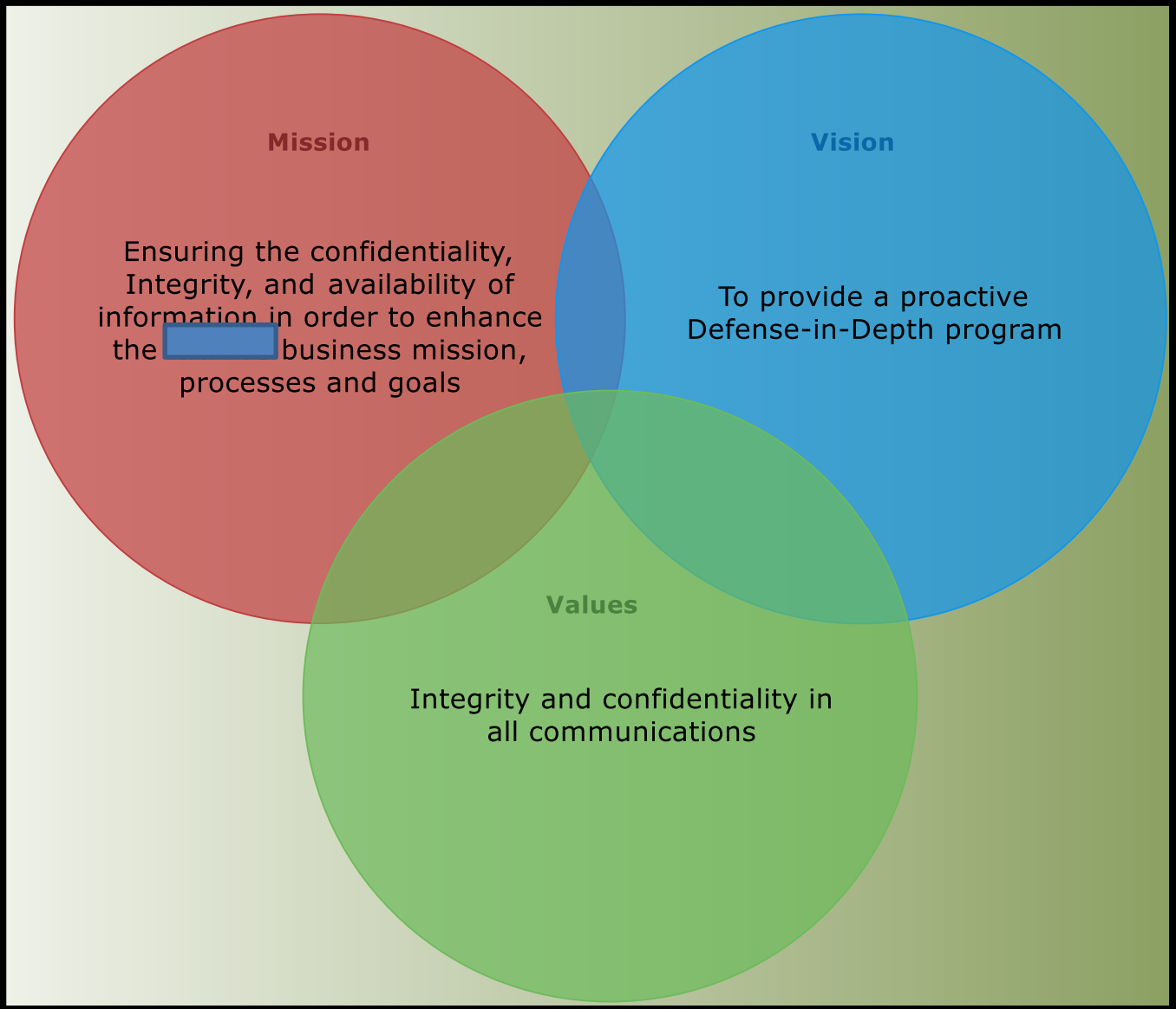
Information Security Governance Committee

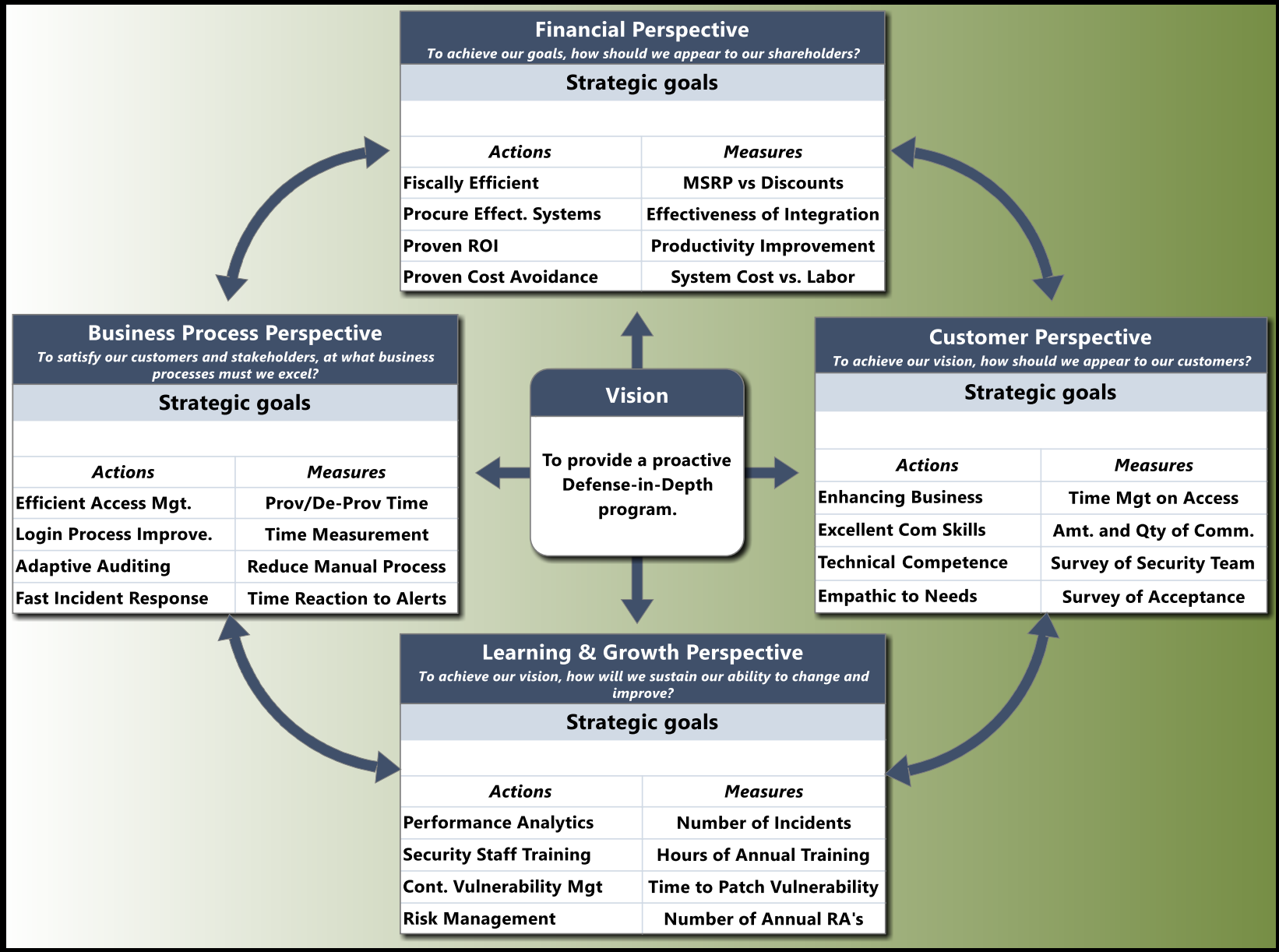
March 14, 2012


Mission
Ensuring the confidentiality, Integrity, and availability of information in order to enhance the [redacted] business mission, processes and goals
Vision
To provide a proactive Defense-in-Depth program
Values
Integrity and confidentiality in all communications

The Goals Grid

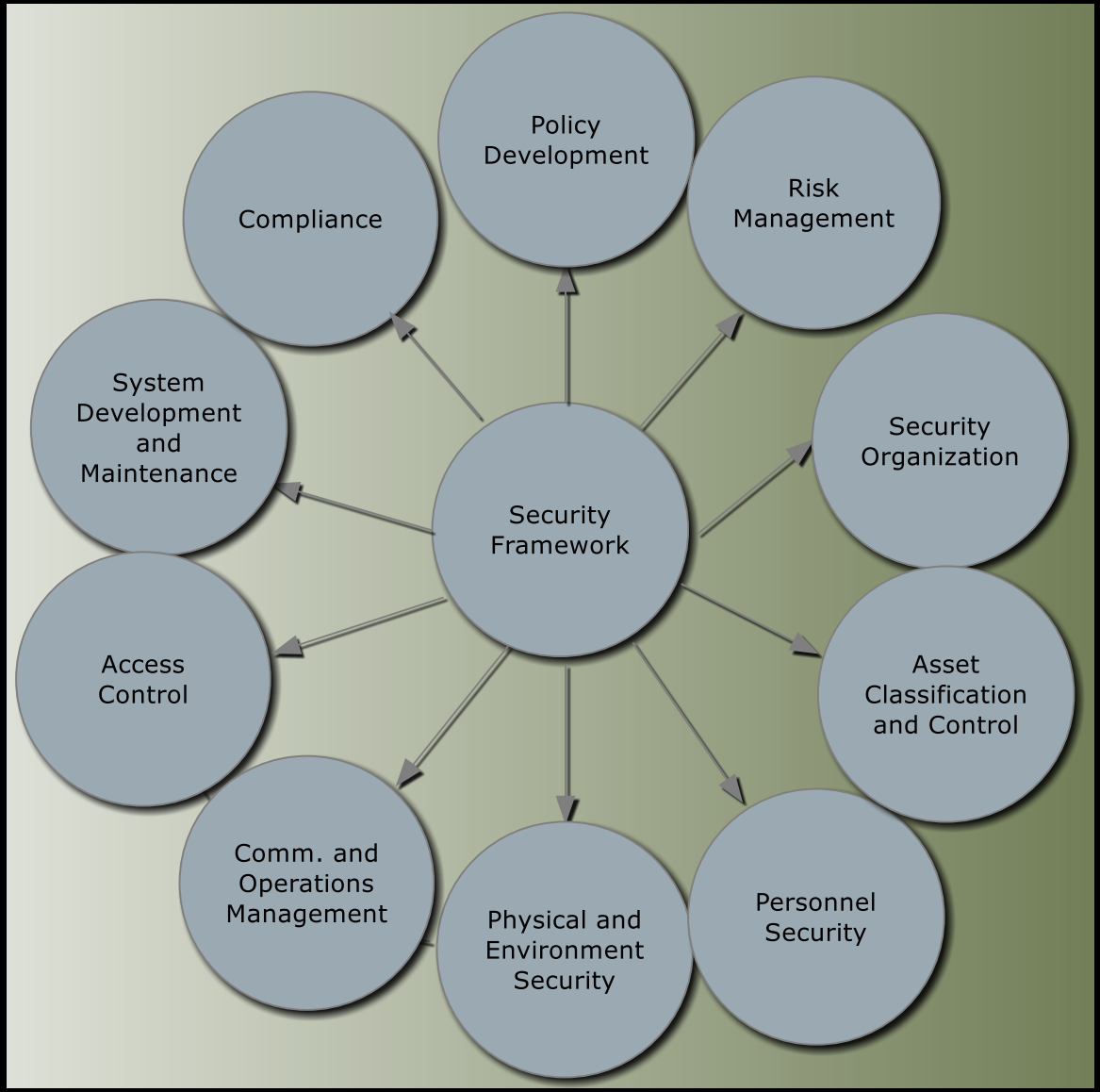
DO YOU WANT IT?	DO YOU HAVE IT?	
	NO	YES
YES	***Achieve***	***Preserve***
	■ Strong Risk Management ■ Adaptive Compliance Alerting ■ Continuous Vulnerability Mgt ■ Data Loss Prevention ■ Continuous SETA ■ Strong Security Architecture ■ Auditing Automation ■ Performance Analytics ■ Enhance Business Process	■ Strong Senior Mgt Support ■ Strong Information Services Commitment ■ High-level Position Within the Organization
NO	***Avoid***	***Eliminate***
	■ Hackers stealing data ■ Increased Labor Costs ■ Data Loss ■ Diminishing Importance of Security to the Organization ■ Security Breaches ■ Apathy ■ Myopia	■ Non-Compliance ■ System Complexity ■ Weak Identity Management ■ Weak Password Management ■ Security Ignorance

Security Balanced Scorecard

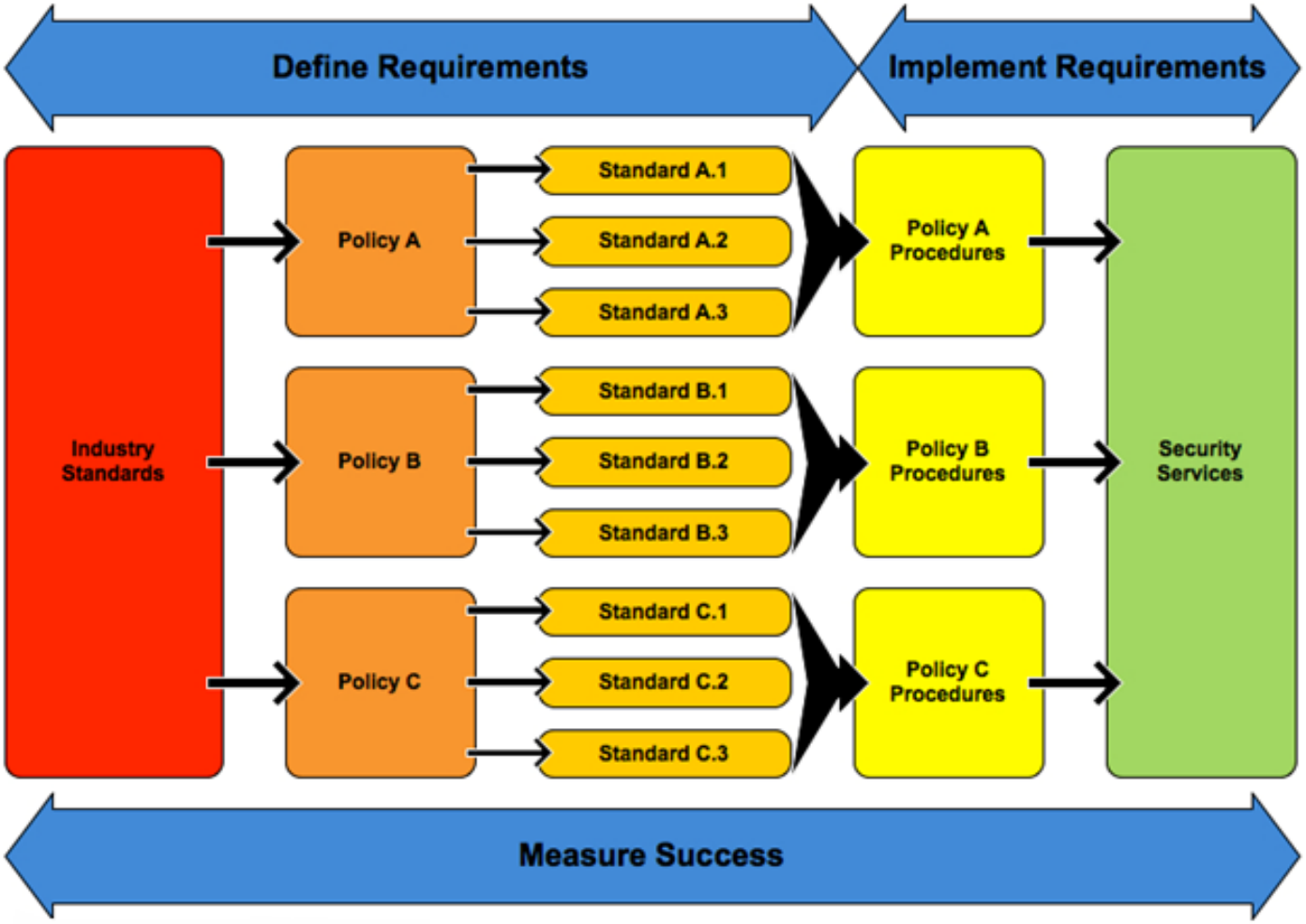



Risk Management
Policies
Standards
Procedures
Training/
Awareness
Systems
Implementation
Performance
Analytics
Security
Development
Life Cycle

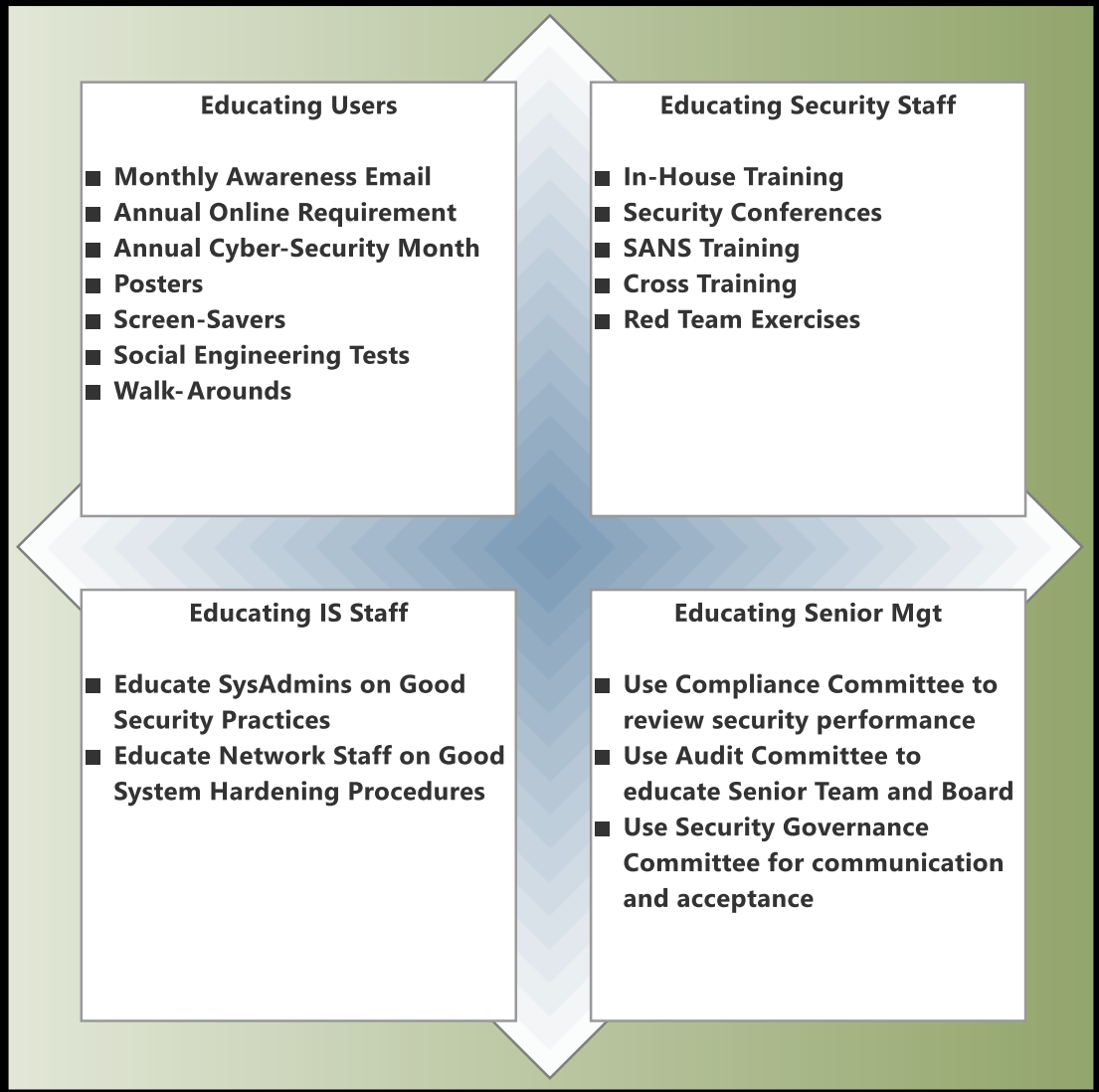
Information Security Framework

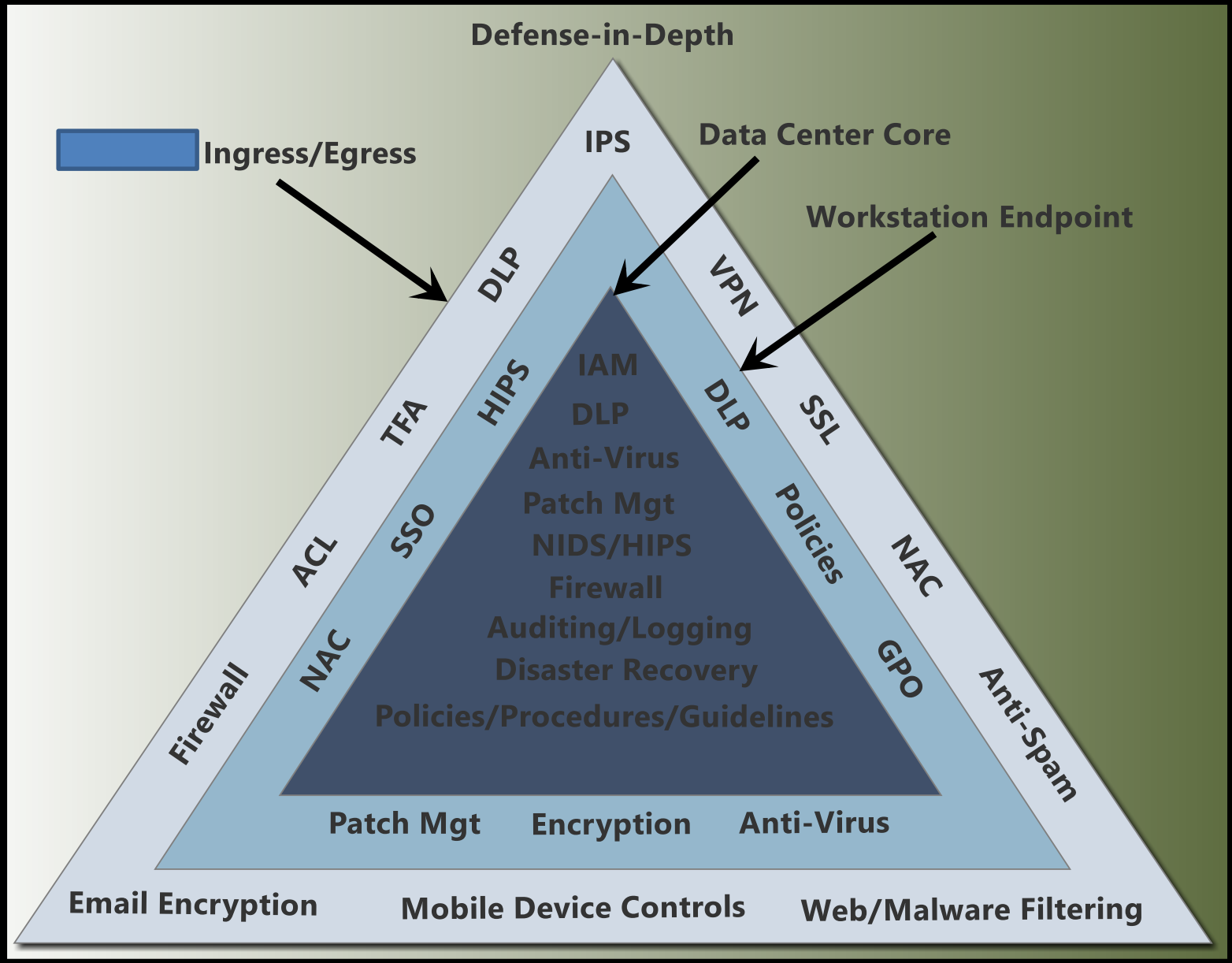


Information Security Framework Architecture

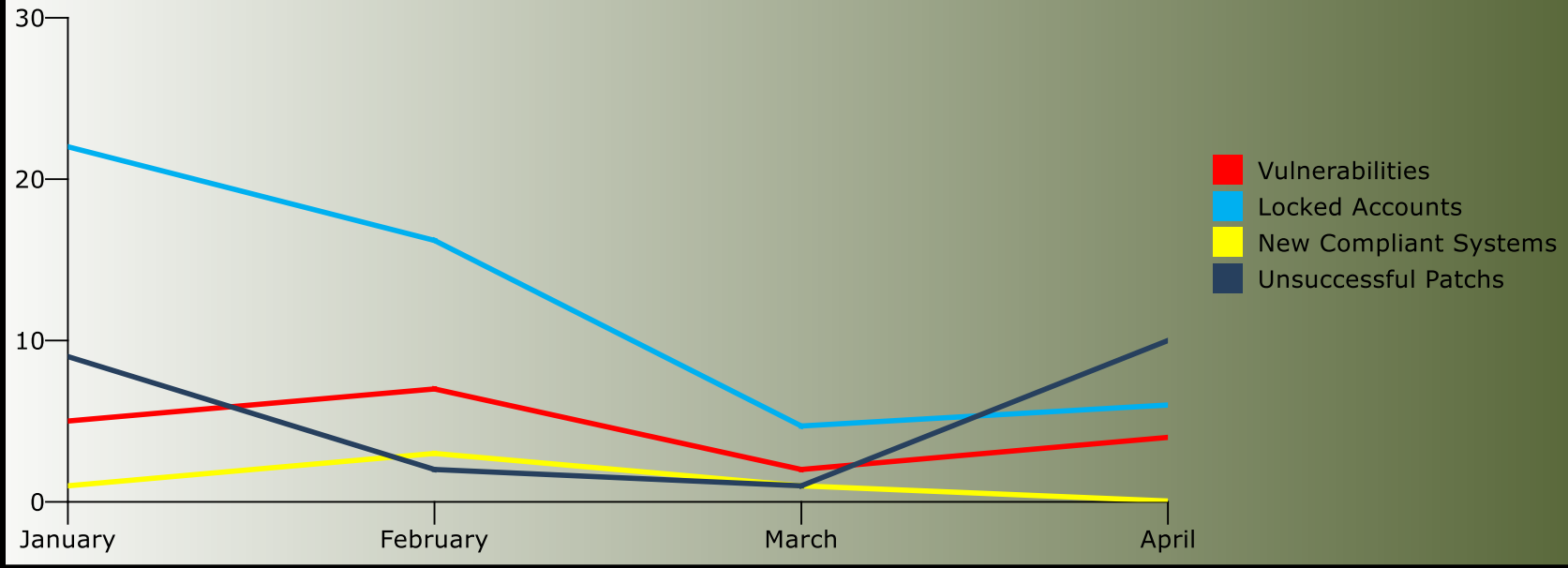


Security Education and Training Awareness




Defense-in-Depth
Ingress/Egress
IPS
Data Center Core
Workstation Endpoint
DLP
VPN
IAM
DLP
Anti-Virus
Patch Mgt
NIDS/HIPS
Firewall
Auditing/Logging
Disaster Recovery
Policies/Procedures/Guidelines
TFA
HIPS
DLP
SSL
ACL
SSO
Policies
NAC
Firewall
NAC
GPO
Anti-Spam
Patch Mgt
Encryption
Anti-Virus
Email Encryption
Mobile Device Controls
Web/Malware Filtering

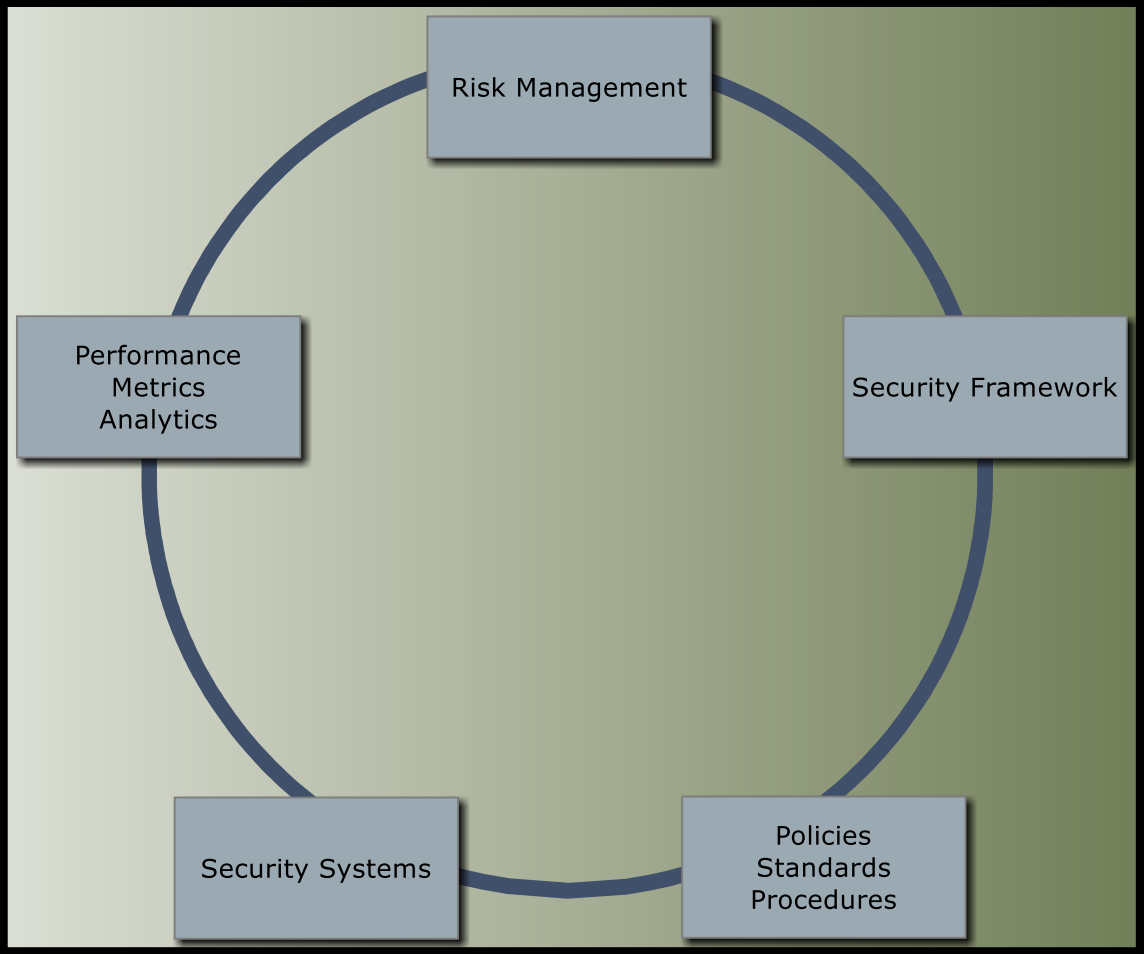
Security Performance



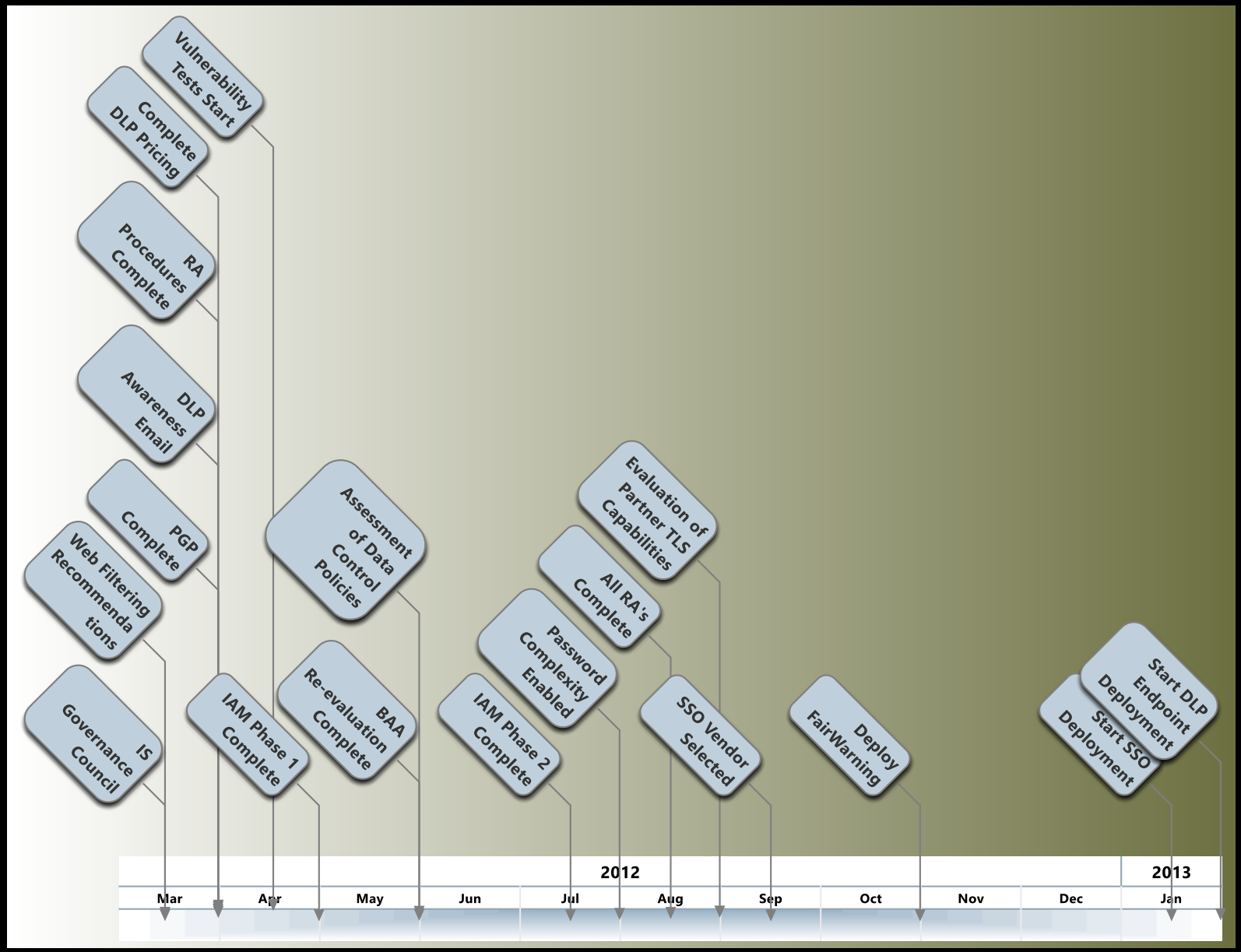
Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
(4) Owner(s) *Who owns this information asset?*		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	

(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*			
❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Security Program Summary



Security Timelines



Decisions

First Security Awareness Communication

Security Awareness

As part of our commitment to provide excellent customer service, the XXXXX IS Security Team will be sending out quarterly security awareness information to all employees:

Purpose: To inform the XXXXX user community on how confidential information loss can occur.
Affected Areas: This affects all XXXXX information system users
Situation: Losing confidential data is a problem for all organizations. It can come in many forms. Below are some scenarios in which confidential information (PHI) can be inappropriately handled.

- Establishing easy to guess passwords.
  - oHackers can use "Brute Force" attacks to guess a user's password. Cyber-criminals could use this data to extort money from the organization.
- Copying confidential data (PHI) to inappropriate locations.
  - o A user decides to copy files with PHI to their home directory, workstation, a USB flash drive, or other mobile media, home PC or laptop which can result in the loss of confidential data.
- Copying confidential data into personal e-mail accounts such as GMail, HotMail, or Yahoo.
  - o Can result in the loss of that data and violates XXXXX policy.
- Printing out confidential data on a printer and carrying it out of the organization.
- Faxing confidential data to a wrong fax number.
  - o Always verify the fax number with the recipient by telephone.

If there is any doubt about transmitting, copying, or storing confidential information (PHI), please contact either the Compliance office or IS Security office.

Password Management

- Initial and Password Reset Formats (mid-April 2012)
  - Upper Case First Letter of First Name; Lower Case First Letter of Last Name; Upper Case Second Letter of Last Name; Full Birth Date MMDDYYYY
    - Example – Joe Smith born July 4 1978 = JsM07041978
- Password Complexity (July 30, 2012)
  - Mandatory
  - Reset Every 90 days
  - 12 Password History
  - Minimum 8 Alphanumeric Characters
    - At least 1 Upper Case; 1 Lower Case; and 1 number
    - Not Easily Guessed
    - Use Passphrases (Why in the World am I here = Witwaih9)
    - Do not use a password that ties something directly to you (children, pets, college, etc…)
    - Do not use words found in dictionary

Web-Filtering

- Filter all Public Internet Document Management Systems
- Filter all Public Email Systems (Gmail; Yahoo; Hotmail; etc…)

Questions