Certified Information Security Manager (CISM) Course 1 - Information Security Governance Workbook
Topic A: Information Security Governance
Overview

- Information can be defined as data endowed with meaning and purpose
  - Information has become important in all aspects of our lives
  - It is an indispensable component of conducting business
  - For some companies, information IS the business - Google, eBay, Microsoft and others
Information Security Governance Overview

- All information today is nothing more than blocks of information stored on hard disks
- Information has become pervasive in society and business
- The dependence of information is higher than it’s ever been
- Information has become resource equaled importance of the traditional land, labor and capital
Information Security Governance Overview
Continued

- Gartner group has estimated that organizations will deal with more than 30 times information than they do today over the next decade
  - Considering the glaring vulnerabilities and perpetual crisis-mode activities this might not be as reassuring as it sounds
- To gain adequate protection for information resources, the issue should be raised regarding critical governance functions
Information Security Governance Overview Continued

- Until recently, the focus has been on protecting IT systems that store the information rather than the information itself
- Now information security takes a larger view than just the content, information and knowledge based on it
- Now we have to look at protecting information in all states of it being processed
- The enormous benefits of information has also seen new risks as well as a confusing patchwork of existing laws and regulations
Information Security Governance Overview
Continued

- Information security governance is a responsibility of the Board of Directors and executive management
- It should be an integral and transparent part of enterprise governance
Importance of Information Security Governance

- Information can be defined as data endowed with meaning and purpose
  - Others have stated that knowledge has become the sole factor for productivity, sideling both capital and labor
  - It goes without saying then that knowledge has become one the most important assets, without which conducting business would not be possible
  - Besides legal and regulatory requirements, good information security governance is simply called good business
The benefits of good management can include:
- Planning for the increase of civil or legal liability
- Assuring policy compliance
- Reducing uncertainty of business operations
- Optimizing allocations of limited security resources
- Ensuring that business decisions are not made on that information
- Improving competence in interactions with trading partners
- Improving trust and customer relationships
- Safeguarding the company’s reputation
Outcomes of Information Security Governance

- Information security governance should include the elements required to improve the assurance and direction to the security posture of the organization.
- With those elements in place, management should be confident that adequate and effective information security will protect these assets.
The objective of information security is to develop, implement and manage the security program to cover the following basic outcomes of security governance:

- **Strategic alignment** – the aligning information security to the business strategy to support:
  - Security requirements that are thoroughly developed to give guidance on what should be done
  - Security solutions that fit into the culture, governance style, technology and structure of the organization
  - Security is aligned with the enterprise strategy and the known threats, vulnerabilities, and risk profile
Outcomes of Information Security Governance
Continued

- Risk management – using appropriate measures to reduce risk and potential impacts on information
  - Understanding the threats, and vulnerabilities
  - Knowing the risk exposure and consequences of compromise
  - Awareness of risk management priorities
  - Reducing risk to an acceptable level
  - Risk acceptance/conference based on understanding of the potential consequences of residual risk
Outcomes of Information Security Governance

Continued

- Value delivery - optimizing security investments to support business objectives
  - This includes a set of security practices or baseline security requirements
  - Prioritizing the efforts to areas with the greatest impact and business benefit
  - Using a standards-based solution
  - Having complete solutions, covering the process as well as technology of the business organization
  - Knowing that security is a process not an event
Outcomes of Information Security Governance Continued

- Resource management – using information security knowledge and infrastructure efficiently and effectively
  - Make sure that knowledge is captured and available
  - Documenting security process and practices
  - Creating security architectures to define and utilize the infrastructure resources

- Performance measurement – monitoring reporting on information security processes to ensure the objectives are achieved
  - Having a set of metrics aligned with objectives
  - Finding shortcomings and receiving feedback
  - Having external audits to confirm security assertions
Outcomes of Information Security Governance Continued

- Integration – integrating all relevant assurance factors to ensure that processes operate as intended
  - List all organizational assurance functions
  - Coordinate assurance functions for complete security
  - Have overlapping roles and responsibilities
  - Use a systems approach to security planning, deployment and management
Topic B: Effective Information Security Governance

- Information security governance is a responsibility of the Board of Directors and executive management
- It must be integral and transparent as a part of the enterprise governance
- Good security governance is required to address legal and regulatory requirements and becoming mandatory in the exercise of due care
Business Goals and Objectives

- Business goals and objectives - the board and executive management should have a goal of providing a strategic direction in making sure the objectives are achieved
- The strategic direction of business is defined by business goals and objectives
- Information security governance is a subset of corporate governance
  - this should provide a strategic direction for security activities and a way to verify the objectives are achieved
The framework of governance usually consists of:

- A comprehensive security strategy linked with business objectives
- Governing security policies that address each aspect of strategy controls and regulation
- A set of standards for each policy
- A good security organizational structure with few conflicts of interest and also having sufficient authority and resources
- Standard metrics and monitoring processes to check on compliance, to provide feedback on effectiveness, and to be used for management decisions
Roles and Responsibilities of Senior Management

- **Board of Directors:**
  - Information security governance needs strategic direction as well as commitment, resources and the assignment of responsibilities
    - The board needs to be aware of the information assets and how critical they are to business operations which can be done through periodic reviews
    - Policies should always be top-down

- **Executive management:**
  - The policy set forth by senior management must have leadership and ongoing support from executive management to succeed
Roles and Responsibilities of Senior Management

- Steering committee:
  - A steering committee can be used to ensure to the stakeholders that all security considerations are reviewed.
  - The goal should be to achieve consensus on priorities and trade-offs.

- CISO:
  - Organizations should have a chief information security officer, even if not as a formal title.
  - This position exists, coupled with a responsibility, authority and required resources to manage information security.
Governance, Risk Management and Compliance

- Governance, risk management and compliance (GRC) is an example of the growing recognition of the convergence or assurance process integration.
- Governance:
  - This is the process by which an organization sets the risk tolerance, identifies risks and their associated impacts, and prioritizes their mitigation based on objectives and risk tolerance.
Governance, Risk Management and Compliance Continued

- Risk management:
  - This is a process that sets the risk tolerance, identifies potential risks, and the possible impacts, and prioritizes their mitigation based on the business objectives and risk tolerance

- Compliance:
  - Recording and monitoring the policies, procedures and controls used to ensure the policies and standards are all followed
  - GRC was initially a response to the Sarbanes-Oxley act
Business Model for Information Security

- (BMIS) started at the Institute for critical information infrastructure protection of the Marshall school of business at the University of Southern California. ISACA has worked on the development of the systematic security management model.
  - This theory says a system should be viewed entirely and not part by part. They should be viewed as a whole.
The four elements of this model are:

- **Organization design strategy** – an organization is a group of people, assets and processes working together towards a common goal. The organization strategy specifies business goals and objectives that should be achieved.
- **People** – human resources and the security issues that surround them are very important. This should be a definition of who implements each part of the strategy.
  - This may include recruitment strategy, hiring practices, employment issues, training and awareness, and termination.
Business Model for Information Security Continued

- **Process** – this includes formal and informal mechanisms that are needed to get things done.
- Processes identify, measure, manage and control risk, availability, integrity and confidentiality and they assure accountability.
- A process should be aligned with security policy business requirements.
- Consider emergence and be adaptable to change.
- Be well documented and communicated to the people.
- Be periodically reviewed.
Business Model for Information Security

Continued

- Technology – composes all of the tools, applications and infrastructure to make processes more efficient
- Technology makes up core part of enterprise infrastructure and is a critical component in accomplishing its mission
- Technology can be used to mitigate risk but should not be viewed as a complete solution
- People are still the weakest link.
Dynamic interconnections link the elements together and exert a multidirectional force that pushes and pulls as things change. This motion that occurs in dynamic interconnections can force the model out of balance or bring it back to a stable point.

The six dynamic interconnections are:
- Governance
- Culture
- Enablement and Support
- Emergence
- Human Factors
- Architecture
Dynamic Interconnections Continued

- Governance – sets the limits within which an enterprise operates and is implemented in the processes that monitor performance, describe activities and achieve compliance while also maintaining adaptability to current conditions.

- Culture – this is a pattern of behaviors, beliefs, assumptions and attitudes about how things are done.
  - Culture evolves like a shared history as a group that goes through a common set of experiences.
  - These behaviors become unwritten rules, which can become the normal way of doing business.
Dynamic Interconnections Continued

- Enablement and support – these are dynamic interconnections of technology to the process.
  - One method of compliance with technical security, measures, policies and procedures as directed make the process usable and easy, you might even say transparent
- Emergence – this can be described as a developing, growing and evolving of patterns that arise out of the life of the enterprise. The emergence of dynamic interaction between people and processes is a place to introduce solutions such as: feedback loops, process improvement, and other issues in the system design lifecycle
Dynamic Interconnections Continued

- **Human factors** – this could be considered the gap between technology and people which is critical to an information security program.
  - If people don’t understand how technology works they will probably not follow policies and potential security problems could evolve.

- **Architecture** – this may be a comprehensive informal encapsulation of the people, processes, policies and technology that comprise an organization’s security practice.
The following are basic concepts, terms and technologies that an information security manager should understand and implement within their job:

- **Access control** – the mechanisms that control access to information systems, resources and physical access
- **Architecture** – the structure and relationship of elements
- **Attacks** – the types of security breaches
- **Auditability** – listing transactions that occurred in a system
- **Authentication** – verification of an identity
Information Security Concepts and Technologies

- Authorization – what actions are allowed
- Availability – how accessible information is
- Business dependency analysis – how important a resource is to an organization
- Business impact analysis – understanding the results and consequences of compromise
- Confidentiality – protecting data in transit and at rest
- Controls – a process that lowers risk
- Countermeasures – an action or process that mitigates vulnerability
- Criticality – how important resources the business
Information Security Concepts and Technologies Continued

- Data classification – a sensitivity label placed on information
- Exposures – areas that may be subject to a threat
- Gap analysis – comparing the current situation to the objective
- Governance – providing control and direction to activities
- Identification – information provided by a person or thing
- Impact – the potential of risk materializing
- Integrity – accuracy and validity of information
- Layered security – Defense in depth
Information Security Concepts and Technologies

- Management – oversight of activities to ensure objectives are met
- Non-repudiation – being unable to deny involvement
- Policies – high-level blueprint of the management’s intent and direction
- Residual risk – that risk that remains after countermeasures
- Risk – the chance that a vulnerability can be exploited
- Security metrics – quantitative and periodic assessment security performance
- Sensitivity – level of impact from unauthorized disclosure
- Standards – boundaries of actions and processes as compared to policy
Information Security Concepts and Technologies Continued

- **Strategy** – the path to achieve an objective
- **Threats** – an action or event that would have a negative impact
- **Vulnerabilities** – a weakness that can be exploited
- **Enterprise architecture** – organizing logic for business processes
- **Security domains** – areas that are bound by different security policies
- **Trust models** – security controls and functions for different levels of security
Technologies

- As the security manager you should have knowledge of a variety of security technologies that can be used such as:
  - Firewalls
  - IDS, AV
  - PKI, SSL, encryption
  - SSO
  - Authentication, biometrics
  - VPNs
  - Forensics
  - Identity and Access Management
Topic D: Information Security Manager

- Most organizations have acknowledged a position of information security manager officer
- Many organizations are creating central information security departments
Reporting structures for information security varies widely from company to company.

- Recent surveys have shown that reporting is often done to the CIO which may be adequate functionally, but still seen as a suboptimal reporting method.
- Security is a regulatory function while IT is operational department.
- This means that issues dealing with security should be reported to the CEO.
- Often the CIO and the IT departments are under pressure to increase performance and cut costs, meaning security could be the victim of those priorities.
**Senior Management Commitment**

- The philosophy should always be “top-down”
  - The importance of security issues need to be approved from the upper management which may also mean educating them on the issues of security
- To gain higher levels of security senior management should be committed to:
  - High standards of corporate governance
  - Treating information security as a critical business issue
  - Showing third parties that their organization deals with security in a professional manner
  - Using principles such as assuming ultimate responsibility for security
Senior Management Commitment Continued

- Senior management can demonstrate commitment to security by:
  - Being directly involved in high-level information security arrangements such as the creation of the security policy
  - Having high level oversight and control
  - Ensuring sufficient resources are available
  - Defining metrics and monitoring
  - Auditing security effectiveness
  - By following security policies and practices
Obtaining Senior Management Commitment

- Most often a formal presentation is used to secure senior management commitment and gaining support of security policies, standards and strategy
  - This can also be a form of educating senior management
Obtaining Senior Management Commitment
Continued

- Senior management acceptance can be illustrated by:
  - Ensuring security objectives are aligned with business objectives
  - Understanding the consequences for failing to achieve security-related objectives and regulatory compliance
  - Identifying budget items that quantify the cost of security program
  - Using TCO or ROI to quantify the benefits of security
  - Defining a method of auditing the security program
Establishing Reporting and Communication Channels

- There should be a regular reporting to the Board of Directors or executive management regarding information security governance. The presentations could include:
  - Status on the implementation of security
  - Results from the BIA
  - Statistics of detected and/or prevented threats
  - Pointing out the weakest links in security
  - Performance measurement data as well as audit reports
  - Showing security support for business objectives
  - Obtaining the approval for renewed plans
Establishing Reporting and Communication Channels Continued

- The following communication channels are crucial to the success of security. The four groups requiring communications are:
  - Senior management – they should attend business strategy meetings become more aware of the updated business strategies and objectives
  - Business process owners – they should be made aware of the challenges and requirements of daily operations and the dependencies
  - Other management – may include line managers, supervisors and other department heads that have some responsibility of security policies
  - Employees – need to be trained about security programs. There should also be a training program for new employees
Topic E: Scope and Charter of Information Security Governance

- Security deals with information, whether spoken, written, or printed, as well as electronic
  - This also includes the lifespan of this information
- The following are considered a core set of principles that should be implemented for effective security governance:
  - CEOs conducting annual audits
  - The company conducting risk assessments, and then implementing policies and procedures based on those assessments
  - Assign explicit individual roles, responsibilities, authority and accountability
  - Employee training
  - Incident response procedures
  - Consider information security in the data lifecycle
Assurance Process Integration and Convergence

- Many companies organize processes into different “silos”. It is important that these processes are integrated together.
- Examples of these silos might be:
  - Risk management
  - Change management
  - Auditing
  - Human resources
  - Legal
Convergence

- Having different aspects of security divided into different bureaucracies often do not provide the optimum results
  - One example may be integration of physical security as it relates to data security
Governance and Third-Party Relationships

- Security governance should also cover the companies dealing with third-party relationships such as:
  - Service providers
  - Outsourced operations
  - Trading partners
  - Mergers
- The potential risks and impacts the third-party relationship should be clear and documented as well as having policies and standards involving information security with this third-party.
Topic F: Information Security Governance

Metrics

- Metrics are often used as a description of measurements
- Security in its meaning is protection from or absence of danger
- Therefore, metrics should then note the state or degree of safety relative to a reference point
Technical metrics can be useful and are often obtained from technical systems such as:
- Intrusion detection systems
- Proxy servers
- Firewalls

These types of metrics do not help from a strategic management or governance standpoint.
- These types of metrics do not relate to organizational objectives or how well risks are being managed.
Metrics Continued

- Technical metrics do not answer questions such as:
  - How secure is the organization?
  - How much is enough security?
  - Has an adequate level of security been achieved?
  - What is the degree of risk?
  - Is the security programming reaching its objectives?
  - How does a lack of security affect business productivity?
  - What is the impact of a catastrophic security breach?
Effective Security Metrics

- Without effective metrics it’s difficult if not impossible to manage any security activity
  - Useful metrics should be fundamental in decision support
- Effective metrics, are not really measured in an absolute sense, but instead with probabilities, attributes, effects and consequences. Useful Approaches would be:
  - Value of risk
  - Return on security investment
  - Annual loss expectancies
Effective Security Metrics Continued

- Some metrics are obtained through security audit, which could measure some of the defenses, but unless all potential attacks are tested it is still not possible to predict the security of an organization
  - For example, some organizations are attacked more often than others
  - It may be true that there is a correlation between good security and relatively fewer incidents and losses but it’s not a given
Effective Security Metrics Continued

- The components of effective security metrics should be composed of:
  - Results oriented metric analysis
  - Quantifiable performance metrics
    - ROI, ALE, VAR
  - Practical security policies and procedures
  - Strong upper-level management support
- Combining these can make up a well governed security program
Implementing security requires a lot of work, therefore there should be some form of metrics in place to monitor the implementation.

- Key goal indicators (KG I)
- Key performance indicators (KPI)

These are useful to provide information about the achievement of a process or service goal as well as determining when milestones and objectives are met.
Strategic Alignment

- The alignment of information security with organizational objectives is the desired goal.
- Without organizational objectives being used as a reference point, then any other gauge which might include, best practices, could be overkill, inadequate or misdirected.
Strategic Alignment Continued

- The best indicator of alignment is as follows:
  - Security programs that enable specific business activities
  - A security organization that is responsive to business requirements
  - The security objectives are understood by all involved
  - Security programs that are mapped to organizational objectives
It can be said that risk management is the ultimate objective of all information security activities.

There is no real direct measurement of risk management’s effectiveness, but there are indicators to show that it can be successful. These indicators could be:

- Understanding the company’s risk type
- A security strategy to achieve an acceptable level of risk
- Demonstration of risk mitigation
- Defined processes to reduce the impacts of risk
- A tested BCP/DRP
- The conducting of a BIA
Value Delivery

- This is a function of the alignment of security business objectives, leading to an optimal investment to achieve acceptable risk. Key indicators could include:
  - Cost of protection as a function of revenue or asset value
  - Security resources allocated by assessed risk and potential impact
  - Periodic testing of controls
  - Periodic review of costs along with compliance and effectiveness
This is thought of as a way to describe the processes to plan, allocate and control information security resources such as:
- People
- Processes
- Technologies
Resource Management Continued

- Indications of good resource management can include:
  - Infrequent problem rediscovery
  - Good knowledge capture and dissemination
  - Standardized processes
  - Well-defined roles and responsibilities
  - Information assets and the threats covered by security resources
  - The proper organizational location, level of authority, and personnel for the security function
Performance Measurement

- Metrics of information security processes are needed to ensure the organizations objectives are achieved
  - You cannot manage what you cannot measure
- Indicators of good performance measurements are:
  - How long it takes to detect and report an incident
  - The number and frequency of unreported incidents
  - Comparison of cost and effectiveness
  - Ability to determine a controls effectiveness
  - Documenting security objectives are being met
  - Consistency of log review practices
Assurance Process Integration/Convergence

- A good integration of these processes should work from end-to-end to minimize hidden risks and should include:
  - Information asset protection
  - Eliminating security overlaps
  - Well-defined roles and responsibilities
  - Understanding one assurance function with another
A quote from Concept of Corporate Strategy, second edition:

“Corporate strategy is the pattern of decisions in a company that determines and reveals its objectives, purposes, or goals, produces the principle policies and plans for achieving those goals, defines the range of business the company is to pursue, the kind of economic and human organization it is or intends to be, and the nature of the economic and non-economic contribution it intends to make to its shareholders, employees, customers, and communities”
Another View of Strategy

- It could be said that strategic outcomes cannot be predetermined from past events
- Well-managed initiatives should be balanced across all activities of adapting the core business to meet future challenges.
Topic H: Creating Information Security Strategy

- In creating a strategy, management should try to avoid common pitfalls while working to achieve the desired outcome
Common Pitfalls

- Overconfidence
- Optimism
- Anchoring
- The status quo bias
- Mental accounting
- The herding instinct
- False consensus
Objectives of the Information Security Strategy

- The objectives for creating information security strategies should be defined in metrics to determine if objectives have been met. Those objectives might be:
  - Strategic alignment
  - Risk management
  - Value delivery
  - Resource management
  - Performance measurement
  - Process assurance integration
What is the Goal?

- How does an organization know if it has an effective security strategy if the goal is unknown?
  - The objectives of a security strategy should have specifics
  - One approach is to assign values to information resources based on importance
  - Another approach could be to rate a business's dependency on an asset
  - Information ratings might be as follows: confidential, internal use, and public
Defining Objectives

- Again, a good security strategy is used as the basis for plan of action, it is necessary to define the objectives to have a “desired state”
  - Without an objective the strategy may be created in an ad hoc fashion
  - Some objectives may simply be made to lower risks
  - Objectives should also deal with aligning the strategy to the business objectives
Business Linkages

- Business linkages should be viewed from the perspective of the business objectives
  - For example, an e-commerce based business may seem relatively straightforward, but most will rely on information from banks, warehouses, suppliers, and protecting customer information
  - Understanding that perspective can help in building the proper objectives
The main purpose of a formal business case process is:

- Introducing a way of thinking that may cause people to recommend projects and consider their cost, risk, and relative priority
- Require those making the proposal to justify its value to the organization
- Determine if the proposal is of value as well as being achievable
A good business case should include some of the following:
- Reference – information
- Context – business objectives
- Value proposition – desired business outcomes
- Focus – problem/solution scope
- Deliverables – outcomes, benefits
- Dependencies – critical success factors
- Project metrics – key goal indicators
- Workload – approach, phase/stage definitions
- Required resources – project leadership team
- Commitments – project controls, review schedules
Business Case Development Continued

- A business case should be evaluated and reviewed to determine:
  - If it actually has value and importance
  - To determine if it will be managed properly
  - Can the benefits be delivered
  - Are there dedicated resources
  - Are interdependent projects being undertaken in the correct sequence
Business Case Objectives

The business case process should be:

- Adaptable – tailored to the size and risk of the proposal
- Consistent – the same basic business issues addressed by each project
- Business-oriented – concerning business capabilities and impact
- Comprehensive – including all relevant factors for evaluation
- Understandable – clearly relevant, logical, and simple to evaluate
- Measurable – key aspects are quantifiable
- Transparent – key elements can be justified directly
- Accountable – costs are clear
The Desired State

- Desired state is a reference to a snapshot of the conditions of a particular point in the future
  - The state of security cannot be quantitatively defined; therefore, it should be defined in qualitative terms regarding attributes, characteristics, and outcomes
  - These should be as well-defined as possible
COBIT focuses on IT related processes from IT governance, management and control perspectives.

- COBIT is a framework of supporting tools to bridge the gap between technical issues and business risks.
- With regards to the CISM, control objectives and procedures should extend beyond IT activities to include any activity that could impact information security.
These are defined as policies, procedures, practices and organizational structures designed to provide reasonable assurance of business objectives being achieved

COBIT defines enterprise governance as a set of responsibilities and practices exercised by the board and executive management
The 34 processes to manage and control information technology are divided in four domains:

- **Plan and organize** – strategy and tactics to achieve business objectives
- **Acquire and implement** – identify, develop, or acquire IT solutions
- **Deliver and support** – deliver of required services or training
- **Monitor and evaluate** – assessment for quality and compliance with requirements
The desired state of security can be defined as achieving its specific level in the capability maturity model, which we described as:

- 0 or nonexistent
- 1 or ad hoc – no formal process
- 2 or repeatable but intuitive – emerging understanding of risk
- 3 or defined process – company wide risk management policy
- 4 or managed and measurable – risk assessment, procedures, policies
- 5 or optimized – organization wide process implemented, monitored and managed
Balanced Scorecard

- This is a management and measurement system to help organizations clarify their vision and strategy and translate them into action.
- The balance scorecard uses four perspectives:
  - Learning and growth
  - Business process
  - Customer
  - Financial
Enterprise Information Security Architecture (EISA) is a subset of enterprise architecture.
- There is a number of different methodologies that have evolved, including process models, frameworks, and ad hoc approaches.
- Architectural approaches that are inclusive of business processes that may help in defining the desired state of security can be exemplified by the open group architecture framework (TOGAF), the Zachman enterprise architecture framework, or the extended enterprise architecture framework (EA2F).
ISO/IEC 27001 and 27002

To cover all relevant elements of security, the standards provide 11 areas as a useful framework:
- Security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information security acquisition development and maintenance
- Information security incident management
- Business continuity management
- Compliance
Risk Objectives

- The major factor in the defining of the desired state involves the approach to risk and risk appetite
  - Without a clear determination of acceptable risk it is difficult to determine whether security is meeting its objectives
  - Operational risk management exemplifies the trade-off of the risk associated with taking an action or the risk of not taking the action
Risk Objectives Continued

- Risks carry cost usually expressed as the annual loss expectation (ALE)
- Acceptable risk can be quantified using the business continuity approach of developing recovery time objectives
- Developing the right strategy objectives usually needs to be an interactive approach based on the analysis of costs to achieve the desired state and reaching acceptable risk levels
The current state of security must be evaluated with the same methodologies that were used to determine the desired state.

- Using different frameworks will not avail the use of a gap analysis to determine if the stated objectives have been achieved.
Current Risk

- Current state of risk should be assessed by a comprehensive risk assessment, just as risk objectives must be determined as a part of the desired state
  - A full risk assessment includes threat and vulnerability analysis
  - May also include a Business Impact Analysis
Current Risk Continued

- Risks can be addressed in different ways such as:
  - Changing risky behavior
  - Developing countermeasures
  - Reducing vulnerabilities
  - Developing controls
The current risk should include a thorough Business Impact Analysis of critical systems and processes to gain a current state of security.

- A Business Impact Analysis will provide some of the information needed to create an effective strategy.
- The difference between acceptable levels of impact and current levels of potential impact must be addressed by the strategy.
Based on a successful risk assessment, a meaningful security strategy can be developed. By knowing the current state of security and the desired state, we have a process of developing a strategy to achieve the desired state. This will provide the framework for creating a road map.
The question is, what should go into a security strategy, and have the starting point and destination been defined?

The roadmap: this should be a document that maps how to achieve the defined, security desired state. These would include:

- People
- Processes
- Technologies
- Other resources
Prior to beginning the roadmap to desired security, an architecture should be chosen as a framework from which to begin.

- Remember that the desired state is usually a long-term goal that may consist of a series of projects and initiatives.
- This means the overall roadmap would be broken down into a series of short-term projects.

The Roadmap
Strategy Resources and Constraints

- Resources are what's available to the organization and should be listed and considered when developing a security strategy; these could typically be:
  - Policies, standards, procedures and guidelines
  - Physical, technical, and procedural controls
  - Countermeasures
  - Layer defenses
  - Technologies
  - Organizational structure
  - Roles and responsibilities
  - Skills, training, awareness and education
  - Audits and compliance enforcements
  - Risk and business impact assessments
Constraints must be considered when developing a security strategy, and these typically include:

- Legal issues
- Physical environment
- Ethics
- Culture
- Costs
- Personnel and organizational structure
- Resources and capabilities
- Time
- Risk tolerance
The information security manager should determine what resources are available as well as being aware of potential constraints.

- Cultural
- Financial
- Resources
- Other reasons
Policies and Standards

- The definitions used in this lesson are in agreement with the major standards bodies and should be adopted to avoid any confusion
  - For example, policies and standards are considered tools of governance and management, respectively
  - Procedures and guidelines would be the purview of operations
Definitions

- Policies: the high-level statements of management intent, expectations and direction; these usually remain static
- Standards: represent the metrics, allowable boundaries, or the process used to decide if procedures, processes or systems meet policy requirements
- Procedures: clarify the responsibility of operations, including security operations; they should provide the step-by-step instructions required for an activity
- Guidelines: are used for executing procedures and contain information that’s helpful and exceeding procedure
Enterprise Information Security Architectures

- This can be a powerful integrating tool when used in developing a strategy
  - Think of this as the blueprint that’s used to build a house
  - Although it is possible to develop a strategy without architecture, there can be some serious drawbacks, such as:
    - Less functional security integration
    - Increased expense and time-consuming
These are the primary components to consider when developing an information security strategy. Controls can be categorized as physical, technical or procedural. Examples may be:

- IT controls
  - COBIT focuses on IT controls; they may have some of the most comprehensive approaches to determining control objectives
- Non-IT controls
  - Controls for handling non-technical events, such as social engineering or device re-use
- Layer defenses
  - One layer failure does not cascade to the next layer
Countermeasures

- These are measures of protection that reduce the level vulnerability to threats. Sometimes these are thought of as targeted controls
  - One example may be in restricting access to important information from a secure subnet
Technologies

- Types of technologies used to improve security has continued to evolve over the years
  - As an information security manager, one should be familiar with how these technologies can help achieve the desired state of security
Personnel

- Personnel security is an important area for an information security manager
- Unfortunately, personnel are often the weakest link with security
  - Damage from personnel can be intentional or accidental
  - Personnel are usually the first line of defense
  - Proper background screening should be conducted on all new hires
  - Methods of tracking the theft information should be developed
Organizational Structure

- It is not enough for the information security manager to simply verify that managers report to the CIO.
- Determine the type of management models that might be used such as:
  - Centralized
  - Decentralized
  - Distributed
Employee Roles and Responsibilities

- A security strategy should include a mechanism that defines all security roles and responsibilities as well as listing them within job descriptions.
  - Including security issues within an employee’s job performance is often sufficient to improve an employee’s security awareness.
Skills

- It would be prudent to create a skills inventory from amongst the existing employees
  - These skills may be important in implementing a security strategy
- Training, education and awareness are always vital to the overall strategy
  - This is especially true in dealing with security issues
Audits

- Internal and external audits are the main methods of determining any information security deficiencies that might exist
  - Internal audits in most large organizations are conducted by internal departments, and they generally report to chief risk officer or to an audit committee
    - Usually the focus is on policy compliance
  - External audits are often under the purview of the finance department
    - These are often not done with the security department
Compliance Enforcement

- Procedures for security violations should be completed
  - Again, these need to be supported from the top-down, especially in the area of enforcement
- One effective approach to compliance is an open system of trust
  - This should include self-reporting
  - There should also be voluntary compliance
Threat Assessment

- This is usually a part of risk assessment that is important for the strategic consideration of the policies
  - The threats will ultimately lead to the choice of controls used for mitigation of the risk
  - Policy development should map to a threat profile
    - Often this is because threats are constant in some sense (fires, floods, malware, theft)
  - Vulnerabilities change frequently as a result of changes in business, processes, technology and personnel
Vulnerability Assessment

- Often conducted by automated scans but by themselves are limited in their value
  - There should also be human involvement
  - These assessments should include:
    - Processes
    - Technology
    - Facilities
Risk Assessment

- Risk assessment is accomplished by first determining the viable threats to information resources
  - This includes physical and environmental as well as technology
  - The assessment should include the likelihood of the threat occurring
  - Frequency of occurrence as well as magnitude should be included in this assessment
- Formal risk assessment should first determine the viable threats
  - The magnitude of the threats
  - The probability of the threat occurring
Insurance

Some risks may be addressed by transference of the risk to a third-party, such as the purchase of insurance:

- Natural disasters
- Property damage
- Liability insurance
- Business interruption
Business Impact Assessment

- Consider this the “bottom line” of risk
  - The BIA is designed to consider the criticality and sensitivity of systems and information
  - Resource dependency analysis
    - Examples can be things such as office supplies or human resources
  - BCP/DRP
Outsourced Security Providers

- This is an increasingly common solution and is considered a way to focus on cutting costs for business, to allow more work on core competencies
  - Some risks can be found by outsourcing
    - Culture
    - Systems
    - Technology
    - Communications with the third-party
Many constraints must be considered when creating a security strategy; these will set the boundaries of available options.
Legal and Regulatory Requirements

- Legal and regulatory requirements for another jurisdiction that the corporation does business in
  - Companies should be familiar with any regulatory issues that deal with business abroad
    - Privacy laws
    - Tax laws
    - Restrictions on data import/export
  - Many requirements exist for the retention of content and business records
    - This is also called E-discovery
Physical Constraints

- A security strategy may be limited by the physical and environmental factors
  - Facilities placement can be of concern - an example might be having facilities in a high crime area
  - Environmental factors might include the frequency of flooding
  - Strategy could simply be constrained based on the infrastructure's capacity
Further considerations for security strategy should include:
- Ethics
- Culture
- Organizational structure
- Costs
- Personnel
- Resources
- Capabilities
- Time
- Risk tolerance
To implement a security strategy often involves one or more projects or initiatives. This should be an analysis of the gaps between the current state and the desired state for each defined metric.
Gap Analysis

- Gap analysis should be required to compare the state of current components to the goal of the strategy
  - This could include:
    - Maturity levels
    - Control objectives
    - Risk and impact objectives
  - The gap analysis can help identify the steps needed to achieve the security strategy
Gap Analysis Continued

- One approach to gap analysis is to start backward from the endpoint to the current state; this process can help determine the steps needed to achieve the objective
- CMM or other methods can be used
Gap Analysis Continued

- The following are areas that should be included:
  - Senior management acceptance
  - Strategy linked to business objectives
  - Policies consistent with strategy
  - Clear assignment of roles and responsibilities
  - Procedures for all operations
  - Assets that have been clearly classified for criticality
  - Proper controls have been chosen
  - A method of evaluation and monitoring
  - A tested BCP/DRP
Policy Development

- IT policy may have to undergo changes in the execution of the strategy
  - Policies should capture the intent, expectations and direction of management as well as stating compliance to regulatory conditions
  - If one of the objectives is an ISO compliance, then the policy should address any relevant domain or subsection of that certification
  - Policies should be linked to strategy elements; if not, then either the strategy or the policy is incorrect
Policy Development Continued

- Policies allow the primary elements of governance and as such must be properly created, except when invalidated by executive management.

- Attributes of a good policy might be:
  - Showing compliance with strategy
  - Each single policy having one security mandate
  - Clear and easily understood
  - Policies should be brief
  - They should reflect the common practices of the business
Standards Development

- Standards are security management tools that set the permissible bounds for procedures and practices regarding technology systems
  - The standard can be thought of as the law supporting policy
  - Standards of responsibility of the information security manager
  - Standards must be communicated to those who have to follow them
  - In some cases, there should also be a plan for exceptions to the standards
Training and Awareness

- Training should be considered as a part of an action plan to implement security strategy
  - Those receiving training should see the link between the standards and the policies
  - Training and awareness is a continual process as standards or policies may evolve as needed
Action Plan Metrics

- This is an important method of monitoring and measuring the progress of the implementation of the strategy
  - Milestones
  - Deviations can be found through metrics
- Monitoring could be done through the following:
  - Balanced scorecard
  - CMM
  - Other key performance indicators (KPI)
  - Critical success factors (CSF)
  - Key goal indicators (KGI)
General Metric Considerations

- All measurements should be relevant to the strategy
  - The main goal of the metric is to provide information to make decisions
  - Metrics generally fall into one of three categories:
    - Strategic
    - Tactical
    - Operational
General Metrics Continued

- There are metrics that exclude the evaluation of a technical perspective but should also be included, such as:
  - Progress compared to the plan and budget
  - Results of disaster recovery testing
  - Audit results
  - Regulatory compliance status
General Metrics Continued

- From the technical perspective there may be more information needed for a tactical perspective, such as:
  - Policy compliance metrics
  - Changes to a process or system that might change the risk profile
  - Patch management status
General Metrics Continued

- From the technical perspective you may want to include items such as:
  - Vulnerability scan results
  - Server configuration standards
  - IDS monitoring results
  - Firewall and other security device log analysis
CMM4 Statements

- The assessment of risk is a standard procedure, and exceptions to following the procedure would be noticed by security management.
- Information security risk management is a defined management function with senior-level responsibility.
- Senior management and information security management have determined the levels of risk that the organization will tolerate and have an appropriate risk/return ratio measurement.
Objectives for CMM4

- **Intermediate goals:**
  - Identify current applications in use
  - Reviewing 25% of information stored to determine ownership, criticality and sensitivity
  - Each business unit conducting a BIA
  - Business units achieving regulatory compliance
  - Security roles and responsibilities have defined risk assessment performed by each business unit
  - Training education, policy
  - Link policy with security strategy
Review Questions:

1. A security strategy is important for an organization primarily because it provides:
   A. A basis for determining the best logical security architecture for the organization
   B. Management intent and direction for security activities
   C. Provides users guidance on how to operate securely in everyday tasks
   D. Helps IT auditors ensure compliance

2. The most important reason to make sure there is good communication about security throughout the organization is:
   A. To make security more palatable to resistant employees
   B. Because people are the biggest security risk
   C. To inform business units about security strategy
   D. To conform to regulations requiring all employees to be informed about security

3. The regulatory environment for most organizations mandates a variety of security-related activities. It is most important that the information security manager:
   A. Relies on corporate counsel to advise which regulations are the most relevant
   B. Stays current with all relevant regulations and requests legal interpretation
   C. Involves all impacted departments and treats regulations as just another risk
   D. Ignores many of the regulations that have no teeth

4. The most important consideration in developing security policies is:
   A. They are based on a threat profile
   B. They are complete, and no detail is left out
   C. Management signs off on them
   D. All employees read and understand them

5. The primary security objective in creating good procedures is:
   A. To make sure they work as intended
   B. They are complete and no detail is left out
   C. Management signs off on them
   D. All employees read and understand them
6. The assignment of roles and responsibilities will be most effective if:
   A. There is senior management support
   B. The assignments are consistent with proficiencies
   C. Roles are mapped to required competencies
   D. Responsibilities are undertaken on a voluntary basis

7. The primary benefit that organizations derive from effective information security governance is:
   A. Ensuring appropriate regulatory compliance
   B. Ensuring acceptable levels of disruption
   C. Prioritizing allocation of remedial resources
   D. Maximizing return on security investments
Answer Key:

1. B
   A security strategy will define management intent and direction for a security program. It should also be a statement of how security aligns with and supports business objectives, and provides the basis for good security governance.

2. B
   Communication is important to ensure continued awareness of security policies and procedures. Communication is an important monitoring tool for the security manager to be aware of potential security issues. Security failures are, in the majority of instances, directly attributed to lack of awareness or failure of employees to follow procedures.

3. C
   While it can be useful to stay abreast of all current and emerging regulations, it can be a full-time job on its own. Treating regulations as another risk puts them in the proper perspective, and the mechanisms to deal with them should already exist.

4. A
   The basis for relevant security policies must be based on viable threats to the organization, prioritized by their potential impact on the business. The strictest policies apply to the areas of greatest risk. This ensures that proportionality is maintained and great effort is not expended on unlikely threats or threats with trivial impacts.

5. B
   All of the answers are obviously important, but the first criteria must be to ensure that there is no ambiguity in the procedures and that from a security perspective, they meet the applicable standards, and therefore comply with policy. While it is important to make sure that procedures work as intended, the fact that they do not may not be a security issue.

6. B
   The level of effectiveness of employees will be determined by their existing knowledge and capabilities; in other words, their proficiencies. Senior management support is always important but not essential to effectiveness of employee activities. Mapping roles to the tasks that are required can be useful, but is no guarantee that people can perform the required task.
7. B
The bottom line of security efforts is to ensure that business can continue with an acceptable level of disruption that does not unduly constrain revenue-producing activities. The other choices are useful but subordinate outcomes as well.