavior for the use of IT systems and information as well as empowers the empowers the audience 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. Through awareness and training, users first should be informed of the expectations. Accountability can be derived from a fully informed, well-trained and aware community.

Goals:

[11] SOURCE: NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* dates April 30, 2013

[12] SOURCE: NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program* dated October 2003.

1. Within one year of publication, the CISO and staff will engage with professors, researchers, business, and IT professionals to define group specific security awareness programs. These face-to-face meetings with research groups will include documented and specific objectives and outcomes to promote security and shared understanding of the community's needs. Successful completion of meetings with 90 % of identified groups will demonstrate completion of this goal.
2. Within one year of publication and in conjunction with Professional Technical Education (PTE), Application Development & Integration (ADI), or other security team members, the CISO and staff will build and implement a website or section within a website to provide a place for campus community to visit for security information and initiatives by hosting IT Security Awareness information in multiple formats, receiving feedback, providing download of materials (posters, etc.), provide resources that refer to best practices, and post questions.
3. As part of the ongoing security awareness efforts, the CISO and staff will continue to raise security awareness of phishing and the threat vectors used. We will conduct quarterly phishing campaigns for identified departments and through the analysis of scripted events, IT Security staff will measure the number of employees who fail on fake phishing email to obtain the trend. Successful completion of this goal is measured by conducting phishing campaigns four times per year with steadily decreasing numbers of staff who respond to the phishing stimulus in a manner contrary to good security practices.

Status Update (Year One): Phishing campaign is a success!!! Developed monthly campaigns and strategy to increase use of PhishLine training licenses across campus. Proven with recent real-world phishing attempts stopped by User actions. Need to gather metrics to prove the efficacy of PhishLine tool and work to expand the licenses used across campus to meet the current contract limit. **GOAL COMPLETE**

4. To empower managers to drive their employees to greater levels of understanding, the CISO will work through MIST to define, identify or develop perpetual training opportunities that include initial training for new or returning employees, those with significant job task changes, or groups with ongoing and incremental requirements for improving knowledge or continuous professional education related to certifications or licenses.
5. (New Goal – Year One) Develop campus policy requiring participation in SETA.
6. (New Goal – Year One) Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the CIC Security Working Group.

Linkage to Campus Strategy/Goals:

1. Nurture growth of our people through professional development and performance excellence.
2. Create the best possible environment in which our people can carry out their responsibilities to the university.

Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services

Tools and technical controls are required to achieve compliance on the scale posed at the UW-Madison. Targeted and continuous surveillance of campus systems and distributed networks will enhance the overall cybersecurity picture and reduce risk to teaching, research, campus operations and systems operations. Based on our experience within the current Enterprise Resource Planning (ERP) team devoted to security operations, we understand that automation of security management functions is required for the continuity of long-term operations and constant mitigation or reduction of threats. Common tools are

anti-virus/anti-malware/anti-spyware applications, firewalls, cryptographic tools, Virtual Private Networks, endpoint management, configuration and patch management, data location and sanitization and file integrity tools among others. Identification and estimation of impact for various risk elements can be enhanced through situational awareness and the measurement of effective deployed services and reviewed through appropriate departmental of campus governance groups. A greater understanding of risk factors at any point in time is achieved through the use of cybersecurity services such as vulnerability management, security event management, intrusion detection, patch management, forensics and incident response.

The UW-Madison has the responsibility to operate and support UW Common Systems and the capability to gain visibility to UW System Campus networks. Conducting and provisioning security operations to all UW campuses can be achieved at a scale that saves considerable cost and resources. Compliance assistance through site visits can be achieved through collaborative IT service models such as the Payment Card Industry model already developed on campus.

This strategy is realized through expanding the role and functions of the ERP Security Operations Team to encompass the broader spectrum of security operating functions and management or oversight of security operations for major systems and networks across campus. This team will be rebranded as the Security Operations and will eventually consist of technically skilled operators capable of understanding the broadest spectrum of security tools and technical security countermeasures.

Goals:

1. Prior to October 2015, the Security Operations Team should research available open source materials and collaborate with UW-Madison, UW System and members of the Committee on Institutional Cooperation's Security Working Group or other higher education collaborative bodies to define criteria needed to describe a security operation or service. A governance structure should be established to provide oversight of common solutions.
2. During November and December 2015, the Associate Chief Information Security Officer (A-CISO) should lead and conduct a survey of UW-Madison and UW System security operations and services with a focus on those following a common service delivery model and leverage the governing committees to identify metrics and reports for decision making efforts.
3. (Revision – Year One) As a separate effort aligned with Goal #2, the survey team will identify industry best practices for enterprise systems and security operations and services in an ongoing study through March 2017 with analysis due in June 2017. Building from policies developed under the guidance of the UW System Information Assurance Council, the Survey team should then identify gaps in service offerings and redundancies by December 2017.
4. To best capture the cost of security operations and set a model for future services in this domain, the A-CISO and Security Operations Team Lead should document and measure costs and effectiveness of current security operations and services by July 1 2016 and develop a future state cost model and projections by July 1, 2017. This includes identifying resources for supporting the operation and identifying processes for ongoing management of the operation (e.g. inputs for feedback).
5. Following substantial completion of goals 1 through 4 and prior to July 2017, the A-CISO and CISO supported by the Cybersecurity Team will determine efficiencies and identify tool sets to automate available services for UW-Madison and UW System and develop budget requirements for July 2018 (Fiscal Year-18).

Link to Campus Strategy/Goals:

1. Be responsible stewards of our resources by developing a solid understanding of the total cost of

ownership of the controls used to protect our environment and the gaps associated with security programs.

2. Provide and support robust and secure IT research and scholarship infrastructure.

Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination, and Remediation

Cyber threat intelligence is critical to understand the current threat landscape, shrink the time between compromise and recovery, and assist in the development of proactive tactics to combat future cyber-attacks. The threat intelligence itself should include inbound data feeds from a variety of sources (e.g. government, private, higher education, open source) and when reviewed by an IT security analyst should provide actionable alerts to our population. In addition, the UW-Madison Cybersecurity team can develop outbound intelligence to share with other entities with the proper data sharing agreements in place.

The keys of a successful cyber threat intelligence program include the generation of actionable alerts targeted for the owners of the risk. Threat analysts provide actionable intelligence to the proper staff at central campus IT and distribute alerts to the individual network managers across campus along with collecting feedback on the remediation or mitigation of risk resulting from the alerts or identification of any needed assistance. Development of alerts rely on the expansion of the current sophisticated monitoring infrastructure; close collaboration with campus partners and the availability of trained IT security analysts.

Creating and maintaining accurate configuration management data is also a key component of the cyber threat intelligence initiative. Ensuring the information from Federal and State Information Sharing and Analysis Centers and other intelligence sources is relevant to the diverse UW-Madison information architectures is important to achieving this strategic element.

Goals:

1. The Monitoring and Incident Response Cybersecurity team will implement an alerts dashboard, visible to MIST Members, IT staff and leadership of campus IT installations and systems that display intrusion detection events and information on severity and quantity of these events by July 1, 2017. MIST Members or other divisional IT staff will be responsible for monitoring the dashboard for information specific to their College or Department's information enterprise.
2. The Monitoring and Incident Response Cybersecurity team will increase the number of external data feeds used to detect suspicious activity beyond existing sources to include direct feeds from at least one Federal Government source by July 1, 2016.
3. The Monitoring and Incident Response Cybersecurity team will implement or improve a system to collect and periodically confirm security contact information by network assignment by July 1, 2016.
4. The Monitoring and Incident Response Cybersecurity team will implement or improve a notification and tracking system for alerting and metric collection by July 1, 2018.
5. The Monitoring and Incident Response Cybersecurity team will identify and collaborate with a campus partner on the implementation of a new security control that will act on collected network intelligence, e.g. "network block list", etc. by September 1, 2016.

Status Update (Year One): Team determined the goal is satisfied by pursuit of the Advanced Threat Protection (ATP) initiative with Palo Alto Networks Next Generation Firewall (NGFW) and associated services and components plus Cisco Active Threat Analytics (ATA) and Advanced Malware Protection (AMP) components. **GOAL COMPLETE**

Link to Campus Strategy/Goals:

1. Be responsible stewards of our resources through developing a solid understanding of the total cost of ownership of the controls used to protect our environment and the gaps associated with security programs.

Strategy 6: Establish Security Metrics, Optimize Services, Promote Compliance, Achieve Continuous Diagnostics and Mitigation

Security metrics are developed to communicate security posture – including risks to operations and maintenance of acceptable levels of system availability, data integrity and confidentiality of sensitive or restricted information. This includes measuring security control status at frequencies sufficient to deliver actionable information to stakeholders and per organizational risk tolerances. By collecting and communicating security metrics, cyber security professionals can (1) validate security controls are working as designed and address inadequate controls; (2) identify emerging threats and trends; (3) ensure successful compliance with required policies, regulatory requirements and standards; and (4) ensure that repeatable funding is being properly allocated to successful security programs.

Campus IT managers and security staff must work closely with the Office of Cybersecurity to assess their network's ability to produce and report cybersecurity metrics which reflect the status and trends associated with key security functions to include firewall access, threat signature detection, evidence of data loss, status of end point security tools, failed authentication or access controls, detection of malware, and presence of false indicators. Wherever possible, centralized monitoring and collection of data should be pursued. Issues related to efficient management of cybersecurity data elements and communicating data values must be addressed with the return of value to the UW-Madison enterprise in mind.

Risk tolerance is determined through a consistently repeatable Risk Management Framework (RMF) with the components as described in Strategy 2. ***Continuous Diagnostics and Mitigation (CDM)*** is a strategy that deploys tools and services that know the state of the Information Technology (IT) enterprise and strengthens the cybersecurity posture of networks in support of risk mitigation. CDM is an integral part of a Risk Management Framework that supports the Systems Development Life Cycle. The following identifies the workflow of a mature CDM model.

Figure A-2 overlays the concepts of mature RMF and CDM models. The benefits of combining these models include understanding the organization cyber assets, the value of those assets, and the level of security the organization is willing to accept. This is known as the organization security posture. These models also identify risk as the organizational drivers evolve. Drivers include changes to business processes, legal/regulatory requirements, technology, financial resources and cyber threats.

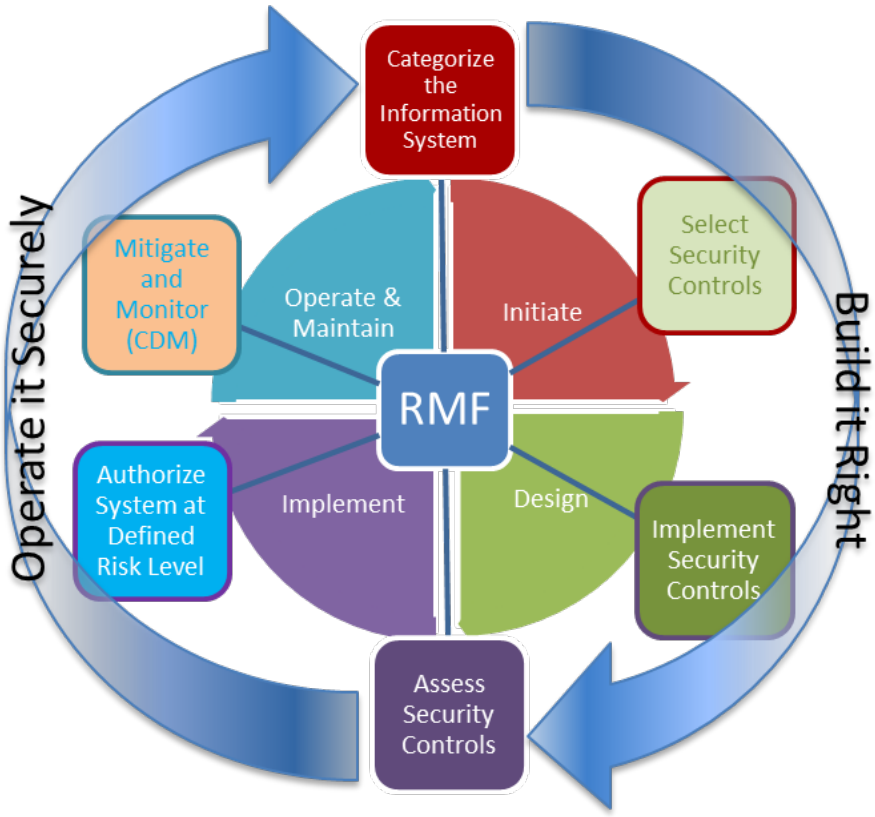

Figure A-2: Risk Management Framework and Continuous Diagnostics and Monitoring Overlay

Goals:

1. Identify and create a budget model for each service managed by each Cybersecurity Domain Team that aligns with the existing budget revenue and expense models to be completed by July 1, 2015.
2. Map each existing campus IT Policy to an existing people, process, technology (PPT) that assists with compliance by August 15, 2015. Each policy may not specifically map to a PPT or be evenly applicable across all departments and units.
3. By May 31, 2015 establish a process for the Cybersecurity Service Leads and corresponding Domain Lead (described in Appendix E) to determine Total Cost of Ownership for each service that currently has measurable attributes to include existing tools demonstrating some form of measurement capability.
4. By September 15, 2015, the Cybersecurity Service Leads should identify the type of metrics to be collected and maintained to ensure success of Goal #1 and #2.
5. By December 2015, A-CISO and CISO establish the framework for CDM using existing tools while determining requirements and acquisition strategy for a tool or suite of tools that meet technology requirements across campus which can be validated through existing governance teams.

Link to Campus Strategy/Goals:

1. Be responsible stewards of our resources by developing a solid understanding of the total cost of ownership of the controls used to protect our environment and the gaps associated with security programs.

Strategy 7: Establish Collaborative Partnerships to assure teaching and research computing resources and results are available to fulfill the Wisconsin Idea and return value to the state and its citizens

Protecting the availability of teaching resources, learning management systems and research networks while assuring important data is available for instruction and research data maintains referential integrity is an important element of the UW-Madison mission. Establishing relationships with Principal Investigators, Institutional Review Boards, key IT leaders in the Colleges and Departments, faculty and researchers will support provision of RMF and security life cycle support to classroom and field instructors, research teams and laboratory managers. Collegial interaction will result in greater efficiency and significant risk mitigation or reduction of vulnerabilities inherent to university and higher education programs[13,14]. Protection of the individual laboratory networks and research data helps protect important grants. We seek partnership with the Wisconsin Institute for Discovery (WID) and their Software Assurance Market Place (SWAMP), the Wisconsin Security Research Consortium (WSRC), Computer Sciences Department's Wisconsin Advanced Internet Laboratory (WAIL), and Institutional Review Boards (IRBs) across campus.

Goals:

1. With collaboration and assistance from the CIOs and Security Staff for the colleges and departments across campus, by December 2015 the CISO will work toward developing a standard model to assess and display operational status and cybersecurity posture. This will enhance the understanding of each system or networks availability and status of vulnerability management leading toward full evaluation of risk.

Status Update (Year One): Completed by establishing processes to forward Weekly Status Report to campus CIOs and acceptance of current metrics through continued engagement at Madison Information Security Team (MIST) and forwarding report to TISC. New effort will be established following implementation and initial operations of the ATP initiatives including ATA, Palo Alto Next Generation Firewall, AMP, TRAPS™ End Point Security, and Autofocus tools. **GOAL COMPLETE**

2. In coordination with the Associate Vice Chancellor for Research and Chief Research Computing and the Assistant Vice Provost for Advanced Computing Infrastructure, prior to September 2015 establish a cybersecurity governance arrangement that addresses the needs of Research Computing environments, special projects and laboratories required to meet Federal guidelines such as the Federal Information Systems Management Act requirements for NIST 800-53r4 or standards required by private or other public grants.

Link to Campus Strategy/Goals:

1. Be responsible stewards of our resources by developing a solid understanding of the total cost of ownership of the controls used to protect our environment and the gaps associated with security programs

[13] Kallberg, Jan; Thuraisingham, Bhavani, "Towards cyber operations - The new role of academic cyber security research and education," Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on , vol., no., pp.132,134, 11-14 June 2012 doi: 10.1109/ISI.2012.6284146

[14] Simson L. Garfinkel. 2012. The cybersecurity risk. Commun. ACM 55, 6 (June 2012), 29-32. DOI=10.1145/2184319.2184330 http://doi.acm.org/10.1145/2184319.2184330

Appendix B: Operational and Enabling Objectives

As a foundation for successful achievement of our long-term strategy, the following near-term operational objectives which must occur to enable the strategic elements and goals to be achieved:

Objective 1: Consider retention of previous strategy's actionable items ("find it", "delete it", "protect it").

Find all restricted data across campus that is required to be stored for business purposes, centralize the data storage and protect usage according to currently applicable standards for high risk data (e.g. PCI data security standards). Key elements of this strategy include:

- *Contacting all campus units 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.*
- *Incorporate VCA restricted data project as a model for campus wide implementation.*

An important measure of completion is obtaining an inventory of all assets (including applications, endpoints, servers, people contacts – data owners, 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 would be a significant activity to support this ovjective.

Objective 2: Enable, support and nourish a culture that values information security and actively works to reduce risk to a level where the remaining potential consequences are acceptable to both management of the local unit and University leadership.

Centrally measure compliance with generally accepted best practices and the *Electronic Devices Connected to the Network* policy. All endpoint devices on the campus:

- *comply with the published IT Security Baseline configuration*
- *are behind a registered network firewall and any exceptions are reviewed and approved by the network owner and the CISO annually; the network firewall is centrally monitored for suspicious activity; and the network firewall rules are reviewed annually;*
- *are regularly patched; Windows devices run the Secunia Corporate Software Inspector (CSI) and centrally report results;*
- *install and run antivirus software and centrally report the results; and*
- *run Identity Finder and report results centrally;*

Objective 3: Based on pending Data Governance Program requirements, establish appropriately secured Data Environments based on the needs of Faculty, Researchers or IT project requirement documents

- *Use the lessons learned from the PCI project[16] to apply to all data environments which house or manipulate sensitive data elements as defined in the Data Governance Policy*
- *Identify, classify and secure 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*
- *Develop a secured environment similar to that currently used for securing credit card information or*

[15] Data Steward is the main role toward ensuring the integrity of UW Madison's data. The Data Steward manages the critical data elements of our 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.

[16] As described in the UW Madison Campus Wide PCI Compliance Project Charter, updated in August 2010

the Controlled Computing Infrastructure (CCI) virtual networked environment.

Objective 4: Centralize data collection and aggregation for analysis of security related events to promote unified measurement of cybersecurity attributes

In order to achieve this objective, the IT Security team will need to collect and centrally manage operational data to support effective security monitoring, incident response and the development of security metrics. The key elements to achieve this objective include:

- *Implementation of a robust event logging infrastructure that units can send operational events*
- *Implementation of an enhanced network security monitoring system for increased network visibility*
- *Collaboration with MIST to identify options for a centralized configuration management database*
- *Implementation of enhanced vulnerability scanning process to identify systems at risk*
- *Development of a formalized cyber security operations center*

Objective 5: Identify and stabilize sources of sustainable funding to enable accomplishment of technical or staffing related strategic goals

To achieve this objective the CISO and A-CISO will partner with DoIT Finance to correct anomalies the current budget model caused by the 2014 re-alignment to a single IT Security team under the CISO and aligning services under a traditional IT Security model. With a goal to control cost, the budget will be designed around the five IT Security domains with funding or revenue, labor and equipment, contract or licensing costs clearly identified for each domain. The budget should accurately forecast funding from UWSA for UW Common Systems support and its alignment to the IT Security domains. The CISO and A–CISO will then work with the CIO, DoIT COO and other leaders on campus to define and document on-time and repeatable funding models. In addition the CISO and A-CISO will explore methods to increase funding through grants and scholarships provided by various granting bodies.

Objective 6: Requirements are imposed upon UW-Madison by other agencies. Identify UW-Madison compliance (FERPA, HIPAA, PCI-DSS, etc.) and then map the IT security components of each to applicable campus units.

To achieve this objective the IT Security Team in conjunction with MIST will (1) Identify requirements that may be imposed on all or parts of the UW-Madison and UW-System cyber infrastructure. (2) Work with the UW-Madison data governance team to identify which requirements apply to specific data classifications. (3) Identify which university departments may leverage these data types. (4) Apply the RMF framework to the department to determine level of compliance against the standard as determined by the Executive Data Governance team.

Objective 7: Develop and refine procedures to ensure security operations and risk assessments are conducted in a sustainable and repeatable manner that ensures standards for timeliness and measurable response are achieved and maintained.

To achieve this objective, the IT Security Team will lead development efforts and work with MIST and Academic Technologies to develop training routines and processes to standardize assessments through technology and development approaches. Assessments must incorporate special security requirements mandated based on information type 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.

Objective 8: Develop and implement marketing and communications plans.

To achieve this objective, the CISO and A-CISO will work with DoIT Communications and UW-

Communications as well as partnering with the School of Business to develop marketing and communications materials to promote the deliverables of the strategic goals and objectives. A plan will be developed with appropriate marketing materials for each of the eight strategic elements. Materials include but not limited to: brochures, reports, presentations, web presence, social presence and marketing handouts (pens, tablets, thumb drives etc.). This plan will include team-branding efforts and may include biographies of team members with formal headshots and team identity logo wear.

Appendix C: Mission, Vision and Guiding Principles of the Office of Cybersecurity

Mission

The Office of Cybersecurity enables the primary institutional missions of teaching, research and service by providing innovative and creative IT security services. We protect vital information and research data by developing, refining and continually delivering comprehensive information security and privacy programs for the University of Wisconsin-Madison and the University of Wisconsin System.

Vision

Embodying the Wisconsin Idea, we embrace the revolution of cybersecurity in higher education, becoming a leading provider of cybersecurity services to the university community. Our work should make a noticeable impact in securing important information and research data to the benefit of Wisconsin communities and beyond.

Guiding Principles

The following principles and values guide us in our daily work and are necessary to successfully meet the demands of cybersecurity operations, planning, education, governance, risk management and compliance:

1. *Cybersecurity services are all about the data!*

   We identify, segregate and secure data based on content and use. Our application of security controls will always focus on identifying, securing and maintaining data to the appropriate levels of availability, confidentiality and integrity

2. *Cybersecurity is a shared responsibility*

   True cybersecurity is a team sport! We provide our services and engage the users, administrators, technicians, managers and data owners with mutual respect and encouragement.

3. *We will intentionally implement a holistic approach to cybersecurity that aligns with the needs of the University*

   We engage communities with frameworks that facilitate business driven solutions that reduce risk across the entire UW-System. This includes being aligned at the beginning of the initiative to ensure security by design, to provide security approval of the system at a specified level of risk; and continue to partner through the lifecycle of the system.

4. *We build and maintain a balanced portfolio of cybersecurity policy, process, services and capabilities that materially reduce risk*

   Cybersecurity solutions are not necessarily tool-centric. Balancing the expertise of our staff, efficacy of tools and technology, and achieving clarity in policy, process and enforcement is the most effective path. When tools are contemplated, we will consider the scale and portability aspects with the goal of using the tool for its intended purpose throughout the UW System.

5. *We actively promote stewardship of our resources by prioritizing the diverse needs of stakeholders and implementing innovative cybersecurity strategies*

   In understanding our assets, the risks those assets pose and having an understanding of the controls to mitigate the risk will allow us to better understand the success of our people, process and

technologies.

6. *We value consensus and shared responsibility as we approach Governance, Risk Management and Compliance as a collaborative cybersecurity commitment*

The UW-Madison IT Security Team (MIST) and the UW- Technology and Information Security Council (UW-TISC) form a community that is a rich resource in developing the components of GRC. Major issues and strategies will be brought to these groups, as appropriate, to gain the feedback and concurrence necessary to press forward.

7. *We value transparency in our approaches and in the application of cybersecurity controls, processes and policies*

We provide our communities with information to become aware of cyber security risks by thoughtfully monitoring, measuring and reporting the success of compliance with policies, processes and controls

8. *We will strive to live the Wisconsin Idea and the state motto as we continuously evaluate and improve cybersecurity capabilities to keep the University moving "Forward!"*

Cybersecurity is a journey, not a destination. The Office of Cybersecurity will continually seek strategies and programs that serve to evolve our cybersecurity posture to achieve success in defending the data against unauthorized access, inadvertent release, or other actions detrimental to the progress of education and research that benefit the State of Wisconsin.

Appendix D: 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 Chief Information Officer (CIO) and Vice Provost for Information Technology, to focus on these six areas:

1. *Identify and manage IT security risk through governance, risk management and compliance programs;*
2. *On behalf of the CIO, develop IT and cybersecurity policy, providing leadership for related program planning and documentation;*
3. *Monitor the UW-Madison campus and UW-System IT Enterprise and respond to cybersecurity incidents;*
4. *Support IT security engineering actions and actively manage applied security controls to reduce risk as part of active cybersecurity defense;*
5. *Promote campus leadership and operational entities awareness of cybersecurity threat vectors, attack surfaces, threat actors, IT Security solutions and industry trends; and*
6. *Provide security education, training and awareness by engaging DoIT Academic Technology and DoIT User Services to elevate the level of understanding among UW-Madison constituents.*

Appendix E: Cybersecurity Organization and Governance

This appendix provides 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.

The UW-Madison cybersecurity organization and descriptions shown in Figure E-1 provides a single touch point for all cybersecurity related groups and organizations. The Office of Cybersecurity 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 Appendix C, performing the role described in Appendix D.

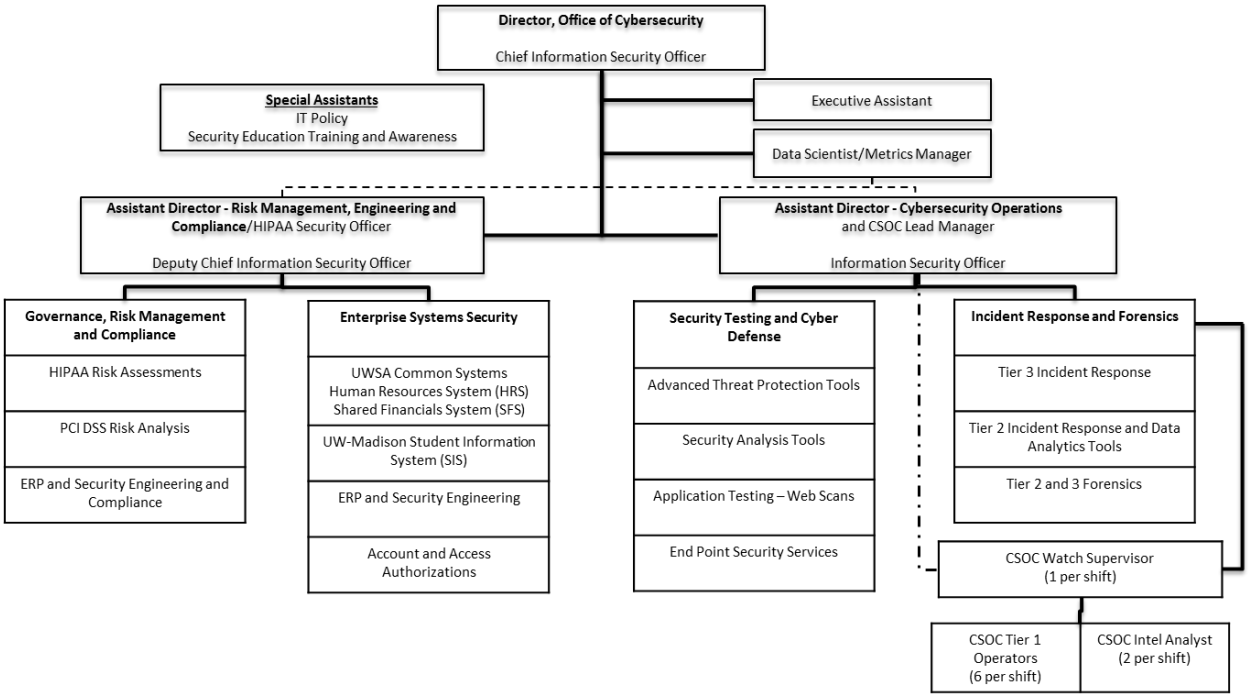

Figure E-1: UW-Madison Office of Cybersecurity Organization (July 2017)

IT Security staff supporting the CIOs in the individual colleges and departments interact with the Office of Cybersecurity on an individual basis or as part of the Madison Information Security Team (MIST). Likewise, the UWSA CISO has 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, 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 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.

Enterprise Systems Security

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.

Security Testing and Cyber Defense

This team supports implementation of frameworks and processes that pro-actively identify, assess and manage vulnerabilities through testing systems throughout the systems development life cycle and 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 & 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.

Note: The following sections are in transition and will be replaced by links to the appropriate web pages for the governance organizations the narratives represent.

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. As shown in Figure E-2, 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*

This would be the "President" at most universities. Since UW institutions are part of the larger UW System, the individual institutions are each lead by a Chancellor.

4. *UW-Madison Vice Chancellor for Finance and Administration (VCFA)* and *UW-Madison Provost*
   - *The VCFA leads most of the administrative units. This would be a Vice President at many other universities.*
   - *The Provost leads the academic and academic support units. The Provost is also a Vice Chancellor.*
   - *The Chancellor, VCFA and Provost collectively lead the institution.*

5. *Deans and Directors of Schools, Colleges and Divisions, one of whom is the UW-Madison CIO and Vice Provost for Information Technology (CIO and VP IT).*
    - *Academic Deans, the CIO/VP IT, and executives leading other divisions that provide academic support report to the Provost. Some executives reporting to the Provost are titled Vice Provosts.*
    - *Most of other administrative Directors report to the VCFA. Some are titled Associate Vice Chancellor or Assistant Vice Chancellor.*
    - *A few units, such as Legal Services, report directly to the Chancellor. Some executives reporting to the Chancellor are titled Vice Chancellors.*
    - *The CIO/VP IT is also the Executive Director of DoIT. The Director of DoIT, (who reports to the Executive Director,) is also titled and usually referred to as the Chief Operating Officer (COO) of DoIT.*
    - *All these leaders are (roughly) peers. The CIO and COO advise the others on IT matters of all kinds, (and vice-versa.) The CISO, (see next tier below,) can represent the CIO on IT security matters.*

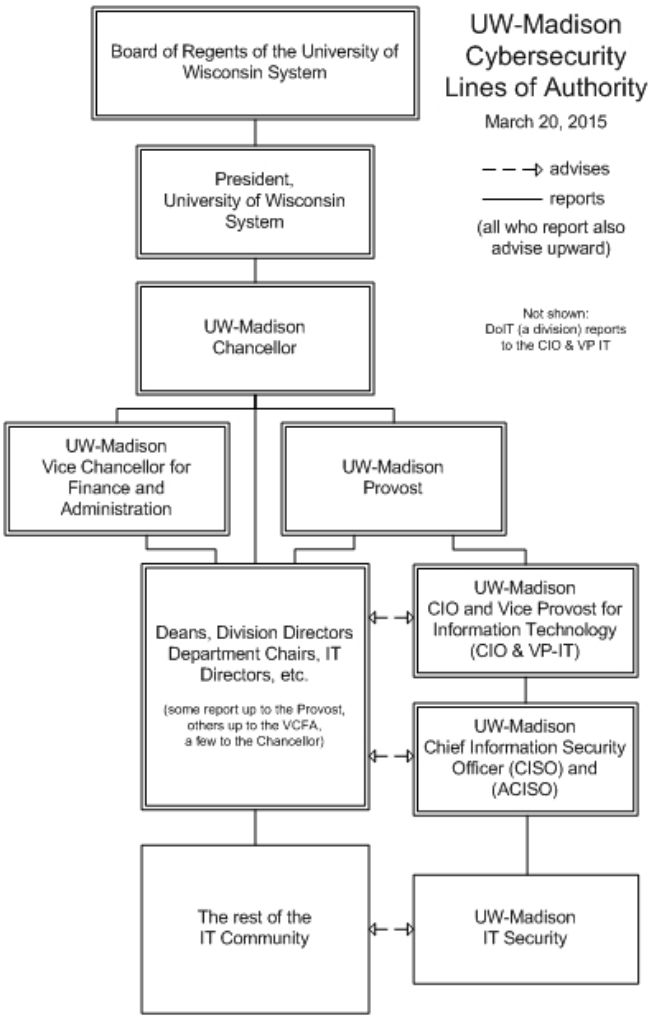

Figure E-2: UW-Madison Cybersecurity Lines of Authority

6. *Department Chairs, IT Directors, and other executives, two of whom are the UW-Madison Chief Information Security Officer (CISO) and the Associate Chief Information Security Officer (ACISO.)*
    - *Department chairs lead academic departments, and report to the Dean, (or in some large schools or colleges, an Associate Dean.) A chair is elected by the other faculty in the department, with the approval of the Dean.*
    - *Some schools, colleges and divisions have a divisional CIO. Some have a divisional IT director. Some larger departments have an IT Director.*
    - *All these leaders are peers. The CISO/A-CISO advise the others on IT security matters, (and vice-versa.)*
7. *"The Rest of the IT Community" consists of all end users and all IT staff other than the "IT Security staff", (who report to CISO/ACISO.) The IT Security staff advise the other IT staff on security matters (and vice-versa.) The IT staff, including the IT Security staff, advises the end users.*
    - *Mid-sized academic departments with only a few IT staff usually have an IT leader (variously titled.)*
    - *Some smaller departments have only one IT person, while others have no dedicated IT staff.*

Official UW-Madison Cybersecurity Advisory Relationships.

These organizations are "official" in the sense that they are recognized and specifically chartered or defined as a shared a governance body or advisory group. As shown in Figure E-3, there are roughly four tiers of IT security advisory relationships at UW-Madison. The relationships are advisory among entities in the same tier. Each tier also advises "upward" to the next tier through the reporting relationships detailed in the section titled Line Organization.

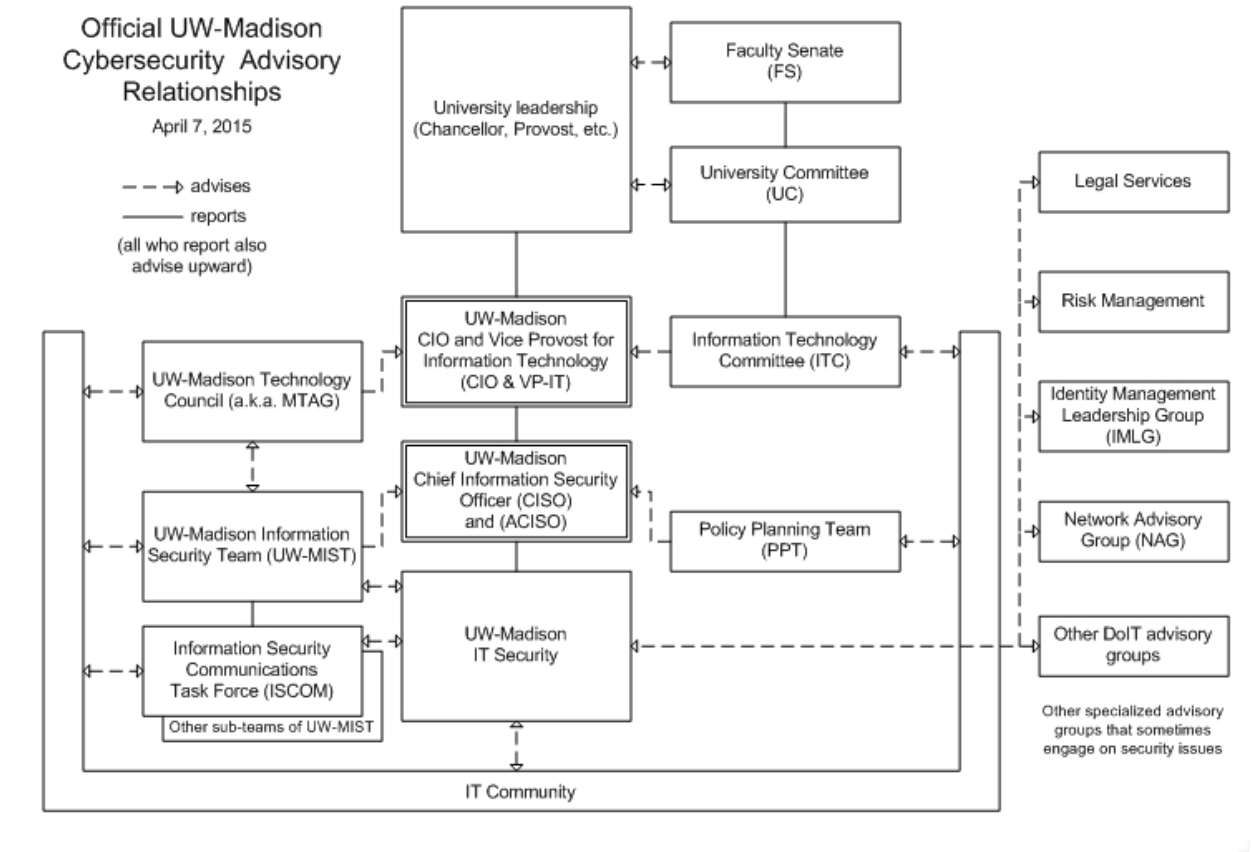

Figure E-3: Cybersecurity Advisory Relationships

1. *Shared Governance*
   - *Shared Governance is written into Wisconsin state statutes. The faculty and administration work together to govern the institution.*
   - *The Faculty Senate is the legislative body of the faculty. The Chancellor is chair of the Faculty Senate.*
   - *The University Committee is the faculty's executive committee.*
   - *Among other specialized entities, Legal Services and Risk Management advise at this level.*
2. *CIO/VP IT and advisors*
   - *The Information Technology Committee (ITC) is the official shared governance committee for IT. The ITC is advisory to the CIO.*
   - *The CIO has an official advisory group that represents the IT community. This is the Madison Technical Advisory Group (MTAG).*
   - *The CIO advises upward to university leadership.*

- *Among other specialized entities, the Identity Management Leadership Group (IMLG) advises at this level. IMLG is particularly relevant to information security.*

3. *CISO/ACISO and advisors.*
   - *The UW-Madison Information Security Team (UW-MIST) is the official advisory group for the Chief Information Security Officer (CISO) and Associate Chief Information Security Officer (ACISO). Most schools, colleges and divisions have an official representative on UW-MIST, along with a number of other IT leaders who are interested in advising on IT security matters.*
   - *The Policy Planning Team (PPT) is an advisory group for IT policy principles and procedures, and overall IT policy planning. The PPT is advisory to the Office of the CIO through the CISO.*
   - *The CISO/ACISO advise upward to the CIO.*
   - *Among other specialized entities, a number of DoIT advisory groups are at this level. For example, the Network Advisory Group (NAG) advises the Director of Network Engineering. NAG is particularly relevant to information security.*
4. *Other groups and teams*
   - *UW-MIST may have one or more sub-teams operating at any given time. These are sometimes working on security-related IT policy. The IT Security staff have representatives on all security-related teams.*
   - *There is sometimes a "Policy Stakeholder Team" (PST) working on IT policy that is partially (or entirely) unrelated to IT security.*
   - *Regardless of the subject matter, each such team is advisory to the group or executives that chartered it.*
   - *Among other specialized entities, some DoIT service teams have user groups or advisory groups. All services require some attention to information security.*

Official UW System Cybersecurity Advisory Relationships

As shown in Figure E-4, 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).

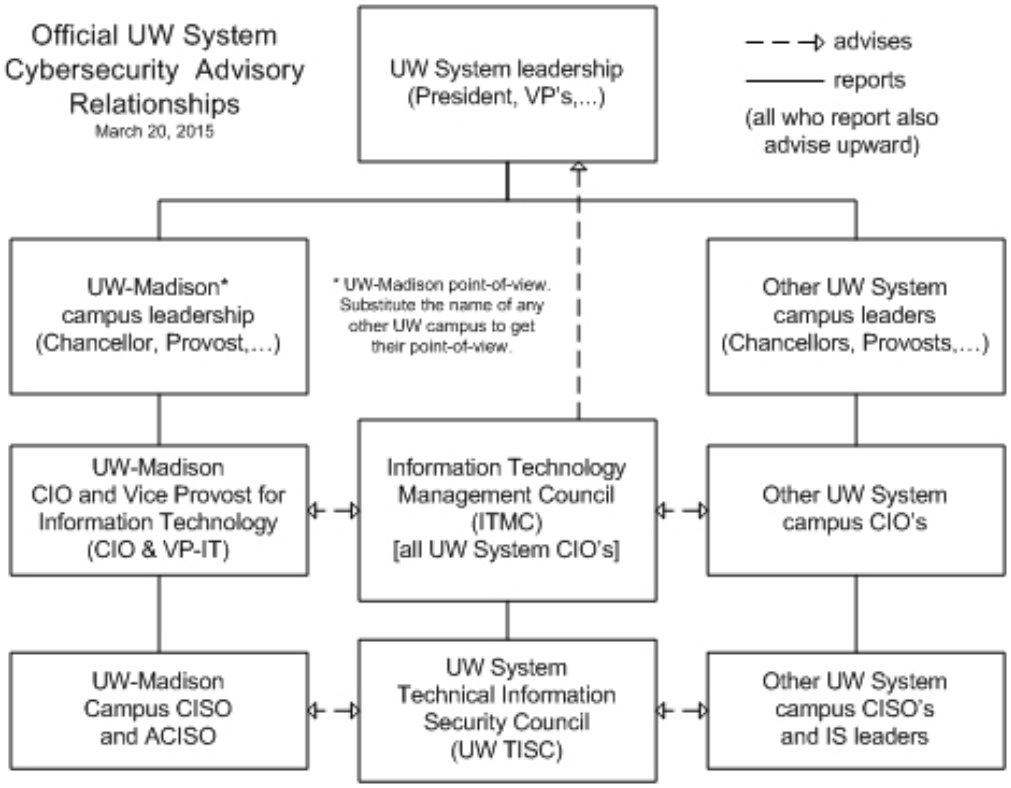

Figure E-4: UW Systems Cybersecurity Relationships

1. *The Information Technology Management Council (ITMC) consists of the CIO of each UW system campuses, (including 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. *In a broader sense, the ITMC also includes the subordinates of the CIO's in a number of specialized areas. These subgroups of the ITMC are called teams, councils, or "breakouts" (a term from the ITMC conference, where the groups meet as "breakout sessions".)*
   - *The information security group is called the UW Technical Information Security Council (UW TISC.) UW TISC consists of the CISO, SO, or other security representative from each institution. Additional people from some institutions also attend the council's meeting at the ITMC conferences. UW TISC is advisory to the CIO council and each other.*
   - *Neither the CIO council nor UW TISC can directly implement their recommendations. Each CIO (or CISO) needs to take the recommendation back to their own campus and consult with their campus leadership and/or advisory groups.*

UW-Madison PCI Governance

Certain data domains, such payment card data or health care data, have their own governance organizations. PCI refers the Payment Card Industry Data Security Standard (PCI-DSS). This is a standard mandated by contract if the institution wants to process payment cards. Figure E-5 portrays the business process and organizational relationships that govern implementation and operation of PCI-DSS.

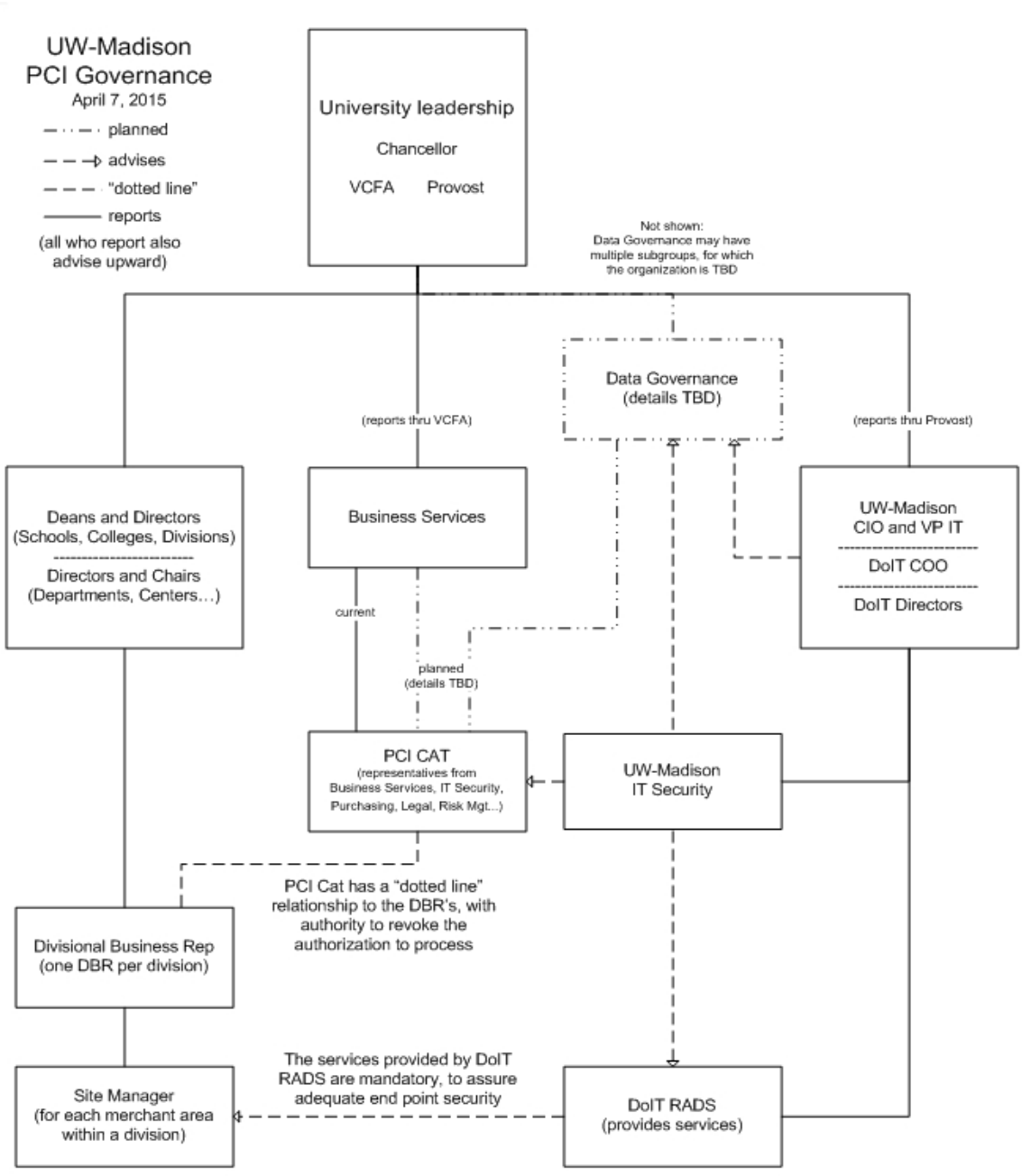

Figure E-5: PCI Governance

1. *UW-Madison, as an institution, is responsible for compliance with the PCI contract. The Vice Chancellor for Finance and Administration (VCFA) is responsible for this, and has delegated the responsibility as outlined below.*
2. *The VCFA has delegated oversight and management to Business Services (which reports to the VCFA.)*
    - *The individual schools, colleges and divisions that actually process payment cards are responsible for compliance on their end. The Dean or Director is ultimately responsible for their division's compliance.*
    - *UW-Madison Data Governance, when implemented, will have a role in PCI administration. This role is TBD.*
3. *PCI CAT does detailed coordination.*
    - *PCI CAT has representatives from Business Services, IT Security, Purchasing, Legal Services and more.*
    - *PCI CAT is advised by UW Madison IT Security.*
4. *Each school, college or division has a Division Business Representative (DBR), responsible for compliance within its division.*
    - *The DBR's report up to the Dean or Director of their Division.*
    - *PCI CAT has a "dotted line" relationship to the DBR's to assure that their division remains in compliance.*
5. *Each site that processes payment cards is called a Merchant Area.*
    - *Each Merchant Area has a Site Manager.*
    - *The Site Manager does not necessarily report up to the DBR, but both the DBR and the Site Manager ultimately report up to the same Dean or Director.*
    - *The Site Manager works with DoIT Repair and Desktop Support (RADS) that provides a mandatory service that configures and maintains the devices and other IT infrastructure at the site that must comply with PCI-DSS.*

UW-Madison HIPAA Governance

Protected Health Information (PHI) is subject to the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule and HIPAA Security Rule are both relevant to information security, (the Security Rule more so.) Some of the governance described and pictured in Figure E-6 is still under development, but the diagram and document are consistent with the current plan.

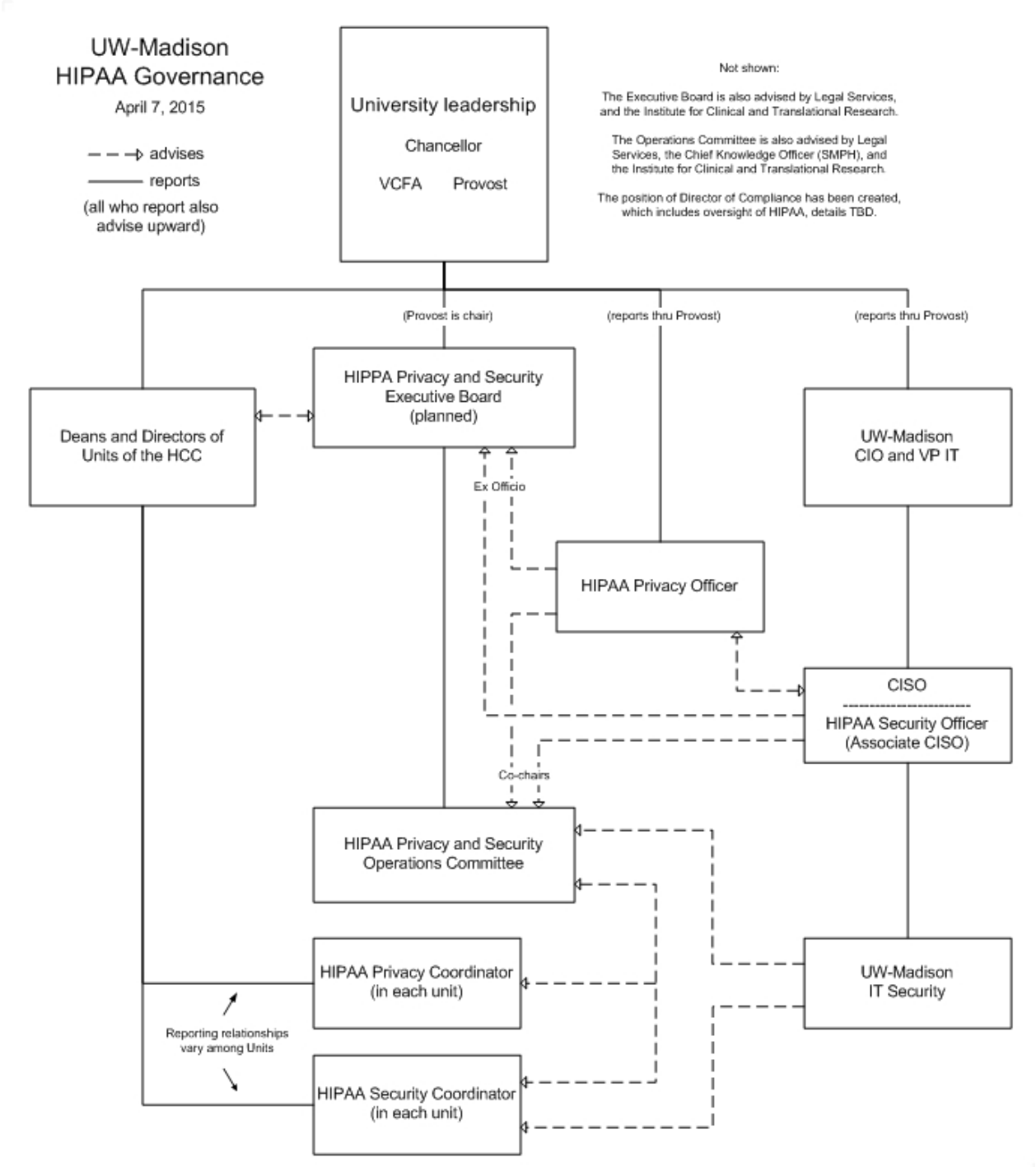

Figure E-6: HIPAA Governance Structure

UW-Madison is a "hybrid entity" under HIPAA. Only certain units at UW-Madison are considered part of the Health Care Component (HCC). Other units and individuals are part of the HCC if they provide certain support services to the HCC. In addition, some units are Business Associates of other covered entities.

1. *UW-Madison, as an institution, is responsible for compliance with the HIPAA. The Provost is responsible for this, and has delegated the responsibility as outlined below.*
2. *There will be a HIPAA Privacy and Security Executive Board, consisting of the Provost, the Deans and Directors of the units of Health Care Component (HCC), the Vice Chancellor for Legal Affairs, and the Director of the Institute for Clinical and Translational Research. The UW-Madison HIPAA Privacy Officer and the HIPAA Security Officer are both ex officio members.*
3. *There will be a HIPAA Privacy and Security Operations Committee consisting of the Privacy Coordinator and Security Coordinator(s) of each unit of the HCC, the Chief Knowledge Officer of the School of Medicine and Public Health, the Associate Director of the Institute for Clinical and Translational Research, and a representative from Legal Services. The committee is co-chaired by the HIPAA Privacy Officer and the HIPAA Security Officer. UW Madison IT Security advises the Operations Committee.*
4. *Each unit of the HCC has a Privacy Coordinator and one or more Security Coordinators (and/or Sub-coordinators). These coordinators report up to their Dean or Director (who is on the Executive Board.) UW-Madison IT Security also advises the individual security coordinators.*
5. *In addition, the position of Director of Compliance has recently been created. The position includes oversight of HIPAA, details TBD.*

The HIPAA Privacy Coordinator reports to the Provost. The HIPAA Security Coordinator reports to the CISO, the Vice Provost for Information Technology, and ultimately to the Provost. The Privacy Officer and Security Officer share responsibility for certain portions of HIPAA compliance, and are advisory to each other in that capacity. Beyond that, the HIPAA Privacy Officer has overall responsibility for HIPAA compliance, while the HIPAA Security Officer focuses more narrowly on the Security Rule.

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. These are:

- *Human Resource System (HRS) – UW System level, governed through the UW Service Center.*
- *Shared Financial System (SFS) – UW System level, which has its own governance arrangements.*
- *Integrated Student Information System (ISIS) – UW-Madison-specific, governed through ISIS Central.*
- *Info Access – UW-Madison-specific, governed as a DoIT service.*
- *Various research areas, including for example:*
    - *The Institutional Review Boards (IRB's) for human subject research.*
    - *More generally, governance of security requirements to accompany grants from different funding agencies, (each agency has its own requirements.)*

Appendix F: Acronyms, Abbreviations, Terms and Definitions

Acronyms and Abbreviations

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

Acronym or Abbreviation	Long Title
A-CISO	Associate Chief Information Security Officer (term changed in July 2017)
D-CISO	Deputy Chief Information Security Officer
ADI	Application Development & Integration
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DoIT	Division of Information Technology
EITDM	Enterprise IT Decision Management
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
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health (HITECH) Act
HRS	Human Resource System
IMLG	Identity Management Leadership Group
IRB	Institutional Review Boards
ISIS	Integrated Student Information System (* Name change in progress)
ITC	Information Technology Council
ITMC	Information Technology Management Council
MIST	Madison Information Security Team
MTAG	Madison Technical Advisory Group
NAG	Network Advisory Group
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
PPT	Policy Planning Team
PTE	Professional Technical Education
RADS	DoIT Repair and Desktop Support
RMF	Risk Management Framework

Acronym or Abbreviation	Long Title
SDLC	Systems Development Life Cycle
SETA	Security Education, Training & Awareness
SFS	Shared Financial System
SWAMP	Software Assurance Marketplace
TISC	Technology and Information Security Council
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
WAIL	Wisconsin Advanced Internet Laboratory
WID	Wisconsin Institute for Discovery
WSRC	Wisconsin Security Research Consortium

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 ing 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)

Appendix G: Cybersecurity Assignments for those Responsible, Accountable, Consulted and Informed

Also known as a RACI Chart, this appendix lists and describes the specific responsibilities involved with Cybersecurity Strategy development, staffing and execution. Table 1 lists the participating offices and specific staff titles that are involved while Table 2 lists the specific tasks or subject areas and the corresponding office or staff that are primarily responsible for accomplishing the activity. It also includes those accountable for the accuracy and quality of the completed item or product; offices, specific staff or processes that are to be consulted when doing the activity; and the specific office, staff or processes that are to be informed of specific milestones or full completion of the activity.

Table G-1: Participating Offices or Staff

Participating Offices or Staff Titles	Acronym	RACI Identifier
Office of the CIO		
Vice Provost for Information Technology and Chief Information Officer	CIO	1
Chief of Staff / Enterprise IT Decision Manager	COS	1a
Chief Data Officer	CDO	2
Office of Cybersecurity		
Chief Information Security Officer	CISO	3
Associate Chief Information Security Officer	D-CISO	4
Governance, Risk and Compliance Lead	GRC	5
Security Testing and Operations Lead	ST&O	6
Monitoring and Incident Response Lead	M-IR	7
ERP Security & Operations Lead	SecOps	8
Security , Training, Education and Awareness Lead	SETA	9
UW-Madison Information Security Team	UW-MIST	10
UW-MIST Co-Chairs	MIST Co-Chairs	11
HIPAA Security Officer	HIPAA-SO	12
HIPAA Privacy Officer	HIPAA-PO	13
UWSA Chief Information Officer	UWSA CIO	14
UWSA Chief Information Security Officer	UWSA CISO	15
UW Technical Information Security Council	UW TISC	16
Division of Information Technology	DoIT	
Chief Operating Officer	COO	17
DoIT Directors	OD's	18
Human Resources Director	DoIT HR	19
Financial Services Director	DoIT FS	20
Madison Technical Advisory Group	MTAG	21
Information Technology Council	ITC	22

Table G-2: Offices, Teams or Named Staff that are Responsible, Accountable, Consulted & Informed

Task or Area	Responsible	Accountable	Consulted	Informed
Strategy #1 Champion	De Clute	3	2, 4, 5, 11, 18	1, 10, 12, 17
Strategy #2 Champion	Eckhardt	3	4, 11, 18	1, 10, 12, 17
Strategy #3 Champion	Imamura	3	9, 10, 11, 18	1, 10, 12, 17
Strategy #4 Champion	Glasson	3	8, 10, 11, 15, 16	1, 10, 12, 17
Strategy #5 Champion	Savoy	3	4, 7, 11, 15, 16	1, 10, 12, 17
Strategy #6 Champion	4	3	5, 6, 7, 8, 9, 10, 15	1, 10, 12, 17
Strategy #7 Champion	3	3	1, 1a, 10, 176, 18, 21, 22	1, 10, 12, 17
Objective #1 Coordinator	3	3	4, 5	1, 10, 17
Objective #2 Coordinator	3	3	1a, 10, 22	1, 10, 17
Objective #3 Coordinator	3	3	18	1, 10, 17
Objective #4 Coordinator	3	3	18	1, 10, 17
Objective #5 Coordinator	3	3	1a, 20	1, 10, 17
Objective #6 Coordinator	3	3	2, 18	1, 10, 17
Objective #7 Coordinator	3	3	18	1, 10, 17
Objective #8 Coordinator	3	3, 12		1, 10, 17

Appendix H: Cybersecurity Strategy – Year One Progress Report

July 21, 2016

To: Bruce Maas, Vice Provost for Information Technology and Chief Information Officer, UW-Madison

From: Bob Turner, Chief Information Security Officer, UW-Madison

Re: UW-Madison Cybersecurity Strategic Plan for 2015 – 2019; Year One Update

The enclosed report is passed for your information and to provide a status of accomplishment for the goals aligned with the seven Strategic Elements. Also included in this report are recommended adjustments to the strategy and goals.

Executive Summary:

Year One has been a great success with several important goals completed. The most significant news is the appearance of a cultural change where the distributed elements of IT activity on campus are more aware of the "enterprise" security environment and appreciate the threat and vulnerability components to a greater extent. Many IT leaders are working hard to get out in front of the cybersecurity events and ensure appropriate protections are in place or mitigations are available.

A summary of the significant accomplishments is provided below. Greater detail is in Enclosure (1).

Completed Goals:

Strategy / Goal #	Action
1 / 1	Established Data Stewardship Council and Data Governance Executive Committee. Approved four tier data classification system.
2 / 1	Team determined the National Institute for Standards and Technology (NIST) model will scale best for UW-Madison. Briefed at UW Technical Information Security Committee (TISC) Summer Meeting (July 2015) with no dissenting opinions. Standard was included in Regent Policy Directive 25-5 Information Security published in February 2016
3 / 3	Phishing campaign is a success!!! Developed monthly campaigns and strategy to increase use of PhishLine training licenses across campus. Proven with recent real-world phishing attempts stopped by User actions. Need to gather metrics to prove the efficacy of PhishLine tool and work to expand the licenses used across campus to meet the current contract limit.
5 / 5	Team determined the goal is satisfied by pursuit of the Advanced Threat Protection (ATP) initiative with Palo Alto Networks Next Generation Firewall (NGFW) and associated services and components plus Cisco Active Threat Analytics (ATA) and Advanced Malware Protection (AMP) components.
7 / 1	Completed by establishing processes to forward Weekly Status Report to campus CIOs and acceptance of current metrics through continued engagement at Madison Information Security Team (MIST) and forwarding report to TISC. New effort will be established following implementation and initial operations of the ATP initiatives including ATA, Palo Alto Next Generation Firewall, AMP, TRAPS™ End Point Security, and Autofocus tools.

New Strategic Elements or Goals

Strategy / Goal #	New Goal
1 / 3	Assist with developing the Restricted Administrative Data Authorization policy & procedures. Ensure that the policy is consistent with anticipated implementation of the Risk Management Framework.
2 / 5	Develop supporting policy for Risk Management Framework.
3 / 5	Develop campus policy requiring participation in SETA.
3 / 6	Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the CIC Security Working Group.

Strategic Elements or Goals Requiring Significant Change:

Strategy / Goal #	Revised Goal Statement / Rationale for Deleted Goal
4 / 3	**Revision**: As a separate effort aligned with Goal #2, the survey team will identify industry best practices for enterprise systems and security operations and services in an ongoing study through March 2017 with analysis due in June 2017. Building from policies developed under the guidance of the UW System Information Assurance Council, the Survey team should then identify gaps in service offerings and redundancies by December 2017.

Next Steps in the Cybersecurity Strategy Life Cycle

Year Two will be highlighted by significant accomplishments as we implement the Advanced Threat Protection components and press on toward the Cybersecurity Surveillance and Operations Center. Significant policy, process and procedure gains will be needed to keep momentum. Years Three and Four are reserved for significant course adjustments and will most likely see retirement of at least one strategic element (#1 - Complete Data Governance and Information Classification Plan).

Bob Turner
Chief Information Security Officer
University of Wisconsin-Madison

Enclosure: (1) Status of Cybersecurity Strategic Goals

Enclosure (1) – Status of Cybersecurity Strategic Goals

The tables below show a summary of the original strategic elements and goals including the status of goals completed, any modifications required, and additional goals recommended. The final table provides a brief status of each one of the enabling objectives.

Strategic Elements and Goals

Strategy	Associated Goals
Strategy 1: Complete Data Governance and Information Classification Plan	1 – **(Completed)** Form data stewards group; create data classification system and process
	2 – Validate compliance with restricted data management policy using UW-MIST
	3 – **(New)** Assist Chief Data Officer with Restricted Administrative Data Authorization Policy consistent with the Risk Management Framework
Strategy 2: Establish the UW-Madison Risk Management Framework to reduce cybersecurity risk	1 – **(Completed)** Achieve agreement with UW System on business rules for adopting NIST Risk Management Framework
	2 – Present staffing needs to complete a new risk assessment to replace the Campus IT Security Baseline
	3 – Define and present the Organizational Parameters of the NIST 800-53 Security Controls and mapping to the IT Security Baseline
	4 – Develop implementation Plan for conducting assessments using the Risk UW-Madison Management Framework
	5 - **(New)** Assist the Chief Data Officer, Data Stewards Council and Data Governance Steering Committee with the Restricted Administrative Data Authorization policy & procedures. Ensure that the policy is consistent with anticipated implementation of the Risk Management Framework.
Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness	1 – Define group specific security awareness programs for IT and security staff, students, administrators, and faculty/researchers
	2 – Develop website to provide a place for campus community to visit and view helpful information and initiatives
	3 – **(Completed)** Raise security awareness through active Phishing campaigns
	4 – Work though UW-MIST to identify and develop training and awareness for new or returning employees
	5 - **(New)** Develop campus policy requiring participation in SETA.

Strategy	Associated Goals
	6 - **(New)** Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the Big Ten Academic Alliance's (formerly the Committee on Institutional Cooperation) Security Working Group 7 - **(New)** Develop and implement a SETA Advisory Committee consisting of a cross section of campus constituencies.
Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services	1 – Define criteria needed to describe a security operation or service. A governance structure should be established to provide oversight of common solutions
	2 – Survey security operations and services to define a common service delivery model. Identify metrics and reports that support decision making efforts
	3 – Using current service models, identify common "best practice" approaches and gaps or redundancies to determine existing business processes and services worthy of distribution across the UW System campuses
	4 – Capture the cost of security operations and examine effectiveness to identify resources necessary for aa Future State Cost Model for ongoing operations
	5 – Determine efficiencies and identify tool sets to automate available services for UW-Madison and UW System in preparation for submitting the FY-18 budget
Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination, and Remediation	1 – Implement a dashboard to display current alerts, intrusion detection events, and information on severity and quantity of events
	2 – Increase number of external data feeds to detect suspicious activity beyond current sources. Place at least three additional feeds including one U/.S. Government source
	3 – Implement or improve a system to collect and periodically confirm security contact information by network assignment
	4 – Implement or improve a notification and tracking system for alerting and metric collection
	5 – **(Completed)** Identify and collaborate with a campus partner on the implementation of a new security control that will act on collected network intelligence, e.g. "network block list"
Strategy 6: Establish Security Metrics, Optimize Services, Promote Compliance, Achieve Continuous Diagnostics and Mitigation	1 – Identify and create a budget model for each service managed by each Cybersecurity Domain Team that aligns with the existing budget revenue and expense models
	2 – Map each existing campus IT Policy to an existing people, process, technology (PPT) that assists with compliance

Strategy	Associated Goals
	3 – Establish a process for the Cybersecurity Service Leads and corresponding Domain Lead to determine Total Cost of Ownership for each service with measurable attributes
	4 – Identify the type of metrics to be collected and maintained to ensure success of Goal #1 and #2
	5 – Establish the framework for CDM using existing tools while determining requirements and acquisition strategy for a tool or suite of tools
Strategy 7: Establish Collaborative Partnerships to assure teaching and research computing resources and results are available to fulfill the Wisconsin Idea and return value to the state and its citizens	1 – **(Completed)** Work toward developing a standard model to assess and display operational status and cybersecurity posture. This will enhance the understanding of each system or networks availability and status of vulnerability management leading toward full evaluation of risk.
	2 – Establish a cybersecurity governance arrangement that addresses the needs of Research Computing environments, special projects and laboratories required to meet Federal guidelines

Goals Accomplished

Strategy / Goal #	Action
1 / 1	Established Data Stewardship Council and Data Governance Executive Committee. Approved four tier data classification system.
2 / 1	Team determined NIST model will scale best for UW-Madison. Briefed at UW TISC Summer Meeting (July 2015) with no dissenting opinions. Standard was included in Regent Policy Directive 25-5 Information Security published in February 2016
3 / 1	**(Significant Partial Accomplishment)** Security Testing and Cyber Defense domain team organized three Qualys Vulnerability Management in-person training sessions in the first and second quarter in 2016. The objective of this training is to introduce Qualys Vulnerability Management tool and primarily focused on host-based vulnerability scanning, reporting, and remediation. Total of 41 people from UW-Madison departments and UW-System schools (System Administration, Extension, Green Bay, Milwaukee, Oshkosh, and Stout) have taken the training, and the tool has been used by 22 different business units as of June 2016.
3 / 3	Phishing campaign is a success!!! Developed monthly campaigns and strategy to increase use of PhishLine training licenses across campus. Proven with recent real-world phishing attempts stopped my User actions. Need to gather metrics to prove the efficacy of PhishLine tool and work to expand the licenses used across campus to meet the current contract limit.
5 / 5	Team determined the goal is satisfied by pursuit of the Advanced Threat Protection initiative with Palo Alto Networks NGFW and associated services and components plus Cisco ATA and AMP components. As the components are delivered we will work toward standardized processes that can be used across the UW-Madison campus and are easily exportable to interested UW System, campuses.

Strategy / Goal #	Action
7 / 1	Completed by establishing processes to forward Weekly Status Report to campus CIOs and acceptance of current metrics through continued engagement at MIST and forwarding report to TISC. New effort will be established following implementation and initial operations of the ATP and ATA initiatives based on WildFire and Autofocus ATP tools.

Goals with End Dates Modified

Strategy / Goal #	Recommended End Date / Rationale
2 / 3	8/1/2016 - Goal date reset due to development delays related to workload and delays in hiring new GRC Lead. Resource requirements submitted in FY-17 budget revision were put on hold with new GRC positions authorized by Provost and VCFA to advance HIPAA Risk Assessments.
2 / 4	8/1/2016 – 85% complete. RMF Development goal reset pending proof of concept testing at Data Center (B350) and Select Agent Labs in July 2016
4 / 1	1/15/2017 - Changed to allow time for installation and testing of Advanced Threat Protection and other components.
6 / 3	12/30/2016 - Due date adjusted based on time needed to implement new ATP and ATA initiatives. New tools will alter composition of services offered for Monitoring and Incident Response domain and the Security Testing and Cyber Defense domain.
6 / 4	3/15/2017 - Development of new metrics placed on hold until new tool suite based on AMP and ATA is at interim operating capability.
6 / 5	5/31/2017 - Goal is 50% complete with current ATP and ATA initiatives plus wider use of Qualys and other tools across campus. Delay in establishing framework due to requirement to establish policy approved through University Committee. Expect to have approval to proceed in early Fall 2016.
7 / 2	1/1/2017 - Changes in Office of the CIO and other research leadership across campus placed this initiative on hold through most of 2015 and first half of 2016.

Goals Modified or Deleted

Strategy / Goal #	Revised Goal Statement / Rationale for Deleted Goal
4 / 3	**Revision**: As a separate effort aligned with Goal #2, the survey team will identify industry best practices for enterprise systems and security operations and services in an ongoing study through March 2017 with analysis due in June 2017. Building from policies developed under the guidance of the UW System Information Assurance Council, the Survey team should then identify gaps in service offerings and redundancies by December 2017.

Goals to be Added

Strategy / Goal #	New Goal
1 / 3	Assist the Chief Data Officer, Data Stewards Council and Data Governance Steering Committee with the Restricted Administrative Data Authorization policy & procedures. Ensure that the policy is consistent with anticipated implementation of the Risk Management Framework.
2 / 5	Develop supporting policy for Risk Management Framework.
3 / 5	Develop campus policy requiring participation in SETA.
3 / 6	Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the CIC Security Working Group.
3 / 7	Develop and implement a SETA Advisory Committee consisting of a cross section of campus constituencies.

Status of Enabling Objectives

Enabling Objective	Status
1 - Consider retention of previous strategy's actionable items ("find it," "delete it," and "protect it").	This will remain an ongoing objective. Enablers are continued build-out of Campus Computing Initiative and data discovery associated with the RMF. As Data Governance continues to mature, the relevance of find/delete/protect will diminish.
2 - Enable and support a culture that values information security and works to reduce risk to a level where the remaining potential consequences are acceptable to management of the local unit and University leadership.	Year one saw a significant and positive change in UW-Madison culture related to the value of information security. While trying to avoid the negative connotations of the term "Culture of Compliance", campus leaders and practitioners are working to reduce, avoid or transfer cybersecurity risk – becoming more of a habit than a requirement.
3 - Establish Restricted Data Environments based on the needs of Faculty, Researchers or IT project requirement documents.	Using the successes of the Purchase Card Industry Data Security Standard efforts over the last five years, progress has been made with success stories pushing UW-Madison toward understanding how to establish the data environments that are appropriate. More work is needed to ensure this objective remains relevant and evolves as success is achieved.
4 - Centralize data collection and aggregation for analysis of security related events to promote unified measurement of cybersecurity attributes.	Establishing ATP and ATA with their associated tools will significant enhance this enabling objective.

Enabling Objective	Status
5 - Identify and seek sources of repeatable funding to enable accomplishment of technical or staffing related strategic goals.	This objective has been met with limited success with the Spring 2016 Wisconsin Alumni Research Foundation gift. More work remains to establish service charge-back rates and methods to gain advantage from that potential revenue source.
6 - Requirements are imposed upon UW-Madison by other agencies. Identify UW-Madison compliance (FERPA, HIPAA, PCI-DSS, Red Flags Rule, etc.) and then map the IT security	Establishing relationships with Institutional Research Boards, Research and Sponsored Programs, research centers and researchers aligned with the Vice Chancellor for Research and Graduate Education and the School of Medicine and Public Health is essential for success enabled by this objective. Increase in interest with research teams calling the Office of Cybersecurity as projects renew is encouraging.
7 - Develop and refine procedures to ensure security operations and risk assessments are conducted in a sustainable manner that ensures standards for timeliness and measurable response are achieved and maintained.	The development of RMF and Security Testing protocols in Year One place this objective on track to increase the success stories in Year Two and beyond.
8 - Develop and implement a marketing and communications plan.	This enabling objective yielded significant success in achieving the strategy in Year One. Updates to the IT web presence and establishing liaison within DoIT Communications has been the key to this enabler.

Appendix I: Cybersecurity Strategy – Year Two Progress Report

July 10, 2017

To: Michael Lehman, Interim Vice Provost for Information Technology and Chief Information Officer

From: Bob Turner, Chief Information Security Officer

Re: **UW-Madison Cybersecurity Strategic Plan for 2015 – 2019; Year Two Update**

The enclosed report is passed for your information and to provide a status of accomplishment for the goals aligned with the seven Cybersecurity Strategic Elements with actions completed between July 2016 and June 2017.

With your concurrence, I will add this report as an appendix to the current strategy document and publish an updated document to the Office of Cybersecurity web site.

Executive Summary:

Year Two surpassed expectations and marks the successful retirement of two of seven strategic elements. We declare Strategy #1 - Complete Data Governance and Information Classification Plan as accomplished and will continue to support the Chief Data Officer and Data Governance program with completing the Restricted Administrative Data Authorization Policy and any follow-on work to ensure the security of information and data remains a prominent part of the Cybersecurity Program. Strategy #2 - Establish the UW-Madison Risk Management Framework to Reduce Cybersecurity Risk has been accomplished as the Risk Management Framework (RMF) components, processes and templates have been created and used in the analysis of over 25 university systems and networks. The Cybersecurity Risk Management Policy is waiting review and approval by the University Committee in the Fall Term of 2017. The effort to define and implement the Continuous Diagnostics and Mitigation program will be cast as a new strategic element.

The second year also brought continued improvement in awareness and engagement from the UW-Madison information security community. The most significant is completion of the Cybersecurity Risk Management Policy and its passage through the new IT Governance structure up to the University Committee. The evolution in IT Governance was a great opportunity for the Office of Cybersecurity to be seen by a larger community of faculty and researchers. An example is bringing the Cybersecurity Operations Center (CSOC) on line with new tools and enhanced collaboration. Continued discussions and negotiation of a Memorandum of Understanding with the iSchool (former School of Library and Information Studies) aligns the Office of Cybersecurity in an advisory role for development of cyber related degree and certificate programs.

A summary of the significant accomplishments and additional detail is provided in Enclosure (1).

Next Steps in the Cybersecurity Strategy Life Cycle

Included in this report are recommended adjustments to the strategy and goals which will be used in developing a revised Cybersecurity Strategic Plan for 2018 – 2023. This effort will be initiated August 2017 with a goal of completing the strategy update to present through IT Governance and to the new Chief Information Officer as early as April 2017 for review and approval by July 1, 2018.

Enclosure: (1) Status of Cybersecurity Strategic Goals

Enclosure (1) – Status of Cybersecurity Strategic Goals

The following tables provide a status summary of the original strategic elements and goals. The last table provides a status of each enabling objective.

Original and Added Strategic Elements and Goals

Strategy	Associated Goals
Strategy 1: Complete Data Governance and Information Classification Plan	1 – **(Completed in Year One)** Form data stewards group; create data classification system and process
	2 – Validate compliance with restricted data management policy using UW-MIST
	3 – **(New in Year Two)** Assist Chief Data Officer with Restricted Administrative Data Authorization Policy consistent with the Risk Management Framework
Strategy 2: Establish the UW-Madison Risk Management Framework to reduce cybersecurity risk	1 – **(Completed in Year One)** Achieve agreement with UW System on business rules for adopting NIST Risk Management Framework
	2 – Present staffing needs to complete a new risk assessment to replace the Campus IT Security Baseline
	3 – Define and present the Organizational Parameters of the NIST 800-53 Security Controls and mapping to the IT Security Baseline
	4 – Develop implementation Plan for conducting assessments using the Risk UW-Madison Management Framework
	5 - **(New in Year Two)** Assist the Chief Data Officer, Data Stewards Council and Data Governance Steering Committee with the Restricted Administrative Data Authorization policy & procedures. Ensure that the policy is consistent with anticipated implementation of the Risk Management Framework.
Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness	1 – Define group specific security awareness programs for IT and security staff, students, administrators, and faculty/researchers
	2 – Develop website to provide a place for campus community to visit and view helpful information and initiatives
	3 – **(Completed in Year One)** Raise security awareness through active Phishing campaigns
	4 – Work though UW-MIST to identify and develop training and awareness for new or returning employees
	5 - **(New in Year Two)** Develop campus policy requiring participation in SETA.
	6 - **(New in Year Two)** Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the Big Ten Academic Alliance's (formerly the Committee on Institutional Cooperation)

	Security Working Group
Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services	1 – Define criteria needed to describe a security operation or service. A governance structure should be established to provide oversight of common solutions
	2 – Survey security operations and services to define a common service delivery model. Identify metrics and reports that support decision making efforts
	3 – Using current service models, identify common "best practice" approaches and gaps or redundancies to determine existing business processes and services worthy of distribution across the UW System campuses
	4 – Capture the cost of security operations and examine effectiveness to identify resources necessary for aa Future State Cost Model for ongoing operations
	5 – Determine efficiencies and identify tool sets to automate available services for UW-Madison and UW System in preparation for submitting the FY-18 budget
Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination, and Remediation	1 – Implement a dashboard to display current alerts, intrusion detection events, and information on severity and quantity of events
	2 – Increase number of external data feeds to detect suspicious activity beyond current sources. Place at least three additional feeds including one U/.S. Government source
	3 – Implement or improve a system to collect and periodically confirm security contact information by network assignment
	4 – Implement or improve a notification and tracking system for alerting and metric collection
	5 – **(Completed in Year One)** Identify and collaborate with a campus partner on the implementation of a new security control that will act on collected network intelligence, e.g. "network block list"
Strategy 6: Establish Security Metrics, Optimize Services, Promote Compliance, Achieve Continuous Diagnostics and Mitigation	1 – Identify and create a budget model for each service managed by each Cybersecurity Domain Team that aligns with the existing budget revenue and expense models
	2 – Map each existing campus IT Policy to an existing people, process, technology (PPT) that assists with compliance
	3 – Establish a process for the Cybersecurity Service Leads and corresponding Domain Lead to determine Total Cost of Ownership for each service with measurable attributes
	4 – Identify the type of metrics to be collected and maintained to ensure success of Goal #1 and #2

	5 – Establish the framework for CDM using existing tools while determining requirements and acquisition strategy for a tool or suite of tools
Strategy 7: Establish Collaborative Partnerships to assure teaching and research computing resources and results are available to fulfill the Wisconsin Idea and return value to the state and its citizens	1 – **(Completed in Year One)** Work toward developing a standard model to assess and display operational status and cybersecurity posture. This will enhance the understanding of each system or networks availability and status of vulnerability management leading toward full evaluation of risk.
	2 – Establish a cybersecurity governance arrangement that addresses the needs of Research Computing environments, special projects and laboratories required to meet Federal guidelines

Current Status of Strategic Elements and Goals

Strategy Status	Action Taken on Associated Goals
Strategy 1: Complete Data Governance and Information Classification Plan **Strategy Met – Action Complete!**	1 – **(Completed in Year One)** Form data stewards group; create data classification system and process
	2 – **(Completed in Year Two)** Validated compliance with restricted data management policies using UW-MIST. A new Enabling Objective will be established for ongoing management and focus on this component of Data Governance.
	3 – (**Completed in Year Two)** The Office of Cybersecurity provided assistance to the CDO by reviewing draft documents and making suggestions. The policy was presented to the ITC on Oct 21, 2016. The ITC requested more time for discussion. The documents were referred back the Data Stewardship Council for more elaboration on layout/workflow, where to get access, and the definition of restricted data.
Strategy 2: Establish the UW-Madison Risk Management Framework to reduce cybersecurity risk **Strategy Met – Action Complete!**	1 – **(Completed in Year One)** Achieved agreement with UW System on business rules for adopting NIST Risk Management Framework. Codified in UW System Information Security Guidelines published in Fall of 2016.
	2 – **(Completed in Year Two)** Presented staffing needs as part of the FY18/19 budget process and also for management of the second installation of Advanced Threat Protection tools. While the six positions requested were not funded, the requirement is clearly established with IT and University Leadership. Continued refinement and subsequent budget discussions will highlight the staffing needed
	3 – **(Completed in Year Two)** The GRC team created a Risk Analysis Tool to support the Risk Management Framework Step-2 Select Security Controls and Step-4 Assess Risk. This tool is based on NIST 800-53. By January 2018 the GRC team will assess if this tool or part of this tool can be established as the campus security baseline.
	4 – **(Completed in Year Two)** As part of the Cybersecurity Risk Management Policy, development of an Implementation Plan for conducting assessments using the Risk UW-Madison Management Framework was completed. The Risk

	Management Framework (RMF) has been implemented to categorize an information system based on the classification of the data in conjunction with the availability and stability of the system. The Risk Analysis Tool will be used to create a matrix of which controls should be in place for each data classification. The CISO will engage the Chief Data Officer to validate control sets with the UW-Madison Data Governance Program.
	5 - **(Completed in Year Two)** Assisted the Chief Data Officer, Data Stewards Council and Data Governance Steering Committee with the Restricted Administrative Data Authorization policy & procedures. Continued development of the plan calls for additional tasking to ensure the approved policy is consistent with implementation of the Risk Management Framework.
Strategy 3: Build a community of experts and improve institutional user competence though Security Education, Training, and Awareness	1 – **(Significant Progress in Year Two)** Define group specific security awareness programs for IT and security staff, students, administrators, and faculty/researchers
	2 – **(Significant Progress in Year One and Two)** During the latter half of Year One, DoIT Communications led the effort to overhaul the CIO related websites to make information more accessible to the customer. Office of Cybersecurity web pages are now in the common format and have been developed or refined to provide a place for campus community to visit and view helpful cybersecurity related information and initiatives. Progress toward this goal included the development and implementation of the ATP Pilot Communications for Monitoring and IR services related to the purchase of the Palo Alto Tools.
	3 – **(Completed in Year One)** Raise security awareness through active Phishing campaigns
	4 – Work though UW-MIST to identify and develop training and awareness for new or returning employees
	5 - **(New in Year Two)** Develop campus policy requiring participation in SETA.
	6 - **(New in Year Two)** Develop list of Continuing Professional Education opportunities using open source materials and in collaboration with the Big Ten Academic Alliance's (formerly the Committee on Institutional Cooperation) Security Working Group
Strategy 4: Consolidate Security Operations and institute best practices for UW-Madison Campus Networks and UW System Common Services	1 – Define criteria needed to describe a security operation or service. A governance structure should be established to provide oversight of common solutions
	2 – **(Completed in Year One)** In 2016 the Deputy CISO drafted a service catalog associated with each Office of Cybersecurity Domain. The catalog has been used as the DoIT Budget narrative as well as to inventory the services provided to campus by DoIT and the Office of the CIO. This goal should be revised and expanded to include review of service alignment and success factors with our peer, partners, customers and stakeholders.

	3 – Using current service models, identify common "best practice" approaches and gaps or redundancies to determine existing business processes and services worthy of distribution across the UW System campuses
	4 – **(Significant Progress in Year Two)** The Office of Cybersecurity has been split into five cost centers that represent the operational activities associated with the CISO and each of the four domains. Tracking revenue and expenses in this model has identified potential areas of service improvement and to better forecast budget planning and resource allocation extending to other DoIT Service Teams as well as to identify short and long term labor requirements.
	5 – Determine efficiencies and identify tool sets to automate available services for UW-Madison and UW System in preparation for submitting the FY-18 budget
Strategy 5: Improve Cyber Threat Intelligence Analysis, Dissemination, and Remediation	1 – **(Significant Progress in Year Two)** The Cybersecurity Operations team deployed the Advanced Malware Protection (AMP) software agent to over 5,000 campus end points. This software provides the individual units with a dashboard of alerts and control of their devices while allowing the Cybersecurity team security visibility of all of the end points.
	2 – **(Significant Progress in Year Two)** The Monitoring and Incident Response team implemented a Collective Intelligence Framework (CIF) server to collect threat intelligence data. Currently, the server is configured with a data feed from REN-ISAC. In the near future, it is anticipated that we will be able to share information with BTAA members. Our goal is to arrange for a Government feed source by July 1, 2018.
	3 – **(Significant Progress in Year Two)** The Cybersecurity Operations Center team made progress by collecting system administrator contact information connected to web servers in support of our campus SSL scans. The goal is to identify and begin to populate a more complete security contact system (including the potential to leverage existing systems such as (WiscIT-Cherwell or InfoBlox) by July 1, 2018.
	4 – Implement or improve a notification and tracking system for alerting and metric collection **(Year Two Progress)** The Cybersecurity team anticipates migrating to WiscIT for the CSOC ticketing system early in the Fall 2017 and will leverage its features for alerting and metrics tracking.
	5 – **(Partially completed in Year One)** Identify and collaborate with a campus partner on the implementation of a new security control that will act on collected network intelligence, e.g. "network block list" **(Year Two Progress)** The Cybersecurity team collaborated with over 25 campus units with the pilot deployment of three Advanced Threat Protection tools, e.g. Palo Alto Next Generation Firewall, Palo Alto Traps and Cisco Advanced Malware Protection agents.
Strategy 6: Establish Security Metrics, Optimize Services, Promote	1 – **(Significant Progress in Year Two)** The Cybersecurity budget has been divided into five cost centers to track and evaluate the services aligned with each of the four domains and the overall responsibilities of the CISO. A

Compliance, Achieve Continuous Diagnostics and Mitigatio	process to continually review performance against the cost centers has been development and is pending review and approval by the CISO. **(Remaining Work)** As part of Goal #3, FY17 cost and spend data will be reviewed and compared during FY18 to determine Total Cost of Ownership for each service with measurable attributes
	2 – **(Completed in Year Two)** The IT Policy Office completed a Policy Infrastructure Map in August 2016. The infrastructure supporting each policy implies the People, Process and Technology (PPT) applicable to each policy. • *People build, maintain, administer, and use the infrastructure. The people vary over time.* • *Process is built around those activities. The processes are documented, readily apparent, or discoverable as needed. Ease of use varies.* • *The infrastructure directly implements or supports the technology. The technology varies relatively slowly over time. In some cases the infrastructure consists of the policy and process documentation, with no specific hardware or software involved.* The document also includes an assessment of how practical it is for units and individuals to comply, and how SETA could contribute to improving compliance. This is a working document, attached to this email.
	3 – Establish a process for the Cybersecurity Service Leads and corresponding Domain Lead to determine Total Cost of Ownership for each service with measurable attributes **(Status)** As noted in Goal #1, activity related to this goal is pending further action by the CISO, Deputy CISO, and the Assistant Director of Security Operations.
	4 – Identify the type of metrics to be collected and maintained to ensure success of Goal #1 and #2
	5 – Establish the framework for CDM using existing tools while determining requirements and acquisition strategy for a tool or suite of tools
Strategy 7: Establish Collaborative Partnerships to assure teaching and research computing resources and results are available to fulfill the Wisconsin Idea and return value to the state and its citizens	1 – **(Completed in Year One)** Refined a Weekly Cybersecurity Summary Report showing the status of daily and weekly issues along with operational status of investigations and cybersecurity posture. The report was expanded in Year Two to include a status of each Cybersecurity Domain and administrative functions of the office. Inclusion of additional Advanced Threat Protection metrics and status pf packages being processed under the RMF were added in Tear Two. Audiences for internal and external version of the report were also refined to include UW MIST and the UW System Technical Information Security Committee.
	2 – **(Completed in Year Two)** As part of the new IT Governance structure the Office of Cybersecurity established relationships with the four Advisory Groups which included the Research Technical Advisory Group that manages and provides advice toe the IT Steering Committee on research related computing environments, special projects and laboratories required to meet Federal guidelines

Status of Enabling Objectives

Enabling Objective	Status
1 - Consider retention of previous strategy's actionable items ("find it," "delete it," and "protect it").	This will remain an ongoing concern and will be defined in the Office of Cybersecurity Guiding Principles. The next strategy revision will include a suitable enabling objective for maintaining effective cyber hygiene that is data centric.
2 - Enable and support a culture that values information security and works to reduce risk to a level where the remaining potential consequences are acceptable to management of the local unit and University leadership.	**This will remain an ongoing objective.** Year one saw a significant and positive change in UW-Madison culture related to the value of information security. While trying to avoid the negative connotations of the term "Culture of Compliance", campus leaders and practitioners are working to reduce, avoid or transfer cybersecurity risk – becoming more of a habit than a requirement. Year Two saw the introduction of the concept of the Risk Executive. This position will determine the level when the remaining potential consequences are acceptable to management of the local unit and the university leadership.
3 - Establish Restricted Data Environments based on the needs of Faculty, Researchers or IT project requirement documents.	**This will remain an ongoing objective.** During Year Two the GRC domain developed, secured funding and began to operate the HIPAA Risk Analysis Program. This program is based on the Risk Management Framework. The output of each of the three phases of the three-year program will provide the HIPAA Privacy and Security Executive Board with the level of risk relating to HIPAA security compliance and a plan of action and milestones to reduce risk to acceptable levels for each of the Health Care Components and other UW-Madison departments managing ePHI. The GRC Domain also participated in UW-Madison efforts to establish processes and controls to address federal research grant requirements for Controlled Unclassified Information (CUI). Working with campus partners, DoIT technologists and cybersecurity risk analysts from other Big Ten Academic Alliance (BTAA) campus, we have developed a tool to assess systems for CUI compliance.
4 - Centralize data collection and aggregation for analysis of security related events to promote unified measurement of cybersecurity attributes.	**This will remain an ongoing objective.** Continuing ATP and ATA deployment with their associated tools are significantly enhancing this enabling objective. In Year Two the establishment and continued development of the CSOC playbook to include additional plays that will be possible with increased deployment of ATP services, e.g. Palo Alto Next Generation Firewall, Palo Alto VPN and Cisco AMP.
5 - Identify and seek sources of repeatable funding to enable accomplishment of technical or staffing related strategic goals.	**This will remain an ongoing objective.** During Year Two the Office of Cybersecurity received additional funding from UW System Administration Shared Financials leadership to staff an additional SFS security analyst to focus primarily on the 18-month Oracle 9.2 upgrade process. This will be the first time there are two SFS security analysts assigned and funded to focus on the SFS Security Program. In May 2017 Cybersecurity received additional funding to complete the purchase of the Palo Alto Next Generation Firewalls and supporting software. This included repeatable funding for license renewal and an Enterprise Agreement that extends to the entire UW System.
6 - Requirements are imposed upon UW-Madison	**This will remain an ongoing objective with modified language as proposed.** During Year Two the Office of Cybersecurity has worked with the Office of

by other agencies. Identify UW-Madison compliance (FERPA, HIPAA, PCI-DSS, Red Flags Rule, etc.) and then map the IT security **Proposed New Language:** **Identify UW-Madison compliance (FERPA, HIPAA, PCI-DSS, etc.) requirements that are imposed upon UW-Madison by other agencies and then map the requirements to IT security components for applicable campus units.**	Compliance to continue building the program and began processing the Health Care Component members through the HIPAA Risk Analysis Program. This includes evaluating reports from the Office for Civil Rights regarding trending security concerns such as ransomware. We have worked to align campus with federal grant requirements for Controlled Unclassified Information. The controls for PCI-DSS have been reviewed and updated during the process of relocating the PCI-CAT infrastructure from an off-premise solution to an on premise solution. Remaining to be addressed are work to establish and refine relationships with Institutional Research Boards, Research and Sponsored Programs, research centers and researchers aligned with the Vice Chancellor for Research and Graduate Education and the School of Medicine and Public Health. Continued increase in interest with research teams calling the Office of Cybersecurity as projects renew is encouraging.
7 - Develop and refine procedures to ensure security operations and risk assessments are conducted in a sustainable manner that ensures standards for timeliness and measurable response are achieved and maintained.	**This will remain an ongoing objective.** The development of RMF and Security Testing protocols in Year One placed this objective on track to increase the success stories in Year Two and beyond. In Year Two, through the HRS 9.2 upgrade the Enterprise System Security (ESS) team worked with consultants and the UW System HRS Service Center to formalize the processes for the intake, prioritization, and processes of issues and change requests. This effort provided improved communications with timely information to our customers concerning the teams focus and expectations for completing work. Similar efforts occurred with our partners supporting the Shared Financials System.
8 - Develop and implement a marketing and communications plan.	**This will remain an ongoing objective.** This enabling objective yielded significant success in achieving the strategy in Year One. Updates to the IT web presence and establishing liaison within DoIT Communications has been the key to this enabler. In Year Two, improvements that include making communications as well as training, awareness, and education was an important component. Adding dedicated funding for the DoIT Communications Manager greatly extends this objective.
(NEW OBJECTIVE FOR NEXT REVISION) **9 – Identify and maintain repeatable funding modules that ensure efficiencies and automation of stable cybersecurity services for UW-Madison and UW System.**	Track costs associated with the delivery of each service, the usage of the service, and the impact of the service to reducing risk to the university. This data will be used as supporting information through the various budget request cycles. The Deputy CISO and the Assistant Director of Cybersecurity Operations will be responsible ensuring alignment with this enabling objective.