Information Technology Security Strategy

Executive Summary

The general proposed strategy is to optimize risk management for information security incrementally and over time. Ultimately, campus will operate with reduced risk before an incident occurs and at all times thereafter (see appendix A). Threats will continue to change and become more complex. Therefore, we are required to continuously improve the level of our Internal Controls Maturity (see appendix B). This implies that security will be a process rather than project.

Achievement of the goal, optimized risk management, requires a multi-faceted approach. The program outlined below provides effective practices, is supported with automated real-time monitoring for accountability and decision metrics for current risk estimation. Employees are proactively involved with continuous improvements. The university will be able to benchmark to external best practices and seek external advice on effectiveness. For critical processes and systems, independent reviews need to take place to provide assurance that the controls are at the desired level of maturity and working as planned.

To accomplish the goal, we need a *motivating factor for change* and a series of *near term objectives* that roll up into the larger strategy over time. Our efforts should be focused on preventing losses of restricted data, followed by refining the processes and procedures for our intellectual property and other sensitive information.

The long term strategy is presented in three parts. Each part is intended to operate in parallel with the other two.

Strategy 1: Establish Governance and Information Classification
Strategy 2: Enriching People though Consulting, Awareness, and Training
Strategy 3: Optimize Services, Measurement and Compliance Assistance

The near term operational objectives presented below are incorporated into our three strategies. They are modeled on the successful implementation of the PCI Compliance Assistance Team's approach to campus PCI compliance. The PCI Compliance Assistance Team utilizes a governance process, technical expertise, and a collaborative IT service model to meet the requirements for compliance (see Appendix E). The PCI Compliance Assistance Team's governance and implementation model is being utilized for the VC for Administration restricted data remediation protocol (see Appendix F). Working with the academic and administrative units to develop a common understanding for how to secure and manage personally identifiable data will provide a framework that can be leveraged across campus. Measuring the status of our environment and comparing it to industry standards will provide valuable information for governance. This process will achieve the long term Internal Controls Maturity in an incremental and actionable fashion.

Objective 1: Central data collection and aggregation for analysis resulting in a unified measurement of the Maturity of Internal Controls.
Objective 2: *Completion of UW Madison PCI compliance project and the application of the successful UW PCI model to the VC for Administration Restricted Data Remediation project*
Objective 3: Use the central measurements to elucidate the next UW Madison campus unit most appropriate for the expansion of the successful Restricted Data remediation project.

Security Strategies

Strategy 1: Establish Governance and Information Classification
Strategy 2: Enriching People though Consulting, Awareness, and Training
Strategy 3: Optimize Services, Measurement and Compliance Assistance

Strategy 1: Establish Governance and Information Classification

Data is an essential currency of the UW-Madison. Real-time, high quality data helps us to use modern intelligence to manage the institution. The "data" of data governance spans the authoritative sources for UW student information, as well as, both research data, and intellectual property. Data governance requires a clear structure for oversight, which is assumed by "Governance," as well as a responsible steward who manages the integrity of the data, control over access, and security. There is a need for clear governance and accountability around a data stewardship policy as well as consistent training around all aspects of data management and retrieval on campus.

Successful achievement of our goals revolves around having campus wide procedures for capturing, classifying, labeling, retrieving and managing all of the various types of data; research, institutional, and academic. Appendix C contains the questions that governance groups should consider as well as some metrics they may find useful. We imagine a commonly understood definition of what *secure environments* and *acceptable risks* mean for institutional data.

Strategy 2: Enriching People though Consulting, Awareness, and Training

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked environments without ensuring that each person involved understands their roles and responsibilities. The key to addressing people factors is awareness, training, and education. Faculty, staff and students in any higher education institution need to receive appropriate awareness training and regular updates in an effort to safeguard the information entrusted to them.

Successful implementation of this strategy includes working together to promote a collaborative and common understanding of governance, risk, processes, roles and responsibilities. This includes consulting with departments to help them understand the risks and requirements for safeguarding information, training for IT professionals to utilize security tools, processes and techniques, new and ongoing employee IT security orientation, awareness of responsibilities for personally identifiable information, and reminding members of the community regarding copyright obligations.

Strategy 3: Optimize Services, Measurement and Compliance Assistance

Tools and technical controls are required to achieve compliance on the scale posed at the University of Wisconsin – Madison. Automation is required for the long term operations and continual reduction of threats. Common tools are Anti-virus/anti-malware/anti-spyware, firewalls, cryptographic tools, Virtual Private Networks, endpoint management - configuration and patch management, data location and sanitization, file integrity tools, and others. Risk estimation can be enhanced through situational awareness and the measurement of effective deployed services. A greater understanding of risk at any point in time is achieved through the use of services such as vulnerability management, security event management, intrusion detection, patch management, forensics, incident response and others. Compliance assistance through site visits can be achieved through collaborative IT service models such as the Payment Card Industry model already developed on campus.

These three Security Strategies link directly to the campus and IT strategic plans.

- Campus Strategic Priority F - Be responsible stewards of our resources
- IT Strategic plan: A Roadmap to Service Excellence (Charter 8.3) – Core Campus Infrastructure - Security Rethinking Information Technology for a Sustainable Future – Priority for MTAG, ITC High Impact Recommendation for Strategic Investment Five – Develop sustainable data stewardship policies, ensure appropriate governance and invest in security services for the campus

Operational Objectives / Near-Term Plans

As a foundation for successful achievement of our long term strategy, we propose three near term objectives:

1. In response to recent security events, create the ability to centrally measure compliance with generally accepted best practices and the Electronic *Devices Connected to the Network* policy. All endpoint devices on the campus:
    a. are behind a registered network firewall and any exceptions are reviewed and granted annually; the network firewall is centrally monitored for suspicious activity; and the network firewall rules are reviewed annually;
    b. are regularly patched; windows devices run the Secunia Corporate Software Inspector (CSI) and centrally report results;
    c. install and run antivirus software and centrally report the results; and
    d. run Identity Finder and report results centrally.
    e. The centrally reported results will be leveraged to develop a dashboard that shows participating departments and risks. This dashboard will be shared with campus leadership and governance to drive informed decisions for continual risk optimization with existing policies and generally accepted best practices. Over time, we will grow our Internal Controls Maturity (appendix B).
2. Complete Payment Card Industry Compliance Project & Implement the VC for Administration Restricted Data remediation protocol for administrative departments. The PCI-CAT model (appendix E) has been used to create the VC for administration restricted data remediation protocol (Appendix F). Working with the administrative units to develop a common understanding for how to secure and manage personally identifiable data will provide a framework that can be leveraged across campus. Measuring the status of our environment and comparing it to industry standards will provide decision information for governance.
    - Use the lessons learned from the PCI project to apply to restricted data environments
    - Develop a baseline minimum desktop configuration standard leveraging results from current endpoint pilots in Veterinary Medicine and College of Agriculture and Life Sciences.
    - Identify and eliminate restricted data or to ensure that it is being used and stored in a secure manner
    - Develop a secured environment similar to that currently used for securing credit card information
    - Regularly review the progress of these projects with the governance team – the governance team will need to establish motivating factors for change (i.e. carrot and stick)
    - Leverage the governance model, technical expertise and IT services of these projects to expand to other departments in future years
3. Work with governance, apply metrics, and lessons learned to determine the most appropriate expansion of the restricted data remediation project.

Actionable items ("find it", "delete it", and "protect it")

The near term task is to 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, establish governance (awareness, responsibility and accountability) and begin data classification.[1]
- Move all restricted data to a centrally managed and monitored location segregated from other data with well controlled inbound and outbound access controls.[2]
- 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.

1 Sensitive but unrestricted data while important will not be the focus of our security strategy. Once classified as sensitive, identified data owners/custodians will be accountable for protecting this data well as restricted data. We will consult on how to protect this data and provide direction to other IT resources, but our priority will be restricted data.

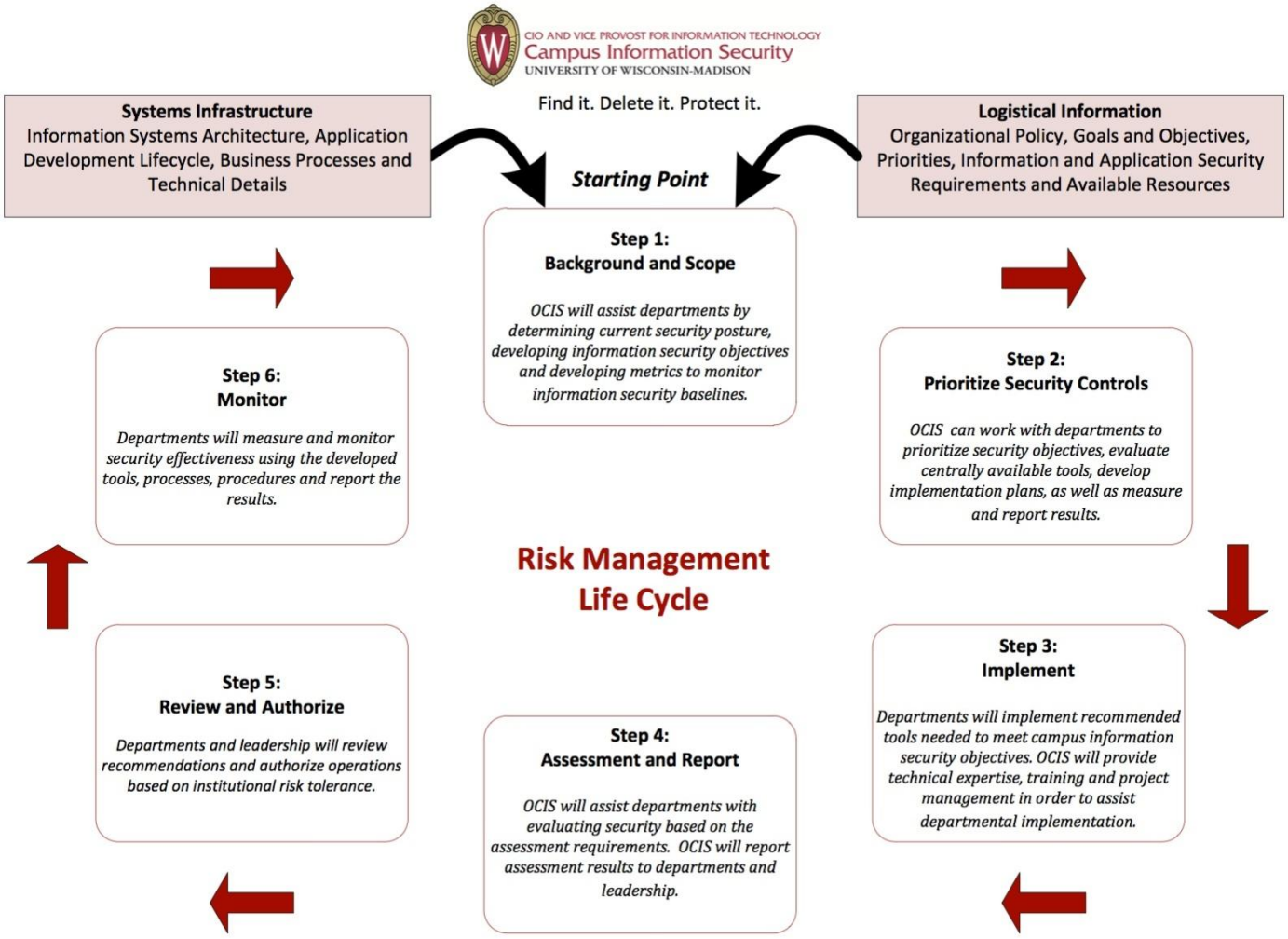
[2] Central security services will be used to manage and monitor restricted data. We will deploy security tools to protect the restricted data and consult with IT administrators to help deploy these tools for sensitive or internal data.

Appendix A: Risk Realization

Risk, can be expressed in mathematical terms as:

Risk = Impact * Likelihood (realized threat) / mitigating controls

Through planning, appropriate mitigation controls can be put in place to reduce the likelihood of realizing a risk as well as reduction of the impact of a realized risk. FISMA/NIST outlines security as a process to manage risk through the reduction of both likelihood and impact.



Overview (a.k.a. - "environmental scan") of IT security at UW-Madison
The Overview *and Environmental Scan* provides real-world context demonstrating how IT security risk affects your department's reputation, a PI's reputation and finances within your operations. Budgets can be reduced by unplanned remediation costs, legal fees, banking fines and permanent data loss.

- **Threat overview**
  - International research community being targeted – February 2011

- Malware (botnets, virus, data stealing software, etc.) volume doubled in 2010 – a new threat appears on average every 0.9 seconds
- Targeted attacks on institutional online banking – January 2010
- The campus is scanned more than 10,000 times daily from different locations in just China alone
- Of the 1466 computers we are currently monitoring, 66% have vulnerabilities with known exploits in the wild, 94% have vulnerabilities but there are no known exploits and 31% have vulnerabilities that would require user interaction to allow system compromise.
- State employees are making 3% less than 2009 in 2010 and are make an average of 8% less in 2011
- The new frontier for hacking is applications and databases – needs stats
- Laptop or other device theft and loss is on the rise – need stats

Restricted data is name and

- Social security numbers
- driver's license number or state identification number
- financial account number (including credit/debit card) or any security code, access code or password that would permit access to an individual's financial account
- deoxyribonucleic acid profile, as defined in S. 939.74(2d)(a)
- unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- protected health information

- **Governance Environment (Impact)**
  - Data stewards do not know how much restricted data people have access to [IA report]
  - Data stewards do not have controls to manage the distribution of restricted data
  - Restricted data is handled by an unknown number of people
  - Developers and sensitive information handlers have an unknown level of training
  - Restricted data is sent off campus to an unknown number of locations with unknown terms/risks
  - Restricted data is in an unknown number of locations with unknown controls
  - There are an unknown number of Databases and applications that contain restricted information
  - Databases and applications that are used to manage our restricted information are not regularly tested for vulnerabilities
  - Our intellectual property is not identified and the locations are unknown
- **Campus realized risk (vulnerabilities)**
  - In the last year we have had
    - 1 major incident that required notification
    - Several investigations in multiple units on campus didn't require notification but show significant deficiencies or errors
    - About 5 machines per day with suspicious network activity
    - costs of investigations alone for the incidents exceeds $40,000
    - Additional costs still to come for some incidents include introducing any mitigation controls so the incidents did not happen again.
  - Phishing, we remove access to about 10 people per week because we detect their NetID is compromised
  - Number of laptops lost in the last year – one is known to have restricted data and required notification.
- Loss through missed opportunities and underutilized resources:
  - In another case, the NIH would not release data unless the appropriate security controls could be put in place and documented – lack of internal controls maturity delayed the approval of data acquisition. During the delay, the research lab had losses: (1) an underutilized FTE and (2) missed getting the lead over other research institutions.
- The final example from UW: National Children's study at UW had to hire full time compliance manager just to become current with FISMA compliance to avoid loss of grant funding.

Appendix B Maturity Model for Internal Control

0 Non-existent	No recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/ad hoc	There is some recognition of the need for internal control. The approach to risk and control requirements is ad hoc and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an ad hoc basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.

5 Optimized	An enterprise wide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

Appendix C: Top information Security Concerns for Campus Executives and Data Stewards, Defined by EDUCAUSE

1. What/Where is my data? *What data are in my part of the organization and where are they located?*
    a. Do I know where paper records that contain sensitive data are located and used?
    b. Do I know where computers are located that store sensitive data?
    c. Do I know if sensitive data is stored on removable media and portable devices?
    d. Do I know the quantity of data?
    e. Is data stored on home computers or personally owned devices or personally managed devices?
    f. Do I know if a third party has access to or holds data from my organization?
2. How sensitive is it? *How sensitive is the data in my part of the organization?*
    a. Do I know what data my institution considers to be sensitive?
    b. What are the consequences if sensitive data gets into the wrong hands?
    c. What are the federal, state, contractual and institutional requirements for data under my responsibility?
    d. Do I know the legal and civil consequences of failing to protect the data or failing to follow the laws and policies regulating the data?
    e. Does my institution have a data privacy and security policy and do I know it is? Do I appropriately mitigate the risk level of data under my responsibility? Do I have a risk mitigation plan?
    f. What are the risks of outsourcing to a third-party data for which I am responsible?
3. Who's responsible for it? *Who's responsible for the security of information in my part of the organization?*
    a. Have I clearly outlined employee roles and responsibilities for securing information?
    b. Have I made information (training, policies, and procedures) available to employees so that they understand how to protect data?
    c. What is my role and responsibility for information in my part of the organization and how do I communicate that to employees?
    d. How do I ensure the data protection policies of my institution are being followed?
    e. Whom may I rely on for assistance outside of my part of the organization and how do I contact them?
        i. Chief Information Security Officer?
        ii. Chief Information Officer?
        iii. Internal Audit?
        iv. General Counsel?
        v. Privacy/Compliance/Risk Officer?
        vi. Chief Financial Officer?
        vii. Others?
4. Who has access to it?
    a. Do only those with a business need have access to the data?
    b. Are they authorized, documented and tracked?
    c. Are authorization records periodically audited?
    d. Do employee transition procedures (new employee, position changes, departure) include steps to update authorization records?
    e. Have I made information (training, policies, procedures) available to users so that they understand how to protect data?
    f. Do those with access to data know where to find information about how to protect it?
5. Do I need to keep it?
    a. How long is the institution required to keep each data type? Does my institution have a retention schedule?
    b. What are the benefits of keeping the data and do the benefits outweigh the costs and risks?
    c. Do I know the institutions procedures for secure disposal?
6. What if it gets into the wrong hands?
    a. Do I know how to recognize a data breach?
    b. Do I know what my institution's procedures are to address it?
    c. Do I know whom to notify in the event of data breach?

Appendix D: Office of Campus Information Security Role

OCIS facilitates the adoption of common policies, processes programs, tools and compliance with University, State and Federal regulations to ensure timely acquisition, analysis and publication of data, appropriate to a world class research institution such that UW continuously delivers World class IT, without the World class news headlines (for a breach), loss of information or loss of financial capital.

OCIS works with campus leadership and staff to ensure the risk to information entrusted to the university is optimized. OCIS efforts ensure that the successful / on-going growth of the university community – retention – recruitment – of the best, brightest, most diverse amalgamation of persons.

We:

- Lead the "Commoditization of information security" so researchers can focus on research, not the latest security issue.
- Benchmark / calculate risk for specific given situation; guide appropriate controls tailored to that situation.
- Create a common understanding for campus leadership and staff for items associated with the safeguarding of information:
    - risks
    - threats
    - and incidents
- Maintain Information dissemination for all information security across campus using the common understanding.
- Lead, coordinate and encourage the adoption of practices which increase our institution's Internal Controls Maturity:
    - Incident response, forensics, and copyright infringement
    - Security awareness and training.
    - Consultation for security risk management and Information compliance assistance, especially:
        - Campus Security Policies, Best Practices, Processes Data Inventory,
        - Technical Controls: Firewall, Intrusion Detection, Event Management, Vulnerability Management, Restricted Data
            - Endpoint security, including server & desktop OS, and other devices as appropriate: Encryption, Anti Virus, Network Access Control, File Integrity and related tools.
- Consult on and perform verification that implemented controls and mitigating factors are actually are functional.
- Ensure the big three of FIPS 140-199: Availability, Integrity, and Confidentiality.

Appendix E: UW-Madison Payment Card Industry Compliance Structure – June 2010

What is PCI compliance for a credit card accepting merchant? PCI compliance means that a merchant accepting credit or debit cards is operating in a way that protects the confidential information (card number, expiration date, name of cardholder and security code) from being released to anyone other than the acquirer of the transactions going into the credit card processing network. The standards are set by the PCI Standards Council established by the major card brands.

1. Computer applications used to accept and process credit cards must be certified to be PA-DSS compliant by the PCI Security Standards Council (certifications appear on their website with version numbers of computer applications of vendors which are deemed compliant).
2. The environment in which that application runs; people, hardware and networks must be deemed PCIDSS compliant as documented by completion of one of 4 Self-Assessment Questionnaires (A, B, C or D) published by the Standards Council.
3. The transaction acquirer (Elavon, a subsidiary of US Bank is the acquirer for 99% of our charge card business) reviews the situation and provides a 1-4 (bad to good) PCI ranking for the "merchant" (merchant can be a collection of merchant IDs). These rankings determine how frequently certain follow-up procedures are required, such as obtaining a report from a Qualified Security Assessor. If there is a data breach a merchant is moved immediately to level 1. Level 1 compliance requirements are costly.

In the event of a compromise, the credit card companies evaluate your compliance and levy fines until such time that you are compliant. Visa fines are $50k first compromise and go up, MasterCard $25k per day for each day of non compliance, American Express, $50k first occurrence of non-compliance, Discover $100k max per violation.

UW-Madison's governance strategy is outlined on the back side of this page. The model follows our normal accountability model of school/college/administrative unit's Dean or Director being the responsibility point for activities happening under their watch through their Divisional Business Representative. A campus-level PCI Compliance Assistance Team (PCICAT) is available to assist and if necessary enforce certain changes if a merchant is to be allowed to continue operations.

Here are some key parts of our operational plan:

1. Every one of our 250+ merchants will be required to fill out a self assessment questionnaire which will be maintained centrally and renewed periodically. We are currently in the process of developing a comprehensive inventory of our merchants, what they sell and how they operate.
2. We have hired a consultant to put our compliance plan together and help us negotiate our level of compliance with Elavon.
3. We are developing a PCI compliant server platform for use with applications which require a server to store or process card numbers. We are identifying a specific very secure band of the 21st Century Network which will be used to communicate between those servers and points of sale.
4. We have contracted with CashNet (now part of Higher One) to manage the card processing originating from our 100+ web storefronts. CashNet's service has been certified PCI compliant.
5. We will be developing standardized training for site managers and operators.

The most important thing any of you or your merchants can do is talk with PCI CAT before making changes in card handling processes, before getting into the credit card business, or to ask for a review of current procedures

UW-Madison PCI Compliance Project Structure	
Sponsors	Darrell Bazzell, Vice Chancellor for Administration Bruce Maas, Chief Information Officer
Middle Managers	Don Miner, Assistant Vice Chancellor for Business Services Jim Lowe, CISO, Office of Campus Information Security (OCIS) George Ketterer, Controller
Core Team	Sharon Hughes, Supervisor of Cash Management Mike Halton, Cash Management, Cashnet interface Janet Hamm, Cash Management, Elavon interface Jeff Savoy, OCIS Jeff Endres, OCIS Carl Hubbard, Purchasing Services Bert Schnell, Project Manager (DoIT)
Divisional Business Representative (DBR)	Responsible for all merchants in their division. Will sign the attestation for PCI compliance for their division.
Site Managers	Those who are responsible for one or more merchant ID numbers
Operators	Those who work within the site manager's unit and process credit card transactions

1. The Site Manager/operator concept is very similar to what we do to manager 2500 purchasing cards. Cardholders are the responsibility of site managers with the average manager handling 12 cards.
2. Our communication of policy and procedure is to the Divisional Business Manager and the site managers who communicate with their cardholders. Separate training is provided to site managers and to card holders.
3. The Divisional Business Rep is responsible for the site managers in their division (school, college, admin unit) and would be responsible for annual attestation of PCI Compliance.
4. The sponsors are generally accountable to the outside world for our compliance with PCI and provide the project with resources to help the site managers and operators comply. They also approve institutional policies.
5. The middle managers provide the central team with resources and enforcement assistance. They also create consensus on institutional policies.
6. The core team members work through the Divisional Business Representative directly with merchants and services providers. They should refer issues to the middle managers if they are having difficulty with any of the site managers or operators.

Appendix F: VCA Restricted Data Policy, Remediation and Scope

VCA Restricted Data Policy and Remediation Protocol Project Scope

The VCA Restricted Data Policy and Remediation Protocol security program will be comprised of the following three efforts: IT Security Practice Assessment, Restricted Data Remediation, and Restricted Data Storage. These efforts will be applied to the following VCA units: AIMS, Auxiliary Operations Analysis, Business Services, Facilities Planning & Management, Office of the VCA, Office of Human Resources, Madison Budget Office, Recreational Sports, University Health Services, University Housing, UW Police, and the Wisconsin Union.

IT Security Practice Assessment

The goal of the assessment is to ensure that all units are operating at a minimally acceptable security control level regardless of the data being handled. This goal will be achieved by doing the following:

- The security team will develop a comprehensive IT Security "Best Practices" Assessment checklist.
- The security Team will work with IT and business staff in each unit to:
    - Assess each unit using the checklist to identify gaps
    - Recommend mitigations for the gaps to the DBR that will bring the unit into compliance with the "Best Practices" checklist (includes ongoing monitoring for compliance)
    - Work with unit personal to develop a plan and time line to close the gaps

Restricted Data Remediation

The goal of restricted data remediation is to identify and eliminate restricted data or to ensure that it is being used and stored in a secure manner. To achieve this goal the security team will:

- Define a restricted data discovery and remediation protocol that will be applied to each VCA unit.
- Work with IT and business staff in each unit to customize and implement the protocol. The process will include:
    - Reviewing the restricted data with an assigned data manager
    - Eliminating when possible
    - Recommend changes to the Division DBR and Data Manager that will bring the use and storage of restricted data into compliance with the VCA Restricted Data Policy.
    - Work with unit personal to develop a plan and time line to implement any changes

Restricted Data Storage

The goal of the restricted data storage effort is to recommend a secured environment similar to that currently used for securing credit card information. To achieve this goal the security team will make recommendations regarding:

- What data, applications and desktops need to be moved into a secure environment.
- Budgeting for, architecting, building and operating the restricted data environment

Vice Chancellor for Administration
Restricted data Policy and Remediation Protocol
May 26, 2011

Policy: Know the level of risk and protect the data. Restricted data (see sidebar) must be protected to the degree that the credit card industry requires protection of credit card data. Other data protection must meet minimum security policies and guidelines. Division directors are responsible for the resources to store and maintain data that is kept.

Restricted data is name and

- Social security numbers
- driver's license number or state identification number
- financial account number (including credit/debit card) or any security code, access code or password that would permit access to an individual's financial account
- deoxyribonucleic acid profile, as defined in S. 939.74(2d)(a)
- unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- protected health information

Division directors under the VC are tasked with providing resources to:

I. Assess where restricted data located, delete it unless impossible, and protect it if kept. Keeping restricted data includes having the division director responsible for restricted data compliance.
II. Utilize OCIS and your IT support staff to assess state of IT security practices and establish a base line minimum acceptable state that meets or exceeds current campus policies for unrestricted data within each division.

Restricted Data Remediation

1. Directors assemble a team of business process and IT professionals within the division. The team must provide period reports on progress to the director, OCIS and internal audit.
2. The team will use identity finder software and other resources to locate restricted data though-out the divisional IT resources. Data that has no apparent business need will be deleted. Restricted data that is not deleted will require a chain of custody and be inventoried with a) location, b) number of unique elements, c) business need or purpose of system, and d) manager responsible for the data. Teams will prioritize structured databases over unstructured data and servers over endpoint devices.
3. The VC will sponsor OCIS to provide leadership, project management and training to divisional teams.
4. Directors will analyze the results of the inventory and recommend exception or purge-by-date. E.g. the test for an SSN exception is anything beyond “minimum number required to meet legal requirements for social security and income withholding & reporting, and eligibility for government programs”
5. Restricted data that is kept is secured to payment card industry data security standards.
6. Restricted data that does not pass the test for an exception and are kept require the VC approval.
7. An ongoing plan for continuous monitoring will follow initial assessment.

IT Security Practice Assessment

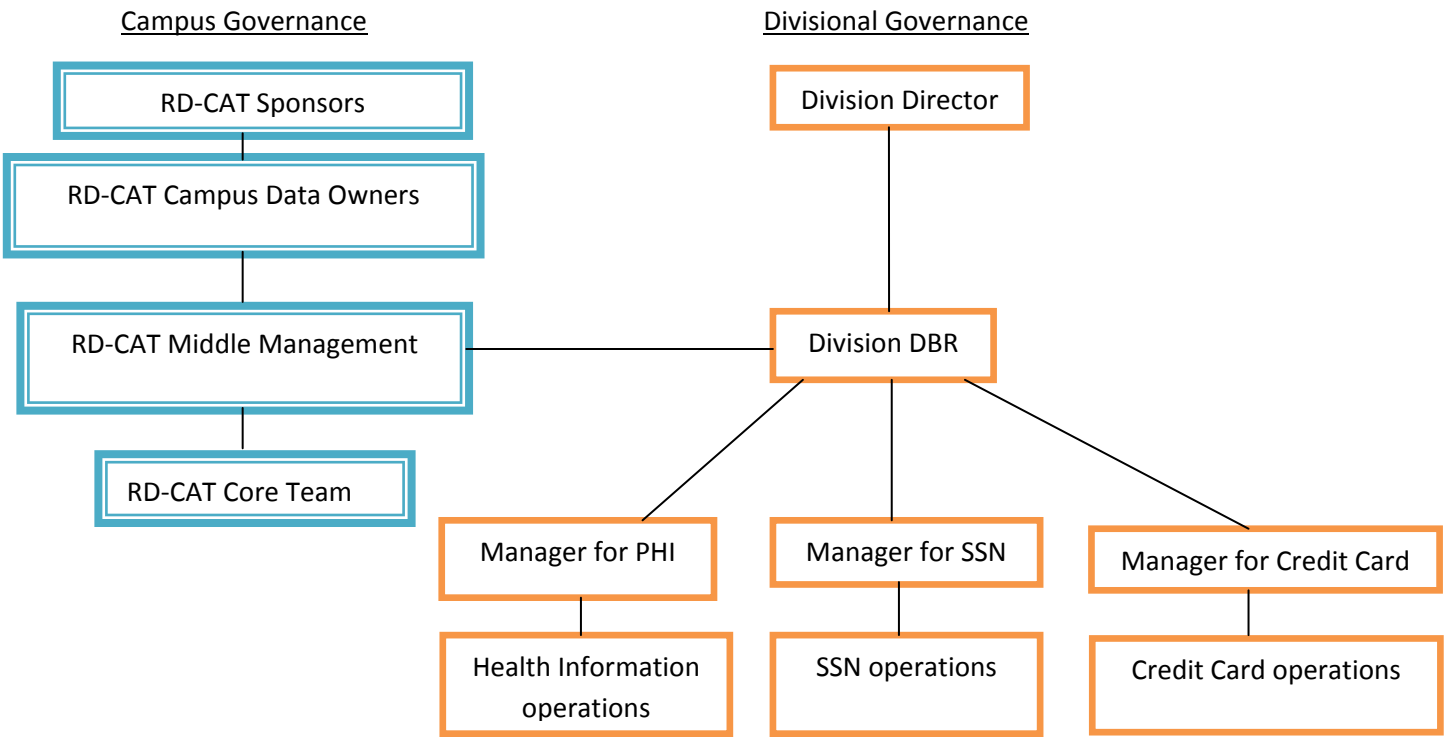
1. Directors assemble a team of IT professionals within their division and charge them to work with OCIS. Resources will be provided by directors, as needed, to complete the assessment.
2. The VC will sponsor OCIS who will coordinate the work with divisional IT personnel to assess the state of IT security practices. OCIS will make recommendations for improvements that will establish a base line minimum acceptable IT security state that meets or exceeds current campus policies. This includes but not limited to: a) Network and host based firewalls, b) Intrusion detection equipment & security event management, c) Identifying credential stores and

auditing passwords, d) identifying and auditing application best practices and d) Reviewing a sample of workstation and server configurations.

UW-Madison Restricted Data Compliance Assistance Team (RD-CAT) Governance Structure	
Sponsors	Darrell Bazzell, Vice Chancellor for Administration (VCA) Joanne Berg, Interim Chief Information Officer
VCA Restricted Data Owners SSN – Employee SSN – Student SSN – Vendor Drivers License Credit Cards Bank Account Number DNA, Bio metric, etc. Protected Health Info (PHI) Student	 Bob Lavigna, Director, Office of Human Resources Dan Edlebeck, Registrar, Enrollment Management Al Benzschawel, Controller, Business Services Don Miner, Assistant Vice Chancellor for Business Services Don Miner Bob Lavigna Sue Riseling, Associate Vice Chancellor, Police Department Sarah Van Orman, Director, University Health Services
Middle Management Campus Info Security Internal Audit Info Tech - AIMS	 Jim Lowe, CISO, Office of Campus Information Security (OCIS) Ed Ruotsinoja, Director, Internal Audit Bobby Burrow, Director, Admin Information Management Svcs
Core Team	Cory Chrisinger IA person(s) AIMS person(s) Project Manager
Divisional Business Representative (DBR)	Responsible for all restricted data in their division. Will sign the attestation for restricted data compliance for their division
Site Managers	Those who are responsible for one or more restricted data elements. There a person assigned to each Restricted Data type in the division
Operators	Those who work within the site manager's unit and use restricted data

1. The Site Manager/operator concept is very similar to what we do to manage 2,500 purchasing cards. Cardholders are the responsibility of site managers with the average manager handling 12 cards. Our communication of policy and procedure is to the Divisional Business Manager and the site managers who communicate with their operators (users of restricted data).
2. The Divisional Business Representative (DBR) is responsible for the site managers in their division (school, college, administrative unit, etc.) and would be responsible for annual attestation of compliance. They are also responsible for creating the divisional teams to address the remediation and assessment efforts.
3. The sponsors are generally accountable to the outside world for our compliance and provide the project with resources to help the site managers and operators comply. They also approve institutional policies that are recommended by the data owners and the middle management.
4. The data owners provide the middle management team with resources and enforcement assistance. They also create consensus on institutional policies.
5. The middle management and core team members work through the Divisional Business Representative. They should refer issues to the data owners if they are having difficulty with the site managers or operators.
6. Restricted data requirements: www.cio.wisc.edu/security/initiatives/restricted.aspx

Example Restricted Data Remediation Governance



Security Assessment Questionnaire A
Baseline minimum acceptable state for all departmental systems

No.	Requirement	Testing Procedures		In Place	Percent Complete
1	**Network Based Firewall: Install and Maintain a network based firewall system with a configuration to protect non-public unrestricted data and the machines using such data.**	1.1	Ensure a network firewall is Installed on all network segments with active nodes:		
		1.1.1	Is each firewall operational		
		1.1.2	Is each firewall registered centrally		
		1.1.3	Is each firewall reporting centrally		
		1.2	Confirm all logs sent to central Security Event Management System		
		1.3	Confirm that the firewall's logical configuration restricts connections inbound to systems of interest		
3a	**Ensure absence of Restricted Data**	3.1	Install and run Identity Finder		
		3.1.1	Use the FORMATED searches for SSN, Driver Licenses, Bank Account Information, and Credit Cards		
		3.1.2	Remove all restricted data stored locally on workstations		
		3.1.3	If restricted data was anticipated but not found, re-run Identity Finder with non-formatted options		
		3.1.4	Are results of Identity Finder scans reported centrally?		
		3.1.5	Is Identity Finder run at least quarterly and steps 3.1.1 – 3.1.4 followed?		
3b	**If Restricted data (RD) was found?**	3.2	Restricted data will be reviewed by the appropriate, knowledgeable personnel to determine if it can be purged		
		3.3	Use the Shred in IDFinder for purge		
		3.4	If Restricted Data is impossible to purge, or if Restricted Data is needed again in the future See Security Assessment Questionnaire B		
4	**Encrypt the transmission of sensitive data over public networks**	4.1.1	Are industry best practices used to implement strong encryption for authentication and transmission for wireless networks transmitting restricted data or connected to the restricted data environment?		

No.	Requirement	Testing Procedures		In Place	Percent Complete
		4.2	b) Are policies in place that state that unprotected restricted data are not to be sent via end-user messaging technologies?		
5	**Run up-to-date anti-virus software:** *Keep Anti-Virus software patched and up to date*	5.1	Is anti-virus software deployed on all systems commonly affected by malicious software (example Symantec Endpoint Protection)?		
		5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?		
		5.1.2	Are all anti-virus programs reporting to a central console		
		5.1.3	Are all anti-virus programs configured to check for new signatures every 24 hours?		
6a	**Maintain Secure Systems**: *Keep all operating system software, application software, and other software current with the latest security-related patches from the vendor*	6.1	Confirm that the operating system is currently supported by the vendor		
		6.1.1	Check operating system for outstanding / uninstalled security patches		
		6.1.2	Has the system successfully checked in the past 24 hours?		
		6.2	Are centralized endpoint management solutions in place to automate OS patching, application patching, workstation inventory, and application inventories? (Examples Include: Microsoft WSUS, BigFix, Altiris, or another endpoint management suite)		
		6.2.1	Is an endpoint management suite utilized		
		6.2.2	Is it operational		
		6.2.3	Is it reporting to a central console		
		6.2.4	Are updates applied within 30 days of release?		
		6.3	Install Secunia: Corporate Security Inspector on all workstations		

No.	Requirement	Testing Procedures		In Place	Percent Complete
		6.3.1	Is Secunia reporting centrally?		
		6.3.2	Are high concern applications updated regularly		
		6.3.3	Are end-of-life applications removed from workstations?		
6b	**Custom Applications & Data Bases**	6.4	Run DBScanner on all databases		
		6.4.1	Analyze the results of database scans		
		6.4.2	Present recommended changes based on results of DBScanner database scans		
		6.4.3	Make approved changes based on results of DBScanner database scans		
		6.3	Run Watchfire AppScan on all custom web applications and web sites		
		6.3.1	Analyze the results of web application and site scan		
		6.3.2	Present recommended changes based on the results of a web application and site scan		
		6.3.3	Make approved changes based on the results of a web application and site scan		
6c	**Run an up-to-date Host Firewall**	6.4	Check that an approved Host-Based Firewall:		
		6.4.1	Is installed?		
		6.4.2	Is operational		
		6.4.3	Is reporting to a central console		
		6.4.4	Has checked for new rules from the console (if available) in the past 24 hours		
		6.4.5	Has checked for application updates from an appropriate source in the past 24 hours		
8	**Implement Strong Access Control Measures**	8.1	Are all users assigned a unique ID before allowing them to access system components or restricted Data?		
		8.2	Are proper user identification and authentication management controls in place for users and administrators on all system		

No.	Requirement	Testing Procedures		In Place	Percent Complete
			components?		
		8.3	Are users identities verified before performing password resets for user requests made via a non-face-to-face method?		
		8.4	Are first-time and reset passwords set to a unique value for each user, and must each user change their password immediately after the first use?		
		8.5	Is access for any terminated users immediately deactivated or removed?		
		8.6	Are inactive user accounts over 90 days old either removed or disabled?		
		8.7	Do passwords adhere to the University of Wisconsin – Madison Chief Information Officer's official password policy?		
		8.8	Are applications IDs with database access only able to be used by the applications?		
		8.10	Local administrative account protection:		
		8.10.1	Administrative accounts not to be used regularly by standard users		
		8.10.2	Administrative accounts not to be used in trust relationships across machines		
		8.10.3	Administrative account Passwords managed centrally		
9	**Control Physical access data and credential stores**	9.1	Is physical access to publicly accessible network jacks restricted?		
		9.2	Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?		
		9.3	Is restricted data on electronic media rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media so that restricted data cannot be reconstructed?		
		9.4	Is strict control maintained over the storage and accessibility of media?		
		9.6	Is all media destroyed when it is no longer needed for business or legal reasons?		
		9.7	Is media classified so the sensitivity of the data can be determined?		
		9.8	b) Are containers that store information to be destroyed secured to prevent access to contents?		

No.	Requirement	Testing Procedures		In Place	Percent Complete
			a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that restricted data cannot be reconstructed?		
10	**Track and Monitor privileged access to systems, network resources and to sensitive data**	10.2	Are the following audit trail entries recorded for all system components for each event?		
		10.3	Are all critical system clocks and times synchronized through the use of time synchronization technology, and is the technology kept current?		
		10.4	Is viewing of audit trails limited to those with a job-related need?		
		10.5	Are audit trail files promptly backed up to a centralized log server?		
		8.6	Are logs for all system components reviewed, and are follow-ups to exceptions required?		
11	**Regularly Monitor and Test Networks** *Regularly Test Security Systems and Processes*	11.1	Is automated monitoring utilized and configured to generate alerts to personnel?		
		11.1.2	Are internal network vulnerability scans run at least quarterly?		
			a) Does the internal scan process include rescans until passing results are obtained, or until all "High" vulnerabilities are resolved?		
			b) Are internal scans performed by a qualified internal resource or qualified external third party?		
		11.3	Are external vulnerability scans performed at least quarterly?		
		11.3.1	Are external vulnerability scans performed by a qualified internal resource or qualified external third party?		
		11.4	Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic at the perimeter of the network infrastructure as well as at critical points inside of the network infrastructure?		
		11.4.1	Are IDS and/or IPS configured to alert personnel of suspected compromises?		
		11.4.2	Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?		
12	**Maintain an Information Security Policy**	12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?		
		12.1.1	Is the information security policy reviewed at least once a year and updated as needed to		

No.	Requirement	Testing Procedures		In Place	Percent Complete
			reflect changes to business objectives or the risk environment?		
		12.2	Are usage policies for critical technologies developed to define proper use of these technologies for all personnel, and require the following:		
		12.2.1	Explicit approval by authorized parties to use the technologies?		
		12.2.2	A list of all such devices and personnel with access?		
		12.2.3	Acceptable uses of the technologies?		
		12.2.4	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?		
		12.2.5	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?		
		12.3	Do the security policy and procedures clearly define information security responsibilities for all personnel?		
		12.4	Are the following information security management responsibilities assigned to an individual or team:		
		12.4.1	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?		
		12.5	Is a formal security awareness program in place to make all personnel aware of the importance of restricted data security?		