CYBRARY

CISM (Certified Information Security Manager)

Created By: Cassandra Brunetto, Teaching Assistant

Module 1: Introduction

Lesson 1.1: Is CISM for me

Skills Learned From This Lesson: Organizational Security, Information Security Governance, Business Management

- Is the CISM (Certified Information Security Manager) For Me?
    - Do you understand the role and need for information security?
    - Do you have a basic understanding of information systems and technology?
    - Would you like to move into the management realm?
    - Do you understand the nature of business management?

Lesson 1.2: Welcome and Intro

Skills Learned From This Lesson: Course Objectives, Earning CISM, Domain Structure

- Course Objectives
    - Introduction to CISM Certification
    - The role of a CISM
    - Understanding the IT Security domains and related concepts
    - Presenting business value and requirements of IT Security
    - Understanding of ISACA Risk IT Framework, structure, concepts, definitions, and processes dedicated to risk management
    - Main goal = Preparing students for CISM exam
    - Secondary goal = Awareness of IT Security best practices
- Information Security supports the business:
    - Minimizes liabilities
    - Helps us to maintain compliance
    - Inspires customer confidence
    - Minimizes losses
    - Shows due care
    - Minimizes downtime

    - Allows business to meet its long-term goals
- How to Earn Your CISM
    - Step 1: Register for the Exam
    - Step 2: Prepare for the Exam
    - Step 3: Take the Exam
    - Step 4: Apply for Certification
    - Step 5: Maintain a Certification
- CISM Domain Structure
    - Domain 1: Information Security Governance
    - Domain 2: Information Risk Management and Compliance
    - Domain 3: Information Security Program Development and Management
    - Domain 4: Information Security Incident Management
- About the CISM Exam
    - The CISM certification is designed to meet the growing demand for professionals who can integrate Information Security (IS) with discrete IS control skills
    - The technical skills and practices the CISM certification promotes and evaluates are the building blocks of success in this growing field, and the CISM designation demonstrates proficiency in this role
    - The CISM certification/designation reflects a solid achievement record in managing security, as well as in such areas as risk analysis, risk management, security strategy, security organization, etc.
    - Certification launched: 2003
    - Number of individuals certified: 23,000
    - CISM exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards
    - PBE & CBE (only pencil and eraser are allowed)
    - 4 hour exam
    - 200 multiple choice questions designed with one best answer
    - No negative points
    - No prerequisite for exam (only for attending the exam)
- Recommended reading for CISM Exam
    - Must
        - ISACA CISM Official Glossary
        - ISACA CISM Item Development Guide

        - ISACA CISM QAE Item Development Guide
    - Should
        - ISACA Risk IT Framework
        - ISACA CISM Review Manual
    - Could
        - Risk IT Practitioner Guide

Module 2: Domain 1 Information Security Governance

Lesson 2.1: Introduction

Skills Learned From This Lesson: CISM Task Statements, CISM Knowledge Statements, Information Security Governance

- Module Agenda
    - Learning objectives
        - Domain 1- CISM exam relevance
        - Tasks and Knowledge Statements
    - Module Agenda
        - Priorities for the CISM
        - Corporate Governance
        - Information Security Strategy
        - Information Security Program
        - Elements of a Security Program
        - Roles and Responsibilities
        - Evaluating a Security Program
        - Reporting and Compliance
        - Ethics
- Learning Objectives
    - After this module, the CISM candidate should be able to
        - Support governance
        - Support business cases to justify security
        - Compliance with legal and regulatory mandates
        - Support organizational priorities and strategy
        - Identify drivers affecting the organization
        - Defines roles and responsibilities

        - Establish metrics to report on effectiveness of the security strategy
- Domain 1 - Task Statements
    - There are 9 general task statements pertaining to IS Governance in CISM
    - Certification Job Practice:
        - Establish and maintain an information security strategy and governance framework
        - Integrate information security governance into corporate governance
        - Establish and maintain information security policy
        - Develop business cases to support investments
        - Identify internal and external influences to the organization
        - Obtain commitment from senior management
        - Define and communicate the roles, and
        - Establish, monitor, evaluate, and report metrics
- Domain 1- Knowledge Statements
    - There are 15 general knowledge statements pertaining IS Governance in CISM Certification Job Practices
    - Knowledge of (selected)
        - Methods to develop an information security strategy
        - Relationship among information security and business goals
        - Methods to implement an information security governance framework
        - Internationally recognized standards, frameworks, and best practices related to information security governance and strategy development
        - Methods to develop information security policies, business cases, strategic budgetary planning and reporting methods
        - Information security management roles and responsibilities
    - Information Security Governance:
        - Determines Strategic Direction
        - Understands and communicates long-term goals
        - Determines enterprise-wide framework and oversees the implementation
        - Establishes the means for development of policies, standards, budgets
        - Determines roles and responsibilities

Lesson 2.2: Priorities for the CISM

Skills Learned From This Lesson: Information Security, C-I-A Triad, Compliance

- Priorities of the CISM Candidate
    - What is Information Security (IS)?
    - The C-I-A Triad
        - **Confidentiality** (prevent unauthorized disclosure)
        - **Integrity** (prevent unauthorized information modification)
        - **Availability** (resources are available as appropriate in a timely fashion
            - The Board of Directors and Senior Management is accountable for the protection of organizational assets
            - Oversight, Culture, and Policies are integral to IS management
        - **Authentication** (prove who you are)
        - **Access Control** (the proper people have the access they need, improper people have no access at all)
        - **Privacy** (the owner determines how the information is distributed),
        - **Nonrepudiation** (sender cannot dispute having sent the message nor the contents of the message)
        - **Compliance** (in regard to company policy, processes, legislation, regulations, applicable law)
        - You audit for compliance but the only way you really know if you will be successful is if you carry out a test (penetration test)

Lesson 2.3: Priorities for the CISM Part 2

Skills Learned From This Lesson: Information Protection, Information Security Considerations, Information Security Importance, Security Breach Impacts

- Information Protection includes:
    - Accountability (information owner makes the final decision and is accountable)
        - We serve the customer and the customer is the business. The business has the ultimate authority
        - Enforce policy, review audits, act upon it
    - Oversight (comes from senior management)
    - Prioritization (comes from senior management)
    - Risk Management (identify assets, threats, vulnerabilities, potential loss, controls and select cost controls that have more benefit than cost) Needs to be incorporated into all our decision-making

    - Regulatory and Compliance Management (usually the top priority)
- Information Security Considerations:
    - Information Security is more than just IT (more than technology)
    - Information Security deals with all aspects of information
    - Information must be protected at all levels of the organization and in all forms (e.g. digital, paper, fax, audio, video, microfiche, networks, storage media, computer systems)
    - Information Security is everyone's responsibility. Senior Management is **accountable**
- Selling the Importance of Information Security
    - Improved trust in customer relationships
    - Protecting the organization's reputation
    - Better accountability for safeguarding information during critical business activities
    - Reduction in loss through better incident handing and disaster recovery
- Information security is only relevant as it impacts the business
- The CISM must understand:
    - Requirements for effective information security governance
- Elements and actions required to:
    - Develop an information security strategy
    - Plan of action to implement it
- The First Priority for the CISM
    - Remember that Information Security is a business-driven activity
    - Security is here to support the interests and needs of the organization
    - Security is always a balance between **cost and benefit** and *security and productivity/performance*
    - Security can never be a one size fits all solution
        - Each organization is different and within this organization security has to be tailored for specific organizational needs
    - Understand the business itself and find the benefit that is worth the cost (cost-benefit analysis)
- What impact can a security breach have on an organization?
    - A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident

- Technical investigation
- Customer breach notification
- Regulatory compliance
- Attorney fees and litigation
- Post-breach customer protection
- Public relations
- Cybersecurity improvements
- Insurance premium increases
- Increased cost to raise debt
- Impact of operational disruption or destruction
- Value of lost contract revenue
- Devaluation of trade name
- Loss of intellectual property
- Lost value of customer relationships

Lesson 2.4: Priorities for the CISM Review Questions

Skills Learned From This Lesson: Encryption, Redundancy, Integrity

- Encryption is best suited to enforce which element of the C-I-A Triad?
  - Privacy
- Availability can best be achieved through _____.
  - Redundancy
- Integrity speaks to the fact that _____.
  - The file has not been modified
  - Integrity is provided through hashes, which will change in the event that a file is modified

Lesson 2.5: Corporate Governance

Skills Learned From This Lesson: Corporate Governance, Information Security Governance, IT Governance

- Corporate Governance
  - Ethical corporate behavior by directors or others charged with governance in the creation and presentation for all stakeholders

    - The distribution of rights and responsibilities among different participants in the corporation, such as board, managers, shareholders, and other stakeholders
    - Governance is responsible for developing the security strategy
    - The Organization for Economic Co-operation and Development (OECD) states: "Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."
- Business Goals and Objectives
        - Corporate governance is the set of responsibilities and practices exercised by the board and executive management
        - Information security governance is a subset of corporate governance
        - Goals include:
            - Providing strategic (long-term) vision and direction
            - Reaching security and business objectives
            - Ensure that risks are managed appropriately and proactively
            - Verify that the enterprise's resources are used responsibly
- 6 Basic Outcomes of Effective Security Governance
    - Strategy Alignment: Aligning with the Business and Providing Collaborative Solutions
    - Risk Management: Safeguarding Assets and Disaster Recovery
    - Value Delivery: Focus on IT Expenses and Proof of Value
    - Resource Management
    - Performance Measurement: IT Scorecards
    - Integration: Security must be integrated into all that we do—not considered as an afterthought
- Benefits of Information Security Governance
    - Effective information security governance can offer many benefits to an organization, including:
        - Compliance and protection from litigation or penalties
        - Cost savings through better risk management
            - Efficient utilization of security investments that support organization's objectives

        - Reduced risks and potential business impacts to an acceptable level
        - Better oversight of systems and business operations
        - Opportunity to leverage new technologies to business advantage
        - Business value generated through the optimization of security investments with organizational objectives
- Performance and Governance
    - Governance is only possible when metrics are in place to determine whether critical organizational objectives are achieved
    - Those metrics are used for
        - Measuring: evaluating the data without context—yields information
        - Monitoring: analyzing the data in context to a baseline set of expectation—yields information
        - Controlling: making adjustments as needed
        - Reporting: presenting information in a meaningful way
    - Enterprise-wide measurements should be developed that will be consistent in all organization activities

Lesson 2.6: Evaluating the Security Environment

Skills Learned From This Lesson: Auditing, Testing, KPIs, KRIs, KGIs, End-to-End Security, Correlation Tools

- Audit and Testing of the Security Environment
    - Audit vs. Testing
        - Audit indicates compliance
        - Is it configured according to policy? (Policy could be wrong, so you should conduct a test)
    - Testing indicates efficacy
        - Will it work?
    - Metrics to measure the results must be determined before implementation
    - Measure results that are important to the business
    - Use metrics that can be used for each reporting period
        - Compare results and detect trends
        - Determine if controls are meeting their objectives
        - **S**pecific, **M**easurable, **A**ttainable, **R**epeatable, and **T**imely objectives

    - Set metrics that will indicate the health of the security program (e.g. is a firewall meeting its objective of protecting the internal network and allowing us an increase in uptime?
    - Incident management
    - Degree of alignment between security and business development
        - Was security consulted
        - Were controls designed in the systems or added later
    - Choose metrics that can be controlled (e.g. number of successful attacks/compromises)
        - Measure items that can be influenced or managed by local managers/security
        - Not external factors such as number of viruses released in the past year
        - Have clear reporting guidelines
        - Monitor on a regular scheduled basis
- Key Performance Indicators (KPIs)
    - Thresholds to measure
        - Are we on track to meet our goals?
        - Compliance/Non-compliance
        - Pass/fail
        - Satisfactory/Unsatisfactory results
        - A KPI is set at a level that indicated action should/must be taken
            - Alarm point
- Key Risk Indicators (KRIs) are like warning bells that indicate a risk may materialize
    - Possibility that you might not meet your performance goals
    - e.g. if attendance falls below 80% on any given day
- Key Goal Indicators (KGIs)
        - Did we meet our goals or not?
- End-to-End Security
    - Security must be enabled across the organization – not just on a system by system basis
    - Performance measures should ensure that security systems are integrated with each other
        - Layered defenses
- Correlation Tools

- The CISO may use Security Event and Incident Management (SEIM, SIM, SEM) tools to aggregate data from across the organization
- Data analysis
- Trend detection
- Reporting tools

Lesson 2.7: The Information Security Program

Skills Learned From This Lesson: Security Program, Information Security Frameworks, Information Security Architecture, Balanced Scorecard, Constraints

- What is a Security Program?
  - "A security program identifies, manages, and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture."
  - Components of a security program:
    - External influencers (PCI, HIPAA, SOX, etc.) dictate what we do and how we do it
    - Policies come from senior management (guide decisions but not detail-oriented). Policies usually don't change
    - Control Objectives (desired state) what we want; what we're focused on when we implement controls
    - Standards change more frequently
    - Guidelines (suggestions or best practices)
    - Procedures (mandatory) documented step-by-step
- Security vs. Business
- Security must be aligned with business needs and direction
- Security is embedded into the business functions and acts as an internal part of business operations providing:
  - Strength (through layered defense)
  - Resilience (can we withstand an attack?)
  - Protection (provide CIA)
  - Stability (dependable, predictable behavior)

    - Consistency (configuration management ensures changes are not made to a system without formal approval)
    - Reliability (redundancy)
- Security must be treated, discussed, and maintained as a business issue
- Security Program Objectives
    - Ensure the **availability** of systems and data
        - Allow access to the correct people in a timely manner
    - Protect the **integrity** of data and business processes
        - Ensure no improper modifications
    - Protect the **confidentiality** of information
        - Unauthorized disclosure information
        - Privacy, trade secrets
    - Protect the **authenticity** and **nonrepudiation** of business transaction and information exchanges
- Information Security Frameworks (Structure)
    - Effective information security is provided through adoption of a common framework which:
        - Defines information security objectives
        - Aligns with the business objectives
        - Provides metrics to measure compliance and trends
        - Standardizes baseline security activities enterprise-wide
- The ISO/EIC 27001:2013
    - ISO/EIC 27001: 2013 Information Technology – Security Techniques, Information security management systems (ISMS) Requirements
    - The goal of ISO 27001 is to help an organization evolve their ISMS through the following
        - Initiate
        - Define
        - Assess
        - Develop
        - Readiness
    - An information security management system contains 14 clauses, 35 control objectives, and 114 controls
- Examples of Other Security Related Frameworks

- SABSA (Sherwood Applied Business Security Architecture)
- COBIT (Control Objectives for Information and related Technology)
- COSOERM and COSO IC
- Business Model for Information Security
- Model originated at the Institute for Critical Information Infrastructure Protection
- Publications from NIST and ISF
- US Federal Information Security Management Act (FISMA)
- Securing Quality
    - ISO standards on quality (ISO 9001:2000)
    - Six Sigma

- Architecture (Design Elements)
    - Information security architecture provides the physical implementation of the framework. Includes:
        - Design/modelling
        - Creation of detailed blueprints
        - Integration of security in the SDLC
        - Selection/Development of Hardware, Software, and Firmware
        - Deployment
- Assessing the Program with a Balanced Scorecard
    - The original balanced scorecard addresses 4 key areas of performance:
        - Financial metrics- provide information about financial performance both revenue and expenses
        - Customer metrics- assess the extent to which the company is meeting customer needs and expectations
        - Internal process measures- provide insight into the efficiency of internal processes and allow leaders to identify and correct problems
        - Measures of learning and growth- give managers information about employee satisfaction and development
- Constraints for a Security Program
    - Constraints
        - Legal- laws and regulatory requirements
        - Physical- capacity, space, environmental constraints
        - Ethics- appropriate, reasonable, and customary
        - Culture- both inside and outside the organization

- Organizational structure (how decisions are made, by whom, turf protection)
- Costs- time/money
- Personnel- resistance to change, resentments against new constraints
- Resources- capital, technology, people
- Capabilities- experience, knowledge, training, skills, expertise
- Time- window of opportunity, mandated compliance
- Risk acceptance and tolerance- risk appetite, threats, vulnerabilities, impacts

Lesson 2.8: Information Security Strategy

Skills Learned From This Lesson: Goal of Information Security, Security Strategy, Desired State of Security,

- The Goal of Information Security
  - The goal of information security is to protect the organization's assets, individuals, mission and vision
  - To achieve this, organization must do:
    - Asset identification
    - Classification of data/information and systems according to criticality and sensitivity.
      - The owner of the data determines its classification. The data custodian is tasked with implementing the controls based on the data's classification
    - Application of appropriate controls (e.g. firewalls, encryption, segregation of duties)
- Business Linkages
  - Start with understanding the specific objectives of a particular line of business
  - Take into consideration all information flows and processes that are critical to ensuring continued operations
  - Enable security to be aligned with and support business levels at:
    - Strategic (3-5 year goals)
    - Tactical (1-3 year goals)
    - Operational (day-to-day goal)

- What is a Security Strategy?
    - “An information security strategy and risk management (ISRM) strategy provides an organization with a road map for information and information infrastructure protection with goals and objectives that ensure capabilities provided are aligned to business goals and the organization’s risk profile.”
- The Desired State of Security
    - The desired state of security should be defined in terms of:
    - Should be clear to all stakeholders what the intended security states is
    - The desired state according to COBIT
        - “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.”
    - Focuses on IT-related processes from IT governance, management and control perspectives
- Developing Information Security Strategy
    - Information Security Strategy
        - Understand the business
        - Long-term perspective
        - Standard across the organization
        - Aligned with business strategy/direction
        - Understands the culture of the organization
        - Reflects business needs and priorities
- Elements of a Strategy
    - A security strategy needs to include
        - Resources needed
        - Constraints
        - A road map (a broad plan for achieving the organizational goals)
            - Includes people, processes, technologies and other resources
            - A security architecture: defining business drivers, resource relationships and process flows
        - Achieving the desired state is a long-term goal of a series of projects or program
- Information Security Strategy Objectives

    - The Information Security Strategy forms the basis for the plan(s) of action required to achieve security objectives
    - The long-term objectives describe the “desired state”
    - Should describe a well-articulated vision of the desired outcomes for a security program
    - Information Security Strategy objectives should be stated in terms of specific goals directly aimed at supporting business activities
    - Security strategy must:
        - Be defined
        - Be measurable
        - Provide guidance
- Business Case Development
    - Included in the Business Case:
        - Reference
        - Context (business objectives/opportunities)
        - Value Proposition
        - Focus
        - Deliverables
        - Dependencies (CSFs)
        - Project metrics (KPIs, KPGs)
        - Workload
        - Requires resources
        - Commitments

Lesson 2.9: Information Security Strategy

Skills Learned From This Lesson: Senior Management Roles and Responsibilities, Senior Management Commitment, IT Security Practitioners

- Roles and Responsibilities of Senior Management

    - Board of Directors
        - Information security governance/Accountability
    - Executive Management
        - Implementing effective security governance and defining strategic security objectives
        - Budget and support
    - Steering Committee
        - Ensuring that all stakeholders impacted by security considerations are involved
        - Oversight and monitoring of security program
- Senior Management Commitment
    - The support of senior management is crucial to success
        - Budget
        - Direction/policy
        - Reporting and monitoring
    - A bottom-up management approach to information security activities is much less likely to be successful
- Steering Committee
    - Oversight of Information Security Program
    - Acts as liaison between Management, Business, Information Technology, and Information Security
    - Assess and incorporate results of the risk assessment activity into the decision-making process
    - Ensures all stakeholder interests are addressed
    - Oversees compliance activities
- Chief Information Security Officer (CISO)
    - Responsible for Information Security related activity
        - Policy
        - Investigation
        - Testing
        - Compliance
    - IT planning, budgeting, and performance, including its information security components
- Information Security Manager

    - Responsible for their organization's security programs, usually including information risk management
    - Playing a leading role in introducing an appropriate, structure methodology
    - Acts as major consultants in support of senior management
- Business and Functional
    - Responsible for business operations
    - Responsible for security enforcement and direction in their area
    - Day to day monitoring
        - Reporting
        - Disciplinary actions
        - Compliance
- IT Security Practitioners
    - Responsible for proper implantation of security requirements in their IT systems
    - Support or use the risk management process to identify and assess new potential risk and implement new security controls as needed to safeguard their IT systems
    - CISMs are NOT the ones doing
- Security Awareness Trainers
    - Must understand the risk management process
    - Develop appropriate training materials
    - Conduct security trainings and awareness programs
    - Incorporate risk assessments into training programs to educate the end users
    - Number of reported security incidents might go increase as a result of good training
    - Use quantitative assessments (e.g. test)

Lesson 2.10: Reporting and Compliance

Skills Learned From This Lesson: Senior Management Roles and Responsibilities, Senior Management Commitment, IT Security Practitioners

- Regulations and Standards
    - The CISM must be aware of national:

        - Laws
        - Privacy requirements
        - Regulations
    - Reporting, Performance
    - Industry Standards
        - Payment Card Industry (PCI)
        - BASELI
- Effect of Regulations
    - Requirements for business operations
        - Cost
        - Reputation
    - Scheduled reporting requirements
        - Frequency
        - Format
- Reporting and Analysis
    - Data gathering at source
        - Accuracy
        - Identification
    - Reports signed by Organizational Officer

Lesson 2.11: Code of Ethics

Skills Learned From This Lesson: Ethical Standards, Ethics Plan of Action, ISACA Code of Ethics

- Ethical Standards
    - Rules of Behavior
        - Legal
        - Corporate
        - Industry
        - Personal
    - Responsibility to all stakeholders
        - Customers
        - Partners
        - Suppliers

        - Management
        - Owners
        - Employees
        - Community
- Ethics Plan of Action
    - Develop a corporate guide to computer ethics for the organization
    - Develop a computer ethics policy to supplement the computer security policy
    - Add information about computer ethics to the employee handbook
    - Find out whether the organization has a business ethics policy, and expand it to include computer ethics
    - Learn more about computer ethics and spread what is learned
- ISACA Code of Ethics
    - Required for all certification holders
    - Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems
    - Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards and best practices
    - Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession
    - Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority
        - Such information shall not be used for personal benefit or released to inappropriate parties

Lesson 2.12: Summary and Review

Skills Learned From This Lesson: Summary, Conclusion, Review

- Summary and Conclusion
    - Priorities for the CISM
    - Corporate Governance
    - Information Security Strategy

    - Information Security Program
    - Elements of a Security Program
    - Roles and Responsibilities
    - Evaluating a Security Program
    - Reporting and Compliance
    - Ethics
- Review Questions
    - Prior to assessing technical vulnerabilities or levels of security awareness, an information security manager needs to gain an understanding of the current business strategy and direction
    - Senior management seeks to understand the business justification for investing in security. This can best be accomplished by tying security risks to key business objectives
    - Hardware, software, firmware and the configurations of the technical environment are defined as architecture
    - Policies are high-level statements of objectives. Because of their high-level nature and statement of broad operating principles, they are less subject to periodic change
    - Investments in security technologies should be based on a value analysis and a sound business case

Module 3: Domain 2 Information Risk Management

Lesson 3.1: Risk Management Intro

Skills Learned From This Lesson: Risk Definitions, Risk Governance Objectives, IT Risk Management

- Chapter 2 Risk Management Agenda
    - Risk Introduction
    - The Risk Management Lifecycle
        - IT Risk Identification
        - IT Risk Assessment
        - Risk Response and Mitigation
        - Risk and Control Monitoring and Reporting

- Introduction to Risk Management
    - Risk
        - The combination of the probability of an event and its consequence
        - Often an adverse event
    - Several factors considered when evaluating risk:
        - Mission of the organization
        - Assets
        - Threat
        - Vulnerability
        - Likelihood
        - Impact
    - The primary focus of risk management is to reduce residual risks to an acceptable level
- Risk Definitions
    - **Asset:** Something tangible or intangible in value and is worth protecting
    - **Vulnerability:** A weakness in the design, implementation, operation, or internal control of a process that could expose a system to adverse threats
    - **Threat:** Something that could pose loss to all or part of an asset
    - **Threat Agent:** What carries out the attack
    - **Exploit:** An instance of compromise
    - **Risk:** The combination of the probability of an event and its consequence. Risks are often seen as an adverse event that can threaten an organization's assets or exploit vulnerabilities and cause harm
        - ISO 31000 defines risks as "the effect of uncertainty on objectives" indicating risk can be positive (opportunities) or negative
        - ISO 27005 considers risks to be negative
    - **Inherent Risk**: With all business endeavors there is some degree of risk
    - **Residual Risk:** Risk that remains after a control has been implemented. Ultimately, risk should be mitigated until residual risk is within the level that management is willing to accept (management's risk tolerance)
    - **Secondary Risk:** One risk response may cause a second risk event
    - **Risk Appetite:** Senior management's approach to risk (Seeking, Neutral, Averse)

    - **Risk Tolerance:** The acceptable level of variation that management is willing to allow for any particular risk
    - **Risk Capacity:** The objective amount of loss an enterprise can tolerate without risking its continued existence
        - Defined by board and executive management at the enterprise level
    - **Risk Threshold:** A quantified limit beyond which your organization is not willing to go
    - **Controls:** Proactive and Reactive mechanisms put in place to manage risks
- Risk Governance Objectives
    - Effective risk governance helps ensure that risk management practices are embedded in the enterprise, enabling it to secure optimal risk- adjusted return.
    - Risk governance has four main objectives:
        - Establish and maintain a common risk view
        - Integrate risk management into the enterprise
        - Make risk-aware business decisions
        - Ensure that risk management controls are implemented and operating correctly
- Context of IT Risk Management
    - Risk Management: Coordinated activities to direct and control the enterprise with regard to risk
    - Understanding of the organization and its context, or environment includes:
        - Intent and capability of threats
        - Assets
        - Relationship of vulnerabilities
        - Vulnerability to changes in economic or political conditions
        - Changes to market trends and patterns
        - Emergence of new competition
        - Impact of new legislation
        - Existence of potential natural disaster
        - Constraints caused by legacy systems an
        -
        - d antiquated technology
        - Strained labor relations and inflexible management
- ISACA's Risk Management Lifecycle

- IT Risk Identification -> IT Risk Assessment -> Risk Response and Mitigation -> Risk and Control Monitoring and Reporting
- Cyclical process
- Process based on the complete cycle of all elements
- Continuous process with refinement, adaptation and improvement and maturity

Lesson 3.2: Risk Identification

Skills Learned From This Lesson: Risk Identification, Risk Culture and Communication, Organizational Structure, Administrative Risk Controls

- Methods to Identify Risk:
  - Identify Assets => Identify Threats => Identify Existing Controls => Identify Vulnerabilities => Identify Consequences => (feed into) Risk Assessment Process
  - Sources of risk documentation
  - Audit reports
  - Incident reports
  - Interviews with SMEs
  - Public media
  - Annual reports
  - Press releases
  - Vulnerability assessments and penetration tests
  - Business continuity and disaster recovery plans
  - Interview and workshops
  - Threat intelligence services
- Risk Culture and Communication
  - Risk aware business decisions
  - Assistance in executive management's understanding of the actual exposure to risk
  - Awareness among all internal stakeholders of the importance of integrating risk management into their daily duties
  - Transparency to external stakeholders regarding the actual level of risk and risk management processes in use
- Alignment with Business Goals and Objectives

    - The first and most important step for a CISM is to understand the business. Review organizational vision and strategy **FIRST**
    - Look beyond IT- Risk is measured by the impact the risk has on the business, not on a particular system
    - In order for risk to be integrated into the enterprise, senior management must be supportive and involved
        - If management funds and supports the risk management processes we will have what we need to be successful
        - Good metrics mean that we have attainable objectives which will help us accomplish our goals
        - Good communication and transparency helps us make risk-aware business decisions
- Organizational Structures and Impact on Risk
    - Risk Context
    - Risk management should be enterprise wide and a common framework should be shared
    - Three lines of defense
        - **1st line Business Units**: Involved in day-to-day risk management, follow a risk process, apply internal controls and risk responses
        - **2nd line Risk and Compliance**: Oversee and challenge risk management, provide guidance and direction, develop risk management framework
        - **3rd line Audit**: Review 1st and 2nd lines, provide an independent perspective and challenge the process, objective and offer assurance
    - RACI (Responsible, Accountable, Consult, Inform) charts can be used to communicate responsibilities
- Administrative Risk Controls
    - Segregation of duties (preventive)
    - Job rotation (detective)
    - Mandatory vacations
    - Dual control (e.g. 2 administrators to recover a encryption key), M of N control
    - Secure state (things should fail in such a way that no further compromise can occur)
    - Principle of Least Privilege
    - Need to Know

- AUP
- Data/System Ownership

Lesson 3.3: Information Security Program Basics

Skills Learned From This Lesson: Information Security Program,

- Information Security Program
  - As defined by ISACA the goal of this domain is to "Develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture."
  - Is best coordinated by the Chief Operating Officer, as this individual should properly see the need for balance between information security and business operations.
- Key Information Security Program Elements
  - Technology
    - System Security
    - UTM/Firewalls
    - IDS/IPS
    - Data Center
    - Physical Security
    - Vulnerability Assessment
    - Penetration Testing
    - Application Security
    - Secure SDLC
    - SIM/SIEM
    - Managed Services
  - People
    - Training
    - Awareness
    - HR Policies
    - Background Checks
    - Roles/Responsibilities
    - Mobile Computing

        - Social Engineering
        - Social Networking
        - Acceptable Use
        - Policies
        - Performance Management
    - Process
        - Risk Management
        - Asset Management
        - Data Classification
        - Information Rights Management
        - Data Leak Prevention
        - Access Management
        - Change Management
        - Patch Management
        - Configuration
- Essential Information Security Practices
    - Management commitment*
    - Risk management*
    - Asset inventory and management
    - Change Management*
    - Incident Response and management
    - Configuration management*
    - Training and awareness
    - Continuous audit* (measuring compliance to the process)
    - Metrics and measurement
    - Vulnerability assessment* (does it work?)
    - Penetration testing* (does it work?)
    - Application security testing
    - Device management
    - Log monitoring, analysis and management*
    - Secure development*

Lesson 3.4: Administrative Controls

Skills Learned From This Lesson: Dual Control, Secure State, Data Ownership, System Ownership

- Administrative Risk Controls
    - Segregation of Duties (preventive control)
    - Job rotation (detective control)
    - Mandatory vacations
    - Dual Control, M of N Control
    - Secure state
    - Principle of Least Privilege
    - Need to know
    - AUP
    - Data/System Ownership

Lesson 3.5: Assets, Threats, and Vulnerabilities

Skills Learned From This Lesson: Assets, Threats, Vulnerabilities, Risk Ownership

- Assets
- Information
- Reputation
- Brand
- Intellectual Property
- Facilities
- Equipment
- Cash and investments
- Customer lists
- Research
- People
- Service/business process
- Contributing factors to calculating asset value:
    - Financial penalties for legal non-compliance
    - Impact on business processes
    - Damage to reputation
    - Additional costs for repair/replacement

    - Effect on third parties and business partners
    - Injury to staff or other personnel
    - Violations of privacy
    - Breach of contracts
    - Loss of competitive advantage
    - Legal costs
- Threats
    - Internal threats
        - Personnel
    - External threats
        - Natural events
        - Theft
        - Sabotage/terrorism
        - Criminal acts
        - Software errors
        - Mechanical failures
        - Accidents
        - Emerging threats
- Vulnerabilities
    - Applications
        - Poorly written applications
        - Lack of testing
        - Reused Code
    - Personnel
    - Weak (or poorly enforced policies)
    - Susceptibility to natural disasters
    - Natural events
    - Difficulty in protecting against emerging threats
- Risk Ownership
    - Ownership & accountability must be assigned to the risk owner
    - Risk owner determines necessary controls
    - Owner is determined following the identification of risk
        - Also responsible for control monitoring
    - Manager or senior official who will bear responsibility for

    - Determining the risk response
    - Monitoring the effectiveness of the control
    - Monitoring and controlling the risk
    - Controls may be managed by IT, but owner is responsible for risk-related decisions

Lesson 3.6: Risk Register

Skills Learned From This Lesson: IT Risk Register, Risk Register Example, Risk Awareness Program

- The IT Risk Register
    - Purpose: to consolidate all information about a risk into a central repository
    - Lists all known risks
        - Severity, source, and potential impact
        - Risk owner
        - Current status and disposition
        - Information gathered by audits, vulnerability assessments, penetration tests, etc.
    - Risk Register includes: Risk Category, Description, Risk ID, Impact, Likelihood, Ranking, Trigger, Prevention Plan, Contingency Plan, Owner, and Residual Risk
- The Risk Awareness Program
    - Creates understanding of risk, risk factors, and types of risk
    - Should be tailored to the needs of the groups within an organization
    - Should not disclose vulnerabilities or ongoing investigations
    - Can serve to mitigate risk through education on policy and procedures
    - Management training: highlight need for management a supervisory role/oversee actions of staff
    - Senior management training: highlight liability, need for compliance, due care and due diligence/culture and ownership

Lesson 3.7: Frameworks

Skills Learned From This Lesson: ISO 27000 Series, COBIT, COBIT Principles

- Security Programs are Based on Frameworks

    - ISO 27000 Series
    - COBIT
    - COSO
    - TOGAF
    - Zachman
    - SABSA
- ISO 27001/27002
    - ISO 27001 is the framework. ISO 27002 is how to implement it
    - Most widely recognized security standard in the world
    - Process based to set up Information Security Management System (ISMS) Framework
    - Addresses information security across industries
    - Comprehensive in its coverage of security controls
- ISO 27001 Culture and Controls
    - ISO 27001 is a culture one has to build in the organization which would help to:
        - Increase security awareness within the organization
        - Identify critical assets via the Business Risk Assessment
        - Provide a framework for continuous improvement
        - Bring confidence internally as well as to external business partners
        - Enhance the knowledge and importance of security-related issues at the management level
    - Combine framework to meet multiple client requirements/compliance requirements
- COBIT 5
    - A comprehensive framework that helps enterprises to achieve their objectives for the governance and management of IT in the enterprise
    - Assists in maintaining a balance between benefits, risks, and resource usage
    - Allows a holistic approach to IT governance and management to provide the greatest benefit
    - Allows the needs of both internal and external stakeholders to be met
    - A generic framework that can benefit organizations of all size, whether commercial, not-for-profit, or public sector
    - 5 main principles and 34 processes
- How does COBIT 5 help?

    - Provide stakeholders a means in determining what they expect from the IT balance of benefits/risk/cost
    - Prioritized stakeholder needs
    - Address an organization's success on 3rd party entities
    - Deal with ever-increasing amounts of data. What is relevant and/or credible? How do we maximize the information we have?
    - Understanding and utilizing the pervasiveness of Information Technology and related resources
    - Facilitate the integration of IT and Business Functions
    - Provide for innovation and emerging technologies
    - Cover the full end-to-end IT and business functional responsibilities and allow for more effective governance and maintenance
    - Deliver more value and increase satisfaction with IT service
    - Connect and align with other major frameworks (ITIL, PMBOK, COSO)
- COBIT 5 Principles
    - Principle 1: Meeting Stakeholder Needs
    - Principle 2: Covering the Enterprise end to End
    - Principle 3: Applying a Single Integrated Framework
    - Principle 4: Enabling a Holistic Approach
    - Principle 5: Separating Governance from Management

Lesson 3.8: Information Security Architecture

Skills Learned From This Lesson: Architecture Purpose, Architecture Types

- Purpose of Architecture
    - Ensure that hardware, software, and firmware all fulfill a stated business objective
    - Components work well together
    - Consistency throughout the enterprise
    - Resources are used effectively and efficiently
    - Infrastructure is scalable
    - Existing elements can be upgraded
    - Additional elements can be added
- Types of Architectures

- Business architecture defines the business strategy, governance, organization and key business processes
- Data architecture describes the relationship between integrated components ensuring that data assets are stored, ordered, managed, and used in systems in support of an organizational strategy
- Application architecture provides a blueprint for individual applications to be deployed, their interactions and relationships to essential business processes
- Technology architecture describes the architectural design principles, components, relationships, and supporting infrastructure (hardware and software) needed to support mission-critical applications

Lesson 3.9: Risk Scenarios

Skills Learned From This Lesson: Business-related Risks, Hardware Risks, Software Risks, Utilities Risks, Network Components Risks

- Risk Scenarios: Business-related Risk
  - IT risk assessment reports must express risk in terms that management can understand
    - Use business terms
    - Refrain from highly technical/IT-specific terminology
  - Business processes and initiatives
    - IT risk assessment process must be aligned with the direction of the business
    - Risk should be examined with changes to business processes
  - Management of IT operations
    - Risk depends on culture
    - IT management should be active in mitigating risk
  - Required for all certification holders
  - Support the implementation of, and encourage compliance with, appropriate standards, procedures, and controls for information systems
  - Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards and best practices
- Risk Scenarios: Hardware
  - Hardware includes:

        - Central processing units (CPUs)
        - Motherboards
        - RAM/ROM
        - Networking components
        - Firewalls and gateways
        - Keyboards
        - Monitors
    - Risks associated are:
        - Outdated hardware
        - Poorly maintained hardware
        - Misconfigured hardware
        - Poor architecture
        - Lack of documentation
        - Lost, misplaced, or stolen hardware
        - Hardware that is not discarded in a secure manner
        - Sniffing or capturing traffic
        - Physical access (not being protected)
        - Hardware failure
        - Unauthorized hardware
- Risk Scenarios: Software
    - Risks associated with software include:
        - Logic flaws or semantic errors
        - Bugs (semantic errors)
        - Lack of patching
        - Lack of access control
        - Disclosure of sensitive information
        - Improper modification of information
        - Loss of source code
        - Lack of version control
        - Lack of input and output validation
    - Risks associated with operating systems include:
        - Unpatched vulnerabilities
        - Poorly written code
        - Complexity

        - Misconfiguration
        - Weak access controls
        - Lack of interoperability
        - Uncontrolled changes
    - Risks associated with applications include:
        - Poor or no data validation
        - Exposure of sensitive data
        - Improper modification of data
        - Logic flaws
        - Software bugs
        - Lack of logs
        - Lack of version control
        - Loss of source code
        - Weak or lack of access control
        - Lack of operability with other software
        - Backdoors
        - Poor coding practices
- Risk Scenarios: Utilities
    - Risks associated with environmental utilities include:
        - Power interruptions
        - Losses
        - Generators
        - Batteries
        - HVAC
        - Water
        - Secure operational area
    - Risks associated with software utilities include:
        - Use of outdated drivers
        - Unavailability of drivers
        - Unpatched drivers
        - Use of insecure components
        - Unpatched vulnerabilities
- Risk Scenarios: Network Components
    - Risks associated with network components include:

        - Network configuration and management
        - Network equipment protection
        - The use of layered defense
        - Suitable levels of redundancy
        - Availability of bandwidth
        - Use of encryption for transmission of sensitive data
        - Encryption key management
        - Damage to cabling and network equipment
        - Tapping network connections and eavesdropping on communications
        - Choice of network architecture
        - Documentation of network architecture
    - Risks associated with:
        - Firewalls
            - Packet filters
            - Stateful firewalls
            - Proxy servers
        - Domain name system
            - Rogue DNS
            - Poisoning
        - Wireless access point
            - Rogue access points
            - Evil Twin
        - Routers
        - Switches
        - VLANs

Lesson 3.10: Risk Scenarios Continued

Skills Learned From This Lesson: Data Ownership Risks, Third Party Risk, Cloud Risks, Project and Program Management RIsks

- Risk Scenarios: Data Ownership
    - Risks associated with data ownership include:
        - Clear ownership of data can be a significant risk
        - Staff awareness of risk associated with improper data management

        - Review processes and policies and compliance
- Risk Scenarios: Third Party Risk
    - Third party management: Data and business process ownership remains with the organization doing the outsourcing, including security requirements
    - Risks associated with outsourcing include:
        - Hiring and training practices of the supplier
        - Reporting and liaison between the outsourcing organization and the supplier
        - Time to respond to any incidents
        - Liability for non-compliance with terms of the contract
        - Nondisclosure of data or business practices
        - Responding to requests from law enforcement
        - Length of contract and terms for dissolution/termination of contract
        - Location of data storage including backup data
        - Separation between data and management of data of competing firms
    - Outsourcing: Considered from risk/regulatory perspective
        - Contracts should address security and regulatory requirements
        - Contracts should address the right to audit
        - Contractual requirements
        - Service level agreements/contractual requirements with the customer
- Risk Scenarios: The Cloud
    - Risks associated with The Cloud include:
        - Unauthorized access to customer and business data
        - Security risks at the vendor
        - The character of the vendor's employees
        - The security of the vendor's technology
        - The access the vendor has to their data
        - Compliance and legal risks
        - Where the data resides
        - Who is allowed access to it
        - How it is protected
        - Risks related to lack of control
        - Availability risks
- Risk Scenarios: Project and Program Management

- Reasons IT projects fail:
  - Unclear or changing requirements
  - Scope creep
  - Lack of budget
  - Lack of skilled resources
  - Problems with technology
  - Delays in delivery of supporting elements/equipment
  - Unrealistic timeline
  - Lack of progress reporting
  - Lack of good project management leads to:
    - Loss of business
    - Loss of competitive advantage
    - Low morale among staff members
    - Inefficient processes
    - Lack of testing of new syst ems or changes to existing systems
    - Impact on other business operations
    - Failure to meet SLAs or contractual requirements
    - Failure to comply with laws and regulations

Lesson 3.11: Risk Assessment Introduction

Skills Learned From This Lesson: Risk Assessment, Qualitative Risk Assessment, Quantitative Risk Assessment

- Risk Assessment
  - Risk Identification
    - The process of determining and documenting the risk that an enterprise faces
    - Documentation of assets and their values
  - Risk Assessment
    - A process used to identify and evaluate risk and its potential effects
    - Assessing critical functions and defining controls in place
  - Risk and Control Analysis
    - Compare current state against desired state
      - Gap analysis

        - Maturity models
        - Effectiveness of controls
    - Data analysis
        - Are all the data available?
        - Have any of the data been altered or changed?
        - Are the data in the correct format?
        - Are the data based on measuring important factors?
- Risk Assessment Methodologies
    - Two main methods
        - Quantitative (cold, hard facts, empirical data)
        - Qualitative (subjective, based on experience and what you know) start with qualitative assessment first*
        - Hybrid: semi-quantitative (brings in subjective numbers)
    - Determine the value of the asset -based on their replacement, not their current cost
- Qualitative Risk Assessment
    - Used to prioritize risks
    - Feedback based on a range of subjective values:
        - Very low
        - Low
        - Moderate
        - High
        - Very high
    - Results usually conveyed in a table that compares likelihood with impact
    - Problem: Though qualitative analysis is quick and easy to perform, it does not provide hard numerical values and doesn't fully justify the expense of controls
- Quantitative Risk Assessment
    - Based on numerical calculations
    - Suitable for cost-benefit analysis and is the basis for justification of control selection
    - Can be difficult to place a quantitative value on subjective elements of risk such as customer confidence and reputation
    - Calculating the cost of an event
        - Unpredictable depending on many factors

    - Threat/vulnerability pairings
        - Be aware of the relationships between threats and vulnerabilities

Lesson 3.12: Examples of Risk Analysis Techniques

Skills Learned From This Lesson: Risk Identification, Risk Culture and Communication, Organizational Structure

- Qualitative Probability and Impact Matrix
    - Semi-qualitative/semi-quantitative
    - Very Low, Low, Medium, and High risk levels
    - Measures likelihood/Probability and Consequence/Impacts
    - Allows us to prioritize risks and risk responses
- Quantitative Analysis Formulas and Terms
    - **Asset Value (AV):** Dollar figure that represents what the asset is worth to the organization
    - **Exposure Factor (EF):** The percentage of loss that is expected to result in the manifestation of a particular event
    - **Single Loss Expectancy (SLE):** Dollar figure that represents the cost of a single occurrence of a threat instance (AV x EF)
    - **Annual Rate of Occurrence (ARO):** How often the threat is expected to materialize
    - **Annual Loss Expectancy (ALE):** Cost per year as a result of the threat (SLE x ARO)
    - **Total Cost of Ownership (TCO):** The total cost of implementing a safeguard. Often in addition to initial costs, there are ongoing maintenance fees as well
    - **Return on Investment (ROI):** Sometimes referred to as the value of the safeguard/control
- What keeps your company going when risk management fails?

Lesson 3.13: Risk Assessment

Skills Learned From This Lesson: IT Risk Assessment Report, Risk Ownership, Risk Accountability

- IT Risk Assessment Report

- Results of risk assessment should indicate gaps between current risk state and desired risk state
- Risk assessment report should provide management documentation of risk along with recommendations for addressing any outstanding risk issues
    - Justifiable and linked with results of the risk assessment
    - Document process used and results of the risk assessment
    - State risk levels and priorities
- The risk assessment report normally includes:
    - Objectives of the risk assessment process
    - Scope and description of the area subject to assessment
    - External context and factors affecting risk
    - Internal factors or limitation affecting risk assessment
    - Risk assessment criteria
    - Risk assessment methodology used
    - Resources and references used
    - Identification of risk, threats and vulnerabilities
    - Assumptions used in the risk assessment
    - Potential of unknown factors affecting assessment
    - Results of risk assessment
    - Recommendations and conclusions
- Risk Ownership and Accountability
    - Each risk must be linked to an owner
        - Makes decisions on the best response to identified risk
    - Owner must be at a level in the organization where they can make the necessary decision and can be accountable
    - Ownership with an individual is needed for accountability
- Summary
    - During risk assessment, the risk practitioner has a responsibility to assess or determine the severity of each risk facing the organization
    - The risk practitioner should also validate the work of the previous phase and ensure that, as much as possible, all risk is identified, assessed, documented, and reported to senior management

Lesson 3.14: BCP and DRP

Skills Learned From This Lesson: Business Continuity Plan, Disaster Recovery Plan, Essential BCP/DRP Terms

- Business Continuity and Disaster Recovery Management
    - Purpose is to enable a business to continue offering critical services in the event of a disruption
    - Identify business processes of strategic importance
        - Risk assessment based on these processes
    - Primary responsibilities of senior management
    - BCP/DRP solutions may differ based on scenario
- Business Continuity Plan
        - Business Continuity focuses on continuing critical business operations in the event of a crisis and having plans in place to support those operations until the business can return to normal operations
        - Business Impact Analysis
            - Examines the impact of an outage over time
        - Long-term focus
- Disaster Recovery Plan
    - The recovery of business and IT services following a disaster or incident within a predefined schedule and budget
    - Focuses on getting critical services back up and running and getting back to a state of permanence
    - Review along with the BCP to ensure they are up to date, reflect risk scenarios, and have been tested
- Essential BCP/DRP Terms
    - **Recovery Time Objective (RTO**): Amount of time necessary to return to full operation. Can be specified for a system, a process, or an offsite facility
    - **Acceptable Interruption Window (AIW)**: Amount of time in which basic functionality must be restored (most critical systems)
    - **Recovery Point Objective (RPO):** Tolerance for data loss-i.e. how current data must be (dictates how frequently we backup data/redundancy)

    - Business Impact Analysis prioritizes business processes based on criticality (incorporates all these terms)

Lesson 3.15: Risk Mitigation Reduction and Avoidance

Skills Learned From This Lesson: Risk Response Options, Risk Mitigation, Risk Avoidance

- Risk Response and Mitigation
    - The key purpose of this function is to reduce residual risk to a degree that is acceptably by senior management
- Aligning Risk Response with Business Objectives
    - Management is responsible for evaluating and responding to the recommendations included in the risk report provided following risk assessment
    - Management must always be aware of the drivers for risk management, such as compliance with regulations and the need to support and align the risk response with business priorities and objectives
- 3.2 Risk Response Options
    - Four options for risk response:
        - Risk mitigation
        - Risk avoidance
        - Risk transfer
        - Risk acceptance
- Risk Mitigation
    - Risk mitigation means that action is taken to reduce the frequency (probability) and/or impact of a risk
        - May require the use of several controls until it reaches levels of risk acceptance or risk tolerance
    - Examples of risk mitigation:
        - Strengthening overall risk management processes, such as implementing sufficiently mature risk management processes
        - Deploying new technical, management, or operational controls that reduce either the likelihood of the impact of an adverse event
        - Installing a new access control system
        - Implementing policies or operational procedures

        - Developing an effective incident response and business continuity plan (BCP)
        - Using compensating controls
- Risk Avoidance
    - Risk avoidance means exiting the activities or conditions that give risk to risk
        - Applies when no other risk response is adequate
    - Examples of risk avoidance are:
        - Relocating a data center away from a region with significant natural hazards
        - Declining to engage in a very large project when the business case shows a notable risk of failure
        - Declining to engage in a project that would build on obsolete and convoluted because there is no acceptable degree of confidence that the project will deliver anything workable
        - Deciding not to use a certain technology or software package because it would prevent future expansion

Lesson 3.16: Risk Transference and Acceptance

Skills Learned From This Lesson: Risk Sharing/Transfer, Risk Acceptance

- Risk Sharing/Transfer
    - Risk transfer is a decision to reduce loss through sharing the risk of loss with another organization (i.e. purchasing insurance)
    - Partnerships with another organization are an example
    - Decision should be reviewed on a regular basis
- Risk Acceptance
    - A conscious decision made by senior management to recognize the existence of risk and knowingly decide to allow (assume) the risk to remain without (further) mitigation
        - Management responsible for impact of the risk event
    - Defined as the amount of risk that senior management has determined is within acceptable or permissible bounds
        - Not the same as risk ignorance/rejection, which is the failure to identify or acknowledge risk

- Risk tolerance: An exception when senior management decides to exceed risk acceptance levels

Lesson 3.17: Selecting a Mitigation Strategy

Skills Learned From This Lesson: Mitigation Strategy Selection, Cost Benefit Analysis, Return on Investment

- Selecting a Mitigation Strategy
  - Control Design and Implementation
    - Controls may be proactive (safeguards) or reactive (countermeasures)
      - Safeguards deter and prevent
      - Countermeasures detect and correct
      - Controls should meet objectives and should be audited
    - Risk assessment should determine the effectiveness of current controls to mitigate risk
    - In cases where current controls are not sufficient, controls must be adjusted, or new controls implemented
  - Vulnerabilities Associated with New Controls
    - New controls present benefits as well as new risk and vulnerabilities
    - Example: An access control system
      - Pro: Protects from unauthorized access
      - Con: Affects normal users who forget passwords, resulting in increased denial of service and more calls for technical assistance
  - Analysis Techniques
    - Analysis techniques can help management to determine the best risk response
    - Considerations for selecting a response include:
      - The priority of the risk as indicated in the risk assessment report
      - The recommended controls from the risk assessment report
      - Any other response alternatives that are suggested through further analysis
      - The cost of the various response options, including requirements for compliance with regulations or legislation

        - Alignment of the response option with the strategy of the organization
        - Possibility of integrating the response with other organizational initiatives
        - Compatibility with other controls in place
        - Time, resources, and budget available
    - Cost Benefit Analysis
        - Used to justify expense associated with the control
        - Factors used in calculating the total cost of the control:
            - Cost of acquisition
            - Ongoing cost of maintenance
            - Cost to remove/replace control
        - Factors used in calculating benefit realized from the control:
            - Reduced cost of risk event
            - Reduced liability
            - Reduced insurance premiums
            - Increased customer confidence
            - Increased shareholder confidence
            - Trust from financial backers
            - Faster recovery
            - Better employee relations (safety)
- Return on Investment
    - ROI is often used as a method of justifying an investment
        - The investment is expected to pay for itself within a set time period
    - Can be difficult to determine cost of control because it is hard to predict the likelihood of an attack
    - Return on security investment refers to ROI in relation to pay back for security controls
        - Costs may or may not provide a direct benefit in the future, like the purchase of insurance

Lesson 3.18: Types of Mitigating Controls

Skills Learned From This Lesson: Administrative Controls, Technical Controls, Physical Controls, Control Groups

- Administrative, Technical and Physical Controls
    - **Administrative controls**: Are managerial in nature and are related to the oversight, reporting, procedures, and operations of a process. These include controls such as policy, balancing employee development, and compliance reporting
    - **Technical controls**: Are sometimes known as logical controls and are provided through the use of a technology, equipment or device. Examples of technical controls include firewalls, network or host-based intrusion detection systems (IDSs), password and antivirus software. A technical control requires proper management (administrative) controls to operate correctly
    - **Physical controls**: Are locks, fences, closed-circuit TV (CCTV) and such devices that are installed to physically restrict access to a facility or hardware. Physical controls require maintenance, monitoring and the ability to assess and react to an alert should a physical control indicate a problem
- Control Groups
    - Technical (Logical)
        - Firewalls
        - Encryption
        - ACLs
    - Physical
        - Door Locks
        - Security Guard
        - Mantraps
    - Managerial (Administrative)
        - Policy
        - Directives
        - Standard Operating Procedures
- Control Activities, Objectives, Practices, and Metrics
    - Reducing IT risk to acceptable risk levels requires measurement and monitoring
    - This phase supports the risk and control monitoring and reporting phase by putting mechanisms into place to measure risk and controls

- Managing Risk Throughout the System/Software Development Lifecycle
    - Risk must be evaluated and monitored at all points during the SDLC
    - New risk may emerge as the system moves through the SDLC
    - The risk practitioner should be alert to circumstances where the development team is not following the standards and policies of the organization regarding system development or the implementation of controls

Lesson 3.19: Risk and Control Monitoring and Reporting

Skills Learned From This Lesson: Risk Control Monitoring, Risk Control Reporting, Control Assessment Results

- Risk and Control Monitoring and Reporting
    - A risk response is designed and implemented based on a risk assessment that was conducted at a single point in time
    - Because of the changing nature of risk and associated controls, ongoing monitoring is an essential step of the risk management life cycle
        1. Controls can become less effective
        2. The operational environment may change, and
        3. New threats, technologies, and vulnerabilities may emerge
- Monitoring Controls
    - The purpose of monitoring controls is to verify whether the control is effectively addressing the risk
    - The purpose of risk monitoring is to collect, validate, and evaluate goals and metrics, to monitor that processes are performing as expected, and to provide reporting
    - Monitoring may be done through self-assessment or independent assurance reviews
    - The risk practitioner should encourage management and process owners to possess ownership of control improvement
    - The steps to monitoring controls are:
    1. Identify and confirm risk control owners and stakeholders
    2. Engage with stakeholders and communicate the risk and information security requirements and objectives for monitoring and reporting

3. Align and continually maintain the information security monitoring and evaluation approach with the IT and enterprise approaches
4. Establish the information security monitoring process and procedure
5. Agree on a lifecycle management and change control process for information security monitoring and reporting
6. Request, prioritize, and allocate resources for monitoring information security

- Results of Control Assessments
    - The effectiveness of control monitoring is dependent on the:
        - Timeliness of the reporting- Are data received in time to take corrective action?
        - Skill of the data analyst- Does the analyst have the skills to properly evaluate controls?
        - Quality of monitoring data available- Are the monitoring data accurate and complete?
        - Quantity of data to be analyzed- Can the risk practitioner find the important data in the midst of all the other log data available?

Lesson 3.20: KRIs

Skills Learned From This Lesson: KRIs, KRI Benefits, KRI Examples

- Key Risk Indicators
    - KRIs are used by organizations to determine their risk exposure vs. risk tolerance
    - By measuring the risks and their potential impact on business performance, organizations can create alerts that allow monitoring, management, and mitigation of key risks
    - Effective KRIs help to:
        - Identify the biggest risks
        - Quantify those risks and their impact
        - Put risks into perspective by providing comparisons and benchmarks
        - Enable regular risk reporting and risk monitoring
        - Alert key people in advance of risks unfolding
        - Help people to manage and mitigate risks
    - Benefits of KRIs
        - Provide early warning

        - Provide backward-looking view on risk events
        - Enable documentation and analysis of trends
        - Provide an indication of risk appetite and tolerance
        - Increase the likelihood of achieving strategic objectives
        - Assist in optimizing risk governance
    - Examples of KRIs:
        - Quantity of unauthorized equipment or software detected in scans
        - Number of instances of SLAs exceeding thresholds
        - High average downtime due to operational incidents
        - Average time to deploy new security patches to servers
        - Excessive average time to research and remediate operations incidents
        - Number of desktops/laptops that do not have current antivirus signatures or have not run a full scan within scheduled periods
    - KRIs support
        - Risk appetite
        - Risk identification
        - Risk mitigation
        - Risk culture
        - Risk measurement and reporting
        - Regulatory compliance
- KRI Optimization: Examples in Which KRIs Should be Optimized
    - **Sensitivity:** Management has implemented an automated tool to analyze and report on access control logs based on severity; the tool generates excessively large amounts of results. Management performs a risk assessment and decides to configure the monitoring tool to report only on alerts marked “critical.”
    - **Timing:** Management has implemented strong segregation of duties (SoD) within the enterprise resource planning (ERP) system. One monitoring process tracks system transactions that violate the defined SoD rules before month-end processing is completed so that suspicious transactions can be investigated before reconciliation reports are generated
    - **Frequency:** Management has implemented a key control that is performed multiple times a day. Based on a risk assessment, management decides that the monitoring activity can be performed weekly because this will capture a control failure in sufficient time for remediation

- **Corrective action:** Automated monitoring of controls is especially conducive to being integrated into the remediation process. This can often be achieved using existing problem management tools, which help prioritize existing gaps, assign problem owners, and track remediation efforts.

Lesson 3.21: Tools for Risk Monitoring

Skills Learned From This Lesson: Internal Data Sources, Logs, External Sources of Information

- Data Collection and Extraction Tools & Techniques
  - Internal Data Sources include:
    - Audit reports
    - Incident reports
    - User feedback
    - Observation
    - Interviews with management
  - Security reports
  - Logs
- Logs
  - Analysis of log data should answer the following:
    - Are the controls operating correctly?
      - Is the level of risk acceptable?
      - Are the risk strategy and controls aligned with business strategy and priorities?
      - Are the controls flexible enough to meet changing threats?
    - Is correct risk data being provided in a timely manner?
      - Is the risk management effort aiding in reaching corporate objectives?
      - Is the awareness of risk and compliance embedded into user behaviors?
    - Logs may contain sensitive information and may be needed for forensic purposes
    - Logs should not contain too much information

        - SEIM are helpful. They pull logs from various systems so they can be examined at a single location
- External Sources of Information
    - Media reports
    - Computer emergency response team (CERT) advisories
    - Security company reports
    - Regulatory bodies
    - Peer organizations
- Summary
    - As risk is identified and assessed, the risk owners select the appropriate response to the risk and create risk action plans to implement or modify controls selected to mitigate risk
    - As controls to mitigate risk are designed and developed, the risk owner also mandates the development of the ability to monitor and report on the effectiveness of controls
    - Regular monitoring and reporting on risk is essential to management, and the use of KPIs and KRIs assists management in the monitoring of trends, compliance, and issues related to risk
    - Risk management is a never-ending process
    - IT risk and controls should be continuously monitored and reported on to ensure continued efficiency and effectiveness

Module 4: Domain 3 Information Security Program Development and Management

Lesson 4.1: Information Security Program and Development

Skills Learned From This Lesson: Information Security Development and Management Agenda

- Domain 3 Information Security Development and Management Agenda
    - Information Security Concepts
    - Information Security Frameworks
        - ISO 27001

        - COBIT
    - Information Security Architecture
    - Security Program Operations
    - Third Party Governance
    - Cloud Integration
    - IT Service Management
    - Control Integration
    - Policies, Procedures, Standards, Guidelines
    - Certification and Accreditation/Authorization
    - Metrics and Monitoring

Lesson 4.2: Information Security Program Concepts

Skills Learned From This Lesson: Information Security Program, Information Security Program Elements, Information Security Practices

- Information Security Program
    - As defined by ISACA the goal of this domain is to "Develop and maintain an information security program that identifies, manages, and protects the organization's assets while aligning to information security strategy and business goals, thereby supporting an effective security posture."
    - Is best coordinated by the Chief Operating Officer, as this individual should properly see the need for balance between information security and business operations
- Key Information Security Program Elements
    - Technology
        - System Security
        - UTM/Firewalls
        - IDS/IPS
        - Data Center
        - Physical Security
        - Vulnerability Assessment
        - Penetration Testing
        - Application Security
        - Secure SDLC

        - SIM/SIEM
        - Managed Services
    - People
        - Training
        - Awareness
        - HR Policies
        - Background Checks
        - Roles/Responsibilities
        - Mobile Computing
        - Social Engineering
        - Social Networking
        - Acceptable Use
        - Policies
        - Performance Management
    - Process
        - Risk Management
        - Asset Management
        - Data Classification
        - Information Rights Management
        - Data Leak Prevention
        - Access Management
        - Change Management
        - Patch Management
        - Configuration
- Essential Information Security Practices
    - Management commitment*
    - Risk management*
    - Asset inventory and management
    - Change Management*
    - Incident Response and management
    - Configuration management*
    - Training and awareness
    - Continuous audit* (measuring compliance to the process)
    - Metrics and measurement

- Vulnerability assessment* (does it work?)
- Penetration testing* (does it work?)
- Application security testing
- Device management
- Log monitoring, analysis and management*
- Secure development*

Lesson 4.3: Information Security Program Requirements

Skills Learned From This Lesson: Security Program Requirements, Enterprise Information Security Program, Information Security Program Concepts

- Security Program Requirements
  - Must develop an enterprise security architecture at conceptual, logical, functional, and physical levels
  - Must manage risk to acceptable levels
    - Risk develops the Business Case that convinces management security should be performed
  - Must be defined in business terms to help non-critical stakeholders understand and endorse program goals
  - Must provide security-related feedback to business owners and stakeholders
  - Must address risks in relation to the five categories of assets
- Enterprise Information Security Program
  - Strategic Planning and Management
  - Security Operations and Maintenance
  - Enterprise Continuity
  - System and Application Security
  - Physical Security
  - Personnel Security
  - Assessments and Review
  - Incident Management
  - Security Awareness
  - Vulnerability Management
  - Risk Management
  - Security Controls

- Information Security Program Concepts
    - An IS Program includes the practical elements that make the information security strategy possible
    - Provides the means for closing the gap between current state and desired state
    - The purpose of the development of a security program is to perform gap analysis. We need to figure out where we want to be and how we are going to shrink the gap

Lesson 4.4: Essential Elements of an Information Security Program

Skills Learned From This Lesson: Information Security Program, Information Security Program Elements, Information Security Practices

- Essential Elements of an Information Security Program
    - An IS Program allows the execution of a well-planned IS strategy, which is closely aligned with business goals
    - Management and key stakeholders must be directly involved in its development
    - Effective metrics must be established to determine the efficacy of the program and implemented controls
- An Information Security Program Should...
    - Provide strategic alignment with business objectives
    - Use risk management as the foundation for security related decisions
    - Deliver value to stakeholders
    - Manage resources efficiently and effectively
    - Provide integration with other assurance functions (operational, security, physical security, facility security, etc.)
    - Use performance measurements to provide a means of measuring progress and monitoring activities

Lesson 4.5: Security Frameworks

Skills Learned From This Lesson: ISO 27001 Framework, COBIT 5, COBIT 5 Principles

- Security Programs are Based on Frameworks
    - ISO 27000 Series
    - COBIT

    - COSO
    - TOGAF
    - Zachman
    - SABSA
- ISO 27001/27002
    - ISO 27001 is the framework. ISO 27002 is how to implement it
    - Most widely recognized security standard in the world
    - Process based to set up Information Security Management System (ISMS) Framework
    - Addresses information security across industries
    - Comprehensive in its coverage of security controls
- ISO 27001 Culture and Controls
    - ISO 27001 is a culture one has to build in the organization which would help to:
        - Increase security awareness within the organization
        - Identify critical assets via the Business Risk Assessment
        - Provide a framework for continuous improvement
        - Bring confidence internally as well as to external business partners
        - Enhance the knowledge and importance of security-related issues at the management level
    - Combine framework to meet multiple client requirements/compliance requirements
- COBIT 5
    - A comprehensive framework that helps enterprises to achieve their objectives for the governance and management of IT in the enterprise
    - Assists in maintaining a balance between benefits, risks, and resource usage
    - Allows a holistic approach to IT governance and management to provide the greatest benefit
    - Allows the needs of both internal and external stakeholders to be met
    - A generic framework that can benefit organizations of all size, whether commercial, not-for-profit, or public sector
    - 5 main principles and 34 processes
- How does COBIT 5 help?
    - Provide stakeholders a means in determining what they expect from the IT balance of benefits/risk/cost

    - Prioritized stakeholder needs
    - Address an organization's success on 3rd party entities
    - Deal with ever-increasing amounts of data. What is relevant and/or credible? How do we maximize the information we have?
    - Understanding and utilizing the pervasiveness of Information Technology and related resources
    - Facilitate the integration of IT and Business Functions
    - Provide for innovation and emerging technologies
    - Cover the full end-to-end IT and business functional responsibilities and allow for more effective governance and maintenance
    - Deliver more value and increase satisfaction with IT service
    - Connect and align with other major frameworks (ITIL, PMBOK, COSO)
- COBIT 5 Principles
    - Principle 1: Meeting Stakeholder Needs
    - Principle 2: Covering the Enterprise end to End
    - Principle 3: Applying a Single Integrated Framework
    - Principle 4: Enabling a Holistic Approach
    - Principle 5: Separating Governance from Management

Lesson 4.6: Purpose of Architecture

Skills Learned From This Lesson: Information Security Architecture, Types of Architectures

- Information Security Architecture
    - Ensure that hardware, software, and firmware all fulfill a stated business objective
    - Components work well together
    - Consistency throughout the enterprise
    - Resources are used effectively and efficiently
    - Infrastructure is scalable
    - Existing elements can be upgraded
    - Additional elements can be added
- Types of Architectures
    - Business architecture defines the business strategy, governance, organization and key business processes

- Data architecture describes the relationship between integrated components ensuring that data assets are stored, ordered, managed, and used in systems in support of an organizational strategy
- Application architecture provides a blueprint for individual applications to be deployed, their interactions and relationships to essential business processes
- Technology architecture describes the architectural design principles, components, relationships, and supporting infrastructure (hardware and software) needed to support mission-critical applications

Lesson 4.7: Information Security Frameworks

Skills Learned From This Lesson: Operational components, Management Components, RACI Matrix, Administrative Components, Educational Components

- Components of an IS Framework
  - Operational components
  - Management components
  - Administrative components
  - Educational components
- Operational Components
  - Identity and access management
  - Redundancy
  - Security event monitoring and analysis
  - System patching procedures
  - Configuration management and change control procedures
  - Security metrics collection and evaluation
  - Maintenance of security controls and support technologies
  - Incident response, investigation, and resolution
  - Secure disposal of data and storage devices
- Management Components
  - Strategic between the business and Information Security
  - Development of policies, procedures, standards, guidelines, baselines
  - Ensure testing and review of incident response and business continuity plans
  - Ensuring roles and responsibilities are clearly defined (RACI matrix)
  - Periodic analysis of assets, threats, vulnerabilities, and risks

    - Ongoing communication with business units for guidance and feedback for IS teams
- RACI Matrix
    - Responsible (assigned the task)
    - Accountable (has final decision-making authority and accountability)
    - Consulted (advisor, stakeholder, or SME who is consulted)
    - Informed (must be informed after a decision or action)
- Administrative Components
    - Financial
        - Budgeting
        - TCO Analysis
        - ROI
    - HR Management
        - Onboarding and offboarding of employees
        - Performance and management
        - Employee education and development
    - 3rd Party Governance
        - Evaluation and selection criteria determination for vendors
        - Development and evaluation of contracts and SLA
        - Audit
    - Functional management
        - Balance project efforts and ongoing operational overhead
- Educational Components
    - General security training and awareness is the responsibility of HR and is often associated with employee orientation and initial new-hire training
    - Role-based issues and responsibilities are addressed within the business unit
    - Online testing can help ensure that information was understood

Lesson 4.8: Security Operations Event Monitoring

Skills Learned From This Lesson: Event Monitoring, Vulnerability Management, Auditing

- Security Program Operations

    - Event Monitoring
        - Event monitoring is the practice of examining events that are occurring on information systems, including applications, operating systems, database management systems, end-user devices, and every type and kind of network device, and being aware of what is going on throughout the entire operating environment
            - Log Reviews
            - Honeypots
            - IDS/IPS
            - SEIM Systems
                - Threat intelligence from external sources
                - Orchestration
- Vulnerability management
    - Vulnerability management is the practice of periodically examining information systems (including but not limited to operating systems, subsystems such as database management systems, applications, and network devices) for the purpose of discovering exploitable vulnerabilities, related analysis, and decisions about remediation. Organizations employ vulnerability management as a primary activity to reduce likelihood of successful attacks on their IT environment
        - Security scan
        - Vulnerability assessment
        - Penetration test
- Auditing
    - Ensures security controls are in place and are performing as expected
    - Can be internal or external
    - Five components:
        - Objective (what is the objective of the audit?)
        - Scope
        - Approach
        - Constraints
        - Result

Lesson 4.9: Secure Engineering and Threat Modeling

Skills Learned From This Lesson: Secure Engineering, Secure Development, STRIDE

- Secure engineering and development
    - Security can add value at each stage of the development cycle:
    - **Conceptual:** Feasibility studies and initial risk assessments-Broad understanding of security framework
    - **Requirements:**
        - Functional Analysis- Customer provides the requirements of the system or product-functional requirements should include security
        - System Analysis- Developers determine the security specifications and plan for implementation of security checkpoints
    - **Design:** Developers plan for implementation of security per requirements. Security is provided for in budget and schedule. Design reviews will help ensure that security remains a focus
        - Security checkpoints are created along the way
    - **Engineering and development:** Developers implement determined security within the code. Unit testing ensures structure and logic of code in the right direction
    - **Testing:** Certification ensures the technical security features of a product meet the developer's description. If so, the product is verified. Accreditation/Authorization is senior management's decision to implement the product, as it solves the problem it was designed to solve. The product is now validated
- Secure Engineering and Development Threat Modeling: STRIDE

Threat	**Mitigation**
Spoofing	Authentication
Tampering	Integrity verification (Message digests/CRCs)
Repudiation	Non-repudiation (Digital Signatures)

Information Disclosure	Confidentiality through encryption
Denial of Service	High Availability/Redundancy/Fault Tolerance
Escalation of Privilege	Authorization

Lesson 4.10: Protecting the Network- Segmentation

Skills Learned From This Lesson: Segmentation, Routers, VLANs, Firewalls, Proxies, DMZ

- Network Protection: Segmentation (separate trusted resources from untrusted entities)
    - Routers
    - VLANs
    - Firewalls
        - Packet Filters (looks at source/destination IP address, port number, protocol usage)
            - Blacklisting- everything is allowed except what is forbidden on the blacklist)
            - Whitelisting- everything is blocked except what is allowed on the whitelist)
        - Stateful Firewalls (aware of the connection state between devices)
        - Application Proxies (specific to application layer protocols)
            - Web proxies
            - Mail proxies
        - DMZ (semi-trusted zone)
        - Air gaps (i.e. one computer on Router A one computer on Router B)

Lesson 4.11: Protecting the Network- Wireless Security

Skills Learned From This Lesson: WEP, WPA, WPA2, 802.1x

- Network Protection: Wireless Networks
    - Encryption
        - WEP: Poor choice, weak keys, weak algorithm, weak implementation

        - WPA: A step in the right direction, but not the solution
        - WPA2: Best choice. Strong keys, strong algorithm, good implementation
    - Authentication
        - 802.1x: RADIUS or some other central server for authentication

Lesson 4.12: Protecting the Network- Services

Skills Learned From This Lesson: DNS, DHCP, LDAP

- Network Protection: Services
    - DNS- how domain controllers/key distribution centers are located, provides name resolution
        - Pharming- modification of DNS records (i.e. A record or host record)
        - Cache Poisoning- modification of the DNS cache
    - DHCP- automatically assigns IP addresses and other information (DNS) to hosts
    - LDAP- database structure AD uses (LDAP in Windows = Domain Controller, LDAP in other OS = authentication server)
    - Web services
    - Mail services

Lesson 4.13: Protecting the Network through Detection and Network Access Control

Skills Learned From This Lesson: IDS, IPS, NAC,

- Network Protection: Inspection and Detection
    - Sniffers
    - IDS/IPS
    - Honeypots/Honeynets
    - Log reviews
    - Internal audit
    - External audit
- Network Protection: Network Access Control (NAC)
    - Verifies Health of System
    - Relies on Client-side and Server-side software
    - Uses a System Health Validator (SHV) on server
    - Client presents a Certificate of Health

- Can provide Denial of access, quarantine, or redirection to a remediation network

Lesson 4.14: Data and Endpoint Security

Skills Learned From This Lesson: Endpoint Protection, System Hardening, Data Security

- Endpoint (Desktops, Laptops, Tablets, etc.) Protection
  - Hardening systems includes:
    - Remove unnecessary services
    - Patch systems
    - Rename guest and administrative accounts
    - Review default settings and configurations
    - Install anti-malware and monitoring software
    - Images are often used to deploy baseline OS and applications
    - Configuration management requires changes to be controlled and documented
    - Remote access tools are often used by the network team to provide assistance and remote admin if needed
    - Many devices have remote destruction capabilities in case of loss or compromise
    - Data should be encrypted for the sake of privacy
    - VDI relies on highly controlled servers running the apps users work with. Client systems work as terminals or thin client
- Data Security
  - Confidentiality:
    - Data at Rest: Encryption
    - Data in Motion: Secure Transport Protocols (SSL/TLS/IPSec)
    - Data in Use: Homomorphic Encryption
  - Integrity
    - Hashes/Message Digests
  - Availability
    - Redundancy
  - Non-repudiation
    - Digital Signatures

- Data traversing unsecured networks can have end-to-end security through the use of VPNs

Lesson 4.15: Identity and Access Management

Skills Learned From This Lesson: Identity Proofing, Account Provisioning, Account Deprovisioning

- Identity and Access Management
  - Identity Proofing
  - Account Provisioning
  - User Identified-username or account number (make a claim)
  - User Authenticates-multifactor (prove the claim)
  - User is Authorized- assigned rights and permissions (best implemented through RBAC)
  - User is Audited/Accountable
  - Account is Deprovisioned

Lesson 4.16: Third Party Governance

Skills Learned From This Lesson: Third Party Providers, Legal Responsibility, MOA, SLA

- Third Party Providers
  - Internet service providers, call centers, data processing centers, etc.
  - Vicarious liability imposes legal responsibility on an entity when the entity had nothing to do with actually causing the injury
    - Often applied through “Respondent Superior” when a superior is liable for the actions of his or her employees
  - Laws are evolving
    - Is an ISP responsible for what its customers do?
    - Is a software service that provides P2P sharing liable when its customers use software to violate copyright restrictions?
  - You can transfer risk but you can’t transfer responsibility or liability
  - Procurement Documents
    - Request for Information (RFI)
    - Request for Quote (RFQ)

- Request for Proposal (RFP)
- Invitation for Bid (IFB)
- Contracts
    - Memorandum of Agreement (MOA)- defines expected responsibilities
    - Service Level Agreement (SLA)- usually a legally binding contract that offers guarantees usually centering on performance and reliability of procured systems as well as response times from the vendor
        - Could also be used internally from department to department
        - A form of risk transference
        - Metrics should be clearly defined in the SLA
        - Usually offer some sort of financial compensation if the metrics are not met

Lesson 4.17: Policies, Procedures, Standards, and Guidelines

Skills Learned From This Lesson: Policies, Procedures, Standards, Guidelines, Baselines

- Policies, Procedures, Standards, and Guidelines
    - Policies
        - A set of policies are principles, formulated or adopted by an organization to reach its strategic goals and typically published in a booklet or other form that is widely accessible
        - Policies are designed to influence and determine all major decisions and actions, and all activities take place within the boundaries set by them
        - Three main types of policies exist:
            - The Corporate (organizational) Security Policy can be thought of as a blueprint for the whole organization's security program. It is the strategic plan for implementing security in the organization
            - A system-specific policy is concerned with a specific or individual computer system. It is meant to present the approved software, hardware, and hardening methods for that specific system

        - An issue-specific policy is concerned with a certain functional aspect that may require more attention. For this reason, a separate policy is prepared for that issue to explain with details the required level of security and the instructions that all staff in the organization must abide by to achieve this level
    - Standards
        - Mandatory
        - Created to support policy, while providing more specific details
        - Reinforces policy and provides direction
        - Can be internal or external
    - Procedures
        - Mandatory
        - Step-by-step directives on how to accomplish an end-result
        - Detail the “how-to” of meeting the policy, standards, and guidelines
    - Guidelines
        - Not Mandatory
        - Suggestive in nature
        - Recommended actions and guides to users
        - “Best Practices”
    - Baselines
        - Mandatory
        - Minimum acceptable security configuration for a system or process
        - The purpose of a security classification is to determine and assign the necessary baseline configuration to protect the data

Lesson 4.18: Policies, Procedures, Standards, and Guidelines

Skills Learned From This Lesson: Certification, Accreditation, Common Criteria, Metrics, Monitoring

- Certification and Accreditation
    - Certification is the technical evaluation of the product’s security mechanisms in a particular environment. Once having passed the certification process, the system is now verified. Usually performed by QA or someone with technical expertise

    - Accreditation: A formal declaration by an AO Authorizing Official (Title that has replaced Designated Accrediting Authority DAA) that information systems are approved to operate at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards. Once accredited, the system is now validated
    - Traditional Evaluation Criteria
        - Trusted Computer System Evaluation Criteria (TCSEC): Evaluates confidentiality
        - Information Technology Security Evaluation Criteria (ITSEC): Evaluates confidentiality, integrity, and availability
        - Common Criteria (CC): provided a common structure and language. It's an International standard (ISO 15408)
            - Protection Profile: Requirements from Agency or Customer
            - Target of Evaluation: System designed by Vendor
            - Security Target: Detail how the TOE meets the PP
            - Evaluation Assurance Level: Function and Assurance (reliability of the process) evaluation level
- Common Criteria Evaluation Assurance Levels
    - EAL 1- Functionally Tested
    - EAL 2- Structurally Tested
    - EAL 3- Methodically tested and checked
    - EAL 4- Methodically designed, tested, and reviewed
    - EAL 5- Semi formally designed and tested
    - EAL 6- Semi formally verified, designed, and tested
    - EAL 7- Formally verified, designed, and tested
- Metrics and Monitoring
    - A metric is a measurement of a process or entity based on its performance in relation to desired objectives
    - Utilizing metrics properly requires collecting these measurements and examining them in the context of the overall information security program
    - Monitoring is the continuous or regular evaluation of a system or control to determine its operation or effectiveness. Can be quantitative or qualitative
- Monitoring Function: Metrics
    - Strategic Metrics

        - Project Plan
        - Budget Metrics
        - Risk performance
        - Disaster Recovery Test results
        - Audit results
        - Regulatory compliance results
    - Tactical Metrics
        - Policy compliance
        - Exceptions to policy/standards
        - Changes in process
        - Incident management
    - Operational Metrics
        - Vulnerability scan results
        - Server configuration
        - Standards compliance
        - IDS monitoring results
        - Firewall log analysis
        - Patch management status

Lesson 4.19: Domain 3 Wrap-up

Skills Learned From This Lesson: Information Security Development and Management Review

- Domain 3 Information Security Development and Management Review
    - Information Security Concepts
    - Information Security Frameworks
        - ISO 27001
        - COBIT
    - Information Security Architecture
    - Security Program Operations
    - Third Party Governance
    - Cloud Integration
    - IT Service Management
    - Control Integration
    - Policies, Procedures, Standards, Guidelines

- Certification and Accreditation/Authorization
- Metrics Monitoring

Module 5: Domain 4 Business Continuity and Disaster Recovery Management

Lesson 5.1: BCP and DRP

Skills Learned From This Lesson: Business Continuity Plan, Disaster Recovery Plan, Essential BCP/DRP Terms

- Business Continuity and Disaster Recovery Management
  - Purpose is to enable a business to continue offering critical services in the event of a disruption
  - Identify business processes of strategic importance
    - Risk assessment based on these processes
  - Primary responsibilities of senior management
  - BCP/DRP solutions may differ based on scenario
- Business Continuity Plan/Disaster Recovery Plan
  - Business continuity plan: focuses on continuing critical business operations in the event of a crisis and having plans in place to support those operations until the business can return to normal operations
    - Business Impact Analysis examines the impact of an outage over time
  - Disaster recovery plan: The recovery of business and IT services following a disaster or incident within a predefined schedule and budget
    - Review along with BCP to ensure they are up to date, reflect risk scenarios, and have been tested
- Essential BCP/DRP Terms
  - **Recovery Time Objective (RTO**): Amount of time necessary to return to full operation. Can be specified for a system, a process, or an offsite facility
  - **Acceptable Interruption Window (AIW)**: Amount of time in which basic functionality must be restored (most critical systems)

- **Recovery Point Objective (RPO):** Tolerance for data loss-i.e. how current data must be (dictates how frequently we backup data/redundancy)
- Business Impact Analysis prioritizes business processes based on criticality (incorporates all these terms)

Lesson 5.2: BCP and DRP

Skills Learned From This Lesson: Preparation, Protection, Detection, Triage, Response

- Incident Management Process Flow
  - Prepare -> Protect -> Detect -> Triage -> Respond
- Prepare
  - Defines the preparation work that has to be completed prior to having any capability to respond to incidents
    - Coordinate planning and design
      - Identify incident management requirements
      - Obtain funding and sponsorship
      - Develop Implementation Plan
    - Coordinate implementation
      - Develop policies, processes, and plans
      - Establish incident handling criteria
      - Define Criticality
      - Evaluate Incident Management capability
      - Define post-mortem review
      - Define process change procedure
- Protect
  - Protect and secure critical data, services, processes, resource when responding to incidents
  - Also includes a proactive plan for improvement on a predetermined schedule
  - Implement changes to mitigate/limit the scope of the incident
  - Implement infrastructure protection improvements as indicated from post-mortem reviews or other process improvement reviews
  - Conduct proactive reviews and assessments of existing infrastructure
- Detect

    - Identify unusual/suspicious activity that might compromise critical business functions or infrastructure
        - Proactive detection- conduct detective monitoring regularly
            - Honeypots
            - Scan for unauthorized servers or hosts
            - Analyze network traffic
            - Review audit logs and files
        - Reactive detection is essential as well to be able to quickly detect an attack
            - Intrusion detection
            - Review audit logs and files
- Triage
    - Helps direct response to areas of highest criticality through the following sub-processes
        - **Categorization**: Uses pre-defined criteria to determine and label the type of incident
        - **Correlation**: Determine/report other relevant information
        - **Prioritization**: Enables minimization of impact to the most critical business function
        - **Assignment**: To the Incident Response Team (can also be referred to as the IMT-Incident Management Team)
- Respond
    - Steps taken to address, contain, resolve, or mitigate an incident
        - Technical responses
            - Collect data
            - Analyze incident
            - Research corresponding technical mitigation techniques
            - Isolate affected systems
            - Deploy patches and workaround
        - Management Response: activities that require supervisory or management intervention- notification, interaction, escalation or approval-business and senior managers

        - Legal Response: activity that relates to the investigation, prosecution, liability, copyright, and privacy issues

Lesson 5.3: Roles and Responsibilities

Skills Learned From This Lesson: Incident Management Policy, Incident Response Plan, Incident Management and Response Teams

- Responsibilities of the CISM for Incident Response
    - The CISM is responsible for:
        - Development of Incident Management policy:
            - Set expectations
            - Maintain the consistency and reliability of services
            - Provide documentation for roles and responsibilities
            - Set requirements for identified alternatives for important functions
        - Development of incident management and response plans
        - Handling and coordinating incident response activities
        - Verifying, validating, and reporting of countermeasures
        - Planning, budgeting and program development for all matters related to IS incident management
- Incident management and Response Teams
    - Emergency action team: Designated evacuation and safety team
    - Damage assessment team: Qualified team who assess the extent of the damage to physical assets and determines salvage capability of resources and assets
    - Emergency management team: Coordinates the actions of other recovery teams and makes key decisions where necessary
    - Relocation team: Responsible for coordination of process of moving to an offsite facility, and back to the restored facility or facility of permanence
    - Security team: Often called the CIRT responsible for monitoring the system and communication links, containing security threats, resolving issues that impede recovery

Lesson 5.4: Making the Case for Incident Response

Skills Learned From This Lesson: Event, Incident, Incident Handling, Incident Response, Incident Response Plan

- Security Incident Response Definitions
    - **Event**: A change in state
    - **Incident**: An event or events that have a negative impact on the company and its security
    - **Incident Handling**: Involves all the processes associated with addressing events and incidents
    - **Incident Response**: The last step of incident management, encompassing planning, coordination and appropriate mitigation, containment and recovery strategies
- The Importance of Incident Response Planning
    - Occurrences are increasing
    - Losses are escalating
    - Increase in vulnerable and misconfigured systems
    - Legal and regulatory groups may require
    - Growing sophistication of attackers
- Outcomes of Incident Response Planning
    - Impact on the business will be minimized
    - Effective plans are in place and understood by stakeholders
    - Incidents are identified and contained, as well as identification of root causes, enabling recovery within the AIW (Acceptable Interruption Window)

Lesson 5.5: Developing the Incident Response Plan- Capability Assessment

Skills Learned From This Lesson: Incident Response Plan, Threats, Vulnerabilities

- Developing the Incident Response Plan
    - Assessing Current Incident Response Capability
        - Survey
        - Self-Assess
        - External Assessment
        - Evaluate Threats
            - Natural

        - Technical
        - Man-made
    - Evaluate Vulnerabilities
        - Technology
        - People
        - Processes
        - Controls
    - Incident History
    - Current State vs. Desire State

Lesson 5.6: Developing the Incident Response Plan- Capability Assessment

Skills Learned From This Lesson: Preparation, Identification, Containment, Eradication, Triage, Lessons Learned

- Elements of an Incident Response Plan
    - Preparation -> Identification -> Containment -> Eradication -> Triage -> Lessons Learned
- Preparation
    - Develop an incident response prior to an incident
        - Develop Approach/Methodology
        - Establish Policy
        - Develop deterrence strategies
        - Determine criteria on when to report an incident to law enforcement
        - Ensure necessary tools are available
- Identification
    - Verify an actual incident has occurred (violation analysis)
    - Assign ownership
    - Establish chain of custody
    - Determine severity of incident and escalate as necessary
- Containment
    - Once the incident has been identified and verified, the Incident Response Plan aka Incident Management Plan is to be activated
    - Notify IT
    - Notify affected stakeholders

    - Obtain agreement of any actions taken that would affect availability of services
    - Obtain and preserve evidence
    - Document actions from this point forward
    - Control and manage communications to the public
- Eradication
    - Determine the root cause of the incident and eliminate it
    - Determine signs and causes
    - Remove root cause
    - Improve defenses by implementing proactive techniques
    - Perform vulnerability analysis to determine additional weaknesses
- Recovery
    - Restore affected systems or services to a condition specified by the Service Delivery Objectives or BCP
    - Restore to normal operations
    - Validation actions taken were successful
    - Involve system owners in testing
    - Facilitate system owners to declare operations have been restored to normal
- Lessons Learned
    - At the end of the incident response processes, team is de-briefed and report must be developed to share what has happened
    - Document the report
    - Analyze issues which occurred during the incident
    - Propose improvement
    - Present reports to stakeholders

Lesson 5.7: Incident Detection Devices

Skills Learned From This Lesson: Protocol Analyzers, IDS, Pattern Matching, Profile Comparison

- Incident Detection Devices
    - Protocol Analyzers (Sniffers)
    - Intrusion Detection Systems
        - Software is used to monitor a network segment or an individual computer
        - Used to detect attacks and other malicious activity

        - Dynamic in nature
        - Two main types:
            - Host-based (local host only)- small agent programs that reside on individual computer. Detects suspicious activity on one system, not a network segment
            - Network-based (packet sniffer + analysis engine)- monitors traffic on a network segment. Computer or network appliance with NIC in promiscuous mode. Sensors communicate with a central management console. Most appropriate placement for an IDS is in the DMZ
- Analysis Engine Methods
    - Pattern Matching
        - Rule-Based Intrusion Detection
        - Signature-Based Intrusion Detection
        - Knowledge-Based Intrusion Detection
    - Profile Comparison
        - Statistical-Based Intrusion Detection
        - Anomaly-Based Intrusion Detection
        - Behavior-Based Intrusion Detection
- IDS vs. IPS
    - IDS (Passive)
        - Page or email administrator
        - Log event
    - IPS (Active)
        - Send reset packets to the attacker's connections
        - Change a firewall or router ACL to block an IP address or range
        - Reconfigure router or firewall to block protocol being used for attack
- IDS Issues
    - May not be able to process all packets on large networks
        - Missed packets may contain actual attacks
        - IDS vendors are moving more and more to hard-ware based systems
    - Cannot analyze encrypted data
    - Switch-based networks make it harder to pick up all packets
    - A lot of false alarms

- Not an answer to all prayers
  - Firewalls, antivirus software, policies, and other security controls are still important

Lesson 5.8: Developing the Incident Response Plan- Capability Assessment

Skills Learned From This Lesson: DRII, NIST 800-34 Rev1, Business Organization Analysis

- BCP Frameworks
  - Standards help solve issues of inconsistency in terms, definitions, and documents (within the organization)
  - The following institutes will provide guidance on BCP/DRP:
    - DRII (Disaster Recovery Institute International)
    - NIST 800-34 Rev 1
    - ISO 27031
    - BCI GPG (Business Continuity International Good Practice Guidelines)
    - ISC2.org Four Processes of Business Continuity
- Step 1: Project Scope and Planning
  - Acquire BCP Policy Statement from Senior Management
  - Business Organization Analysis: Structured analysis of the business organizational assets **FIRST**
  - BCP Team Creation, including Project Manager, should be cross-functional team, including representation from Senior Management
  - An assessment of the resources available and commitment to support the BCP Process from Senior Management
  - An analysis of the legal and regulatory landscape that governs an organization's response to a catastrophic event

Lesson 5.9: BCP Intro

Skills Learned From This Lesson: BCP, DRP, Disruption Categories

- BCP vs. DRP
  - Business Continuity Planning: Focuses on sustaining operations and protecting the viability of the business following a disaster, until normal business conditions

can be restored. The BCP is an “umbrella” term that includes many other plans including the DRP. Long-term focused
    - Disaster Recovery Planning: Goal is to minimize the effects of a disaster and to take the necessary steps to ensure that the resources, personnel, and business processes are able to resume operations in a timely manner. Deals with the immediate aftermath of the disaster and is often IT focused. Short-term focused
- BCP Relationship to Risk Management
    - Identify Assets
    - Identify Threats/Vulnerabilities
    - Identify Impact
    - Identify Cost-effective Mitigating Strategy
    - BCP is the safety net under Risk Management
- Categories of Disruptions
    - Non-disaster: Inconvenience (hard drive failure)
        - Disruption of service
        - Device malfunction
    - Emergency/Crisis
        - Urgency, immediate event where there is the potential for loss of life or property
    - Disaster
        - Entire facility unusable for a day or longer
    - Catastrophe
        - Destroys facility
    - A company should understand and be prepared for each category
    - ANYONE CAN DECLARE AN EMERGENCY, ONLY THE BCP COORDINATOR CAN DECLARE A DISASTER (Anyone can pull the fire alarm or trigger an emergency alarm. Only the BCP coordinator or someone specified in the BCP can declare a disaster which will then trigger failover to another facility)

Lesson 5.10: BCP Step 1

Skills Learned From This Lesson: Business Organizational Analysis, BCP Team Selection, BCP Resource Needs, BCP Regulations

- Step 1: Project Scope and Planning: Business Organizational Analysis

    - Business Organizational Analysis provides:
        - The groundwork necessary to help identify potential members of the BCP team
        - Second, it provides the foundation for the remainder of the BCP processes
    - Evaluates considerations such as:
        - Operational departments that are responsible for the core services
        - Critical support services
        - Senior executives and other key individuals essential for the ongoing viability of the organization
- Step 1: Project Scope and Planning: BCP Team Selection
    - Representatives from each of the organization's departments responsible for the core services performed by the business
    - Representatives from the key support departments identified by the organizational analysis
    - IT representatives with technical expertise in areas covered by the BCP
    - Security representatives with knowledge of the BCP process
    - Legal representatives familiar with corporate legal, regulatory, and contractual responsibilities
    - Representatives from senior management
- Step 1: Project Scope and Planning: BCP Assess Resource Needs
    - **BCP Development**: The BCP team will require some resources to perform the four elements of the BCP process (project scope and planning, business impact assessment, continuity planning, and approval and implementation). It's more than likely that the major resource consumed by this BCP phase will be effort expended by members of the BCP team and the support staff they call on to assist in the development of the plan.
    - **BCP Testing, Training, and Maintenance**: The testing, training, and maintenance phases of BCP will require some hardware and software commitments, but once again, the major commitment in this phase will be effort on the part of the employees involved in those activities
    - **BCP Implementation**: When a disaster strikes and the BCP team deems it necessary to conduct a full-scale implementation of the business continuity plan, this implementation will require significant resources. This includes a large

amount of effort (BCP will likely become the focus of a large part, if not all, of the organization) and the utilization of hard resources. For this reason, it's important that the team uses its BCP implementation powers judiciously yet decisively.

- Step 1: Project Scope and Planning: Legal and Regulatory Compliance
    - Senior management has the ultimate legal responsibility. They may be:
        - Held responsible and liable under various laws and regulations
        - Sued by their stockholders if not managing with due diligence and due care
        - Sued by employees or families in the event of injury or loss of life
- BCP Regulation Examples:
    - HIPAA (Health Information Portability and Accountability Act)
    - FISMA (Federal Information Security Act)
    - FFIEC (Federal Financial Institutions Examination Council)

Lesson 5.11: Step 2 Business Impact Analysis

Skills Learned From This Lesson: BIA, Criticality, Service Level Objectives, Recovery Priorities

- Step 2: Phases of the Plan: Business Impact Analysis
    - BIA (Business Impact Analysis)
        - Initiated by the BCP Committee
        - Identifies and prioritizes all business processes based on criticality
        - Addresses the impact on the organization in the event of a loss of a specific service or process
            - Quantitative: Loss of revenue, loss of capital, los due to liabilities, penalties, and fines, etc.
            - Qualitative: Loss of service quality, competitive advantage, market share, reputation, etc.
        - Establishes key metrics for use in determining appropriate countermeasures and recovery strategy
        - IMPORTANCE (relevance) vs. CRITICALITY (downtime)
            - The Auditing Department is certainly important, though not usually critical
            - THE BIA FOCUSES ON CRITICALITY
        - Key Metrics to Establish

        - Service Level Objectives:
            - RPO (Recovery Point Objective): how much data we are willing to lose
            - MTD (Maximum Tolerable Downtime): the longest we can be without a process before we suffer a loss that is unacceptable to senior management
                - RTO (Recovery Time Objective)
                - WRT (Work Recovery Time)
            - MTBF (Mean Time Between Failures)
            - MTTR (Mean Time To Repair)
            - MOR (Minimum Operating Requirements)
    - Management should establish recovery priorities for business processes that identify:
        - Essential personnel
            - Succession Plans
            - Memorandums of Agreement/Understanding (MOAs/MOUs)
        - Technologies
        - Facilities
        - Communications systems
        - Vital records and data
- Results From the BIA
    - Results from the Business Impact Analysis contain:
        - Identified ALL business processes and assets, not just those considered critical
            - Impact company can handle dealing with each risk
            - Outage time that would be critical vs. those which would not be critical
            - Preventive Controls
    - Document and present to management for approval
    - Results are used to create the recovery plans

Lesson 5.12: BCP Step 3

Skills Learned From This Lesson: Continuity Planning, Recovery sites, Infrastructure

- Step 3: Continuity Planning
    - Step 3: Continuity Planning: Strategy Development
        - Examines the BIA for metrics and maps controls to meet the objectives
        - Determine appropriate responses:
            - Reduce
            - Assign/Transfer
            - Accept
            - Reject
        - Some risks will have to be accepted (based on cost/benefit) while others require a more active strategy
    - Step 3: Continuity Planning: Provisions and Processes
        - BCP designs the specific procedures necessary to mitigate the risks to a level that is acceptable to senior management
        - Three assets:
            - People-first priority always
            - Buildings/Facilities
                - Hardening Provisions-mitigating harm to the facility
                - Alternate Sites
                - Leased Sites
                    - Cold
                    - Warm
                    - Hot
            - Infrastructure
                - Redundancy of Critical Systems and Services
                - Recovery Strategies
                - Failover/Failback
    - Step 3: Continuity Planning: Facility Recovery
        - Dedicated site owned or operated by the organization
        - Reciprocal agreement or memorandum of agreement with an internal or external entity
        - Commercially leased facility
            - Hot: has your equipment and you do a restore of the most recent backups (outage measured in hours/minutes)

        - Warm (most popular): have some equipment including furniture, bare bones infrastructure, phones, computer systems, Internet access (outage measured in days/hours)
        - Cold: building with plumbing and electricity (outage measured in weeks). Inexpensive but takes a while to transition over.
    - MOAs or SLAs should be obtained from the provider
- Step 3: Continuity Planning: Infrastructure
    - Infrastructure supports the critical elements of the business. Servers, systems, routers, switches, processes, architecture
    - High Availability
        - Redundancy (clustering, RAID, backups)
        - Resiliency
        - Fault Tolerance
    - Hardened Systems

Lesson 5.13: Step 4

Skills Learned From This Lesson: BCP Plan Approval, BCP Plan Implementation, BCP Training and Education

- Step 4: Plan Approval and Implementation
    - Plan Approval
        - If possible, CEO should endorse plan
        - Otherwise another senior officer
        - Indicates dedication of the business to the process of business continuity planning
    - Plan Implementation
        - Create Implementation guide/schedule
        - Deploy resources
        - Supervise maintenance of plan
    - Training and Education
        - Distribute plan on need to know basis
        - Everyone should get at least an overview

Lesson 5.14: BCP Roles and Responsibilities

Skills Learned From This Lesson: BCP Roles/Responsibilities, BCP Team Development

- Roles and Responsibilities
    - Senior Executive Management
        - Consistent support and final approval of plans
        - Setting the business continuity policy
        - Prioritizing critical business functions
        - Allocating sufficient resources and personnel
        - Providing oversight for and approving the BCP
        - Directing and reviewing test results
        - Ensuring maintenance of a current plan
    - Senior Functional Management
        - Develop and document maintenance and testing strategy
        - Identify and prioritize mission-critical systems
        - Monitor progress of plan development and execution
        - Ensure periodic tests
        - Create the various teams necessary to execute the plans
    - BCP Steering Committee
        - Conduct the BIA
        - Coordinate with department representatives
        - Develop analysis group
            - Plan must be developed by those who will carry it out
            - Representatives from critical departments
    - BCP Teams
        - Rescue: Responsible for dealing with the immediacy of disaster-employee evacuation, “crashing” the server room, etc.
        - Recovery: Responsible for getting the alternate facility up and running and restoring the most critical services first
        - Salvage: Responsible for the return of operations to the original or permanent facility (reconstitution = restore least critical services first)
    - Developing the Teams

- Management should appoint members
- Each member must understand the goals of the plan and be familiar with the department they are responsible for
- Agreed upon prior to the event:
  - Who will talk to the media, customers, shareholders
  - Who will set up alternative communication methods
  - Who will set up the offsite facility
  - Established agreements with off-site facilities should be in place
  - Who will work on the primary facility

Lesson 5.15: BCP Sub-plans

Skills Learned From This Lesson: Crisis Communication Plan, Occupant Emergency Plan, Business Recovery Plan, IT Contingency Plan, Incident Response Plan, Disaster Recovery Plan, Continuity of Operations Plan

- Business Continuity Plan Sub-Plans
  - Sub-plans of BCP have 3 main purposes:
    - Protect
      - Crisis Communication Plan
        - Purpose: Provides procedures for disseminating **status reports to personnel and the public**
          Scope: Addresses communications with personnel and the public; not IT focused
      - Occupant Emergency Plan (OEP)
        - Purpose: Provide coordinated procedures for **minimizing loss of life or injury and protecting property damage** in response to a physical threat
        - Scope: Focuses on **personnel and property** particular to the specific facility; not business process or IT system functionality based. May also be referred to as **Crisis or Incident Management** plans. However, the OEP concept should be recognizable as the "**initial response to the emergency event**"
    - Recover

- Business Recovery or Resumption Plan (BRP)
  - Purpose: Provide procedures for recovering business operations immediately following a disaster
  - Scope: Addresses business processes; not IT-focused; IT-addressed based only on its support for business processes
- Continuity of Support Plan/IT Contingency Plan
  - Purpose: Provide procedures and capabilities for recovering a major application or general support system
- Cyber Incident Response Plan
  - Purpose: Provide strategies to detect, respond to, and limit consequences of malicious cyber incident
  - Scope: Focuses on information security responses to incidents affecting systems and/or networks
- Disaster Recovery Plan (DRP)
  - Purpose: Provide detailed procedures to facilitate recovery of capabilities at an alternate site
  - Scope: Often IT-focused; limited to major disruptions with long-term effects

- Sustain
  - Continuity of Operations Plan (COOP)
    - Purpose: Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days. This term is sometimes used in US Government to refer to the field of Business Continuity Management, but per NIST 800-34, it is a unique sub-plan of the BCP **Note: BCP addresses ALL business processes, not just mission critical**
    - Scope: Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused

Lesson 5.16: Testing the Plan

Skills Learned From This Lesson: Checklist Test, Structured Walk-through, Simulation Test, Parallel Test, Full-Interruption Test

- Types of Tests
    - Checklist Test
        - Copies of plan distributed to different departments
        - Functional mangers review
    - Structured Walk-Through (Table Top) Test
        - Representatives from each department go over the plan
    - Simulation Test
        - Going through a disaster scenario
        - Continues up to the actual relocation to an offsite facility
    - Parallel Test
        - Systems moved to alternate site, and processing takes place there
    - Full-Interruption Test
        - Original site shut down
        - All of processing move to offsite facility