J. A. "Drew" Hamilton, Jr., Ph.D.

Chair, NSA Cyber Operations Community of Practice

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

This work funded by NSA Contract #H98230-19-1-0291

CCI
2 Research Blvd.
Starkville, MS 39759

Voice: (662) 325-2294
Fax: (662) 325-7692
drew@drew-hamilton.com

Certified Information Security Manager – Domain 3

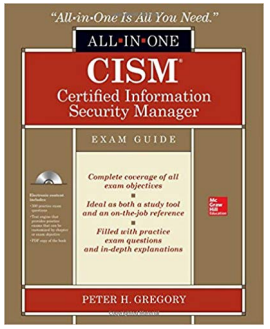
Domain 3: Information Security Program Development and Management

References:

Drew Hamilton Lecture Notes

CISM Review Manual, 15th Edition

CISM All-in-One Exam Guide, 1st Edition



Domain Outline

- Information Security Program Development and Management Overview
- Information Security Program Management Information Security Program Objectives
- Information Security Program Concepts
- Information Security Program Concepts Scope and Charter of IS Program
- Information Security Management Framework COBIT 5 ISO/IEC 270001:2013
- Defining an Information Security Program Road Map
- Information Security Infrastructure and Architecture
- Architecture Implementation

Domain Outline (cont.)

- Security Program Management and Administrative Activities
- Security Program Services and Operational Activities
- Controls and Countermeasures
- Security Program Metrics and Monitoring
- Information Security Program Challenges

Information Security Program Development and Management Overview

Domain 3: Information Security Program Development and Management

Learning Objectives

- **Ensure that the CISM candidate has knowledge necessary to:**
  - **Understand the broad requirements and activities needed to create, manage and maintain an information security program and how to implement an information security strategy**
  - **Define and utilize the resources required to achieve the IT goals consistent with organization objectives**
  - **Understand the people, processes and technology necessary to execute the information security strategy**

Introduction

- Development of an information security program is for the purpose of executing organizational strategies and objectives for developing acceptable levels of risk and business disruption
- This normally starts with a roadmap with high-level objectives, goals, and a step-by-step guide for achieving everything specified
- Built into this plan should be the ongoing activities required to manage, maintain, and improve the efficiency of the program

Introduction cont.

- These programs encompass all departments of the organization and each activity is designed to protect its information assets
- The information security program exists to support and bring value to the components of the organization
  - Must be deliberately aligned to business goals and managing risk
- An information security plan should implement the proper processes to support business activities and leave room for continued growth

Purpose of an Information Security Manager (ISM)

- A main purpose of this role is to highlight to senior management the security controls that are implemented and to describe the risks that are being addressed
  - The executives want to understand the investments and benefits that go into managing the controls within a program
- Due to these requirements, the manager must expand their knowledge beyond just technology to the understanding of various business activities as well

Roles of an Information Security Manager

- Ensures policies developed by the organization adhere to any required standards, laws, regulations, etc.
- Plays a key role in the assessment of organizational processes to develop an information security strategy that addresses risks in a cost-effective manner
- This position also articulates important details to high level executives and assists in making sure tasks align with business activities

Roles of an Information Security Manager cont.

- Establishes periodic assessments for external service providers and makes sure that they are privy only to the data necessary to perform that service
- After a security program is operational, establishes reporting mechanism that can be monitored for trends over time
- A manger must also expand their capabilities in management functions such as budgeting, planning, business case development, recruiting, etc.

Information Security Program Management and Information Security Program Objectives

Domain 3: Information Security Program Development and Management

Information Security Management Trends

- An ISM is often a member of a senior management team or counsel for the organization
- In additional to this, companies have been trending toward having a single body or entity responsible for security functions and other business units are required to report to this group
  - The functions include physical and information security, IT security, compliance, privacy, business continuity planning/ disaster recovery (BCP/DR) and security architecture

Information Security Management Trends cont.

- The benefit of placing the previously stated functions under one group is valid because all the subjects are interdependent
  - Segmented security activities will inevitably introduce security holes
  - Also it is cost effective to manage such functions together

- Some industries do still observe information security as a low-level activity that serves more compliance needs rather than being a core organizational objective

Information Security Program (ISP) Essential Elements

- **Three key characteristics have been identified for ensuring successful security program design, implementation and ongoing management**
  1. **The program must be the execution of a well-developed information security strategy closely aligned with and supporting organizational objectives**
  2. **The program must be well designed with cooperation and support from management and stakeholders**
  3. **Effective metrics must be developed for program design and implementation phases as well as the subsequent ongoing security program management phases to provide the feedback for achieving future outcomes**

Objectives Alignment

- **Developing a strategy for an ISP goes beyond simply conducting a risk assessment**
  - **Security objectives should be strictly aligned with those of the organization**
  - **It should ensure the organization's preservation and optimize security resources and activities**

Executive Cooperation

- **An ISM must not only specify objectives for the security program, but also elicit consensus among management and stakeholders**
  - **A manager should realize that describing the benefits of the program should be addressed from the perspective of business terms**
    - **This helps nontechnical stakeholders understand and potentially endorse the program goals**
  - **Structuring information in this manner will generate feedback which, in turn, will help the program to better align with organizational objectives**

Objectives to Metrics

- **Objectives are key components to an information security program**
  - **Without objectives it is impossible to develop metrics**
  - **Without objectives there will be no point of reference to show progress**
  - **Development is likely to be ad-hoc and haphazard**

Importance of the ISP

- A quality program protects information assets, satisfies regulatory obligations, can minimize potential legal and liability exposures
  - When the program is properly implemented and maintained, it provides critical support to key business functions
- The program moves designs, plans, and objectives to actuality through defined processes and methods
  - A good program can also provide flexibility to address changing security requirements as needed

ISP Core Outcomes

- Each security program should have specific outcomes it is designed to deliver

- The following should be considered the basis for developing the objectives of an effective ISP:
  - Strategic alignment
  - Risk management
  - Value delivery
  - Resource management
  - Assurance process integration

Strategic Alignment

- **Programs must be developed in harmony with the organization**

- **Methods for doing this include:**
  - **Adapting to new business initiatives that are under consideration**
  - **Selecting an organizational risk tolerance that business leaders and stakeholders are comfortable with**
    - **Continuously cultivating relationships with leaders and stakeholders will facilitate a program that empowers the business, not stifle it**

Strategic Alignment cont.

- Regularly providing updates on issues associated with strategic alignment and any potential new risks that have been identified can build a sense of responsibility among executives
  - This can build rapport between groups and ease the resolution of problems

- The ISM must take into account information such as existing processes, cost, culture, governance, organizational structure, etc. before deciding if a security solution is a good fit

Risk Management

- Managing the risks of information assets in a company is an essential element of an ISP
- All security activities geared toward protecting information assets essentially stem from addresses their risks
- To manage risk effectively, the ISM must develop a comprehensive understanding of threats to an organization, vulnerabilities, its risk profile, and risk deemed to be acceptable by management

Risk Management cont.

- The potential impact of the threats identified must be evaluated and used to determine acceptable courses of action

- The risk landscape is always evolving and new risk can arise during the development of a security program
  - There must be mechanisms in place where reassessments are performed to identify and remediate any potential new issues

Value Delivery

- An effective ISP delivers value to the organization
- This is accomplished by aligning security activities that are directed toward risk reduction in the organization's most critical activities
  - Application of resources should be towards the activities providing the most benefit
- Security measures should be optimized to offer the maximum benefit to an organization
  - This requires good planning and project management skills to do so efficiently

Resource Management

- Resources for an ISP can include permanent and temporary staff, outside service providers, and other tools
- These resources must be assigned and used effectively within an organization
- Applying resources well can help manage and adjust to fluctuating financial budgets
- A track record of managing resources well can be very helpful when making addition resource requests

Resource Management cont.

- An additional factor for resource management is capturing key information and making it available to those who require it
  - Effectively cataloging and managing knowledge resources can be a great asset for an ISP

Performance Management

- For any ISP, key monitoring and metrics requirements will be built in
  - These items should be performing as expected to ensure the program is executing properly
- Security processes should have measurable and monitorable control points that an auditor can assess to verify effectiveness
  - The same principle should be used when evaluating objectives
  - Monitorable and measurable objectives can be reviewed to identify progress

Performance Management cont.

- **Metrics should be agreed upon by the various constituencies and be implemented at various levels**
  - **Strategic**
  - **Tactical**
  - **Operational**

- **Care should be taken that metrics are representative of the security activities of interest**
  - **These values should be periodically reported to management to help keep the program functioning as expected**

Assurance Process Integration

- A security program should be aligned with other assurance processes and programs in an organization
  - Human resources
  - Finance
  - Legal
  - Audit
  - Enterprise risk management
  - Etc.

- The security manager should have relationships with the heads of these departments and develop procedures for protecting assets in each

Information Security Program Objectives

- There are a set of goals that all programs should target to achieve
  - Implement the selected strategy in the most cost-effective manner
  - Maximize support of business functions
  - Minimize operational disruptions

- These elements will depend heavily on work that should be done prior to this with selecting the proper governance and risk management objectives
  - The success of these previous steps will determine how well program objectives will be understood

Developing Objective Tasks

- If a security strategy is developed well, the next steps will be taking the abstract plan and making it concrete with initiatives and projects

- The security manager and staff must keep in mind that requirements, environments, business functions, etc. change frequently so strategies may have to undergo modifications
  - Another factor that could cause delays and/or changes is push-back from the users that will be affected by the security program

Developing Objective Tasks cont.

- **Another method that provides benefits is using system development life cycle (SDLC) approaches**
  - **This provides a formal process for bringing a security program to life**
  - **Drafting and editing this plan in a collaborative manner helps to minimize future implementation and operational problems**

Defining Objectives

- For most managers a security program will not be built from scratch
  - There job is to identify the current state of the program and identify the desired state
  - This is formally done by performing a gap analysis

- An additional exercise that should be done is to figure out the primary drivers for an ISP
  - Picking these drivers will help to clarify the objectives and assist in selecting correct metrics

Defining Objectives cont.

- With gaps in the program and the driving forces of the organization identified, the processes and projects to close the gaps can be developed
  - This includes selecting the necessary controls, implementing them, developing metrics, and monitoring control points in support of the objectives

Information Security Program Concepts

Domain 3: Information Security Program Development and Management

ISP Concepts

- When developing a security program the designers must stay aware that the fundamental outcome is to implement the strategy and achieve the desired outcomes

- If a strategy has not been established, then off the shelf objectives from defined standards or achieving a defined maturity level based on the CMMI model can be selected
  - CMMI is a process level improvement and appraisal program developed by Carnegie Mellon University
    - It is used to guide process improvement for projects, divisions, or entire organizations

ISP Concepts cont.

- Also if a strategy has not been selected, some specific controls such as those outlined in COBIT or the ISO 27000 family should be used
  - Much of a security program will depend on designing, developing and implementing controls
    - These controls can be technical, procedural or physical
  - The monitoring and metrics associated with this selected control are key items to ensure a successful outcome
    - Building methods to check control effectiveness and/or failure is also essential

ISP Concepts cont..

- **Concepts that will also play a role within a security program are:**
  - **Program management skills, resource utilization, budgeting, setting and meeting timelines and milestones, quality assurance, and user acceptance testing**

- **In the next slide is a list of concepts that a security manager may need to be aware of**
  - **This list is not exhaustive, but simply highlights the breadth of knowledge required**

ISP Concepts cont.

Architectures	Budgeting, costing and financial issues	Business case development	Business process reengineering	Communications
Compliance monitoring and enforcement	Contingency planning	Control design and development	Control implementation and testing	Control monitoring and metrics
Control objectives	Deployment and integration strategies	Documentation	Personnel issues	Problem resolution
Project management	Quality assurance	Requirements development	Risk management	SDLCs
	Specification development	Training needs assessments and approaches	Variance and noncompliance resolution	

Technology Resources

- **An ISM must have an awareness of the possible solutions available to solve problems**
  - **Basic prevention, detection, containment, reaction and recovery framework, etc.**
  - **The manager should also understand the interconnections between software components**

- **The following slides will present security related technology and broadly applicable technologies that will affect how a security plan is implemented**

Security Related Technologies

Antivirus systems	Application security methodologies	Authentication and authorization mechanisms	Backup and archiving approaches (RAID)	Cryptographic techniques
Data integrity controls	Data leak prevention methodologies	Digital signatures	Identity and access management systems	Firewalls
Intrusion Detection Systems (IDS)	Intrusion Prevention Systems (IPS)	Log collection, analysis, and correlation	Mobile computing	Mobile devices
Remote access methodologies	Security features for networking devices	Smart cards	Vulnerability scanning and penetration testing tools	Web security techniques
		Wireless security methodologies		

Broader Information Technology Concepts

Bring your own device (BYOD)	Cloud Computing	Databases	Enterprise architectures
Internet and network protocols	Local area networks (LANs)	Network routing concepts and protocols	Operating systems
Servers	Storage are networks (SANs)	Virtualization	Web-related technologies and architectures
Wide area networks (WANs)	Internet of things (IoT)	Application server	Middleware

Information Security Program Concepts Scope and Charter of IS Program

Domain 3: Information Security Program Development and Management

Organizational Expectations

- Whether an ISM is starting a new program or entering an existing one, they will be responsible for determining the scope, responsibilities, and charter for their department

- Without these details being set, it will be difficult to determine what to manage or how well the security functions are meeting objectives
  - A recommendation is for a security manager to spend significant time with management to understand and reach an agreement on expectations when the job is taken

Organizational Expectations cont.

- Another factor to outline is where in the organizational chain of command do the security functions fit
  - Structural conflicts could arise so these should be carefully considered as the program is being put in place
- Often ISMs are tasked to enforce internal regulations, but their effectiveness can be diminished if required to report to those who are being monitored
  - This design tends to limit the ability to enforce information security across the enterprise

Organizational Expectations cont..

- A security manager should also determine if all responsibilities of the department are clearly defined
  - Instances can arise where roles have been taken on by the previous manager, but no official documentation has been draft to support these activities
    - If the outgoing manger is available, this should be a targeted discussion to have

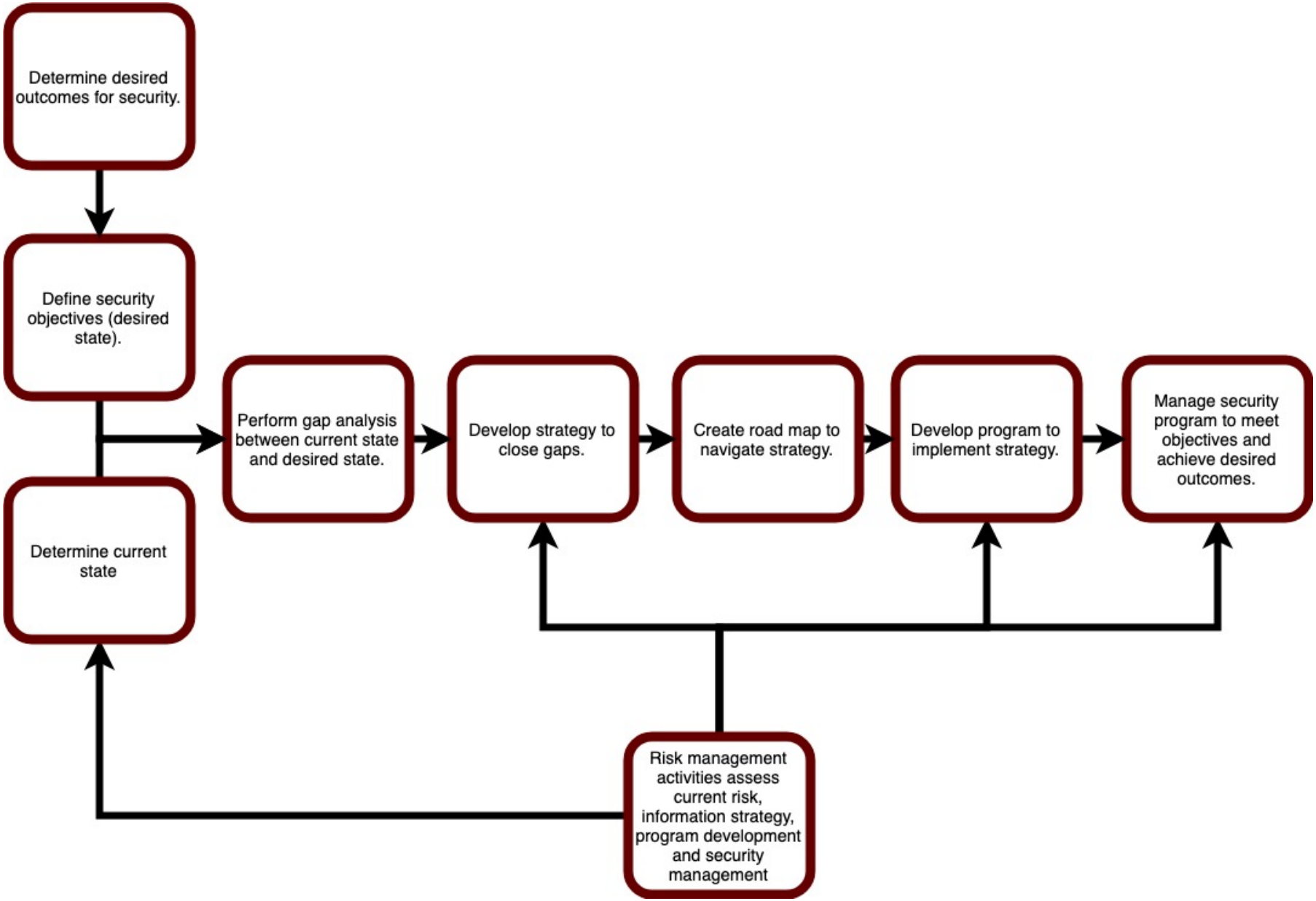
Activities for Getting Started

- Security can be a politically charged topic within an organization

- In some cases even more important than a manager's technical expertise will be the ability to gauge the culture of the organization and identify key relationships for being able to move the security program forward

Activities for Getting Started cont.

- An incoming ISM may also want to obtain the current status of the security program and security functions by performing their own risk assessment and business impact analysis (BIA)
  - Reviewing previously performed audits, incidents, or reports can also provide some much needed insight



Steps for Information Security Program Development

Scope

- An important step in the process of creating a security program is the definition of its scope
- Management should be thorough and determine the departments, business units, affiliates, and locations that are to be included in the program
  - This defines the boundaries and what organizational components are subject to the program's policies and governance
- Scope becomes very important in larger organizations where business units can operate independently of one another

Scope cont.

- Autonomous business units can still adhere to a single set of business policies, but adhere to them based on their own processes, personnel, and standards of the unit

- There is no wrong way to an ISP structure, the decisions should simply be made to maximize its benefit for the entire organization

Charter Development

- The scope of an ISP is established by the development of a strategy in combination with risk management responsibilities
  - The extend to which management supports the implementation of the strategy and risk management activities determines the charter

- For a manager coming into an organization with no strategy and no formal charter, industry standards and customize versions of ISACA's description of a mature information security program can be used

- **Example ISACA information security program description**

Information security is a joint responsibility of business, information security and IT management and is integrated with corporate business objectives. Information security requirements are clearly defined, optimized and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. Information security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organization wide.

Information Security Management Framework COBIT 5 ISO/IEC 270001:2013

Domain 3: Information Security Program Development and Management

What is an information security framework?

- A conceptual representation of an information security management structure

- There are several aspect that a framework should define
  - Technical, operational, managerial, administrative and educational components of the program
  - Organizational units and leadership responsibilities for each component
  - The control or management objective that each component should deliver
  - The interfaces and information flow among components
  - The tangle outputs of each component

What is an information security framework? Cont.

- Although various frameworks will achieve this in varying ways, a framework should describe the information security management components (e.g. roles, policies, standard operating procedures, management procedures, security architectures) and their interactions

Other Security Management Framework Outcomes

- In addition to long-term objectives and program structure, the ISM must also focus on short-term requirements
  - This includes determining the risk and mitigation options for addressing current organizational initiatives and projects
  - The manager must also make sure operations are conducted in a manner that are in alignment with policies and standards

Other Security Management Framework Outcomes cont.

- **Other than the direct outcomes addressed previously, the security manager must also make sure they are achieving the following soft outcomes**
  - **The program adds tactical and strategic value to the organization**
  - **The program is being operated efficiently and with concern to cost issues**
  - **Management has a clear understanding of information security drivers, activities, benefits and needs**
  - **Information security knowledge and capabilities are growing because of the program**
  - **The program foster cooperation and good will among business units**
  - **Program includes provisions for business continuity**

COBIT 5

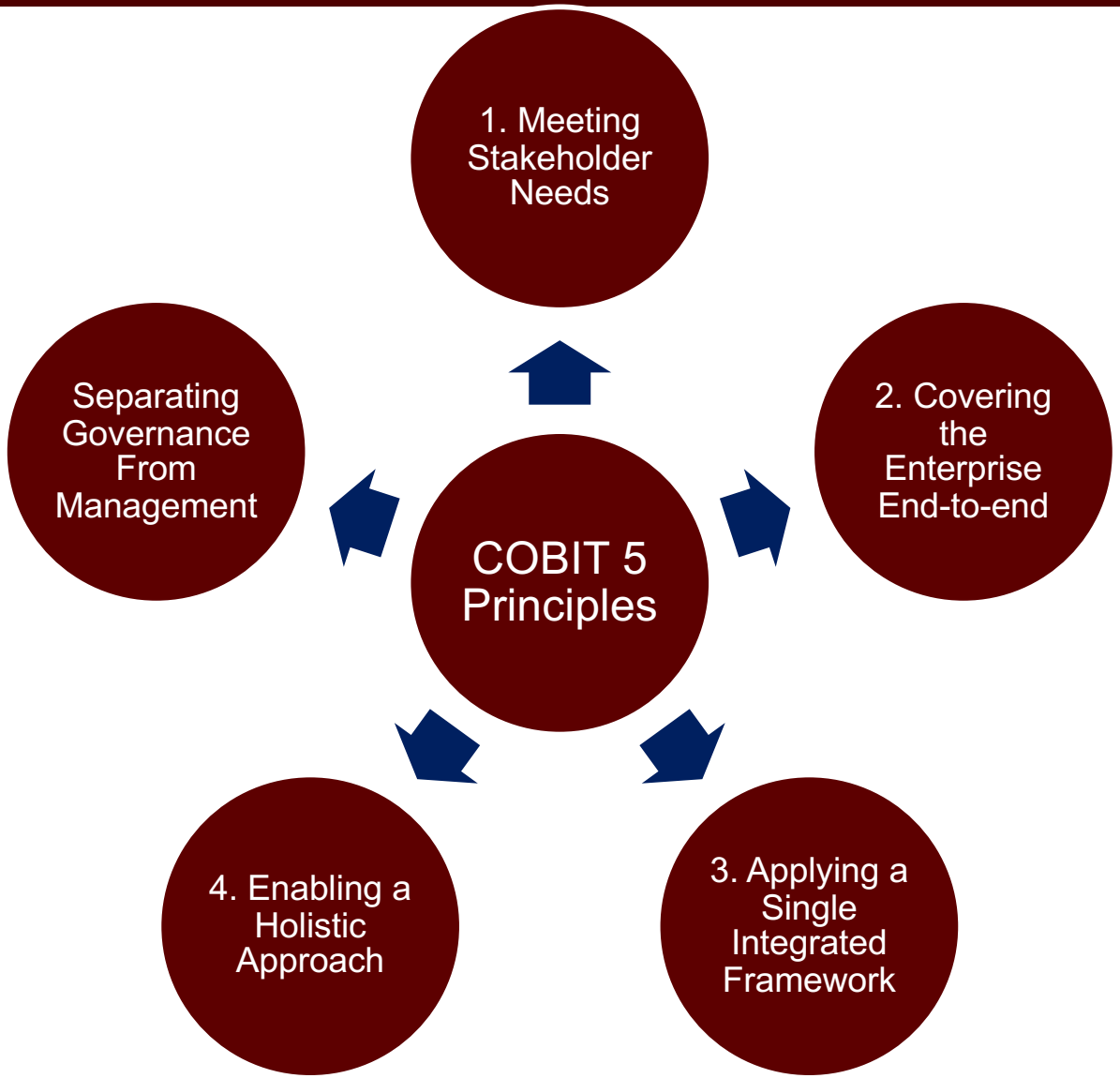
- **Developed by the Information System Audit and Control Association (ISACA)**

- **Provides a comprehensive framework that focuses on providing optimal value from IT by balancing between realizing benefits and optimizing risk levels and resource use**
  - **Allows IT and information security to be governed and managed in a holistic manner for the enterprise**
  - **Addresses business and IT functional areas of responsibility**

COBIT 5 cont.

- The *COBIT 5 for Information Security* resource provides tools to help implement and direct core information-security-related activities and make more informed decisions
  - Also helps IT and business leaders communicate and manage risk associated with information

COBIT 5 Principles



ISO/IEC 27001:2013

- "Information technology – Security techniques – Information security management systems – Requirements
  - Details the requirements and steps to take for running an information security management system (ISMS) within an organization

- International standard that provides a widely accepted framework and approach to information security management

ISO/IEC 27001:2013 cont.

- **Divided into two sections of requirements and controls**
  - **Requirements section describes required activities of an effective security program**
  - **Controls section gives the baseline set of controls that can serve as a starting point for an organization**
  - **Designed with 114 controls within 14 domains**

- **Although ISO/IEC is a highly respected control framework, it has experienced a modest adoption partly due to the $117 cost for the standard**
  - **It is growing in popularity around the world**

ISO/IEC 27001 Requirements Sections

Context of the organization	Leadership	Planning
Support	Operation	Performance evaluation
	Improvement	

ISO/IEC 27001 Control Categories

Information security policies	Organization of information security	Human resource security	Asset management
Access control	Cryptography	Physical and environmental security	Operations security
Communications security	System acquisition, development, and maintenance	Supplier relationships	Information security incident management
	Information security aspects of business continuity management	Compliance	

Information Security Framework Components

- For any management framework, there are five components that should be given the appropriate security consideration
  - Technical
  - Operational
  - Managerial
  - Administrative
  - Educational

Technical Framework Components

- **Information security is most likely involved with each technical IT component within an organization**
  - **Some of the involvement includes maintaining suitable security standards, reviewing of procedures for policy compliance, designing and implementing security metrics and other types of oversight activities**
- **A key activity that will occur within the framework for technical components is identifying the risk associated**
  - **This includes activities such as configuration, monitoring, maintenance, and operation for each component**

Technical Framework Components cont.

- An important point to highlight is that for systems within an organization, the owner of the system should be known and should be aware of the policies and standards that are necessary for their system to be compliant
  - IT normally either owns the system or acts as the custodian of other unit's systems and data
  - Making sure the owner is known helps to identify who has responsibility for proper treatment of risks to acceptable levels

Operational Framework Components

- **Operational components are administrative and management activities that are performed to provide the proper level of security assurance**
  - **Some of these include having a standard operating procedure (SOP) for how things in the organization are done**
  - **Establishing best practices that must be followed for different tasks**
  - **Periodically conducting maintenance and administration on security technologies**

- **These types of tasks are performed on a daily or weekly basis**

Operational Framework Components cont.

- One of the major roles of the security program and the security manager is to provide continued operational component support as environments and standards change
- Some operational activities are not in the direct control of the security manager and they must work with other business units and provide oversight to make sure these issues are addressed
  - The security manager should help to create schedules and tasks lists of activities that provide assurance that operations are meeting requirements and objectives

Example Operational Components

- **This list includes:**
  - Identity management and access control administration
  - Security event monitoring and analysis
  - System patching procedures and configuration management
  - Change control and/or release management processes
  - Security metrics collection and reporting
  - Maintenance of supplemental control technologies and program support technologies
  - Incident response, investigation and resolution
  - Retirement and sanitization of data processing equipment and media storage

Management Framework Components

- Other than the technical and operational components that a security manager must be aware, managerial activities include actions such as standards development or modification, policy reviews, and oversight of programs and/or initiatives

- These types of tasks tend to occur on the span of months, quarters, or years

Management Framework Components cont.

- Management objectives have a great impact on the overall success of a security program and defines what must be managed

- As the process is conducted the security manager must take in to account any legal, regulatory, risk and resource issues when making decisions
  - Defined metrics can also be used to support any necessary decisions

Management Framework Components cont..

- The manager will have to continue to refine and update policies as ongoing analysis of assets, threats, risk and organizational impact change
  - Early versions of policies tend to be too permissive, too restrictive or misaligned with operational realities so the the manager must be flexible as adjustments are made in the initial stages of a security program
  - Constant communication and receiving feedback from business units can help to expediate this process
- When developing management components for technical and operational activities, oversight reviews by executives and review boards should be conducted to make sure strategies are consistent with objectives

Administrative Framework Components

- As the resources, personnel and financial aspects of information security grows, so do the needs to manage these things from an administrative perspective
  - Major areas of focus are financial, HR and other management functions
- The activities associated with financial administration involve:
  - Budgeting, time line planning, total cost of ownership (TCO) analysis/management, return on investment analysis/management, acquisition/purchasing and inventory management

Administrative Framework Components cont.

- HR management functions include:
  - Job description management, organizational planning, recruitment and hiring, performance management, payroll and time tracking, employee education and development, and termination management
    - The ISP must take into account the time and resources necessary to perform such activities

- Almost no ISP tends to have an over abundance of resources, the executive steering committee and executive management should be consulted to determine which projects are most important

Administrative Framework Components cont..

- It is also not unusual for a security manager to receive pressure to divert resources allocated for daily operations

- The security manager should document and inform executives of the security risk associated with not performing full security diligence
  - Security operations resources should only be diverted to project efforts if they are not fully utilized

Educational and Information Framework Components

- Educational activities are normally integrated with employee orientation and initial training
- General organizational information such as acceptable use policies and employee monitoring policies are controlled and administered at the HR level
- Interactive educational techniques are normally more effective than purely informational training

Educational and Information Framework Components cont.

- The security manager should collaborate with HR and other business units to determine the best delivery methods for the overall organization

Defining an Information Security Program Road Map

Domain 3: Information Security Program Development and Management

ISP Road Map

- A roadmap is the implementation of an information security strategy
  - If a well organized strategy has been developed, then a high level roadmap to achieve these steps should also exist
- Taking a security program from a strategy to a concrete plan takes moving the logical architecture to a physical one through projects and initiatives
  - Tasks include: Project and initiative planning, budgeting, scheduling, identifying and hiring personnel, and other tactical aspects

Information Security Program Road Map cont.

- If a strategy has not been developed and risk management objectives are not clearly defined, the program runs the risk of being sub-optimal in its effectiveness and may have components that are not properly integrated

Developing a Roadmap

- Key to developing a program roadmap is being able to identify the security level of data, applications, systems, facilities, and processes in a company
  - Having this knowledge will have to develop specific project objectives
  - How to conduct security reviews will be discussed later in this domain

- A roadmap boils down to being a high-level project plan or architectural design
  - Either can be used to achieve the program objectives
  - These provide an overview of steps required and their sequence

Developing a Roadmap cont.

- **The roadmap will also provide milestones that will provide key goal indicators (KGI), key performance indicators (KPI), and define critical success factors (CSF)**

Basis for an Action Plan: Gap Analysis

- When the organizational roles and responsibilities have been identified and inventory of equipment has been taken, the security manager can then figure out where control objectives are not adequately supported by controls

- The manger should also have the staff in place to identify control points and create processes so that they are properly monitored

Basis for an Action Plan: Gap Analysis cont.

- It is key that the procedures for monitoring achievements of control objectives are established
  - Effectively performing this monitoring will provide the basis for the security program to evolve and mature

Information Security Infrastructure and Architecture

Domain 3: Information Security Program Development and Management

What is Infrastructure?

- Generally referred to as the base or foundation on which information systems are deployed
  - Includes computing platforms, networks and middleware layers, and it supports a wide range of applications
  - Infrastructure and security infrastructure refer to the same thing

- When infrastructure is designed and implemented according the appropriate policies and standards, it should, essentially, be secure

Enterprise Architecture (EA)

- **(EA) is both a business function and a technical model**
  - **Consists of activities that ensure that important business needs are met by IT systems**
  - **Used to map business functions into the IT environment and IT systems in increasing levels of detail**

Focus of Enterprise Architecture

- **The purpose of enterprise architecture and enterprise security architecture ensures that:**
  - **All hardware and software components fulfill a stated specific business purpose**
  - **All components work well together**
  - **There is overall structure and consistency in infrastructure throughout the organization**
  - **Infrastructure resources are used efficiently**
  - **Infrastructure is scalable and flexible**
  - **Existing elements can be upgraded as needed**
  - **Additional elements can be added as needed**

Focus of Enterprise Architecture cont.

- There are several ways to represent the information, but they tend to fall into three basic categories:
  - Frameworks
    - Provides flexibility in how each element of the architecture is developed
    - Goal is to show how elements in the framework relate to one another
  - Process approaches
    - Clearly outlines the processes performed by the various elements
  - Reference models
    - Provide a small representation of an actual implementation

Common EA Frameworks

- **Two EA Frameworks will be discussed in detail here:**
  - **The Open Group Architecture Framework (TOGAF)**
  - **Zachman Framework**

- **An important distinction is not to confuse enterprise architecture models with security architecture models**
  - **EAs focus on ensuring that business needs are met by IT systems**
  - **Security architectures focus on the interplay between security controls to effectively protect information systems**

The Open Group Architecture Framework (TOGAF)

- **Life-cycle EA framework used for designing, planning, implementing, and governing an enterprise technology architecture**
  - **Could be considered a high level approach for designing enterprise infrastructure**

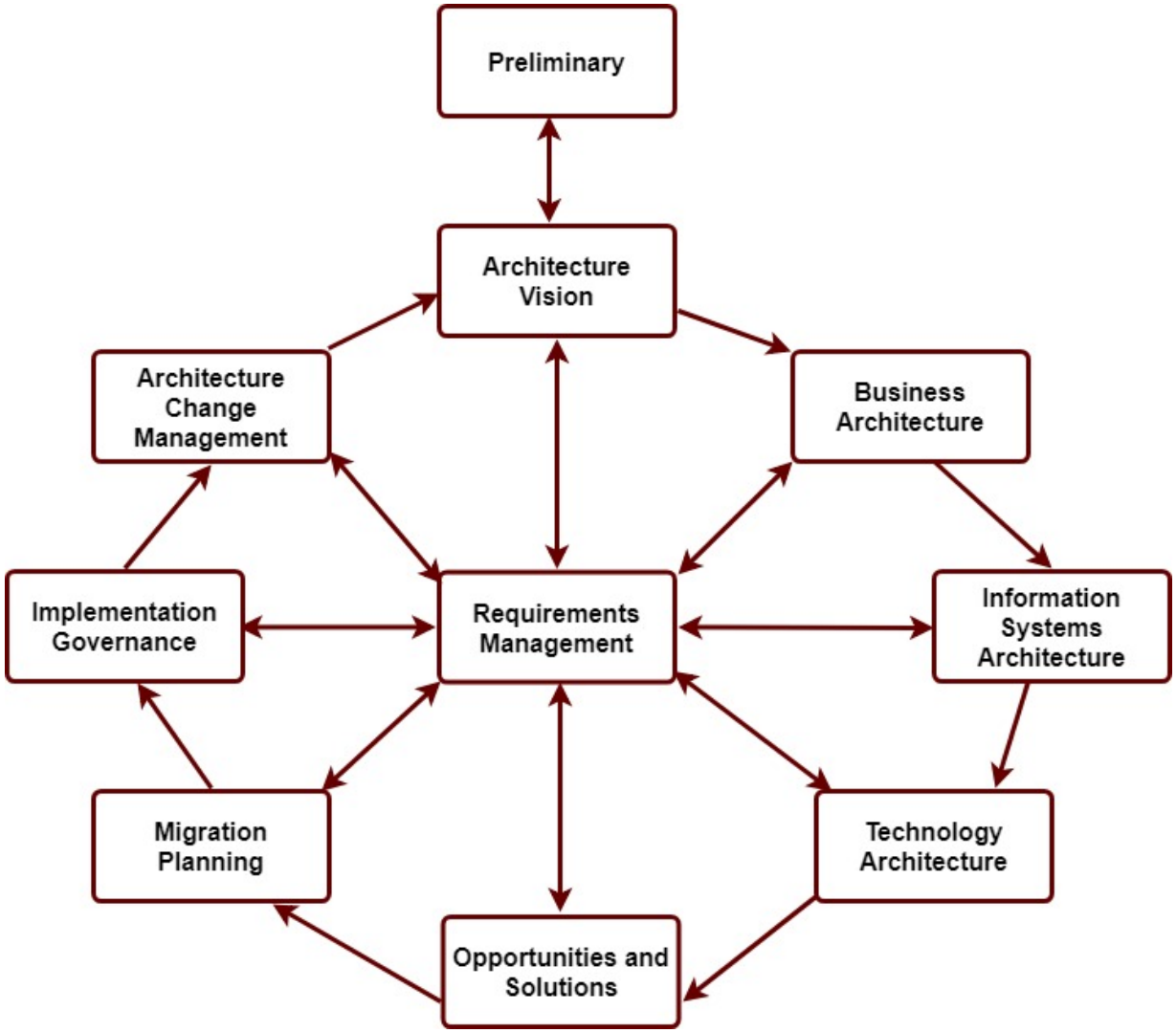
- **The phases of TOGAF are:**
  - **Preliminary, Architecture vision, Business architecture, Information systems architecture, Technology architecture, Opportunities and solutions, Migration planning, Implementation governance, Architecture change management, Requirements management**

The Open Group Architecture Framework (TOGAF) cont.

- TOGAF is a business-driven life-cycle framework that can be used for information security architecture

- Additional TOGAF related sources can be found below
  - https://www.opengroup.org/togaf

TOGAF Diagram



TOGAF Phases Summary

- **Preliminary phase**
  - Outlines definitions and principles of the architecture
  - Also includes information about scope, objectives, and assumptions for the project
- **Architecture vision**
  - Defines the segments of work that must be done to achieve the vision and architecture of the project
- **Business architecture**
  - Provides a description of the current state of the business architecture, defines the desired state, and performs gap analysis on the two

TOGAF Phases Summary cont.

- **Information systems architecture**
  - Provides a description of the current state of the information systems architecture, defines the desired state, and performs gap analysis on the two
- **Technology architecture**
  - Provides a description of the current state of the technology architecture, defines the desired state, and performs gap analysis on the two
- **Opportunities and solutions**
  - Formulates the high-level implementation and migration strategies that will move architectures from the current state to the desired state

TOGAF Phases Summary cont..

- **Migration planning**
  - Formulates the detailed plan for migrating architectures from the current state to the desired state
    - This includes any costs considerations plus benefits and risk
- **Implementation governance**
  - Confirms that all implementation strategies conform to the defined architecture
- **Architecture change management**
  - Highlights methods for keeping the architecture up to date and ensuring it is flexible to deal with changing enterprise needs

TOGAF Phases Summary cont…

- **Requirements management**
  - **Ensures the architecture projects are based on business requirements that business requirements are validated against the architecture**

Zachman Framework

- Enterprise architecture framework created in the 1980s and is still heavily used
- This framework can easily be used to develop an enterprise security architecture
  - It has the flexibility to include other required plans, standards, maintenance methods, etc.
- In the framework IT systems and environments are described at a high, functional level and then in increasing detail
  - This can include encompassing systems, databases, applications, networks, etc.

Zachman Framework cont.

- Although details of systems can be expressed here, the Zachman framework does lack in displaying the relationships between systems

- Additional information is available at https://www.zachman.com/about-the-zachman-framework

	Data	Functional (Application)	Network (Technology)	People (Organization)	Time	Strategy
Scope	List of data sets important in the business	List of business processes	List of business locations	List of organizations	List of events	List of business goals and strategy
Enterprise Model	Conceptual data/object model	Business process model	Business logistics	Workflow	Master schedule	Business plan
Systems Model	Logical data model	System architecture	Detailed system architecture	Human interface architecture	Processing structure	Business rule model
Technology Model	Physical data/class model	Technology design	Technology architecture	Presentation architecture	Control structure	Rule design
Detailed Representation	Data definition	Program	Network architecture	Security architecture	Time definition	Rule speculation
Function Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Zachman Framework Table

Enterprise Architecture Domains

- **Four commonly accepted overall enterprise architecture subset exist**
  - **Business architecture**
    - **Business strategy, governance, organization and key business processes**
  - **Data architecture**
    - **Structure of an organization's logical and physical data assets and data management resources**
  - **Application architecture**
    - **Blueprint for the individual application systems to be deployed and how they interact with core business processes**

Enterprise Architecture Domains

- **Technology architecture**
  - **The architectural principles, component relationships, and hardware and software infrastructure intended to support the development of core, mission-critical applications**

- **Regardless of architectural design approach, an effective solution starts by aligning with the enterprise business architecture**

Objectives of Information Security Architectures

- **Architecture can be used as a tool to help manage complexity**
  - **Using architecture in this way can help a project that has many designers and design influences appear to be created by a single design authority**

- **Architecture can be used as a road map**
  - **Architecture can help to organize small projects and servers that will be integrated together**

Objectives of Information Security Architectures cont.

- **Architecture can be used for simplicity and clarity**
  - **Provides the rules and standards for the design and construction of computers, communications networks, and distributed business systems that delivery business services**
  - **Use to take care of the following details**
    - **The goals that are to be achieved through the systems**
    - **The environment in which the systems will be built and used**
    - **The technical capabilities of the people to construct and operate the systems and their component subsystems**

Objectives of Information Security Architectures cont.

- **Architecture can provide a view outside of just the technical domain**
  - **This type of architecture focuses on the overall goals that an enterprise wants to achieve based on the environmental factors that must be dealt with**
- **Architecture can ease the development of control objectives**
  - **System architects can use combinations of technologies to provide control points in a system infrastructure**
  - **Designing systems with security constraints in mind can help to ensure that future additions will also follow the standards intended in the first place**

Architecture Implementation

Domain 3: Information Security Program Development and Management

Architecture Implementation

- Some organizations have the experience level with technologies that architecture designs are elevated to the policy level
  - Combinations of technologies are mandated based on their intended use cases
- In some cases this is done because certain combinations provide easy implementation of security features that accomplish desired controls

Architecture Implementation cont.

- Common architectural policy domains include:
  - Database management systems
  - Telecommunications
  - Web application access

- Few organizations have created a comprehensive security architecture, determined how to manage it, and have clearly defined how it relates to the organizations business objectives
  - This is analogous to designing the parts of a machine and not testing how the components work together before sending it to market

Architecture Implementation cont.

- These needs highlight the benefits that frameworks such as COBIT and ISO/IEC 207001:2013 can provide when dealing with a variety of standards and methods

Security Program Management and Administrative Activities

Domain 3: Information Security Program Development and Management

What is Management?

- Defined as the process of achieving the objectives of the organization by effectively using personnel, financial, and physical resources with processes and technology for making decisions in the context of the operating environment

- Multifaceted process that requires an understanding of a number of different parameters to be done efficiently

Security Program Management

- Security programs often have a variety of projects and initiatives that require both day-to-day and long term planning
- Security program management will also include activities for risk management, incident management and response functions, as well was other administrative oversight and monitoring functions
- A key aspect that must not remain static and adapt with other aspects of information security to be effective is governance

Responsibilities in Program Management

- The security manager must ensure that the outcomes for the security program are achieved in a cost-effective manner
  - These should be specifically outlined when creating the program structure
- Another role that a security manager can have is a facilitator
  - Help resolve competing objectives between security and performance
  - This role can help to work with other departments and highlight solutions that minimizes risk while also minimizing effects on business operations
  - This role allows a security manager to stay informed on business activities and help to manage the security program

Responsibilities in Program Management cont.

- Senior management is responsible for supporting the objectives outlined by the security manager and providing the resources and authority to ensure all tasks are completed
  - Any other services provided should also be clearly defined and documented to prevent any type of gaps in protection

- Because the roles and tasks for an ISM are always expanding, they may consider using checklists of important operations to make sure no items are neglected

Security Program Administration

- As with other business units, there will be a series of repetitive functions required to be performed periodically

- Example tasks that may be necessary are listed on the following slides

Security Program Administration cont.

- **Periodic Administrative Tasks**
  - Personnel performance, time tracking and other record keeping
  - Resource utilization
  - Purchasing and/or acquisition
  - Inventory management
  - Project monitoring and tracking
  - Awareness program development
  - Budgeting, financial management and asset control
  - Business case development and financial analysis
  - HR administration and personnel management
  - Project and program management
  - Etc.

Security Program Administration cont..

- **Periodic Technical Administrative Tasks**
  - Cryptographic key management
  - Log reviews and monitoring
  - Change request review and oversight
  - Configuration, patch, and other life cycle management reviews and oversight
  - Vulnerability scanning
  - Threat monitoring
  - Compliance monitoring
  - Penetration testing

Personnel, Roles, Skills and Culture

- The ISM is tasked with understanding the requirements associated with their security program and allocated personnel resources
  - This requires hiring employees with an array of skillsets to meet needs
  - For smaller organizations this may mean seeking candidates that can cover multiple positions

- Where skills that are rarely required are needed, this may be a sign to pursue external providers
  - The manager must weigh the costs/benefits of hiring temporary outside help vs attempting to train or hire full-time personnel

Role

- **Designation assigned to an individual by virtue of job function or other label**
  - **It is a description of the procedure or function that a person is responsible for performing**
- **Designating roles is good for information security**
  - **Allows responsibilities and access rights to be given to a role and not an individual**
  - **Roles can be assigned to staff during the HR process and can streamline activities**
  - **Changes can be made to a role and not to each employee that has that given role**

Skills

- Training, expertise and experience held by the personnel in a given job function
- The abilities of available personnel should map to the competencies required for program implementation
  - Skills can be acquired via training or by utilizing external resources
- As the required skills for certain personnel are identified, formal employee agreements should be established that reference the jobs responsibilities
  - Candidates can then be screened accordingly

Culture

- Organizational behavior, methods for navigating and influencing the organization's formal and informal structures to get work done, attitudes, norms, level of teamwork, existence or lack of turf issues, and geographic dispersion
- Elements that affect culture include:
  - Backgrounds, work ethics, values, past experiences, individual filters/blind spots and perception of life that are brought into the work place
  - Each organization has a culture, whether specifically designed or whether it grows naturally over time

Culture cont.

- Can drastically impact the acceptance of a security plan or affect the relationships necessary to build the program
- Each employee in the company should be able to articulate how information security affects them and their work
  - Security managers must make sure the proper communications and training are in place to highlight why the security requirements benefit each role within the organization

Culture cont..

- **Signs of positive outcomes include:**
  - **The information security department is brought into projects at the appropriate times**
  - **End users know how to identify and report incidents**
  - **The organization can identify the security manager**
  - **People know their role in protecting the information assets of the organization and integrating information security into their daily practices**

Security Awareness Training and Education

- Risk associated with operating information systems cannot be purely handled by with technical solutions
- The behavioral element of security can be addressed through an active security awareness program
  - Focuses on common concerns such as passwords, emails and web usage, appropriate system usage, social engineering attacks, etc.
- Employees should also receive catered training depending on their job role for how information security relates to their day-to-day activities

Security Awareness Training and Education cont.

- **Training of employees should start when joining the organization and continue periodically**
  - **The method for training should also be diversified to prevent the message from become stale**
  - **Can/should include some variety of online training, quizzes, security awareness reminders (posters, emails, screen savers, etc.) and regularly scheduled refresher training**

Security Awareness Training and Education cont..

- **The security manager should do the following when constructing training material:**
  - **Identify the intended audience (Senior management, end users, etc.**
  - **Craft the central idea of the content (Recent events, policies, etc.**
  - **Understand the desired result (Better practices, policy compliance, etc.**
  - **How will the information be presented? (Computer-based training, formal presentation, newsletter, etc.)**

Mechanisms for Raising Security Awareness

- Computer-based security training
- Email reminders and security tips
- Written security policies and procedures
- Nondisclosure statement signed by the employee
- Visible enforcement of security rules
- Simulated security incidents for improving security
- Rewarding employees who report suspicious events
- Job descriptions
- Performance reviews

General Rules of Use/Acceptable Use

- A summary of the activities that can and cannot be performed by employees with organizational systems
- Explains the obligations and responsibilities of all users in everyday terms
- Policy should be displayed in places where it can easily seen.
  - E.g. During system login
- Provides a general security baseline for the entire organization

Ethics

- Many organizations have created ethics training to train employees on what is seen as legal and appropriate behavior
- Common when employees are required to interact with data that may be considered sensitive
  - Monitoring user activities, performing penetration tests, using personal data
- Security personnel must especially be sensitive when possible conflicts of interests arise in the organization

Ethics cont.

- It is also common to have security personnel sign a Code Ethics and Conduct document which is saved in their personnel file

Documentation

- **Keeping security documentation maintained and up-to-date is a key administrative function of a security program**
  - **Policies, standards, procedures and guidelines**
  - **Technical diagrams of infrastructure and architectures, applications, and data flow**
  - **Training and awareness documentation**
  - **Risk analyses, recommendations and related documentation**
  - **Security system designs, configuration policies and maintenance documentation**
  - **Operational records such as shift reports and incident tracking reports**
  - **Etc.**

Documentation Responsibilities

- Individual personnel should be assigned documents or document templates to keep updated
  - Recommendation on what changes should be made are provided by executive committees or management
  - The owner of the document should make sure the document is appropriately available and auditable
- The security manager should ensure that technical documents are properly secured and labeled according to organizational standards
  - This can be difficult when developing a new security program due to required adjustments and changes

Documentation Responsibilities cont.

- An essential tool to ensure all users are working from the appropriate versions of a document is to use version control software

Documentation Maintenance

- As the security program grows and evolves, the security manager should implement procedures for adding, modifying, and eventually retiring security policies, standards, procedures and other documentation
  - Automated tools can be used that provide only the most up-to-date version of documents to help avoid confusion
  - As changes are made to policies and standards it must be ensured that technical mechanisms reflect the changes
    - This can also trigger changes in documents such as guidelines, acceptable use policies, etc.

Program Development and Project Management

- A security program cannot remain static to keep up with the changing conditions and risks of an organization
  - It must reach its defined objectives and take the steps necessary to identify how to get to that desired state
    - This is done by using Gap Analysis and outlines the projects that need to be performed to reach the desired objectives
    - Many changes will include the implementation of technical solutions or their reconfiguration to make them more secure
    - Each project should have a designated timeframe, budget, and measurable results
      - It should also make the environment more secure without introducing additional weaknesses

Program Development and Project Management cont.

- The security manager must prioritize projects so that those that overlaps do not delay one another, resources are allocated efficiently, and new operations are smoothly integrated or old operations are phased out

- This should be done by using proven project management techniques
  - Goals, tracking deadlines, and assigning responsibilities in a controlled and repeatable manner

Risk Management

- **Virtually all components of program management function to reduce risk to acceptable levels**
  - **The information security unit within an organization is required to ensure the business is capable of dealing with changing risk conditions**

- **The reality is that no matter how diligent an information security unit is, there is no way to avoid having a security incident**
  - **What the unit can control is an effective response to what occurs**

Risk Management Responsibilities

- **A security manager must have a good understanding and develop the requisite skills regarding evaluation and management of risk. This includes:**
  - **Knowledge of program development life cycle risk**
  - **Knowledge of program management risk**
  - **Knowledge of methods for assessing the vulnerabilities in technical and operational environments**
  - **Ability to analyze exposures, the general threat environment and threats specific to the information security manager's organization**
  - **Knowledge of risk analysis approaches including quantitative and qualitative methods**
  - **Etc.**

Business Case Development

- In building an ISP, the most successful projects will have a direct business impact
  - Articulating these impacts to the steering committee or management is key to securing approval and funding
- The value provided if the project is performed and the risk introduced if the project is not performed must be clearly identified and stated
- The business case should show a clear return on potential investment and show the feasibility of the project

Program Budgeting

- Budgeting is a key component of managing an ISP
- The proper preparation and defense of a budget can be the difference between being able to complete projects and not have sufficient staff to complete needed tasks
- Before a budgeting cycle begins, a security manager should conduct self-education and become aware of how these financial processes are conducted within the organization

Program Budgeting cont.

- All line items for a budget associated with an information security program should support a defined strategy
  - This helps to show rational for expenditures and is key to a successful budget proposal

Elements of an ISP Budget

- There are sections of an information security program budget that are no-brainers
  - E.g. Salaries, basic hardware, subscriptions to services
  - Operating, start-up, and short-term and long-term costs also show be accurately accounted

- The security manager should utilize the project management office (PMO) and the appropriate subject matter experts to help estimate expenses for the the upcoming fiscal year

Elements of an Information Security Program Budget cont.

- **Elements of each project that should be included:**
  - Employee time
  - Contractor and consultant fees
  - Equipment (hardware, software) costs
  - Space requirements (data center rack space, etc.)
  - Testing resources (personnel, system time, etc.)
  - Training costs (staff, users, etc.)
  - Travel
  - Creation of supporting documentation
  - Ongoing maintenance
  - Contingencies for unexpected costs

Elements of an Information Security Program Budget cont..

- Expenses outside of normal costs could be addressing incident response activities within an organization
  - Historical data can be used to estimate incidents and remediation costs of previous security events that required unbudgeted external resources

- The average cost of previous years can be used as a baseline for creating a budget

IS Problem Management Practices

- **The security manager will encounter and have to resolve both crisis or event management situations**
  - **Being able to handle such problems effectively is a skill that is very important while running a security program**

- **Problem management involve a very systematic approach**
  - **Identifying the root issues of a situation**
  - **Defining the problem**
  - **Designing an action plan**
  - **Assigning responsibility for problem resolution**
  - **Selecting due dates for the problem to be addressed**

IS Problem Management Practices cont.

- As a security program grows and changes it is not uncommon for security controls in place to occasionally present unexpected problems
  - When such events happen, it is the job of the security manager to effectively resolve the issue

- The manager should also be aware of alternative controls if a primary control is experiencing a problem
  - This will help to prevent placing the entire organization at risk while working to solve primary control problem
  - With these options, clear guidelines for the security manager's authority must be set by management to avoid any alternative actions that could affect business operations

Vendor Management

- A security manager has the responsibility of monitoring the external providers of hardware and software, general supplies, and various services
  - The goal is to understand any risk that the provider introduces into processes and to make sure that it is handled accordingly
  - There can also be other business units that will be involved in aspects vendor management
    - Legal, finance, procurement, etc.

- Among the vendors that must be managed could be security vendors that can provide access to specialized skills that the security manager may need

Vendor Management cont.

- The security vendors can provide services that help to free resources that the security manger may need for projects or operations where the specialized skills of personnel can be better utilized

- If the security manager can handle risk such as financial viability, quality of service, adequate staffing, and adherence to organizational policies presented by the external vendors, then they can provide significant benefits

Program Management Evaluation

- **Periodically there will be a need to reevaluate how a security program is operating**
  - **This can provide the ability to identify deficiencies and correct them or highlight strengths and continue to make strides forward**

- **There will inevitably be changes that are needed just because of shifting environments, organizational demands, and constraints**
  - **Any elements that are identified as change candidates should be shared with the steering committee or higher management**

Program Management Evaluation cont.

- When performing an evaluation there are several key aspects that should be studied:
  - Program Objectives
  - Compliance Requirements
  - Program Management
  - Security Operations Management
  - Technical Security Management
  - Resource Levels

Evaluating Program Objectives

- The documented security objectives established for the program must be reviewed
- Questions to consider
  - Has the information security strategy and development road map been developed?
  - Have criteria for acceptable risk and impact been determined?
  - Do complete and current policies, standards and procedures exist?
  - Are program goals aligned with governance objectives?
  - Are objectives measurable, realistic and associated with specific timelines?
  - Do program objectives align with organization goals, initiatives, compliance needs and the operating environment?

Evaluating Compliance Requirements

- A security program should be clearly aligned with any compliance standards that must be followed
- The following aspects should be considered:
  - Has management determined the level of compliance the organization will undertake as well as the timelines and milestones?
  - Is there facilitation of close communication between compliance and information security groups? Are information security compliance requirements clearly defined?
  - Does the ISP specifically integrate compliance requirements into policies, standards, procedures, operations and success metrics?

Evaluating Compliance Requirements cont.

- **The following aspects should be considered:**
  - **Do the program's technical, operational and managerial components align with the components required by regulatory standards?**
  - **What have been the results of recent audit and compliance reviews of the information security program?**
  - **Are program compliance deficiencies tracked, reported and addressed timely?**
  - **Are compliance management technologies used to increase the efficiency of fulfilling security compliance demands?**

Evaluating Program Management

- **Evaluating these components display the amount of management support and the depth of a security program**
  - **Technical programs tend to have few management components implemented**
  - **Strategic programs take a more comprehensive approach to ensure that requirements are established and fulfilled**

Evaluating Program Management cont.

- **Things to consider:**
  - Is there thorough documentation of the program itself? Have key policies, standards and procedures been reduced to accessible operating guidelines and distributed to responsible parties?
  - Do responsible individuals understand their roles and responsibilities?
  - Are roles and responsibilities defined for members of senior management , boards, etc.? Do these organizations understand and engage in their responsibilities?
  - Are responsibilities for information security represented in business managers' individual objectives and part of the individual performance rating?

Evaluating Program Management cont..

- **Things to consider:**
  - **Are policies and standards complete, formally approved and distributed?**
  - **Are business unit managers involved in guiding and supporting information security program activities? Is there a formal steering committee?**
  - **How is the program positioned within the organization? To whom is the program accountable? Does this positioning impart an appropriate level of authority and visibility for the objectives that the program must fulfill?**
  - **Does the program implement effective administration functions (e.g. budgeting, financial management, HR management, knowledge management)?**
  - **Are meaningful metrics used to evaluate program performance?**

Evaluating Program Management cont..

- **Things to consider:**
  - **Are there forums and mechanisms for regular management oversight of program activities? Does management regularly reassess program effectiveness?**

Evaluating Security Operations Management

- The methods in which the security program implements security operational activities both within the organization and in other organizational units must be evaluated
- Things to consider:
  - Are security requirements and processes included in security, technology and business unit standard operating procedures (SOPs)?
  - Do security-related SOPs provide for accountability, process visibility and management oversight?
  - Are there documented SOPs for security-related activities such as configuration management, access management security systems maintenance, event analysis and incident response?

Evaluating Security Operations Management cont.

- **Things to consider:**
  - Is there a schedule of regularly performed procedures (E.g. Technical configuration review)? Does the program provide for records of scheduled activities?
  - Is there segregation of duties (SoD) among system implementers, security administrators and compliance personnel?
  - Does the program provide for effective operation, tactical and strategic metrics reporting that provides management with needed information for oversight? Are other oversight mechanisms in place?
  - Does management regularly review security operations? Is there a forum for operational issues to be escalated to management for resolution?

Evaluating Technical Security Management

- **Implemented security mechanisms are critical aspects of a security program that must be reviewed**
- **For managing technical controls a security manager should consider the following:**
  - **Are there technical standards for the security configuration of individual network, system, application and other technology components?**
  - **Do standards exist that address architectural security issues such as topology, communication protocols and compartmentalization of critical systems?**

Evaluating Technical Security Management

- **For managing technical controls a security manager should consider the following:**
  - **Do standards support and enforce high-level policies and requirements? Are standards a collaborative effort among technology, operations and security staff?**
  - **Are technical standards uniformly implemented? Do procedures exist to regularly evaluate and report on compliance with technical standards? Is there a formal process to manage exceptions?**
  - **Is there continuous monitoring of key controls? Do controls provide notification on failure?**
  - **Is separation of development, test and production environment enforced?**
  - **Do systems enforce SoD, especially where high levels of administrative access are concerned?**

Evaluating Technical Security Management

- **For managing technical controls a security manager should consider the following:**
  - **Is there reliable and comprehensive visibility (logging) into system activities, configurations, accessibility and security-related events? Is this visibility continual or intermittent?**
  - **Are proper decommissioning processes in place to prevent data leakage?**

Evaluating Resource Levels

- The financial, human and technical resources allocated to a program must be evaluated
  - Any problem areas must be highlighted and passed on to senior management and/or steering committee
- Financial considerations:
  - What is the current funding level?
  - Is a comprehensive capital and operating budget maintained?
  - Do financial allocations align with program budget expectations?
  - Are there linkages between resource allocation and business objectives?
  - Are functions within the program prioritized in terms of financial allocation?

Evaluating Resource Levels cont.

- **Financial considerations:**
  - Which functions are likely to suffer from underfunding?
- **HR considerations:**
  - Does the program implement a workload management methodology?
  - What is the current staffing level for the program?
  - Are existing resources fully utilized in terms of time and skills?
  - Are existing resources adequately skilled for the roles they are in?
  - Are there low-value tasks that other resources could be leveraged to complete?
  - What other human resources (e.g. IT staff) is the program dependent on to operate effectively?

Evaluating Resource Levels cont.

- **HR considerations:**
  - Is information security a formal part of the resources' job descriptions and activity plans?
- **Technical considerations:**
  - What technologies currently support information security program objectives?
  - Is the capacity of supporting technologies sufficient to support current demands? Will these technologies scale to meet future needs?
  - Does the program account for maintenance, administration and eventual replacement of supporting technologies?
  - Are there other technologies that could make the program more efficient or effective?

Total Quality Management (TQM)

- Security programs are based on the effective and efficient management of controls that are designed and implemented to solve the following types of problems:
  - Risk, threats, vulnerabilities, etc.
- TQM and governance methodology can help provide a security manager with the tools necessary to implement and maintain a highly effective program
  - TQM is made up of four primary processes, plan-do-check-act (PDCA)

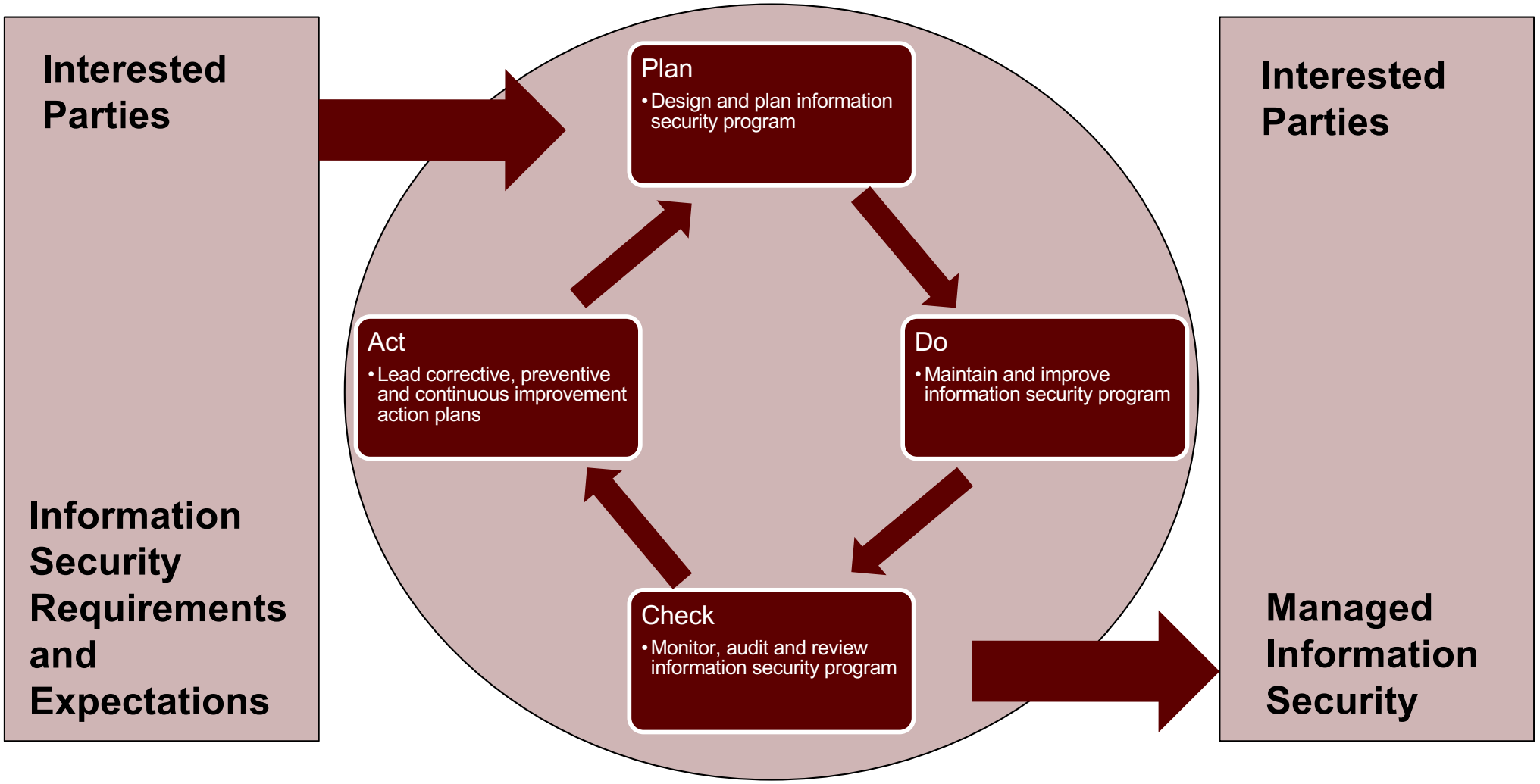
PDCA (Plan Do Check Act)

- **Plan**
  - Design, plan and initiate the information security program. These activities include creating a strategy; socialization concepts; and policies, goals, objectives and practices as necessary to manage risk

- **Do**
  - Execute and control the information security strategy include the integration into organizational practices

PDCA

- **Check**
  - Facilitate semi-annual audits to determine conformance to the statement of applicability and identify opportunities for improvement. Where applicable, create performance matrices to support information security program goals and objectives
- **Act**
  - Upon the discovery of nonconformities and/or opportunities, create and track corrective, preventive and continuous improvement action plans.
  - Show finding from internal/external audits and risk assessments to the management review committee for decisions regarding the acceptance, rejection or transfer of risk and the commitment of resources and capital to facilitate those efforts



PDCA Methodology

Governance Methodology

- **Basic element of a governance methodology include:**
  - **Strategic vision**
  - **Objectives**
  - **Key Goal Indicators (KGIs)**
  - **Critical Success Factors (CSFs)**
  - **Key Progress Indicators (KPIs)**
  - **Created action plans**

Governance Methodology Terms

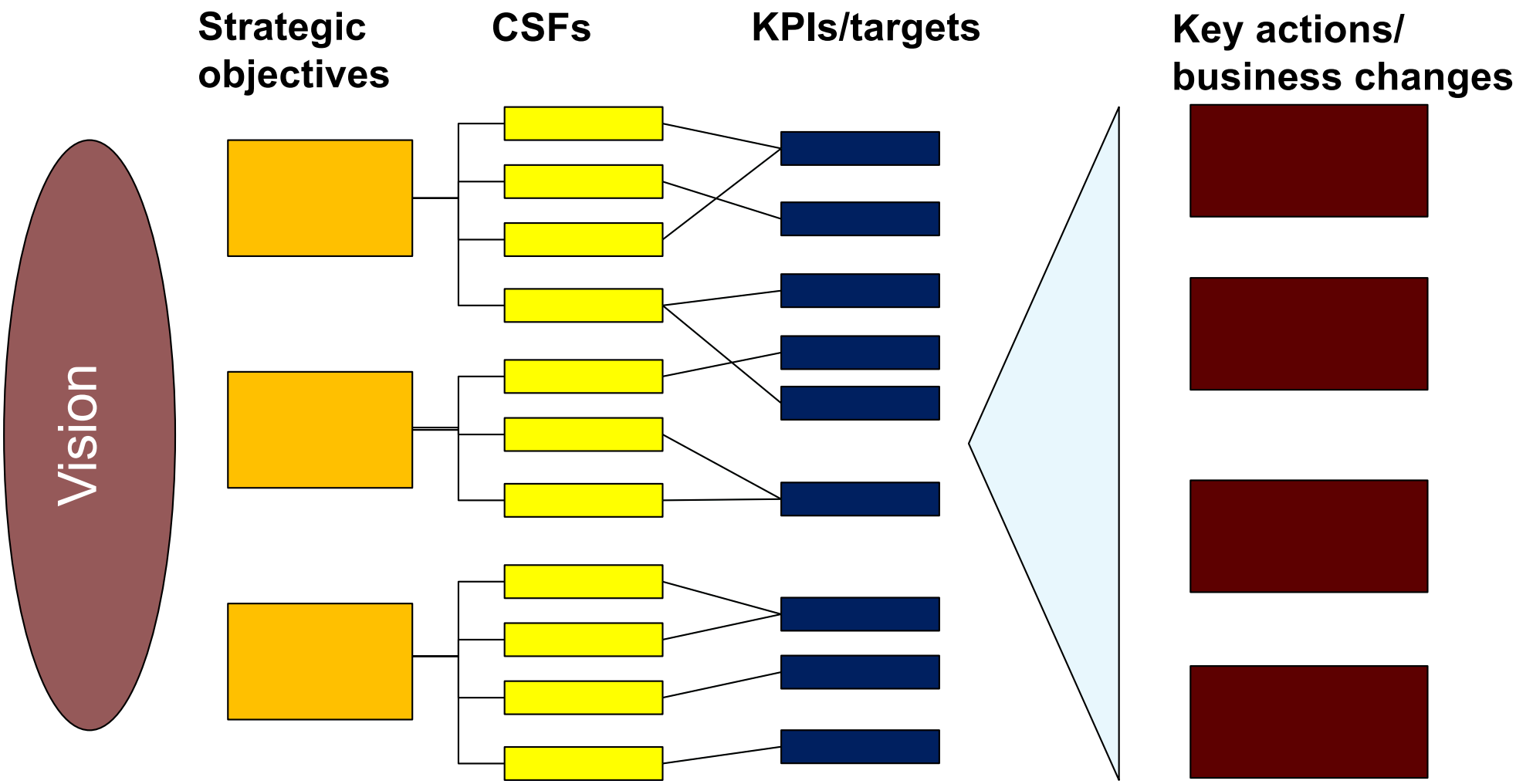
- **Vision**
  - Broadly defined as a clear and compelling statement about the organization's purpose.
  - This should include the desired outcomes of the information security program
- **Strategic objectives**
  - Set of goals that are necessary and sufficient to move the organization toward its vision
    - Reflected in KGIs
- **CSFs**
  - Set of circumstances or events that are necessary to achieve the strategic objectives

Governance Methodology Terms cont.

- **KPIs**
  - **Concrete metrics tracked to ensure that the CSFs are being achieved**

- **Key actions, including tactical and annual action plans**
  - **Initiatives to be delivered to achieve the strategic objectives and KGIs**

Strategic Objectives, CSFs, KPIs, Key Actions



Legal and Regulatory Requirements

- Corporate legal departments often have a number of issues to focus on such as contracts and securities or stock-related matters
  - They may not be accustom to possible regulatory requirements and the ISM should not rely on the department to identify them
  - Often those most closely affected by regulation will be most knowledgeable

- The ISM can request assistance with the interpretation of legal requirements for clarity and to understand the organizations position on the matter

Legal and Regulatory Requirements cont.

- An ISM may also be asked to assist the legal department in cases where legal standards related to privacy of information and transactions, the collection and handling of audit records, email retention policies, incident investigation procedures, and cooperation with legal authorities arise

- Careful consideration should be taken when monitoring employees for improper conduct, legal and regulatory standards can vary and so HR and the legal department should be consulted

Physical and Environmental Factors

- **Confidentiality, integrity and availability can be threated when unauthorized physical access and damage or destruction occurs to physical components**

- **The proper level of security around such items is dependent on a number of factors**
  - **Criticality of the system, sensitivity of the information stored, significance of the application being housed, the cost of equipment, the availability of an equipment back-up, etc.**

Physical and Environmental Factors cont.

- Increasing the responsibility of managing physical security is falling to the information security group

- Regardless of who is ultimately responsible, the ISM must ensure physical security policies, standards, and activities sufficient to not compromise information security efforts

Physical Security Layout and Design

- **Key aspects for proper security is the environmental for systems within an organization**
  - **E.g. Systems that contain sensitive information and mission critical applications should not be located in high traffic, easily accessible areas**
  - **E.g. Key documentation or storage systems should not be co-located with water pipes or other hazard types**
  - **Computing environments should have control over environmental factors such as temperature, humidity and electrical power quality**

Protecting Other Asset Types

- Even a common workstations should be given special consideration depending on where they are located and the type of information that is present
  - Depending on how it is being used, it may be a good idea to isolate systems

- Because mobile devices have an added element of potential loss or theft, incorporating policies such as using full-disk encryption can be desirable

Protecting Other Asset Types cont.

- ISMs must also take into consideration the proper placement of stored media and even printing equipment

Protecting Facilities from Disaster Events

- When selecting facilities, research must be conducted to determine any areas at risk to events such as earthquakes, hurricanes, flooding or other natural disaster

- Primary processing facilities, disaster recovery sites and offsite data storage facilities should be located far enough away from one another to ensure that a disaster does not impact more than one site

Culture and Regional Variances

- The ISM must be aware that there are differences in perception, customs and appropriate behavior across different regions and cultures
  - With this awareness, the ISM must identify the audience being addressed that was affected by information security activities

- Along similar lines is the way that personal information is managed in different areas
  - Policies, controls, and procedures should be developed and implemented with respect to these differences
  - If in doubt, consult HR and the legal departments

Logistics

- Due to the interactive nature of the ISP with other business units, the ISM should be sensitive to logistical issues
- Details that must be accounted for include:
  - Cross-organizational strategic planning and execution
  - Project and task management
  - Coordination of committee meetings and activities
  - Development of schedules of regularly performed procedures
  - Resource prioritization and workload management
  - Coordination of security resources and activities with larger projects and operations

Security Program Services and Operational Activities

Domain 3: Information Security Program Development and Management

ISP Operational Responsibilities

- As previously stated, the ability of the of the ISM to cultivate and maintain relationships with leadership of other departments has a great impact on effectively implementing and managing a security program
- Departments that will be discussed in this section are:
  - Physical/Corporate Security, IT Audit, Information Technology, Business Unit Managers, Human Resources, Legal Department, Employees, Procurement, Compliance, Privacy, Training, Quality Assurance, Insurance, Third-party Management, and the Project Management Office

Physical/Corporate Security

- Large organizations will often have security departments with physical security responsibilities
  - Often these are led by individuals from law enforcement with minimal information security background
  - With small organizations, this is normally handled within the facilities department
- Regardless of the size both cases will have an impact on information security so a good working relationship is paramount
  - The ISM should understand relevant physical security policies, standards, procedures and practices to make sure they do not undermine the ISP

IT Audit

- This action is normally performed to assure policy compliance and to identify risk
- In the absence of complete policies and standards an auditor may use their own discretion on what is proper security practices when reviewing findings
  - The auditors findings can or cannot agree with the ISMs methods and approach
  - This is why clear governance documentation is important for the ISM
- This information also points to the need for a good relationship with the internal audit group

Information Technology

- **An organization's IT department has a critical role in information security program development and management**
  - **This unit will have a critical role in ISP development and management**
  - **Developing a strong working relationship with the IT department will help to foster rapport, trust, an understanding of common goals and open communication**
  - **This relationship can become strained because of the notion that security is an impediment to IT's efforts**

Information Technology cont.

- A common problem that IT has to deal with is conflicting requirements between policies and standards vs. performance and efficiency requirements
  - This can result in sacrificing security to meet operational objectives
  - The ISM will have to look for flexible solutions to help IT reach compliance while keeping functions based on performance, capacity and scalability intact

Business Unit Managers

- These groups are kept in the loop as an ISP is being developed because there is a great need to keep the program in alignment with the business operations
  - These relationships will have a direct impact on doing this successfully
- Having a steering committee of members from the various business units will help the ISM keep consistent information on the direction of the business
  - It also can help the ISM point out the security responsibilities of each department and inform the group of planned security activities and issues

Business Unit Managers cont.

- **Business units will include personnel responsible for developing new products and services for the organization**
  - **Having the ISM involved in the development process will help ensure no surprises arise when these items are ready to be unveiled for use**

Human Resources

- Normally has significant information security responsibilities with regard to employee policy distribution, background checks, education and enforcement
  - HR and the ISM should work together to determine the best way to administer computer resource usage policies and procedures
- The ISM must have HR and legal involved when the monitoring of employee's actions or there is suspension of computing resources due to abuse
  - Procedures should be in place so that all know their defined responsibilities

Legal Department

- Most legal department will handle domains such as compliance, liability, corporate responsibility and due diligence
  - Information security will frequently have intersections with these topics
- Legal will also be highly engaged on items such as outsourcing and service providers
  - The ISM should take the lead on discussions to include the necessary security considerations in any agreements
- Having this department involved in such activities can help protect the organization from legal liability

Employees

- These are the first line of defense when it comes to the protection of an organization's information
  - Because of this, the appropriate training on policies, standards, and applicable procedures must be given periodically or as needed
    - These training results are used to confirm the knowledge of an employee and is kept in their personal records
- After being trained the employees are then responsible for informing the proper channels of any potential threats, violations, or potential methods for improving processes

Procurement

- The procurement process for most organizations has been formalized and can have a direct impact on an ISP
  - ISM should have visibility on these procedures and be able to provide input on how to improve acquisition practices
- Mature organizations often have an approved equipment list which helps to avoid the majority of threats in the acquisition process
  - Most of these devices have been vetted by compliance policies and standards
  - If these procedure have not been established, the ISM should be used to identify any risk that is introduce by the products under consideration

Compliance

- To navigate the growing complexities of the legal and regulatory landscape, many organizations are establishing compliance offices to help manager these requirements

- An ISM will need to have a working relationship with this office because their will be a need to identify the ramifications and the required actions from applicable policies, standards, and procedures

Privacy

- **Privacy restrictions have become commonplace in the current world climate**
  - **In response to these trends, organizations have created privacy offices or a privacy officer**
- **In some cases privacy regulations are vigorously enforced and have been made a major focus of information security**
- **The ISM must continuously coordinate with the privacy office or officer to avoid sanctions that have grown increasingly severe**

Training

- Larger organizations have built a separate training and education department

- The ISM should be engaged with this group to provide the necessary security and awareness training content to help employees to properly response to situations they may encounter

Quality Assurance

- **Must include the acceptable levels of security related-controls**
- **An ISM must understand the QA process and ensure that security-related testing is included in any procedures**

Insurance

- Organizations will hold a variety of insurance policies that have relevance for information security activities
  - E.g. Business interruption coverage related to incident response, business continuity, and disaster recovery

- The ISM must have an awareness of the types of policies that the organization has to include them in any risk analysis and recovery planning exercises

Third-party Management

- This references all outsourced functions and services
- The ISM must understand what functions or services are provided by external parties and the associated risk
  - Managing risk to an acceptable level may require a number of preventive, detective and compensatory controls including oversight and monitoring

Project Management Office (PMO)

- **This relationship is important because it provides the ISM with a high-level view of all projects, especially IT related ones, that are active across the organization**
  - **Having the ability to review projects and provide insight on potential risks or required security measures can greatly impact the smooth execution of the ISP**

Cross-Organizational Responsibilities

- An ISM can have a number of different roles, and even more responsibility in smaller organizations
  - This can lead to problems with having the proper separation of duties
- The ISM must ensure that roles and responsibilities are assigned across senior managers within the organization to avoid conflicts of interest
- Roles and the associated key performance indicators can be outlined, but also must have key goal indicators to show if adequate progress is being performed or if additional efforts are required

Cross-Organizational Responsibilities cont.

- ISPs typically cross a number of departments so it is the role of the ISM to be the ambassador for the program
- This includes getting consensus on planned activities and ideas before projects are started from the affected departments
  - Awareness ahead of time can help smooth any potential bumps in the road while work is already underway
  - The ISM must make sure that departments understand, accept, and have the resources to accommodate the ISP
- This is one of the major reasons that a steering committee of department representatives is key

Incident Response

- **Typically an operational requirement for the information security department**

- **Tasked with providing first responders to address security incidents within the organization**
  - **Goal is to quickly identify and contain incidents to prevent significant interruptions to business activities, restore affected services, and determine root causes so improvements can be implemented**

Security Reviews and Audits

- A key aspect of an ISP is to have clear, documented, and structured approaches for assessing and evaluating the state of various aspects of the program
  - These consistent methods can be used to signify trend metrics for improving the program
- This can be done by using an audit process
  - Standard approaches for auditing, security reviews are as follows:
    - An objective, a scope, constraints, an approach, and a result

Security Review Terms

- **Review objective**
  - **Statement of what will be determined by conducting the review process**
    - **E.g. Determine if users who access a shared storage system are uniquely identifiable**
- **Scope**
  - **Mapping of the objective to the aspect that is being reviewed**
  - **For the example above the scope would be the shared storage system**

Security Review Terms cont.

- **Constraints**
  - Aspects that may affect how a reviewer conducts a their process
  - A constraint that could be applied to our ongoing example is requiring that a test is performed during non-peak hours for the shared system (9 am – 5 pm)

- **Approach**
  - Set of activities that meets the objective while adjusting for the given constraints
    - There can often be a number of different approaches that can be acceptable
    - The goal is to select the set which is least affected by the provided constraints and fulfills the objective

Security Review Terms cont..

- **Result**
  - Assessment of if the review objective was met
  - This would answer the question, “Are all users accessing the system identified?

- **Conducting assessments can assist with test policies and standards within an organization**
  - This helps to understand what should be prioritized for the continued growth of the program

Audits

- These are extremely useful when trying to identify weaknesses within the ISP
  - Especially when the organization has compliance standards that must be tested to ensure all objectives are properly covered
- The audit team normally assembles documentation that does the following:
  1. Maps controls to control objectives
  2. States what the team did to test those controls
  3. Links those test results to the final assessment
- This documentation is often called “work papers”

Audits cont.

- If an ISP is still under development, then an ISM may have auditors use a publicly defined standard to help identify the level of compliance that an organization currently holds

- Work papers, in this context, can be very valuable because the existing controls are mapped to associated objectives from a standard
  - This help to identify work that the ISM must do moving forward

Audits cont.

- **Potential standards to use include:**
  - **COBIT**
  - **The Standard of Good Practice for Information Security**
  - **ISO/IEC 27001 and 27002**

Auditors

- Even though these roles can be seen in a negative light by IT and information security, an effective auditor is essential for the assurance process and to achieve information security compliance

- Including auditors in overall security management can be a powerful tool for improving an organization's security culture

Auditing Notes

- ISM must coordinate with organizational auditors to ensure that time and resources are allocated to perform the necessary audit activities
  - Procedures should be established in advance for scheduling, observation of employee activities and provision of configuration data from technical systems
- For any deficiencies identified by an auditor, the ISM should work with the individual to agree upon mitigation mechanisms and associated risk
  - The ISM can then craft solutions for the issue based on the organizational environment

Management of Security Technology

- Although the ISP spans technical, operational and managerial domains, a significant portion of the program will be technical
- There should be an agreement between the ISM and the security steering committee on the level of technical competency that should be present within the security department
- Wide spectrums are present when looking at the technical scope of information security departments

Security Department Technical Scope

- At one extreme is an ISP that operates at the corporate level and primarily sets security standards at a high level
- Security personnel can also be used as technical subject matter experts that provide advice to system administrators and other information technologists
- The other extreme is where information security is responsible for pieces of infrastructure
  - Access control systems, intrusion detection and monitoring systems, and compliance and vulnerability assessment automation tools

Technology Consideration

- An ISM must consider the skillset they personally possess and that of the members of the department in regards to organizational changes

- There will be a variety of security issues that will arise and being widely knowledgeable about issues can be a major asset
  - It must be remembered that the compromise of one element can disrupt the operations of an entire enterprise
  - An ISM must plan and prepare for the potential domino effect of cascading risk

Due Diligence

- This refers to the notion of taking the reasonable number of steps necessary to complete a task, analyze an event, etc.
- For an ISM it means ensuring the basic components of a reasonable security problem are in place
  - Senior management support, comprehensive policies, standards and procedures, appropriate security education training and awareness through the organization, periodic risk assessments, effective backup and recovery processes, implementation of adequate security controls, effective monitoring and metrics of the security program, effective compliance efforts, tested business continuity, etc.

Due Diligence cont.

- **Due diligence must also be taken when screening and using third-party services**
  - **These types of entities introduce significant risk to the organization and the proper care must be taken to make sure the third-party is performing responsibilities effectively and that the organization is covered from liability properly**

Managing and Controlling Access

- **The ISM must be aware of standards required for managing and controlling access to information resources**
  - **Depending on the sector of the organization, there can be specific regulatory bodies that have defined standards**

Vulnerability Reporting Sources

- Vulnerabilities in hardware and software are found daily
- The ISM should subscribe to entities that publish information on discovered vulnerabilities such as:
  - US Computer Emergency Readiness Team
  - MITRE's Common Vulnerabilities and Exposures database
  - Security Focus' BUGTRAQ mailing list
  - SANS Institute
  - OEMS
  - Etc.

Vulnerability Reporting Sources cont.

- These warning organizations can be a huge help when trying to get in front of vulnerabilities that are being actively exploited

Compliance Monitoring and Enforcement

- **Compliance enforcement processes must be considered during the development of an ISP so that they are in place once the program is implemented**
  - **This refers to any activities within the security program that are designed to ensure compliance within organizational policies, standards, and procedures**
- **When selecting controls, a primary concern is the difficulty in monitoring the control process**
  - **Complex control processes that are difficult to monitor generally provide little value**

Policy Compliance

- **Policies form the base of all accountability with respect to security responsibilities throughout the organization**
  - **They must be comprehensive in nature, but flexible to allow different processes and procedures to evolve for different technologies**

- **All systems within an organization should have leaders assigned to putting compliance policies in place on a system**
  - **The ISM is responsible for oversight and for developing the policy compliance processes**

Policy Compliance cont.

- **An ISM should also have a clear policy exception process in place**
  - **This process highlights where a policy is not being followed based upon various factors**
  - **There should also be a procedure in place where exceptions are periodically reviewed to confirm that the understood risk is still at an acceptable level**

Standard Compliance

- Present boundaries for system processes and actions that still comply with policy
- Standards should be designed in a way that all systems of the same type with the same security domain are configured and operated in the same way based on criticality and sensitivity of the resources
  - This helps with scale configuration to additional systems and devices
    - The proper configurations only have to be studied and created once and then applied to all similar systems

Resolution of Noncompliance Issues

- These can result in risk to the organization
  - Processes should be in place to deal with issues in an effective and timely manner
- In most cases a timetable is developed to document each noncompliant item and responsibilities for addressing it is assigned and recorded
  - Follow-ups should be scheduled to ensure the noncompliance issue is satisfied in a timely manner

Resolution of Noncompliance Issues cont.

- **Noncompliance issues can be identified using a number of mechanisms including:**
  - **Normal Monitoring**
  - **Audit reports**
  - **Security reviews**
  - **Vulnerability scans**
  - **Due diligence work**

Compliance Enforcement

- Ongoing process that helps reduce risk and ensure positive audit opinions
  - Aims to ensure that policy and standards requirements that are not being met are brought into compliance
- Information security department is often responsible for conducting independent evaluation of technical standards
  - Preferably using automation tools
- Most standards will be geared towards compliance for the organization, but the ISP can also be subject to evaluation and performance

Compliance Enforcement cont.

- An ISM should be prepared to work closely with audit personnel to demonstrate compliance of the ISP with pertinent standards and regulations
  - Any issues identified should be defined in terms of risk, mitigating factors and acceptable control objectives
    - Depending the size of a concern, the ISM can deal with the problem independently or collaborate with executive management or the security steering committee

Assessment of Risk and Impact

- As stated before a primary operation responsibility for the ISM and the reason for an ISP is to manage risk to an acceptable level
- The goal is to minimize disruptions to organizational activities while balancing an acceptable cost
- The following slide will identify activities to achieve those ends

Vulnerability Assessment

- The information security department should have an ongoing automated process for detecting vulnerabilities and unexpected system changes
  - The goal is to identify any actions that could threaten confidentiality, integrity, and availability
- The ISM should also ensure that routine updates to the technical environment does not introduce unexpected vulnerabilities
  - These can be monitored and checked by using a change management system
    - Formal processes for studying the ramification of system changes among a group of experts and business stakeholders

Threat Assessment

- **Threats are always growing and changing both internally and externally**
  - **The threats can be both technical and behavioral in nature**
  - **The threat landscape should at least be reassessed annually to help identify the changes in a threat environment**

- **As the threats and their impact level change, the ISM must evaluate the ability of existing controls to mitigate risk associated with these threats**

Threat Assessment cont.

- Depending on the threat, they can be addressed in a number of different manners
  - Modification of a technical security architecture
  - Implementation of a threat-specific countermeasure
  - Compensating controls
  - Implementation of new processes until a mitigating control can be developed
- All possible threats must be evaluated from the following perspectives:
  - Is the threat viable?
  - What is the likelihood of a threat materializing?
  - What is the magnitude of the threat?
  - What is the potential impact to systems, operations, and personnel?

Risk Assessment and Business Impact Analysis (BIA)

- **Risks Assessment has a few primary goals**
  - Identify , analyze, and evaluate risk
  - Determine the probability of compromise
  - Determine the potential impact on an organization in both qualitative and quantitative terms

- **A BIA is an exercise that determines the impact of losing the availability of any resource to an organization**
  - Also identifies the minimum about of resources necessary to recover for a disruption

Risk Assessment and Business Impact Analysis (BIA)

- Impact is the primary concern in terms of risk
  - The range of severity to an organization must be defined and will be used to guide risk management activities
- The ISM must make decisions on how achieving control objectives will impact confidentiality, integrity and availability of information resources
  - The ISM will basically perform a cost/benefit analysis to determine the maximum impact for the minimum cost
  - Mapping a control's benefits and impact onto business objectives is not a straightforward process
    - Business cases to show immediate business impact can be very important in describing benefits of controls, equipment, or projects to management or the steering committee

Risk Assessment and Business Impact Analysis (BIA) cont.

- The ISM should be proactive in describing threats and vulnerabilities as they emerge
  - This can result in an annual meeting where a "state of affairs" address is provided for the entire organization or can be done incrementally by discussing sections of the business monthly
- Keeping management engaged and aware can help to keep the ISP developing as expected
  - Information collected from risk assessments and BIA case studies can help management make informed decisions on the direction of the organization

Resource Dependency Assessment

- If resources or other constraints do not allow for comprehensive BIAs, a business resource dependency assessment is a less expensive alternative

- These assessment reviews the resources necessary to conduct business
  - Depending on the criticality of the business function, this can provide a baseline for what resources should be prioritized in protection efforts

Outsourcing and Service Providers

- There are two types of outsourcing that an information security department will have to deal with
  - Outsourcing of security services
  - Outsourcing of IT or business processes

- Both pose significant risks that the ISM must find a way to mitigate
  - The risk presented by the services must be weighed against the cost benefit that outsourcing provides
  - Other factors that must be considered is any change in cost that may result from a need for additional services
  - Yet another issue that could arise is the need to insource services if a breach in contract may occur
    - This adds additional costs that may not have been anticipated

Outsourcing and Service Providers cont.

- Other important considerations when evaluating options that can negatively impact the organization:
  - Loss of essential skills
  - Lack of visibility into security processes
  - New access and other control risk
  - Viability of the third-party vendor
  - Complexity of incident management
  - Cultural and ethical differences
  - Unanticipated costs and service inadequacies

Monitoring Third-Party Vendors

- Regardless of if entire operations are being outsource or just a particular service, an ISM must have methods for monitoring the quality of the services being provided
  - This can be achieve with independent audits or onsite visits at the third-party facility
- If additional, when privacy laws come into play it may be a good idea to develop additional enforcement processes to safeguard data
- Training could also be required for the third-party vendor to make sure standards are being followed at acceptable levels

Evaluating Third-Party Vendors

- For a vendor to be viable, they must be able to adhere to the security standards outlined by the ISM
  - Not being able to meet these standards can result in security breaches

- High on the factors for selecting a vendor is the maturity of there own security program and the ability to provide assurance of compliance

Outsourcing Contracts

- The purpose of a contract is two-fold for the contracting parties
  1. Understand the responsibilities and obligations of both parties for the duration specified by the contract terms
  2. Outline the steps that should be taken if any disagreements arise once the contract has started

- The ISM should work with the organization's legal department to ensure important security clauses, such as data protection, are included in the terms of the contract
  - Additional requirements could be the security controls used by each party and the management of how data is stored

Outsourcing Contracts cont.

- Additional contract items of interest should be the ability to perform a risk assessment without notice if a service provider is determined to be beyond a predetermined risk threshold
  - This would normally be for third-party vendors that store or process business-critical information, provide mission-critical services, etc.

- The roles of each party also should be outlined in the contract for if a security breach occurs at either of the entities facilities

Third-Party Access

- Any type of access to an ISMs processing facility should be determined by a risk assessment and be clearly defined in a service level agreement (SLA)
  - SLA is a documented agreement on the minimum performance targets that are acceptable by a service provider
    - It also details how the performance targets will be measured
- Access should be granted based on the principles of least privilege, need-to-know, and need-to-do

Third-Party Access cont.

- **Access rights should be fully logged and reviewed by the security manager on a regular basis**

Cloud Computing

- The concept of "utility computing" has been around since the 1960s, but has come to prominence with increased bandwidth and almost universal access to the Internet

- NIST defines it as:
  - "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction"

Cloud Computing cont.

- A key trait of the cloud is that data is somewhere in "the cloud" rather than being in a specific location
  - Cloud services can be provided in a public shared format or as a private hosting solution where a larger business wants to have more control of the environment

- Five essential characteristics of the cloud include:
  - On-demand self-service – Provision without human interaction
  - Broad network access – Available over the network
  - Resource pooling – Supports a multitenant model
  - Elasticity – Resource scale up or down in response to business needs
  - Measured service – Resources utilization can be optimized by leveraging charge-per-use capabilities

Cloud Computing cont.

- The types of cloud models and deployment methods are detailed in the following slides

- The overall risk and benefit of each model differs for each type and an ISM must consider each based on the needs of the organization
  - The continued advances of cloud computing offers some unique services that can provide major benefits to organizations

Cloud Computing Service Models

Service Model	Definition	To Be Considered
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	• Availability • Confidentiality • Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) • Data ownership • Concerns around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	• Who owns the applications? • Where do the applications reside?

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives
ISACA, USA 2009

Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	• Operated solely for an organization • May be managed by the organization or a third party • May exist on-premise or off-premise	• Cloud services with minimum risk • May not provide the scalability and agility of public cloud services
Community cloud	• Shared by several organizations • Supports a specific community that has shared mission or interest. • May be managed by the organizations or a third party • May reside on-premise or off-premise	• Same as private cloud, plus: • Data may be stored with the data of competitors.
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services	• Same as community cloud, plus: • Data may be stored in unknown locations and may not be easily retrievable.
Hybrid cloud	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	• Aggregate risk of merging different deployment models • Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives
ISACA, USA 2009

Security as a service (SecaaS)

- **Can be provided in two forms:**
  - **The cloud service provider (CSP) provides managed security services such as anti-virus scanning or mail security for coverage of end-point security**
  - **The CSP performs CPU or memory intensive activities within the cloud instead of on local appliances**
    - **E.g. Anti-virus services being performed in the cloud instead of on a local unified threat management (UTM) device**

Data storage and data analytics as a service (Big Data)

- Aims to take away constraints on the volume, variety, velocity and veracity of data

- Without these issues, organizations can use data for a variety of new business purposes and begin to find the patterns that can spark new business insights and products
  - This can be done by leveraging real-time reporting and predictive analysis within the business for example

Information as a service (IaaS)

- **Continuing to address the benefits of big data, this type of service would actually collect the information necessary for a business**

Advantages

- **Without a doubt cloud computing provides many benefits**
- **Optimized resource utilization**
  - **Enterprises normally use less computing resources than actually required**
  - **The pay-as-you-go strategy will better align needs to actual demand**
- **Cost savings**
  - **Moving to a renting paradigm for computing resources provides significant up-front and total cost savings**

Advantages cont.

- **Better responsiveness**
  - On-demand, agile, scalable and flexible services that can be implemented quickly provide organizations with the ability to respond to changing requirements and peak periods

- **Fast cycle of innovation**
  - Using the cloud provides fast access to patch management and upgrades to new software versions
    - This can be as easy as changing a URL in the browser

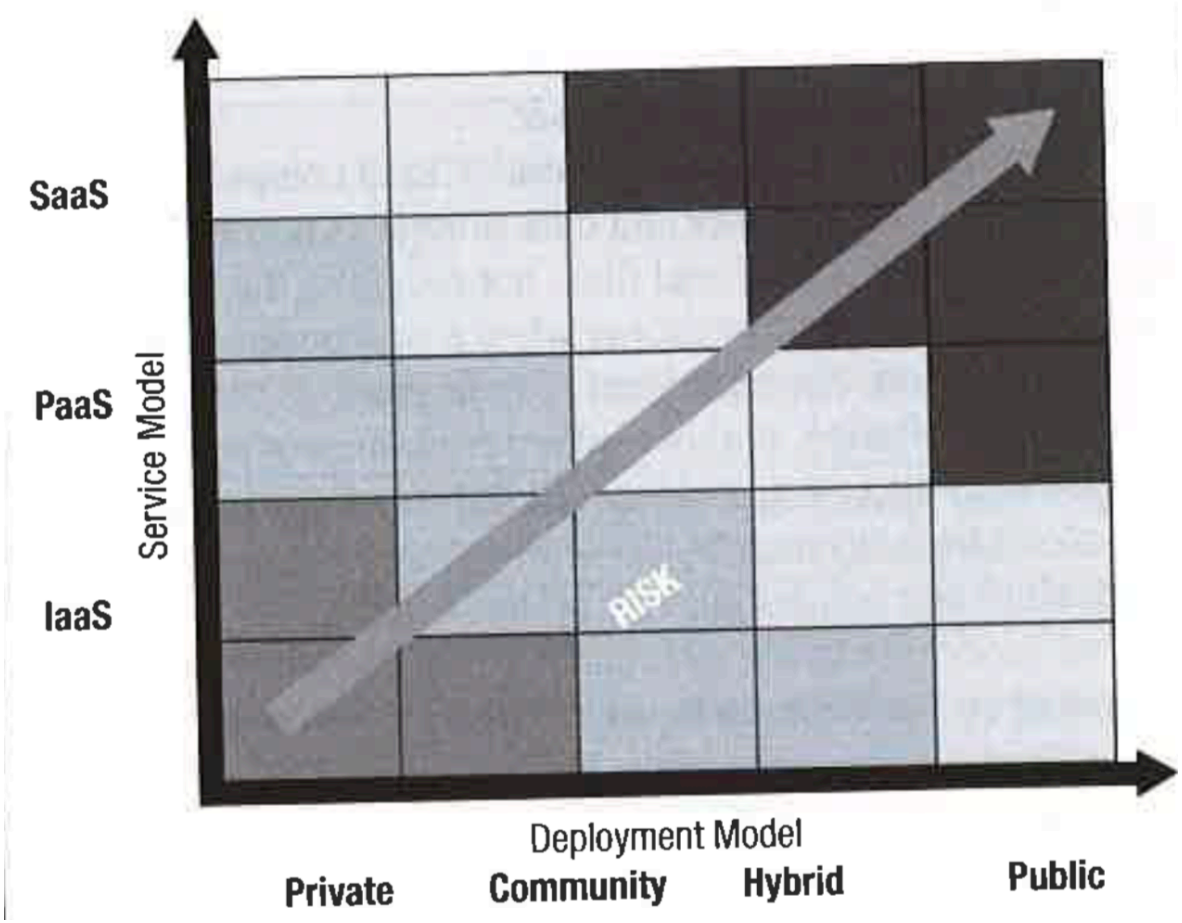
Advantages cont.

- **Reduced time for implementation**
  - Doesn't require the time normally needed for standing up enterprise initiatives
- **Resilience**
  - The size and resources leveraged by the cloud reduces the potential for system failures

Security Considerations

- For the ISM security considerations within the cloud can be a significant issue that must be carefully assessed
  - Things to note is the loss of control of potential sensitive information and not managing the location of the actual data itself
- The relationship of cloud services and risk is shown in the following slide

Cloud Computing Risk Map



Controls and Assurance in the Cloud Using COBIT 5
ISACA, USA 2014

Evaluating Cloud Service Providers

- As with other outsourced services, the driving factor for cloud computing is the economic benefits
  - This cost is not the only factor that should be made when making such a decision
    - Especially if the information that will be stored in the cloud is critical in nature

- A more acceptable approach for the ISM and the business is to critique the service providers based on their security posture and risk appetite
  - The residual providers for the cloud service must also be taken into the consideration process when quantifying risk

Integration with IT Processes

- For processes to run smoothly, there should be defined interfaces between security-related functions and assurance functions within the organization
  - E.g. Making sure that activities for BCP integrate well with incident response activities
- Ensuring the integration of components such as these help to prevent security gaps or duplication of effort
  - The interfaces between the ISP and the assurance function should be bidirectional
    - Assurance bodies provide information about activities, while the ISP generates metrics to inform the assurance departments of potential improvements

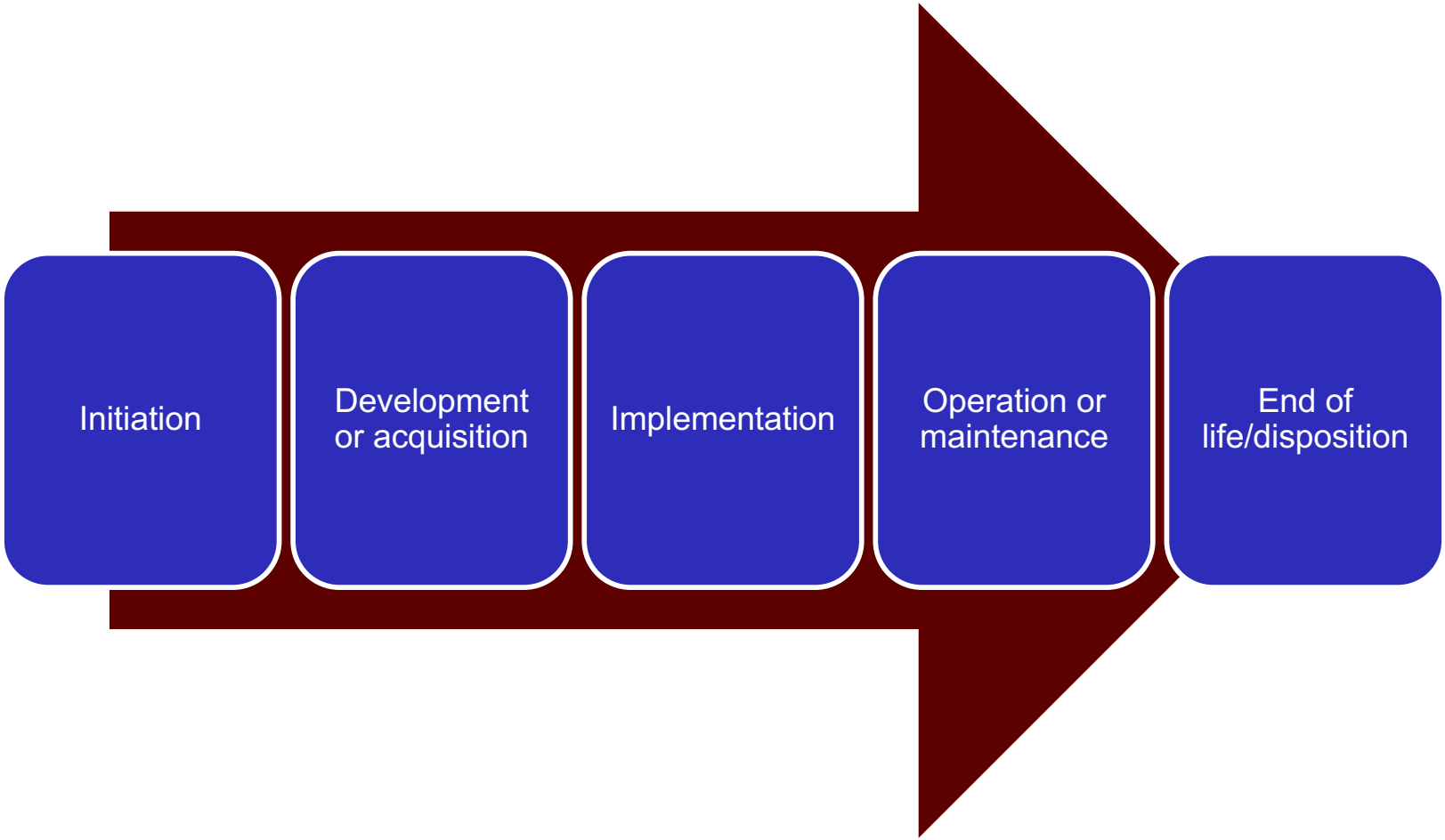
Integration with IT Processes cont.

- This highlights again the need for the ISM to be a great communicator and the need for them to work collaboratively with each unit of the organization
  - The impact of the ISP should be pervasive within the organization

System Development Life Cycle Processes

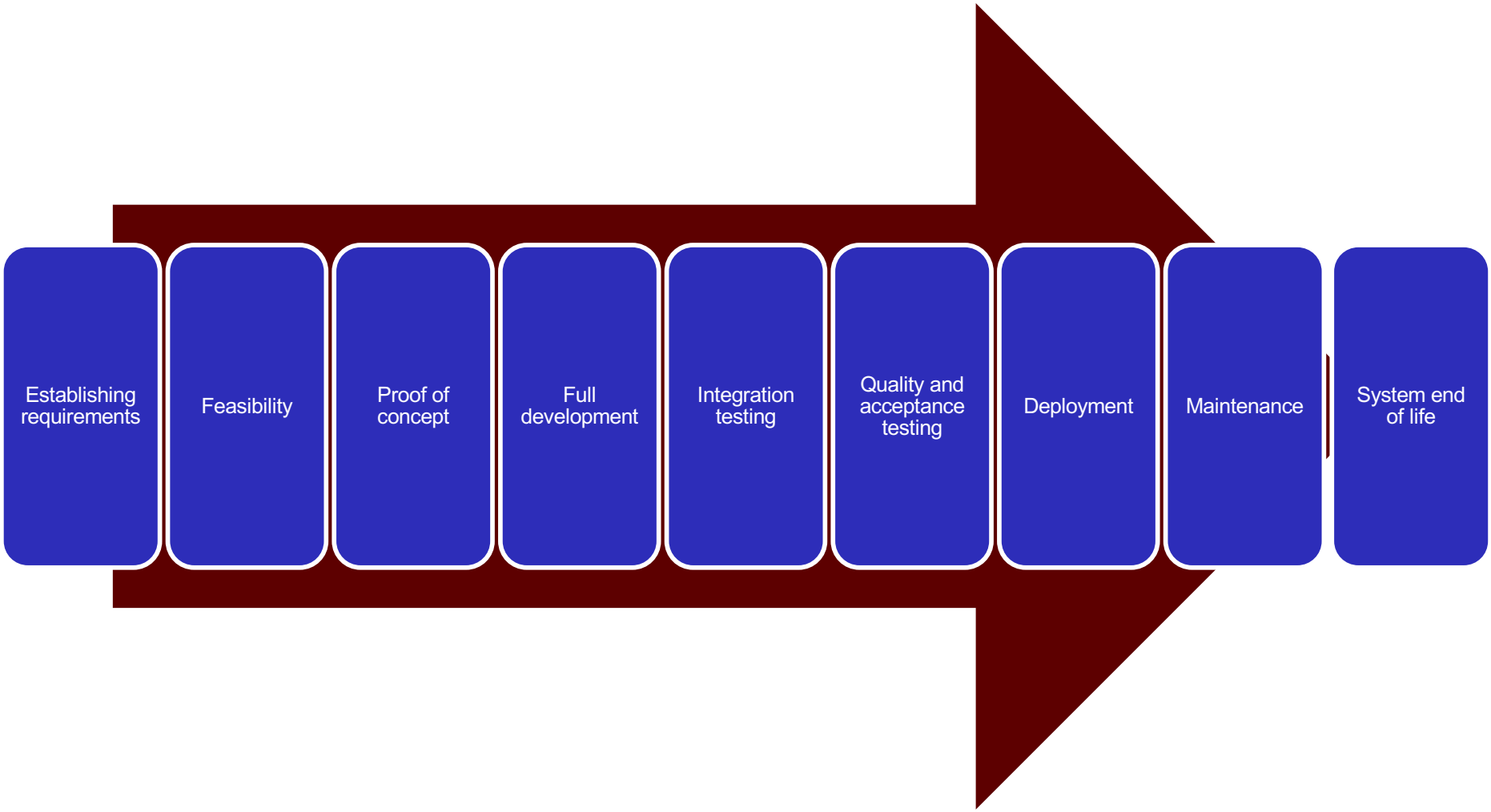
- When risk and protection strategies are built into the SDLC it makes the process of providing effective information systems security that much more effective
  - The SDLC is often managed by other groups within the organization so the ISM must put processes in place to be informed of any proposed system changes
  - These types of processes can help the ISM to ensure associated risk is accessed and mitigated as needed

System Development Life Cycle Processes cont.



Traditional SDLC stages

System Development Life Cycle Processes cont.



Expanded SDLC stages

Change Management

- Change management is often either formally or informally included within an organization
- It is integral that the change management processes have a clear security focus
  - Insecure configurations is one way that vulnerabilities can be introduced into an organization
  - The ISM should identify all change management processes within the company and incorporate a notification process when changes are taking place that could impact security
- The ISM must also structure processes so that looking at security implications is a common practice

Change Management cont.

- It can be difficult for an ISM to monitor all business units in an organization, especially when they are structured to run autonomously
  - These types of considerations must be made when determining the structure for an ISP to make sure to establish effective change management processes

Release Management

- When done well release management can set a standard of tests and operational assurance for new software, devices, or systems

- The ISM should establish the proper procedures and standards so that products are not put into production environments prematurely
  - Oversight must also be enforced to help identify any breach in procedures

Controls and Countermeasures

Domain 3: Information Security Program Development and Management

Control Definition

- Policies, procedures, practices technologies and organizational structures designed to provide reasonable assurance that business objectives are achieved and undesirable events are prevented or detected and corrected

- Any regulatory process, whether physical, technical, or procedural

- Controls are chosen based on a number of considerations including:
  - Cost, effectiveness, restriction of business activities, etc.

Control Types

- **Controls within an organization are categorized into two broad groups:**
  - **General controls**
    - **Those controls that apply to the entire organization and that support such things operating systems, network, and facility security**
    - **Also may include centralized user administration policies, standards and procedures, access controls, firewalls, and IDSs**
  - **Specific controls**
    - **These are noncentralized business processing protections that may be implemented at the application level**
    - **These types of control are often managed by department**

Control Categories

- **Preventive**
  - Inhibit attempts to violate security policy
    - E.g. Access control enforcement, encryption, and authentication
  - These controls directive address risk
- **Detective**
  - Provides notification of violations or attempted violations of security policy
    - E.g. Audit trails, intrusion detection logs
- **Corrective**
  - Remediate impact
    - E.g. Backup restore activities

Control Categories

- **Compensating**
  - Responsible for reducing the risk of existing controls or those that are found to have weaknesses
    - E.g. Insurance can compensate for breach losses
  - Corrective and compensating controls address impact

- **Deterrent**
  - Provide warnings that aim to deter potential compromises
    - E.g. Warning banners on login screens
  - Deterrent controls address threats

Control Importance

- Primary method for managing information security risk and a major responsibility for the information security department
- Controls for physical elements such as administrative processes and procedures are just as critical as controls applied to technology
  - Controls are not all technical
  - Most security failures can ultimately be attributed to failures of management, and it must be remembered that management problems typically do not have technical solutions
    - Because of this the ISM cannot depend on technical solutions solely to solve all issues

Control Importance cont.

- The goal for an ISM is to find a balance between protecting the organization and not being overly restrictive
  - Restrictive solutions often just cause personnel to circumvent controls to get the job done
  - Controls should avoid being disruptive while mitigating risk to an acceptable level

Information Security Controls

- Controls have to be put in place for both IT-related and non-IT related information processes
  - This can include having the proper secure marking, handling, transport, and storage requirements for physical information
    - Also under this umbrella could be implementing processes to help avoid social engineering
- From an environmental control perspective, systems must also be properly protected from thief and intentional and unintentional damage

Control Design Considerations

- With the current regulatory environment, it is suggested that controls and countermeasures be approached from a top-down, risk-based approach
  - Control objectives are essentially determined by the acceptable risks levels selected by management
    - The control objective basically turns into both the design goal and the control metric for effectiveness
      - The control effectiveness metric is the extent that a control meets the objectives
- Detailing control objectives is a key step in ISP development
  - It impacts physical, administrative, and technical controls

Controls and Strategy Implementation

- Putting an ISP strategy into place is highly dependent on implementing combinations of controls
  - It is also dependent upon ensuring the proper risk level are supported by the controls put into place
  - The combination of controls that can be selected is essentially limitless
    - This is another aspect that makes selecting the proper controls a daunting tasks
- As an ISM selects the controls to support a strategy, they must carefully review the features associated with different technology
  - One technology can provide several different control solutions

Control Best Practices

- **Mechanisms that embody the following principles make it difficult to bypass controls**

- **Access (logical) control**
  - **Users accessing information should be identified, authenticated, and authorized prior to accessing information**

- **Secure failure**
  - **Device or system is design to stop processing when a malfunction is detected that could affect access control mechanisms**
    - **Can affect availability so must be considered carefully**

Control Best Practices cont.

- **Principle of least privilege**
  - Access design strategy where the minimum security privileges are provided to users for accomplishing their responsibilities
- **Compartmentalize to minimize damage**
  - Divides system resources into subsets and implements different authorization controls for each subset
    - E.g. Segmenting network resources by departments
- **Segregation of duties**
  - Restricts the ability of users from having multiple functions meant to provide supervisory or oversight features
    - E.g. Prevents a user from being able to print and change the name on checks

Control Best Practices cont…

- **Transparency**
  - Principle that an average person should be able to understand how system security is suppose to work
    - This allows stakeholders to easily see the effect of their activities on overall security
  - This is achieved by keeping system designs as simple as possible

- **Trust**
  - Design strategy where the identify of a user or device can be determined by their relationships to an identity provider that is trusted by a relying party
    - E.g. Using certificates and certificate authorities

Control Best Practices cont….

- **Trust no one**
  - **Design principle where oversight controls are built into the actual information system design**

Control Strength

- The strength of different controls can be measured by its type and its quantitative and qualitative compliance testing results

- Criteria for strength can include its design strength and the likelihood of its effectiveness
  - Example of strongly designed controls would be requiring 2-factor authentication (username/password and a token) to access a network

Control Methods

- There exists both technical and non-technical controls for developing an ISP
  - These include administrative, technical and physical controls
- Technical controls are safeguards that are built into computer hardware, software or firmware
- Nontechnical controls are management and operational controls

Control Methods Explained

Category	Description
Managerial (administrative)	Controls related to the oversight, reporting, procedures and operations of a process. These include policy, procedures, balancing, employee development and compliance reporting.
Technical	Control also know as logical controls and are provided through the use of technology, piece of equipment or device. Examples include firewalls, network or host-based intrusion detection systems (IDSs), passwords, and antivirus software. A technical control requires proper managerial (administrative) controls to operate correctly.
Physical	Controls that are locks, fences, close-circuit TV (CCTV), and devices that are installed to physical restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to assess and react to an alert should a problem be indicated.

Control Recommendations

- **Additional details that should be considered when considering control strength**

- **The following questions should be presented**
  - **Is the control preventive or detective?**
  - **Is the control manual or automated?**
  - **Is the control formal or ad hoc?**
    - **Formal controls have documented procedures and evidence of their operational maintenance**

Control Recommendations cont.

- The following considerations are reviewed when recommending controls and alternative solutions to reduce identified risk to acceptable levels
  - Effectiveness of recommended options
  - Compatibility with other impacted systems, processes, and controls
  - Relevant legislation and regulation
  - Organizational policy and standards
  - Organizational structure and culture
  - Operational impact
  - Safety and reliability

Countermeasures

- Countermeasures are specific controls that aid in the mitigation of a particular threat
  - Because these types of solutions focus on particular problems they are often effective, but not efficient as they have little impact on other types of threats
- Countermeasures can be preventive, detective, corrective, or any combination of the three
- They can also be nontechnical such as offering a reward for information leading to the arrest of hackers

Countermeasures cont.

- It is often better to avoid using many countermeasures as longer term solutions
  - Countermeasures can be expensive to implement and can be a distraction from core security operations
  - It can be viable to use countermeasure as short-term solutions until long-term controls can be applied

- An ISP should be flexible enough to apply countermeasures in emergency situation
  - The solution should still be thoroughly documented and should go through any change management processes after the fact

Physical and Environmental Controls

- For any ISP the basis for protecting any type of information is having sufficiently strong physical barriers to protect the physical media where information resides
  - This is often provided by facilities management in most companies
- These physical controls can be a combination of technical mechanisms and procedures
  - The ISM should validate technology choices in support of physical security processes and make sure that policies and standards ensure adequate protection

Physical and Environmental Controls cont.

- An ISM must also understand the roles and responsibilities associated with physical controls and have a method to ensure that these responsibilities are met
  - If physical controls are faulty, then this could provide direct unauthorized access

- Basic methods for keeping unauthorized individuals from gaining access to tangible information resources include:
  - ID badges, authentication devices, security cameras, security guards, fences, lighting, locks, sensors, etc.

Control Technology Categories

- The types of controls that can be use are broken into three different categories
  - Native, supplemental, and support controls

- These categories are being considered in respect to the operational authority that will be responsible for managing the security of the controls
  - Often operational authority for technical controls will either be given to the information security department, the IT department, or split between the two groups

Native Controls

- These are controls that come standard with most business information systems
  - Servers
  - Databases
  - Routers
  - Switches
  - Etc.

- The policies that govern these systems are often governed by the information security department, but the actual configuration is done by IT
  - This structure can help to reduce of SoD issues

Supplemental Controls

- Control solutions that can be added on to an information system environment
  - Often provides an additional function that does not come natively with the system or device

- These types of controls normally require specialized security support and the resources of both IT and security departments can be leverage to achieve the proper implementation and oversight

Supplemental Controls cont.

- **Common supplemental control technologies include:**
  - **Federated identity management systems**
  - **Single Sign On (SSO) systems**
  - **Intrusion Prevention Systems (IPSs)**
  - **Firewalls**

Management Support Controls

- These types of controls provide the added benefits of automating security-related procedures, providing management information processing, or allowing for increased management efficiency

- These technologies are normally used by the security organization and do not directly impact production environments

Management Support Controls cont.

- **Some of the most common supporting technologies include:**
  - **Security Information Management (SIM) Tools**
  - **SIEM systems**
  - **Compliance monitoring and management tools**
  - **Access management workflow systems**
  - **Vulnerability scanning tools**
  - **Security configuration monitoring tools**
  - **Policy management and distribution systems**

Control Testing and Modification

- Changes to the technical or operating environment within a company can render controls ineffective or unexpectedly open security holes
  - Changes should always be made with great caution
    - Changes should go through an official change process that will require ISM and management/steering committee approval

- To ensure controls are functioning as expected, they should be periodically tested to confirm they are providing the protection expected

Control Testing and Modification cont.

- After implementation of the proposed changes, acceptance testing should also be performed
  - This is where the policies that the controls should support are tested and confirmed
- Similar reviews and confirmations should be performed when changing operational processes
  - Walk-throughs for these types of controls should be conducted to analyze if the desired changes have been captured in the new process and that no residual negative changes have been added

Baseline Controls

- Any new system that is brought to life should have a baseline of controls that will be configured depending on the environment and the type of system
  - These controls should be clearly documented and be in highlighted in the standard processes for managing organizational systems

- To determine these baseline controls the ISM should use both internal and external resources to analyze and determine the best solutions for the current operating environment
  - Controls normally do not provide a perfect solution and the trade-offs between options must be examined

Security Program Metrics and Monitoring

Domain 3: Information Security Program Development and Management

Security Program Metrics

- To properly manage an ISP, metrics for how to mark the progress of the program must be determined and collected
- They must not only be collected during the development phase, but also for the program's ongoing development
- A consideration that an ISM must make when selecting potential controls is the ability of the control to generate meaning and easily obtainable metrics

Security Program Metrics cont.

- **The ability to quantify the status of an ISP allows for the proper design, accurate implementation to specifications, and effective management of activities**
  - **This includes goal setting, tracking progress, benchmarking and prioritizing**

Metrics and Business Alignment

- **Technical metrics are important for managing the information systems within an organization, but they tend to lack contextual information that would be impactful or relatable to business objectives**

Metrics and Business Alignment cont.

- From a management perspective the following questions would be desirable to answer:
  - How secure is the organization?
  - How much security is enough?
  - How do we know when we have achieved adequate security?
  - What are the most cost-effective solutions?
  - How do we determine the degree risk?
  - How well can risk be predicted?
  - Are we moving in the right direction?
  - What impact is lack of security having on productivity?
  - What impact would a catastrophic security breach have?
  - What impact will proposed security solutions have on productivity?

Metrics Development

- Crafting metrics that align with the control objects and goals are essential to managing a security program

- Metrics are solely used to assist in making decisions
  - Measurement assists management

Metrics Development cont.

- Being able to know where decisions have to be made throughout the organization will help to determine the metrics that are needed to support those decisions
  - Three questions sum up metric design:
    - Who needs to know?
    - What do they need to know?
    - When do they need to know?

- Metrics should provide information at one or more of the following three levels:
  - Strategic
  - Management
  - Operational

Strategic Metrics

- A compilation of management metrics designed to indicate if an ISP is on track, on target, and on budget to produce the desired outcomes
  - At this level the information that is needed is navigational in context
    - Is the ISP moving in the right direction
  - This information is needed by both the ISM and senior management

Management Metrics

- **Metrics used to effectively manage the ISP by understanding its current state and making decisions that will guide its future**
  - **At the policy and standards level information such as:**
    - **Compliance**
    - **Incident management and response effectiveness**
    - **Manpower utilization**
    - **Resource utilization**
  - **At the security management level information such as:**
    - **Information on compliance**
    - **Emerging risk**
    - **Resource utilization**
    - **Alignment with business goals**

Management Metrics cont.

- The ISM will also need a summary of technical information to ensure that machinery is operating properly in acceptable ranges
  - This information will not identify the proper direction, but will help ensure that if/when pivots are necessary the equipment will be able to support the change

Operational Metrics

- More of the common technical and procedural metrics
  - Often utilized by IT managers and system administrators
- These types of measure may include:
  - System access logs
  - Firewall configuration data
  - VPN traffic data
  - Syslog reviews
  - Etc.

Metrics Considerations

- **There are essential considerations when developing quality metrics**
  - **Manageable**
    - Data should be easily sorted, stored, accessible, and understandable
  - **Meaningful**
    - Information should be understandable relevant to those reading it
  - **Actionable**
    - Data should provide clear direction on what should be done next
  - **Unambiguous**
    - Content should be clear

Metrics Considerations cont.

- There are essential considerations when developing quality metrics
  - Reliable
    - There should be a process and mechanisms in place that provide consistent information under the same circumstances
  - Accurate
    - Data should be extremely close to actual results
  - Timely
    - Feedback must be available when needed
  - Predictive
    - Effectively being able to point to a expected result is valuable
  - Genuine
    - Data must be trustworthy

Metrics Considerations cont.

- **The previous list can be used as metametrics for determining if a metric is of value**
  - **Any metrics understand consideration that can't meet this criteria is suspect at best**

Metric Value

- In some cases the metrics used by organizations will not measure well against the metametrics discussed previously
  - For some businesses there are simply few ways to measure objectives effectively
  - Internal discussion should be had to determine the feasibility of metrics before they are selected

Monitoring Approaches

- An ISM must develop a comprehensive strategy for reliably monitoring the ongoing effectiveness of the program

- A solution for handling this is to regularly conduct either external and/or internal scanning and penetration testing to determine system vulnerabilities
  - This can help to discover trends of the ISP improvement

Monitoring Approaches cont.

- **Another method that can be used is to track the organizations change management activities**
  - **This can also provide feedback on what activities are being conducted and can give insight on any trends that may need to be improved**

Monitoring Security Activities

- **Vulnerabilities that exist within an organization are exploitable at any time so 24/7 monitoring is a staple of prudent business practices**
  - **The ISM should outline clear monitoring requirements with details on what constitutes various severity levels**
    - **This can help provide earlier indicators of a potential breach**

Success of Security Investments

- The ISM should have processes in place that can determine the effectiveness of security investments and the extent to which objects have successfully been met
  - Any time costs can be justified this can position an ISP well for additional funding
- The actual cost of components within the ISP should be calculated to determine cost-effectiveness
  - It can use useful to use Total Cost of Ownership (TCO) when evaluating ISP components

Success of Security Investments cont.

- In addition to procurement and implementation costs, it would be important to include:
  - Costs to administer controls
  - Training costs
  - Maintenance costs
  - Monitoring costs
  - Update fees
  - Consultant or help desk fees
  - Fees associated with other interrelated systems that may have been modified to accommodate security objectives

Measuring Information Security Management Performance

- **The ISM should understand how to apply the proper processes to effectively assess the success and deficiencies of the ISP**
  - **The specific objectives of the ISP will vary depending on the operating level and scope of the security department**

Measuring Information Security Management Performance

- **An ISP generally includes a core set of common objectives:**
  - **Achieve acceptable levels of risk and loss related to information security issues**
  - **Support achievement of overall organizational objectives**
  - **Support organization achievement of compliance**
  - **Maximize the program's operational productivity**
  - **Maximize security cost-effectiveness**
  - **Establish and maintain organization security awareness**
  - **Facilitate effective logical, technical, and operational security architectures**
  - **Maximize effectiveness of program framework and resources**
  - **Measure and manage operational performance**

Measuring Information Security Risk and Loss

- Primary objective of an ISP is to manage risk to an acceptable level and to minimize the impact of adverse events to within acceptable limits
  - Achieve perfect security while enabling total system usability is virtually impossible
  - There are methods for balancing operational efficiency against adequate safety

- The following slides will discuss how to periodically measure the program's success against risk management and loss prevention objectives

Measuring Technical Vulnerability Management

- The following questions are posed:
  - How many technical or operation vulnerability exist?
  - How many have been resolved?
  - What is the average time to resolve them?
  - How many recurred?
  - How many systems (critical or otherwise) are impacted by them
  - How many have the potential for external exploit?
  - How many have the potential for gross compromise (e.g. remote privileged code execution, unauthorized administrative access, bulk exposure of sensitive printed information)?

Measuring Risk Management

- **The following questions are posed:**
  - **How many high, medium, or low risk issues are unresolved?**
    - **What is the aggregate annual loss expectancy (ALE)?**
  - **How many were resolved during the reporting period?**
    - **What is the aggregate ALE that was eliminated**
  - **How many were completely eliminated vs partially mitigated vs transferred?**
  - **How many were accepted because no mitigation or compensation method was tenable?**
  - **How many remain open because of inaction or lack of cooperation?**

Measuring Risk Management cont.

- In addition to quantitative metrics there are also qualitative metrics
  - Do risk management activities occur as scheduled?
  - Have IRPs and BCP been tested?
  - Are asset inventories, custodianships, valuations and risk analyses up to date?
  - Is there consensus among information security stakeholders as to acceptable levels of risk to the organization?
  - Do executive management oversight and review activities occur as planned?

Measuring Loss Prevention

- **The following questions are posed:**
  - **Were there loss events during the reporting period?**
    - **What is the aggregate loss, including investigation, recovery, data reconstruction and customer relationship management?**
  - **How many events were preventable (i.e., risk or vulnerability identified prior to the loss event)?**
  - **What was the average amount of time taken to identify loss incidents?**
    - **To initiate incident response procedures?**
    - **To isolate incidents from other systems?**
    - **To contain event losses?**

Measuring Support of Organizational Objectives

- ISP should always support the objectives of the organization
  - In some cases this can be difficult because organizational objectives can change quickly under pressure from evolving operational needs and market conditions

- The qualitative metrics discussed on the next slide can be reviewed by information security steering committee and/or executive management

Measuring Support of Organizational Objectives cont.

- **The questions include:**
  - **Is there a documented correlation between key organization milestones and the objectives of the ISP?**
  - **How many information security objectives were successfully completed in support of organizational goals?**
  - **Were there organization goals that were not fulfilled because information security objectives were not met?**
  - **How strong is consensus amount business units, executive management, and other information security stakeholders that program objectives are complete and appropriate?**

Measuring Compliance

- **An ISP has a primary and ongoing concern for policy and standard compliance**
  - **Most security failures are the result of personnel failing to follow procedures in compliance with standards and essential elements of security**
- **Compliance with technical standards are often straightforward and can be automated**
  - **Compliance with procedural or process standards is more troublesome**

Measuring Compliance cont.

- Depending on the standard being addressed, continuous monitoring may be installed or a more detective approach such as logging may be selected
  - It all depends on the criticality of the data being protected

Measuring Operational Productivity

- Managing the productivity of organizational resources is a key factor to properly utilizing the systems resources that are available

- There are several ways to increase the productivity within an organization
  - Use automation where possible
  - Outsource low-value operational tasks
  - Leverage business units activities that can be shared

Measuring Operational Productivity cont.

- The ISM should set periodic goal for increasing the productivity of the information security program through specific initiatives
  - The result should then be reviewed to determine the effectiveness

Measuring Security Cost-Effectiveness

- An ISP should be financially sustainable to avoid common security problems that result from improperly budgeting ongoing maintenance requirements

- The ISM must maximize investment expenses to ensure sustainable achievement of objectives
  - Key aspects of doing this are properly cost forecasting and budgeting
    - Comparing budget utilization vs. original projections is an useful tool for identifying security cost planning issues

Measuring Security Cost-Effectiveness cont.

- The ISM can also implement procedures to measure the ongoing cost-effectiveness of security components
  - This is often accomplish by tracking cost-result ratios
  - From this cost-efficiency goals can be set for new technologies

- A regular task of the ISM should the consideration of maintaining, operating and administering technical security components
  - The personnel costs associated with these expenses should also be reviewed

Measuring Organizational Awareness

- As stated previously the first line of defense for the organization are the employees
- They must be sufficiently trained and the effectiveness of the awareness programs should be properly measured
- Since awareness is most effectively tracked at the employee level, the ISM should work with HR to implement metrics
  - Metrics may include initial training, acceptance of policies and usage agreements, and ongoing awareness updates

Measuring Organizational Awareness cont.

- Tracking at this level can help to pinpoint individuals that may be in need of training and business units that may need to be addressed directly
- Other metrics for success could include results from short tests once employees complete a training session
  - Random quizzing could also be performed on samples of employees to determine the lasting effect of the training

Measuring Effectiveness of Technical Security Architecture

- The technical controls within an organizational should have quantitative measures of effectiveness
  - It is the job of the ISM to identify the metrics that will be most meaningful to the expected audience

- Examples of technical effectiveness metrics are provided on the next slide

Measuring Effectiveness of Technical Security Architecture cont.

- **Example quantitative metrics include:**
  - **Probe and attack attempts repelled by network access control devices**
  - **Probe and attack attempts detected by IDSs on internal network**
  - **Number and type of actual compromises**
  - **Statistics on viruses, worms, and other malware identified and neutralized**
  - **Amount of downtime attributable to security flaws and unpatched systems**
  - **Number of messages processed, session examined and kilobytes of data examined by IDSs**

Measuring Effectiveness of Technical Security Architecture cont..

- **Example qualitative metrics include:**
  - **Individual technical mechanisms have been tested to verify control objectives and policy enforcement**
  - **Control mechanisms are properly configured and monitored in real time, self-protection is implemented, and information personnel are alerted to faults**
  - **All critical systems stream events to information security personnel or to event analysis automation tools for real-time threat detection**

Measuring Effectiveness of Management Framework and Resources

- An ISP should have the ability to maximize the results from the processes that it implements
- Mechanisms should exist that can collect feedback, track consistently implemented systems, share knowledge well and articulate changes effectively
- Methods of tracking a program's success are included in the next slide

Measuring Effectiveness of Management Framework and Resources cont.

- **Methods include**
  - Tracking the frequency of issue recurrence
  - Monitoring the level of operation knowledge capture and dissemination
  - Degree to which process implementation are standardized
  - Clarity and completeness of documented information security roles and responsibilities
  - Incorporating information security requirements into every project plan
  - Efforts and results in making the program more productive and cost-effective
  - Overall security resource utilization and trends
  - Etc.

Measuring Operation Performance

- The proper measuring, monitoring and reporting on of information security processes helps the ISM to ensure operational components of the program support control objectives
- Measures of security operational performance include:
  - Time to detect, escalate, isolate and contain incidents
  - Time between vulnerability detection and resolution
  - Quantify, frequency, and severity of incident discovered after their occurrence
  - Average time between vendor release of vulnerability patches and their application
  - Etc.

Monitoring and Communication

- **Monitoring of controls are often broken up into three major categories**
  - **Technical monitoring**
  - **Procedural monitoring**
  - **Operational monitoring**

Technical Monitoring

- **Monitoring these types of controls normally consists of reviewing logs and various alerts for potential security vulnerabilities or emerging threats**
  - **IDS or firewalls**

Procedural Monitoring

- Monitoring these types of controls are just as important as the other, but can be difficult to implement

- The best way to perform this is the monitoring of physical processes with technical methods
  - Personnel usually interface with information systems at various points in processes and these are the control points that can be monitored

Operational Monitoring

- Monitoring information systems security is a critical operational component of any ISP
- The ISM should consider the implementation of a centralized monitoring environment that can provide visibility into all enterprise information resources

Operational Monitoring cont.

- **Commonly monitored event types include:**
  - **Failed access attempts to resources**
  - **Processing faults that may indicate system tampering**
  - **Outages, race conditions and faults related to design or other issues**
  - **Changes to system configurations, particularly security controls**
  - **Privileged system access and activities**
  - **Technical security component fault detection**

Information Security Program Challenges

Domain 3: Information Security Program Development and Management

ISP Potential Impediments

- Organizational resistance due to changes in areas of responsibility introduced by the program
- A perception that increased security will reduce access required for job functions
- Overreliance on subjective metrics
- Failure of strategy
- Assumptions of procedural compliance without confirming oversight

ISP Potential Impediments cont.

- Ineffective project management, delaying security initiatives
- Previously undetected, broken or buggy security software

Management Support

- A major problem that is seen in smaller organization is lack of management support
- Such companies often don't have standards that compel them towards addressing information security or simply don't make it a priority
  - Reasoning such as this show a lack of understanding of the organizations dependency on information systems, risk, or the impact the company faces
- The ISM must use information such as industry statistics, organizational impact reports, etc. to try and convince management of their judgment errors

Funding

- An additional frustration of ISMs can be found in the financial resources necessary to get started
- Some issues that the ISM must fight include:
  - Management not recognizing the value of security investments
  - Security being viewed as a low-value cost center
  - Management not understanding where existing money is going
  - The organizational need for security investment not being understood
  - The need for more awareness of industry trends in security investment

Funding cont.

- In an attempt to try and compensate for financial gaps, an ISM can try to exercise some of the following strategies
  - Leverage the budgets of other organization units to implement needed security program components
    - Product development, internal audit, information systems, etc.
  - Improve the efficiency of existing information security program components
  - Working with the information security steering committee to reprioritize security resource assignments and providing senior management with analysis of what security components will become under resourced and the associated risk implications

Staffing

- The problem of funding extends to proper staffing to meet the ISP requirements

- Some obstacles include the following:
  - Poor understanding of what activities new resources will do
  - Questioning the need or benefit of new resource activities
  - Lack of awareness of existing staff utilization levels or activities
  - Belief that existing staff are underutilized
  - Desire to examine outsourcing alternatives

Future Positives for Establishing ISPs

- **With increased legal and regulatory mandates the improvement of security is becoming an issue of national security and competitive viability**
  - **The expectations of customers and business partners is another positive nudge toward improving an organization's security posture**

- **Another push includes increased PCI DSS council security requirements**
  - **This affects the manner in which organizations process credit card information and as a result will improve aspects of information security globally**