

JANUS Associates



How To Structure An Information Security Program Without Breaking The Bank

Presented to: Maryland Education Enterprise Consortium - December 8, 2009

Moderator: Lyle A. Liberman, Director

Presenter: Karl W. Muenzinger, CISA, CISM, CISSP, MBCI



Agenda

- Introductions
- Initiate an Information Security Program
- Conduct Ongoing Risk Management
- Q and A



About JANUS Associates

Focused on Information Security and Business Continuity consulting for two decades, oldest in the nation

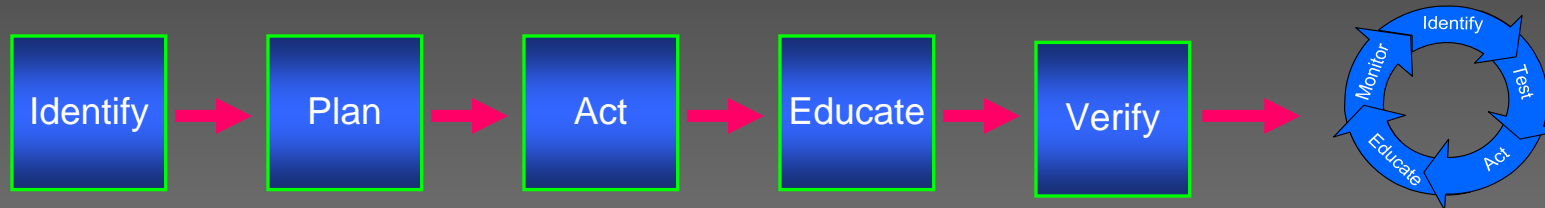
Consulting Services:

- Information Security & Privacy
- Business Continuity and Disaster Recovery Planning
- Regulatory Compliance, including PCI
- Security Awareness Training
- Data Breach Response
- Computer Forensics
- Electronic Discovery

Locations in Stamford, Albany, Boston, Baltimore, Washington, DC



Essential Elements of an Information Security Program



Objectives	Targets	Policies	Awareness Training	Monitoring	The Risk Management Cycle
Environment	Staffing	Standards	Role-Based Training	Metrics	
Risk Tolerance	Resources	Procedures			

Information Security In A College Setting

Identify

Students come first

- Confidentiality requirements in a Facebook age.
- Lack of restrictions on what students plug into the network.
- Powerful hacking tools in the hands of students.
- Rise in data breaches.
- Bleeding-edge technology needed for academic research and instruction.
- Shared public space: Where is the network perimeter?

Identify Ownership



Tone at the Top

Executive Ownership: More than technology

- Human Resources
- Finance
- General Council
- Student Affairs
- Academic Planning and Research
- Information Services
- Facilities



Identify Your Requirements

Identify

Protect Data And Privacy

- Payment Card Data (PCI)
- Student Health Records (HIPAA)
- Student Academic Records (FERPA)
- Personally Identifiable Information (PII)
- Red Flag Rules
- Intellectual Property

Protect Reputation

- Student Enrollment
- Partnerships and grants
- Retention of Faculty

Protect Continuity of Operations

- Payroll, essential administrative functions
- Investment in capital assets
- Reduce legal exposure



Plan Roles and Responsibilities

Plan

The Three Roles Of Information Security Personnel

- Oversight and Assurance (policy, monitoring, and reporting)
- Engineering (security architecture and standards development)
- Operations (implementation and procedures)

The Role Of The Chief Information Security Officer

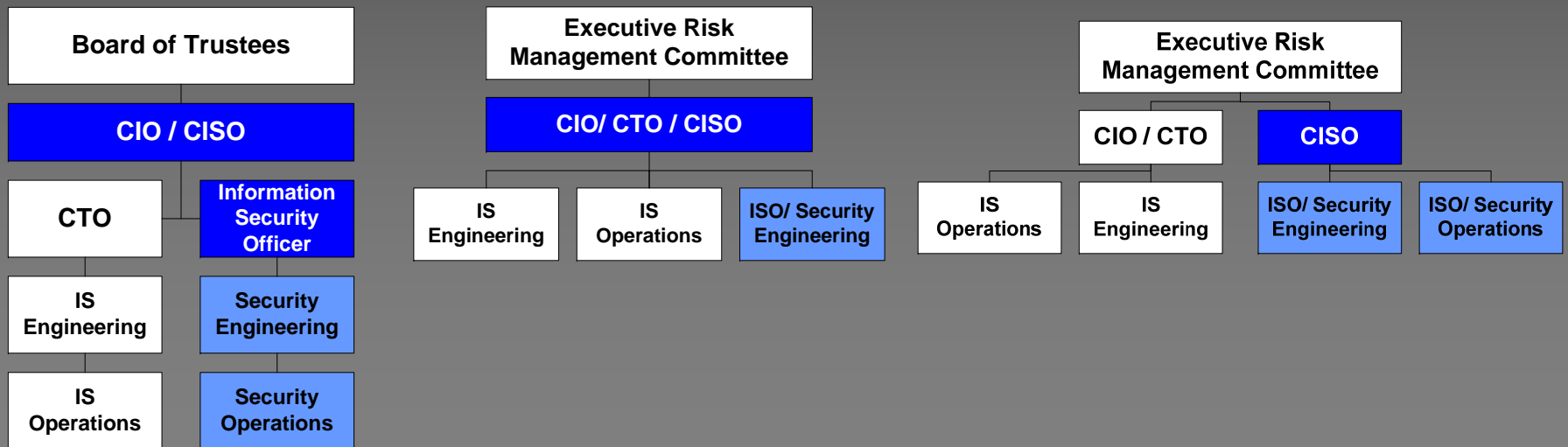
- The ideal candidate combines a strong technical background with a solid understanding of how the college operates, and why.
- Promotes teamwork across the entire organization for the protection of data
- Provides reports on risk management and compliance
- Included in discussions on information security budget
- Independent from IT operational responsibilities (Separation of Duties) to promote an unbiased perspective



Plan the Reporting Structure

Plan

Information Security officers report to the CTO, CIO, CISO, a Chief Risk Officer, or Executive Risk Management Committee, as long as an unbiased and unfiltered voice reaches the executive level



Act: Establish Expectations



Policies

- Approved by the Board or Executive Committee
- Driven by **Requirements**
- Brief statements, General in tone
- Change infrequently

Standards

- Approved by Data Owners
- Driven by **Policy**
- Detailed, technical, and proscriptive in tone
- Reviewed annually

Procedures

- Approved by managers
- Driven by **Standards**
- Specific, task oriented, document action taken
- Change as needed

Educate participants on what is expected of them

Educate

Policies, standards, and procedures define the requirements for security training

All users require training

Including contractors, vendors, and temps.

Training comes first, network access comes later

User Awareness Training should be a mandatory pre-condition of receiving access to restricted networks and data.

Include Human Resources in the process of providing training

to ensure comprehensive and efficient delivery of training.

Provide annual re-training for all staff

because technology and security threats are always evolving.

TIP: Document and retain accurate attendance records to demonstrate due diligence.



Beyond User Awareness Training

Educate

Provide Role-Based Security Training

- **Managers** who approve access
- **Managers and HR** involved in transfers, promotions, or terminations
- **Data Owners-** are responsible for setting expectations on how their data is handled
- **System owners** – are responsible for implementing security controls
- **Developers** – are responsible for security coding and change management
- **IT Operations staff** – follow security procedures and monitor for incidents
- **Physical security staff** – protect assets and staff

Professional Certifications and Continuing Education are critical for security staff



Verify That Policy, Standards, And Procedures Have Been Implemented

A blue square button with a green border and the word "Verify" in white text.

Verify

Have procedures been followed?

Enable monitoring of procedures. Design your procedures so that they are self-documenting, by using operation check lists, system logs and reports.

Have objectives been met? Are you really more secure?

Conduct penetration tests and vulnerability assessments.
Design audit methods that test for results, not just completion of procedures.

What are your lessons learned?

Compare your procedures to the end results.
Was the expected outcome was achieved when the procedure was followed? Can the procedure be improved?

Program Review for Information Security Management Assistance (PRISMA) *

Where would you place your organization ?

Maturity Level 1		Maturity Level 2		Maturity Level 3		Maturity Level 4		Maturity Level 5	
Policy		Procedures		Implemented		Test		Integration	
Formal and Documented		Procedures Exist		Implemented Policy & Procedures		Procedures have been tested		Integration of Security throughout organization	
Compliant		Compliant		Compliant		Compliant		Compliant	
Partially Compliant		Partially Compliant		Partially Compliant		Partially Compliant		Partially Compliant	
Non-compliant		Non-compliant		Non-compliant		Non-compliant		Non-compliant	

* Based on NIST Special Publication 800-53 and the Federal Information Security Management Act (FISMA)



Information Risk Management Maturity Model*

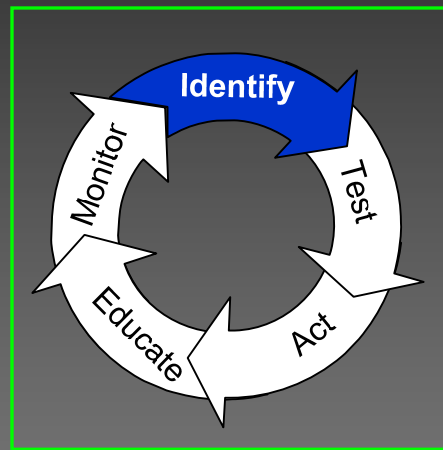
Where would you place your organization ?

0	1	2	3	4	5
Non-existent	Initial/Ad Hoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimized
Complete lack of any recognizable processes.	No standardized processes. However, the enterprise has recognized that the issues exist and need to be addressed.	Processes have been developed. There is no formal training or communication of standard procedures. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	Procedures have been standardized and documented, and communicated through training. However, it is unlikely that deviations will be detected.	Management monitors and measures compliance with procedures . Processes are under constant improvement	Processes have been refined to a level of good practice, based on the results of continuous improvement

* Based on the management maturity model of CMMI, COBIT, and ISO 27001/27002



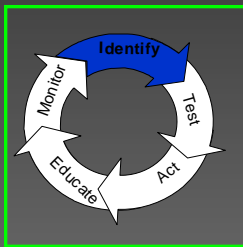
Risk Management : A Continuous Cycle of Improvement



Once your program is in place, Risk Management optimizes value for your organization

Use these five steps to raise the maturity level of your program. Lets take a second look ...

Identify Your Assets, Risks, and Compliance Requirements



Each year, compliance requirements change:

- New technology is added
- New threats emerge
- Business requirements change
- Your understanding of the effectiveness of your current controls improves

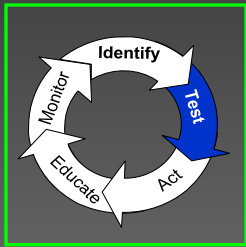
TIP: Update your program requirements annually.

Compliance does not equal Security.

You can be compliant but not secure, you can be secure but not compliant.

TIP: Do not rely solely on regulations to define your security requirements.

Conduct Vulnerability Assessments, Accreditation and Certification



Accredit (approve) all systems and certify all changes

- Document the baseline security of each major system.
- Then certify that every subsequent change meets your security standards by incorporating Security into the System Development Life Cycle.
- Test all changes *Prior To* deployment into the production environment.

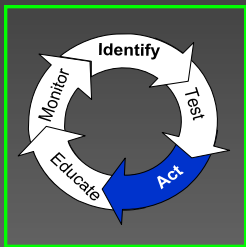
Perform penetration tests and vulnerability assessments regularly.

Maintain an active inventory of risks and vulnerabilities discovered during testing.

TIP: Test you vendors. If your vendors and outsourced business partners handle your confidential data, you must review their security as well. You remain responsible for your data even when it is in the hands of a vendor.

Information Security Risk cannot be outsourced.

Risks can be mitigated, accepted, or transferred but never ignored



Take Action to Reduce Risks

Step 1: Track risks identified during testing

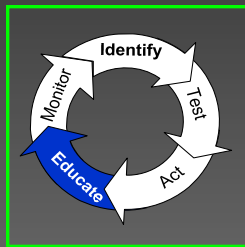
Step 2: Prioritize Risks

Step 3: Conduct Cost/Benefit Analysis of Mitigation Strategies

Step 4: Decide

TIP: Require that data owners signoff on risk acceptances

Notify and Educate on Risks Discovered and Actions Taken

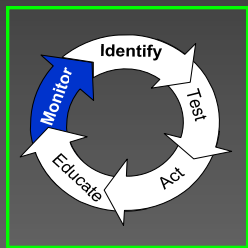


When lapses in actual user behavior are discovered, update security awareness training and enforcement

Present executive management with meaningful reports on existing levels of risk, stated in business terms. Present trends

TIP: update your security awareness training annually, employees should retake security awareness training annually

Monitor for Effectiveness - Collect Lessons Learned



Every procedure and control objective should have a method of monitoring for effectiveness.

Automated monitoring includes

- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Security Information and Event Management (SIEM) systems
- Anti-virus/Anti-malware protection
- File Integrity Protection, Web Content Monitoring
- Application Firewalls, and more.

TIP: Tools are indispensable, but humans are your first line of defense. IDS/IPS/SIEM products are not optimized upon first install. Plan sufficient time and resources (weeks or months) to configure and fine-tune these products for your environment.

Additional Resources

Sample policies and procedures for a higher education environment

Security Frameworks and Standards

Information Risk Management Models



Thank You For Your Time Today

JANUS Associates

7000 Security Boulevard, #334
Baltimore, MD, 21244

Kevin Hawkins

Office: 410-597-9815 x302

Cell: 202-215-3519

kevinh@janusassociates.com

www.JANUSassociates.com

