CISM STUDY GUIDE

Contents: Page

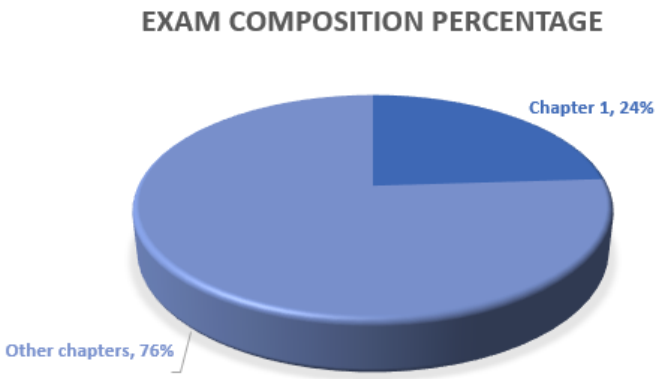
Chapter 3 & 4 in CISM Certification Study Guide Part 2

Take the CISM Practice Assessment to See if You Are Ready To Get CISM Certified

CHAPTER 1:

Information Security Governance

Exam Relevance: 24% (approximately 48 questions)



Objective

Ensure that the information security manager has the knowledge to establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly

Information Security Governance Overview

- **Information** has become an indispensable component of conducting business for virtually all organizations.
- **Information security governance** is the set of responsibilities and practices exercised by the board and executive management

Information vs. Knowledge

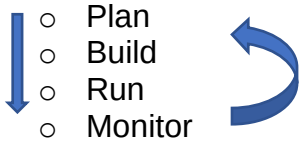
- **Information** can be defined as "**data endowed with meaning and purpose**." It is the substance of knowledge.
- **Knowledge** is, in turn, captured, transported and stored as **organized information**.

Information Security Governance

- Must be addressed at the **highest organizational level**
- Is part of **enterprise governance**
- **Executive management & board of directors** are accountable and must provide the necessary:
    - Leadership
    - Organizational structures
    - Processes

Management Tasks

- Any management process involves four key phase:
    - Plan
    - Build
    - Run
    - Monitor



Repeat as necessary

- IS governance focuses on high-level planning as a foundation for management activities

Information Security Manager's Responsibility

Executive management looks to the ISM to:

- **Define and manage** the information security program
- **Provide education and guidance** to the executive team
- **Present options** and information to enable decision making
- Acts an **information security advisor**

Importance of Information Security Governance

Benefits of strong information security governance include:

- Improving trust in customer relationships
- Protecting the organization's reputation
- Providing accountability for safeguarding information during critical business activities

Importance of Information Security Governance

Effective information security can add significant value to organizations by:

- **Reducing losses** from security-related events

- **Providing assurance** that security incidents and breaches are not catastrophic

Frameworks Enable Governance

- Establish:
  - Basis for consistent/ **repeatable behavior**
  - Eliminates the "**moving target**"
- Formal, documented evidence of stewardship
- Demonstrates due diligence to employee / business partners/customers/other stakeholders
- Should serve as basis for audit criteria and employee evaluations

IT is a Basic Business Requirement

- Rules are required for all types of business processes and activities:
  - Sales processes, hiring firing routines, payables accounting, workplace etiquette, environmental/ disposal practices
- Information security is no different:
  - Relatively complex rules need to be spelled out to all information system stakeholders/users

Most Governance Transcends Technology

- Based on principles that go beyond a particular technology or platform:
  - "**Information is a valuable asset that requires protection from unauthorized access or disclosure**."
- Anchored in sound **business goals** and ideals
- Helps organization deal with rapidly changing technological environment:
  - Passwords… pass phrases… two keys… biometrics

Governance Owner/ Sponsor

- Depends on how information security is integrated into the organization
- Elevation of information security to the level of an officer within an organization is evidence that **senior management understands** the need to integrate information security governance into the overall enterprise governance framework
  - Example: if role exists, Chief Information Security Officer
- The **CISO** position has been gaining popularity.

- Percentage of respondents saying their companies have a security executive:
  - In 2011, > 80%
  - In 2006, 22%
- One-third of CISOs report to CIOs
- 35% of CISOs report to CEOs
- 28% of CISOs report to board of directors

Outcomes of Information Security Governance

- **Strategic alignment**:
  - Aligned with **business strategy** to support objectives
- **Risk management**
  - **Mitigate** risk and **reduce** impacts to **acceptable levels**
- **Value delivery**
  - Optimizing security investments **in support of objectives**
- **Resource optimization**
  - Security knowledge/ infrastructure used efficiently/ effectively
- **Performance measurement**
  - Monitoring and reporting to ensure objectives achieved
- **Integration**
  - Integrate relevant assurance factors to ensure that processes operate as intended from end to end

Effective Information Security Governance

- **BMIS-** a clear organizational strategy for preservation is equally important to and must accompany a strategy for progress
- **CMU-** viewing adequate security as a non-negotiable requirement of being in business

Business Goals and Objectives

- **Corporate governance** is the set of responsibilities and practices exercised by the board and executive management:
- Goals include:

    - Providing **strategic direction**
    - Ensuring that objectives are achieved
    - Ascertaining that risk is **managed appropriately**
    - Verifying that the enterprise's resources are used responsibly
- What is information security governance?
    - Is a subset of corporate governance
    - Provide strategic direction for security activities and ensures that objectives are achieved
    - Ensures that information security risk is appropriately managed
    - Also helps ensure that information resources are used responsibly
- To achieve effective information security governance, management must establish and maintain a **framework**
    - **Framework** will guide the development and management of a comprehensive information security program that supports business objectives
- The governance framework generally consists of:
    - A comprehensive **security strategy** linked with business objectives
    - **Security policies** that address each aspect of strategy, controls and regulation
    - A complete set of **standards** for each policy
    - An **organizational structure** void of conflicts of interest with sufficient authority and resources
    - **Metrics and monitoring** processes to ensure compliance and provide feedback

Scope and Charter of Information Security Governance

- Information security deals with ***all*** **aspects** of information.
- **IT security** is concerned with security of information within the boundaries of the technology domain

Roles and Responsibilities of Senior Management

- **Board of directors/ senior management**
    - Information security governance
- **Executive management**
    - Implementing effective security governance and defining the strategic security objectives
- **Steering committee**

    - Ensuring that all stakeholders impacted by security considerations are involved
- **Chief information security officer (CISO)**
    - Responsibilities currently range from the CISO who reports to the CEO to system administrators who have part-time responsibility for security management

Information Security Roles and Responsibilities

- **Information Security Manager**
    - Develops security strategy with input from key business units and approval of strategy by senior leadership
    - Educates management
- Information Security Requires:
    - **Leadership** and ongoing **support from senior management**
    - Integration with and **cooperation from organizational business unit** management
    - Establishing reporting and communication channels

Governance, Risk Management and Compliance

GRC-approach adopted by many organizations to combine assurance processes including:

- Internal Audit
- Compliance programs (SOX)
- Enterprise risk management (ERM)
- Incident management

An IT GRC program generally includes:

- Controls and policy library
- Policy distribution and response
- IT control self-assessment and measurement
- IT asset repository
- Automated general computer control collection
- Remediation and exception management
- Reporting
- Advance IT risk evaluation and compliance dashboards

Business Model for Information Security

- Model originated at the Institute for Critical Information Infrastructure Protection
- A business-oriented approach to managing information security
- Best viewed as flexible, 3-D, pyramid-shaped structure made up of four elements linked by six dynamic interactions

Assurance Process Integration-Convergence

Information security has traditionally been executed in silos, using different terminology and reporting structures. Drivers for convergence are:

- Rapid expansion of the enterprise ecosystem
- Value migration from physical to information-based and intangibles assets
- New protective technologies blurring functional boundaries
- New compliance and regulatory regimes
- Continuing pressure to reduce cost

Goals of convergence are to:

- Reduce security gaps
- Minimize duplication of efforts
- Increase return on security investment

Information Security Concepts and Technologies

- **Access Control**-who/how someone can access a resource
- **Auditability**-enable reconstruction, review and examination of sequence of events
- **Authentication**-verify identity: something you know, something you have and something you are
- **Authorization**-what you can do once you have access
- **Availability**-accessible and usable when required
- **Confidentiality**-data secrecy
- **Integrity**-assurance of no unauthorized modification in processing, transmission and storage
- **Layered security**-defense in-depth
- **Nonrepudiation**-cannot deny

Governance and Third-party Relationships

Rules in processes for:

- Service providers

- Outsourced operations
- Trading partners
- Merged or acquired organization

Information Security Governance Metrics

- **Metrics** is a term used to denote measurements based on one or more references and involves at least two points, the measurement and the reference.
- **Contemporary security metrics** usually *fail* to tell us about the state or degree of safety relative to a reference point.
- It is difficult or impossible to manage any activity that cannot be measured
- Standard security metrics may include:
    - Downtime due to viruses
    - Percentage of servers patched
    - Number of penetrations of systems
- No metric in and of itself actually provides information on how *secure* the organization actually is, however-all that can be stated is that:
    - Some organizations are attacked more frequently and/or suffer greater losses than others.
    - There is a strong correlation between good security management and practices and relatively fewer incidents and losses.
- Key goal indicators **(KGIs)** and key performance indicators **(KPIs)** can be useful in providing information about achievement of process or service goals
- KGIs tend to reflect more **strategic goals**
- KPIs tend to reflect more **tactical goals**
- **Strategic alignment** of information security in **support of organizational objectives** is a highly desirable goal
- The best overall indicator that security activities are in alignment with business objectives is a **security strategy that defines security objectives in business terms**
- Indicators of alignment are as follows:
    - The extent to which the security program demonstrably enables specific business activities
    - Business activities delayed or not undertaken because of inadequate risk management capability
    - A security organization that is responsive to **defined business requirements**
    - Organizational and security objectives that are defined and clearly understood by all involved in security and related assurance activities
    - Security programs that are mapped to organizational objectives
    - A security steering committee consisting of key executives with a charter to ensure ongoing alignment of security activities and business strategy
- **Value delivery** occurs when security investments are optimized in support of organizational objectives
- **KPIs and KGIs** are used to demonstrate value delivery

- Information security resource management includes:
  - Processes to plan, allocate, and control information security resources
  - People, processes, and technologies for improving the efficiency and effectiveness of business solutions
- Indicators of effective resource management can include:
  - Infrequent problem rediscovery
  - Effective knowledge capture and dissemination
  - The extent to which security-related processes are standardized
  - Clearly defined roles and responsibilities
  - Information security functions incorporated into every project plan
  - The proper organizational location, level of authority and number of personnel for the information security function
- **Measuring, monitoring, and reporting** on information security processes is required to ensure that organizational objectives are achieved
- Metrics that provide an indication of the performance of the security machinery are among the most frequently used types of performance measures
- Indicators of effective performance measurement:
  - The **time** it takes to detect and report security-related incidents
  - The number and frequency of subsequently discovered unreported incidents
  - **Benchmarking** comparable organizations for costs and effectiveness
  - The ability to determine the effectiveness/efficiency of controls
  - Clear indications that security objectives are being met
  - The absence of unexpected security events
  - Knowledge of **impending threats**
  - Effective means of determining **organizational vulnerabilities**
  - Consistency of log review practices
  - Results of business continuity planning/ disaster recovery tests
  - The extent that key controls are **monitored**
  - The percentages of metrics **achieving defined criteria**

Assurance Process Integration

- It is important for the ISM to **integrate assurance functions** in order to: Increase security effectiveness, reduce duplication efforts, and minimize gaps in protection
- KGIs to support assurance integration may include:
  - No gaps in information asset protection
  - Elimination of unnecessary **security overlaps**
  - Seamless integration of assurance activities
  - Well-defined roles and responsibilities

Information Security Strategy

- An information security strategy should:
  - State **objectives/ purpose/ goals**
  - Delineate principal policies and plans for achieving objectives/ purpose/goals
  - Define the range of business and desired state for the business
  - Provide the **basis for an action plan** – based on available resources and constraints; must contain provisions for monitoring and metrics to determine the level of success
- Below are some of the common **pitfalls** for an Information Security Strategy that an ISM must be cautious from:
  - Overconfidence
  - Optimism
  - Anchoring
  - The status quo bias
  - Mental accounting
  - False consensus
- Objectives of information security strategy must be **clearly defined** and **accompanied by metrics** developed to determine if the objectives are being achieved
- The six major **goals of governance** are:
  - Strategic alignment
  - Effective risk management
  - Value delivery
  - Resource management
  - Performance management
  - Process assurance integration
- The goal of the information security strategy is to **protect the organization's information assets**
- In order to achieve the goal of the strategy, relevant information assets must be: **located, classified, labelled, and protected** based on its classification
- **Information** is an asset only to the degree it supports the primary purpose of the business
- Long term security strategy objectives should be in terms of a '**desired state'**
- Objectives should reflect well-articulated vision of desired outcomes for a security program
- **Business linkages** can uncover information security issues at the operational level
- The desired state should include a **snapshot of all relevant conditions** at a particular point in the future
- A **'desired state of security'** must be defined qualitatively in terms of attributes, characteristics and outcomes

- According to **COBIT**, the desired state is – 'Protecting the interests of those relying on information, and the processes, systems and communications that handle, store and deliver the information, from harm resulting from failures of availability, confidentiality and integrity
- The five key principles for governance and management of enterprise IT based on COBIT 5:
    - Meeting stakeholder needs
    - Covering the enterprise end-to-end
    - Applying a single, integrated framework
    - Enabling a holistic approach
    - Separating governance from management
- The desired state of security may also be defined as levels in the **Capability Maturity Model (CMM):**
    - **0. Nonexistent**: no recognition of need
    - **1. Ad hoc**: Risks are considered on an ad hoc basis – no formal processes
    - **2. Repeatable but intuitive**: Emerging understanding of risk and need for security
    - **3. Defined process**: Companywide risk management policy / security awareness
    - **4. Managed and measurable**: Risk assessment standard procedure, roles and responsibilities assigned, policies and standards in place
    - **5. Optimized**: Organization-wide processes implemented
- Determining the **current state of security** is also a critical activity where the same methodology can be applied as to finding out the desired state.
- A security strategy needs to include:
    - Resources needed
    - Constraints
    - A road map that includes people, processes, technologies, and other resources and a security architecture defining the business drivers
- Achieving the **desired state** is a **long-term goal** of a series of projects
- Information security strategy resources include:
    - Policies
    - Standards
    - Procedures
    - Guidelines
    - Architecture(s)
    - Controls – physical, technical, procedural
    - Countermeasures
    - Layered defenses
    - Technologies
    - Personnel security
    - Organizational structure
    - Roles and responsibilities
    - Skills
    - Training
    - Awareness education

- Information security strategy constraints include:
    - Legal: laws and regulatory requirements
    - Physical: Capacity, space, environmental constraints
    - Ethics: Appropriate, reasonable and customary
    - Culture: Both inside and outside the organization
    - Costs: Time, money
    - Personnel: resistance to change, resentment against new constraints

Policies and Standards

- **Policies** are the high-level statements of management intent, expectations and direction
- **Standards** are the metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements
- **Procedures** are the responsibility of operations, but are included here for clarity
- **Guidelines** for executing procedures are also the responsibility of operations
- **Information security architecture** is analogous to the architecture associated with buildings:
    - Concept
    - Design
    - Model
    - Blueprint
    - Build, development
- **Controls** are defined as the policies, procedures, practices, and organizational structure designed to provide reasonable assurance that business objectives will be achieved
- Controls can be physical, technical, or procedural
- **Countermeasures** are protection measures that reduce the level of vulnerability to threats and can be considered targeted controls
- **Technology** is one of the cornerstones of an effective security strategy accompanied by policies, standards, and procedures
- The first line of defense is trying to ensure the trust worthiness and integrity of new and existing personnel
- Personnel-related measures must be proportional to the sensitivity and criticality of the requirements of the position held
- Security **centralization/standardization** depends on the organizational structure
- A **decentralized security process** allows security administrators to be closer to the users and understand local issues better
- An employee's annual job performance and objectives can include security-related measurements
- The ISM needs to work with HR o define security roles and responsibilities
- A **skills inventory** is important in determining the resources available in developing a security strategy

- **Recurring security awareness program** aimed at end users reinforces the importance of information security
- Evidence indicated that the majority of end users are not aware of existing security policies and standards
- **Security awareness and training** has often produced the most cost-effective improvement in overall security
- **Audits** – both **internal** and **external** are one of the main processes used to determine information security deficiencies
- **Internal audits** in most larger organizations are performed by an **internal audit department**, generally reporting to either a chief risk officer (CRO) or to an audit committee of the board of directors
- **External audits** are most often conducted by the **finance department**
- The ISM must develop procedures for **handling compliance violations**
- **Threat assessment** is a task within risk assessment, but has a strategic component. It helps optimize risk response and facilitates policy development
- **Vulnerability assessments** should include assessing vulnerabilities in: processes, technologies, facilities
- The most common types of insurance that can be considered: first party, third party, fidelity bonds
- Business impact is the **'bottom line'** of risk
- It is generally easier to reduce a potential impact than to mitigate a risk or reduce a vulnerability
- **Outsourcing** is being used increasingly to cut costs but risks due to outsourcing may be difficult to quantify and potentially difficult to mitigate
- Outsourced security services must not become a critical single point of failure

Action plan to Implement Strategy

- Analysis of the **gap** between the **current state** and the **desired state** for each defined metric identifies the requirements and priorities for the overall plan or road map to achieve the objectives and close the gaps
- Policies must capture the intent, expectations and **direction of management**
- Security policies generally must be related to **the security strategy**
- Each security policy should state only **one general security mandate**
- Policies should rarely be more than few sentences long
- **Standards are the 'law'** developed from policy. It governs the creation of procedures and guidelines
- **Action plan metrics** are methods to monitor and measure progress and the achievement of milestones. Senior management is typically not interested in detailed technical metrics

Implementing Security Governance

- **Capability Maturity Models (CMM)** are available for use on the implementation of security governance
- Risk assessment is a standard procedure and exceptions to following the procedure would be noticed by IT management
- Depending on the structure of the organization, each significant area needs to be evaluated separately
- Policies need to be reviewed to determine whether they address each of the CMM elements
- Objective is to achieve consistent maturity levels across specific security domains

Action Plan Intermediate Goals

- **Intermediate goals** are defined once the overall strategy has been completed

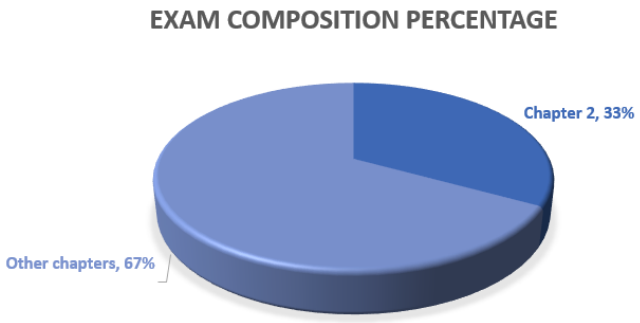
Information Security Program

- Foundations of an information security program are: the **security strategy** and the **action plan**
- The objective of the information security program is to protect the interests of those relying in the information and the processes, systems, and communications that handle, store and deliver the information from harm, resulting from failures of:
    - **Confidentiality**
    - **Integrity**
    - **Availability**
- Information is **available** and usable when required, and the systems that provide it can appropriately resist attacks
- Information is observed or disclosed to only those who have a right to know
- Information is protected against unauthorized modification
- Business transactions and information exchanges between enterprise locations or with partners can be trusted

CHAPTER 2:

Information Risk Management and Compliance

Exam Relevance: 33% (approximately 66 questions)



Objective

Ensure that the information security manager understands how to manage information risk to an **acceptable level** to meet business and compliance requirements of an organization.

Risk Management Overview

- Risk management is a process aimed at achieving an **optimal balance** between realizing opportunities (+) and minimizing (-) vulnerabilities and loss.
- Risks are being **managed** so that they do not have an **adverse material impact** on business processes.
- Risk is **inherent** to all business activities.
- Risk management provides rationale and justification for virtually all information security activities.
- **Risk assessment** is a key requirement for effective information security strategy.
- Risk management **balances risk exposure** against **mitigation strategies**.
- **Controls and countermeasures** are designed as part of Risk Management Framework.
- Risk has its corresponding **likelihood**/probability of occurrence and consequence/business **impact**
- **Informed decision making:**
    - based on the organization's threat, vulnerability and risk profile
    - based on **risk exposure** and **potential consequences** of compromise
- Risk management results to organizational **acceptance** / **deference** based on an understanding of potential consequences of **residual risk.**

Risk Management Strategy

- A risk management **strategy** is an integrated business process and **has defined objectives**.

- Incorporates all processes, activities, methodologies and policies of risk management carried out in an organization.

Effective Information Security Risk Management

- Activities must be **continuously supported** by all members of the organization.
- **Senior management commitment** is required to achieve the objectives of the risk management program.
- All personnel must understand their **responsibilities** in terms of information security
- Personnel must also be **trained in applicable control procedures**
- Compliance must be **tested** and **enforced** consistently.
- Develop a Risk Management Program based on the following requirements:
    - Establish context and purpose
    - Define scope and charter
    - Define authority, structure, and reporting
    - Ensure asset identification, classification and ownership
    - Determine objectives
    - Determine methodologies
    - Designate program development team
- Risk management is part of the **responsibility of the board of directors** or the equivalent to ensure that these efforts are effective.
- Management must be involved in and signs off on **acceptable risk** levels and risk management objectives.
- **Steering committee** sets the risk management **priorities**.
- Steering committee defines risk management **objectives** in terms **of supporting business** strategy.
- Information Security Manager is responsible for developing, collaborating, and managing the risk management program to meet the defined objectives.

Information Security Risk Management Concepts

- **Information security-related risk management** falls to the information security manager.
- Key information **security risk management concepts**:
    - Threats
    - Vulnerabilities
    - Exposures
    - Risk
    - Impacts

    - Controls
    - Countermeasures
    - Resource valuation
    - Information asset classification
    - Criticality
    - Sensitivity
    - Recovery Time Objectives **(RTOs)**
    - Recovery Point Objectives **(RPOs)**
    - Service Delivery Objectives **(SDOs)**
    - Acceptable Interruption Window **(AIW)**
    - Redundancy
- **Risk management functions** related to information security:
    - Service Level Agreement (SLAs)
    - System robustness and resilience
    - Business continuity/disaster recovery
    - Business process re-engineering
    - Project management timelines and complexity
    - Enterprise and security governance
    - Systems life cycle management
    - Policies -> standards -> procedures
- Information security manager (ISM) must have conceptual understanding of the following technologies:
    - Application security
    - Physical security
    - Environmental controls
    - Logical access controls
    - Network access controls
    - Routers, firewalls, and other network components
    - Intrusion detection/prevention
    - Wireless security
    - Platform security
    - Encryption and PKI
    - Anti-virus software and malware
    - Spyware and adware
    - Anti-spam
    - Telecommunications and VoIP

Risk Management Implementation

- Risk management contains a series of process of **weighing policy alternatives** in consultation with interested parties
- Risk management should be a **continuous and dynamic process** to ensure that changing threats and vulnerabilities are addressed in a timely manner.
- Risk management consists of the following processes:
    - Establish scope and boundaries

    - Risk assessment
    - Risk treatment
    - Acceptance of **residual risk**
    - Risk communication and monitoring
- Risk acceptance can be optional and be covered by both **risk treatment** and **risk communication**
- Determining the **appropriate level** of security depends on the potential risks that an organization faces.
- **Framework** for risk management should have the following requirements:
    - Policy
    - Planning and resourcing
    - Implementation program
    - Management review
    - Risk management process
    - Risk management documentation
- An efficient framework corresponds to **understanding the background** of the organization and its risk
- **Risk management framework** should also develop a structure and process for the development of risk management initiatives and controls
- **Framework approach** is critical in developing a set of criteria against which the risks will be measured
- Following key areas are essential in providing a comprehensive view of the organization's **internal environment**
    - Key business drivers
    - The organization's strengths, weaknesses, opportunities, and threats
    - Internal stakeholders
    - Organization structure and culture
    - Assets in terms of resources
    - Goals and objectives, and the strategies already in place to achieve them
- **Risk profile** is essential for effective risk management and can be easily achieved through a **risk register**
- Risk management context can be determined through defining the following:
    - Organization range and the process or activities to be assessed
    - Duration
    - Full scope of the risk management activities
    - Roles and responsibilities of various parts of the organization participating in the risk management process
- Evaluation of risk must be decided upon three important criteria: **Impact, likelihood**, and the **rules** that will determine whether the risk level is such that further treatment activities are required

Risk Assessment

- **Aggregate risk** can exist when a particular threat affects a large number of minor vulnerabilities that, in the aggregate, can have a significant impact.
- **Cascading risks** can also manifest unacceptable impacts as a result of one failure leading to a chain reaction of failures.
- The first step in a risk management program should be generating a comprehensive list of sources of **threats, risks, and events** that might impact achieving each objective
- Risk can be characterized by the following:
    - Origin
    - A certain activity, event or incident
    - Its consequences, results or impact
    - Specific reason for its occurrence
    - Protective mechanisms and controls
    - Time and place of occurrence
- Risk identification methodology can be any one of the following:
    - **Team-based brainstorming**: effective in building commitment and making use of different experiences
    - **Structured techniques**: flow charting, system design review, system analysis, hazard and operability studies, and operational modeling
    - **What-if and scenario analysis**: for less clearly defined scenarios such as identification of strategic risks and processes with a more general structure
- Threat categories are as follows
    - **Natural**: Flood, fire, cyclones, rain/hail, plagues, and earthquakes
    - **Unintentional**: fire, water, building damage/ collapse, loss of utility services and equipment failure
    - **Intentional physical**: Bombs, fire, water and theft
    - **Intentional nonphysical**: fraud, espionage, hacking, identity theft, malicious code, social engineering, phishing attacks and denial-of-service attacks
- The ISM must understand the **business risk profile** of the organization
- Risk is an **inherent** part of the business
- Risk **cannot entirely be eliminated**; every organization has a **level of risk it will accept**
- The ISM must determine the point where cost of losses **intersects** with cost of risk mitigation
- **Risk analysis**: the level of risk and its nature are assessed and understood
    - Involves thorough examination of the **risk resources**
    - Analysis of both positive and negative **consequences**
    - Assessment of existing **controls** that tend to minimize negative risks or enhance positive outcomes
- Risk level can be analyzed using **statistical analysis** of impact and likelihood
- Data that can be used to **estimate** impact and likelihood comes from: past experiences, international standards, market research, experiments, economic or engineering models, and specialist or expert advise

- **Quantitative risk analysis**: numerical values are assigned to both impact and likelihood; consequences may be expressed in monetary, technical, or operational terms
- **Semi-quantitative analysis** involves detailed analysis of magnitude and likelihood of potential consequences
- **Risk evaluation** involves the decision to which risk to treat and the treatment priorities
- **Risk treatment** involves four strategic options: Terminate, Transfer, Mitigate, Tolerate
- To **terminate** a risk is to stop the activity giving rise to that risk
- **Transferring** a risk involves tapping a third party to manage that specific risk
- **Mitigation** is to reduce the risk through appropriate control measures
- **Tolerating** a risk means it falls to a certain acceptable level
- The **cost of mitigating risk must not exceed the value** of the asset
- Accepted risks should be evaluated and reviewed **regularly**
- **Residual risk** is the amount of risk that remains after countermeasures have been implemented
- Acceptance of residual risk depends on: **regulatory compliance, organizational policy, sensitivity and criticality of assets, acceptable levels of potential impacts, uncertainty inherent in the risk assessment approach, cost and effectiveness of implementation**
- **Impact** is the bottom line for risk management
- All risk management activities are designed to reduce impacts to **acceptable levels**
- **Impact** is a result of any **vulnerability exploited** by a **threat** that causes a **loss**
- **Business Impact Assessment (BIA)** helps prioritize risk management and provides the levels and types of protection required
- **Controls** that address the same risk are excessive and wasteful
- Risk assessment is important to be conducted from the **beginning of process through to the end**
- If the cost of specific controls or countermeasures exceed the benefits of mitigating a given risk, the organization may choose to **accept the risk** rather than incur the cost of mitigation
- **Total Cost of Ownership (TCO)** must be considered for the full life cycle of the control or countermeasure
- **Monitoring processes** is essential to have warning for events that could impact the security program

Information Resource Valuation

- **Resource valuation** is an essential undertaking required for an effective information risk management program
- It is essential for an ISM to **locate and identify all information resources**, determine **ownership and custodianship** of information, **assign classes** or

levels of sensitivity and criticality to information resources, and make **classifications simple**

- **Asset classifications** are being used by end-user managers and security administrators to determine access levels
- **Data classification** reduces the risk and cost of over or under protecting information resources by correlating security to business objectives
- **Business Impact Analysis (BIA)** helps to identify the impact of adverse events on critical business processes or activities
- Common approach to performing impact assessment is to identify an asset's value proposition to the organization in terms of the impact associated with the loss of **integrity, availability, and confidentiality**
- Some impacts can be measured quantitatively, where others cannot

Recovery Time Objectives

- **Recovery Time Objectives (RTO)** depend upon numerous factors such as: cyclical need of the information and organization, interdependencies upon the information, organizational requirements, senior management requirement, legal or regulatory requirement, and customer service levels
- RTOs are needed to identify and develop **contingency strategies**
- **Shorter** RTOs require **costlier** contingency procedures
- There is a **break-even point** where the impact of the disruption will begin to be greater than the cost of recovery
- **Recovery Point Objective (RPO)** is determined based on the acceptable data loss in case of disruption of operations
- **Service Delivery Objective (SDO)** is the minimum level of service that must be restored after an event to meet business requirements
- **Third-party service providers** are sometimes tapped for risk transfer.
- It is important for the ISM to assess the **risk of any outsourcing process** where there should be appropriate information **risk management clauses** in the contract
- For outsourcing arrangements, the organization must have **appropriate controls** in place to facilitate the activity
- Considerations for outsourcing include: **criticality** of the business function, **complexity** of the process, **separation** setting control requirements, **regulatory** requirements, **changes** in internal and external business environment
- Some key clauses that should be part of **Service Level Agreements (SLA)** are: **right to audit** the vendor's books of accounts, **right to review** their processes, insistence on **standard operating procedures (SOP), right to assess skill sets** of vendor resources and advance information if the resources are to be changed

Integration with Life Cycle Processes

- **Change management** is an effective method to maintain adequate security protection
- **Proactive approach** enables the ISM to better plan and implement security policies and procedures in alignment with business goals and objectives
- It is more cost effective to **update risk regularly**
- **Life cycle approach** is the best way to employ to identify, analyze, assess and track risk
- **Top-down systematic approach** can benefit from supporting tools, training and assistance
- **Software tools** are also available to track the risk management life cycle

Security Control Baselines

- **Baselines** specify minimum security control requirement
- It is important to assess the level of security that is appropriate for an organization
- **Reporting significant changes** in risk to appropriate levels is a primary role of the ISM
- Risk assessment should be **updated as the organization changes**
- Risk assessment process should include an entry whereby a significant security breach or event will trigger a report to upper management

Training and Awareness

- **People** are generally the **greatest risk** to an organization, appropriate training can significantly mitigate risk
- End users should receive **training** on the importance of adhering to the security policies and procedures of the enterprise, responding to emergency situations, significance of logical access in an IT environment, privacy and confidentiality requirements

Documentation

- Appropriate **risk management documentation** that is **readily available** is required to effectively manage risk
- Inclusions to a **risk management documentation** should include: objective, audience, information resources, assumptions, and decisions
- **Risk management policy** document may include information such as:
    - Objectives of the policy
    - Scope and charter of risk management

    - Links between the risk management policy and the organization's strategic and corporate business plans
    - Extent and range of issues to which the policy applies
    - Guidance on what is considered acceptable risk
    - Risk management responsibilities
    - Support expertise available to assist those responsible for managing risks
    - Level of documentation required for various related activities
    - A plan for reviewing compliance
    - Incident and event severity levels
    - Risk reporting and escalation procedures, format, and frequency
- **General risk management documentation** should include:
    - A **risk register**
    - Consequences and likelihood of compromise
    - Initial risk rating
    - Vulnerability to external/internal factors
    - An inventory of information assets
    - A risk mitigation action plan