**Lesson 1 – Risk Management Fundamentals:**

* Risk: The likelihood that a loss will occur.
* Threat: Any activity that represents a possible danger.
* Vulnerability: A weakness.
* Loss: Occurs when a threat exposes a vulnerability; results in a compromise to business functions or assets; either tangible or intangible
* Importance of Risk Management:
  + Identifies threats and vulnerabilities
  + Reduces adverse impact
  + Improves organization survivability
  + Enhances cost-benefit awareness
  + Shows the need for risk reduction
* Risk-Related Concerns for Business:
  + Compromise of business functions
  + Compromise of business assets
  + Driver of business costs
  + Profitability versus survivability
* Seven Domains of a Typical IT Infrastructure:
  + User Domain
  + Workstation Domain
  + LAN Domain
  + LAN-to-WAN Domain
  + Remote Access Domain
  + WAN Domain
  + System/Application Domain
* Confidentiality: Prevents unauthorized disclosure of systems and information.
* Integrity: Prevents unauthorized modification of systems and information.
* Availability: Prevents disruption of service and productivity.
* Risk Management Control Objectives:
  + Red: Immediate action should be taken to reduce the risk.
  + Orange: Actions should be planned and initiated to reduce the risk.
  + Yellow: Should be monitored and prepared to respond if they are realized.
  + Green: No specific actions need to be taken.
* Total Risk: Threats, Vulnerability, & Asset Value
* Residual Risk: Total Risk – Countermeasures
* Risk Management Elements/Process:
  + Assess risks
  + Identify risks to manage
  + Select controls
  + Implement and test controls
  + Evaluate controls
* Survivability and Balancing Risk and Cost:
  + Consider the cost to implement a control and the cost of not implementing the control.
  + Spending money to manage a risk rarely adds profit; important point is that spending money on risk management can help ensure a business’s survivability.
  + Cost to manage a risk must be balanced against the impact value.
* Role-based Perceptions of Risk:
  + Management
  + System Administrator
  + Tier 1 Administrator
  + Developer
  + End User
* Risk Identification Process:
  + Identify threats
  + Identify vulnerabilities
  + Estimate the likelihood of a threat exploiting a vulnerability
* Risk Identification Elements:
  + Threats:
    - External or internal
    - Natural or man-made
    - Intentional or accidental
  + Vulnerabilities:
    - Audit
    - Certification/accreditation records
    - System logs
    - Prior event
    - Trouble reports
    - Incident response teams
* Techniques of Risk Management:
  + Avoidance
  + Mitigation
  + Transfer
  + Acceptance
* Aspects of Risk Management:
  + Residual Risk
  + Cost-Benefit Analysis

**Lesson 2 – Threats, Vulnerabilities, and Exploits:**

* Threats can’t be eliminated.
* Threats are always present.
* You can take action to reduce the potential for a threat to occur.
* You can take action to reduce the impact of a threat.
* You cannot affect the threat itself.
* Unintentional Threats:
  + Environmental (Ex: Fire, wind, lightning, flooding)
  + Accidents/Human (Ex: Keystroke errors, political changes, programming bugs, accidents in general)
  + Failures (Ex: Equipment)
* Intentional Threats:
  + Profit
  + Passion
  + Psychosis
  + Individuals or Organizations:
    - Hackers
    - Criminals
    - Disgruntled Employees
* Common Attackers:
  + Criminals
  + Advanced Persistent Threats (APTs)
  + Vandals
  + Saboteurs
  + Disgruntled Employees
  + Activists
  + Other Nations
  + Hackers
* Best Practices for Managing Threats:
  + Create a security policy
  + Purchase insurance
  + Use access controls
  + Use automation
  + Include input validation
  + Provide training
  + Use antivirus software
  + Protect the boundary
* Understanding and Managing Vulnerabilities: Countermeasures reduce risk and loss; they also reduce vulnerabilities and impact of loss
* Threat/Vulnerability Pair:
  + Occurs when a threat exploits a vulnerability.
  + A vulnerability provides a path for the threat that results in a harmful event or a loss.
  + Both the threat and the vulnerability must come together to result in a loss.
  + Ex:
    - Threat: Ex-employee
    - Vulnerability: Ex-employee who still has access to the system
    - Threat Action: Accessing proprietary data
  + Ex:
    - Threat: Fire or negligent person
    - Vulnerability: Sprinklers used to suppress fire damage
    - Threat Action: Sprinkler system turned on
  + Ex:
    - Threat: Unauthorized users (e.g., hackers)
    - Vulnerability: Identified flaws in system design; new patches not applied
    - Threat Action: Unauthorized access to files
* Vulnerability Mitigation Techniques:
  + Policies and procedures
  + Documentation
  + Training
  + Separation of duties
  + Configuration management
  + Patch management
  + Intrusion detection
  + Incident response
  + Continuous monitoring
  + Technical controls
  + Physical controls
* Best Practices for Managing Vulnerabilities:
  + Identify vulnerabilities
  + Match the threat/vulnerability pairs
  + Use as many of the mitigation techniques as feasible
  + Perform vulnerability assessments
* Understanding and Managing Exploits:
  + Exploit: The act of taking advantage of a vulnerability.
    - Executes a command or program against an IT system to take advantage of a weakness.
    - Results in a compromise to the system, an application, or data.
  + Attacks executed by code primarily affect public-facing servers:
    - Web servers
    - Simple Mail Transfer Protocol (SMTP) e-mail servers
    - File Transfer Protocol (FTP) servers
* Exploits:
  + Attack public-facing servers
    - Buffer Overflow
    - SQL Injection
    - DoS Attack
    - DDoS Attack
* Risk Mitigation Techniques for Protecting Public-Facing Servers:
  + Remove or change defaults
  + Reduce the attack surface
  + Keep systems up to date
  + Enable firewalls
  + Enable intrusion detection systems (IDSs)
  + Enable intrusion prevention systems (IPSs)
  + Install antivirus software
* Best Practices for Managing Exploits:
  + Harden servers
  + Use configuration management
  + Perform risk assessments
  + Perform vulnerability assessments
* U.S. Government Risk Management Initiatives:
  + The National Institute of Standards and Technology (NIST)
  + The Department of Homeland Security
  + The National Cybersecurity and Communications Integration Center (NCCIC)
  + U.S. Computer Emergency Readiness Team (US-CERT)
  + The MITRE Corporation – Common Vulnerabilities Exposure (CVE) List

**Lesson 3 – Maintaining Compliance:**

* Covered Entity & Business Associates:
  + Covered Entity: Anyone who provides treatment, payment and operations in healthcare
  + Business Associate: Vendor or subcontractor who has access to PHI.
  + This definition creates an Extended Enterprise perspective as discussed earlier.
* U.S. Compliance Laws:
  + Health Insurance Portability and Accountability Act (HIPAA): Passed in 1996, and among other things, outlines the requirements for the management of, storage and transmission of protected health information (PHI) in both physical and digital form.
    - In 2013, the Final Omnibus Rule Update was passed that amended HIPAA and greatly expanded the definition of who needed to be HIPAA compliant. Now, all entities (Business Associates) that store, manage, record or pass Protected Health Information (PHI) to and from covered entities are also required to be HIPAA compliant.
    - PHI: Any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health service.
    - Four Rules: Security, Privacy, Enforcement, and Breach rules
      * Security: Standards for the security of electronic protected health information (Limits Scope compared to Privacy Rule). It defines administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.
    - Implications of Non-Compliance:
      * Hospitals, private practices, health insurance companies, and companies that do not comply with HIPAA face:
        + Financial penalties for each violation
        + Criminal charges for failure to protect patients
  + Federal Information Security Management Act (FISMA)
  + Gramm-Leach-Bliley Act (GLBA)
  + Sarbanes-Oxley Act (SOX)
  + Family Educational Rights and Privacy Act (FERPA)
  + Children’s Internet Protection Act (CIPA)
* U.S. Compliance Laws and their Applicability:
  + FISMA: Federal agencies
  + HIPAA: Any organization handling medical data
  + GLBA: Banks, brokerage companies, and insurance companies
  + FERPA: Education institutions
  + CIPA: Schools and libraries using E-Rate discounts
* U.S. Compliance Regulatory Agencies:
  + Office for Civil Rights (OCR) – HIPAA – DHHS
  + Federal Deposit Insurance Corporation (FDIC)
  + Department of Homeland Security (DHS)
  + State Attorney General (AG)
  + U.S. Attorney General (U.S. AG)
* Organizational Policies for Compliance – Fiduciary Responsibility:
  + Fiduciary: Refers to a relationship of trust; could be a person who is trusted to hold someone else’s assets.
  + Trusted person has the responsibility to act in the other person’s best interests and avoid conflicts of interest.
  + Examples of Trust Relationships:
    - An attorney and a client
    - A CEO and a board of directors
    - Shareholders and a board of directors
  + Fiduciary is expected to take extra steps (due diligence and due care)
* PCI DSS Compliance:
  + Created by Payment Card Industry Security Standards Council
  + American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
  + Modernized by the Security Standards Council
  + Effort to obstruct and prevent further theft of personal information
* PCI DSS Standards:
  + Use of personal identification numbers (PIN)
  + Installation of software used to store, process, and/or transmit cardholder data
  + PCI DSS standards serve as PCI DSS goals
  + Merchants who store, process, and/or transmit cardholder data must comply
  + Merchants should establish processes that work toward PCI DSS goals
* Goals and Process Steps to PCI DSS:
  + Goal: Build and maintain a secure network that is PCI compliant
  + Process Steps:
    - Install a firewall system
    - Perform testing when configurations change
    - Identify all connections to cardholder information
    - Review configuration rules every six months
    - Change all default passwords
  + Goal: Protect cardholder data
  + Process Steps:
    - Display the maximum of the first six and last four digits of the primary account number
    - Encrypt all online information
  + Goal: Maintain a vulnerability management program
  + Process Steps:
    - Install anti-virus software
    - Install vendor-provided security patches
  + Goal: Implement strong access control measures
  + Process Steps:
    - Limit the accessibility of cardholder information
    - Assign an unreadable password
    - Monitor the physical access to cardholder data
    - Maintain a visitor log and save the log for at least three months
  + Goal: Regularly monitor and test networks
  + Process Steps:
    - Use a wireless analyzer to check for wireless access points
    - Scan internal and external networks
    - Install software to recognize any modification by unauthorized personnel
  + Goal: Maintain an information security policy
  + Process Steps:
    - Include annual and day-to-day security procedures and policies to recognize security breaches
    - Perform background checks on potential employees
    - Educate employees on compliance regulations
* PCI DSS Process:
  + Build and maintain a secure network that is PCI compliant
  + Protect cardholder data
  + Maintain a vulnerability management program
  + Implement strong access control measures
  + Regularly monitor and test networks
  + Maintain an information security policy
* Seven COBIT Enablers:
  + Principles, Policies, and Frameworks
  + Processes
  + Organizational Structures
  + Culture, Ethics, and Behavior
  + Information
  + Services, Infrastructure, and Applications
  + People, Skills, and Competencies
* Roles:
  + Senior Management
  + IT Management
  + Governance and Audit Departments (Legal, Accounting, IT)
  + IT Employees

**Lesson 4 – Developing a Risk Management Plan:**

* Objectives of a Risk Management Plan:
  + A register of assets & threats
  + A register of vulnerabilities
  + Costs associated with risks
  + A list of recommendations to reduce the risks
  + Costs associated with recommendations
  + A cost-benefit analysis
  + One or more reports
* Scope of Plan Dimensions:
  + Extent the plan will be organized
  + Level of implementation
  + Range of view and outlook
  + Degree of application and operation
  + Measurement of effectiveness
* Assignment of Responsibilities: Align resources, assign responsibilities, and evaluate relationships
* Describing Procedures and Schedules for Accomplishment:
  + Include a recommended solution for any threat or vulnerability, with a goal of mitigating the associated risk; the solution will often include multiple steps
  + Describe each step in detail; include a timeline for completion of each step
  + Remember:
    - Management is responsible for choosing the controls to implement.
    - Management is responsible for residual risk.
* Reporting Requirements:
  + Present recommendations
  + Document management response to recommendations
  + Document and track implementation of accepted recommendations
  + Create plan of action and milestones (POAM)
  + Report should include findings, recommendation cost and time frame, and cost-benefit analysis
  + Reports are often summarized in risk statements
    - Use risk statements to communicate a risk and the resulting impact
* Plan of Action and Milestones (POAM):
  + A document used to track progress.
  + Used to assign responsibility and to allow management follow-up
  + Is a living document
* Risk Management Functions:
  + Senior Management
  + IT Management
  + System and Information Owners
  + Functional Management
  + Information Security (IS) Management
  + Security Awareness Trainers

**Lesson 5 – Defining Risk Assessment Approaches:**

* What is Risk Assessment?:
  + Key step in a risk management process
  + Determination of quantitative or qualitative value of risk
  + Conducted for concrete situation and recognized threat
  + Used to help identify which safeguards (controls) to implement
  + Required for evaluating risk or control
  + Often conducted after implementation of a control
* Why is Risk Assessment Important?:
  + Identifies which systems/assets to protect
  + Gives insight into which controls provide the most value
* When Should a Risk Assessment Be Conducted?:
  + When evaluating risk
  + When evaluating a control
  + Periodically after a control has been implemented
* Critical Components of Risk Assessments:
  + Identify scope of assessment
  + Identify critical areas
  + Identify team
* Identify Potential Scope for Web Server RA:
  + Web Server
  + Database Server
  + Firewalls
  + DMZ
* Protecting Your Assets:
  + Hardware Assets
  + Software Assets
  + Personnel Assets
  + Data and Information Assets
* Quantitative Risk Assessments: Calculates absolute financial values, losses, and costs
  + Uses numbers such as dollar values
  + Results can help you:
    - Identify the priority of risks
    - Determine the effectiveness of controls
  + Key Terms:
    - Single Loss Expectancy (SLE)
    - Annual Rate of Occurrence (ARO)
    - Annual Loss Expectancy (ALE)
    - Safeguard Value
  + Benefits:
    - Becomes a simple math problem
    - Provides a cost-benefit analysis (CBA)
      * Accurate values for SLE, ARO, and safeguard value lets you calculate CBA
    - Management often familiar with quantitative assessment terminology; easy to grasp details of the assessment and its recommendations
    - Formulas use verifiable and objective measurements
  + Limitations:
    - Accurate data isn’t always available
      * Especially true when identifying ARO reductions
    - Ensuring that people use the control as expected
      * May need to take additional steps, such as training, to ensure users are aware of the importance of the control
* Qualitative Risk Assessments: Calculates relative values, losses, and costs
  + Subjective
  + Probability: The likelihood that a threat will exploit a vulnerability.
  + Impact: The negative result if a risk occurs.
  + Uses the opinions of experts
  + Is easy to complete
  + Uses words that are easy to express and understand
  + Limitations:
    - Subjective
    - Based on the expertise of the experts
      * Value of the assessment is only as valuable as the expertise of the experts
    - No CBA
    - No real standards
* Comparing Assessment Methods:
  + Quantitative:
    - Objective
    - Monetary values
    - Historical data
    - Key Terms: SLE, ARO, ALE
  + Qualitative:
    - Subjective
    - Word values
    - Expert opinions
    - Key Terms: Probability and impact
* Risk Assessment Challenges:
  + Using static process to evaluate a moving target
  + Availability
  + Data consistency
  + Estimating impact effects
  + Providing results that support resource allocation and risk acceptance
* Best Practices for Risk Assessment:
  + Start with clear goals and a defined scope
  + Enlist senior management support
  + Build a strong RA team
  + Repeat the RA regularly
  + Define a methodology to use
  + Provide a report of clear risks and clear recommendations

**Lesson 6 – Performing a Risk Assessment:**

* Steps Used in Risk Assessments:
  + Identify assets and activities to address
  + Identify and evaluate relevant threats
  + Identify and evaluate relevant vulnerabilities
  + Identify and evaluate relevant countermeasures
  + Assess threats, vulnerabilities, and exploits
  + Evaluate risks
  + Develop and present recommendations
* Prior to Conducting a Risk Assessment:
  + Define the Assessment:
    - Operational characteristics
    - Mission of the system
  + Review Previous Findings:
    - Recommendations
    - Current status of accepted recommendations
    - Unapproved recommendations
* Identifying the Management Structure:
  + Refers to how responsibilities are assigned
    - Helpful to keep the scope within the ownership of a single entity
  + Large organization may have multiple divisions:
    - Network infrastructure
    - User and computer management
    - E-mail servers / Web servers / Database servers
    - Configuration and change management
* Identifying Assets and Activities:
  + Perform asset valuation
    - Base on replacement or recovery value of the asset
    - Ensure RA performed on current systems
    - Evaluate only assets that are within the boundary of the RA
  + Prioritize importance
* Elements to Consider when Determining Asset Value:
  + System access and system availability
  + System functions
  + Hardware and software assets
  + Personnel assets
  + Data and information assets
  + Facilities and supplies
* Identifying and Evaluating Countermeasures:
  + In-Place Controls:
    - In place in the operational system
    - Supported by associated documentation
  + Planned Controls:
    - Identified in planning documents
    - Specified implementation date
  + Control Categories:
    - National Institute of Standards and Technology (NIST)
    - Three classes, 18 families of controls
    - Grouped as procedural, technical, and physical
* Control Classes:
  + Procedural:
    - Examples: Policies and procedures, security plans, insurance, and awareness and training
  + Technical:
    - Examples: Login identifier, system logs, and firewalls
  + Physical:
    - Examples: Locked doors, video cameras, and fire detection and suppression systems
* Developing Mitigating Recommendations:
  + After performing analysis, provide specific recommendations that mitigate risks
  + Supporting data may include:
    - Threat/vulnerability pairs
    - Estimate of cost and time to implement
    - Estimate of operational impact
    - Cost-benefit analysis
* Best Practices for Performing Risk Assessments:
  + Ensure systems are fully described
  + Review past audits
  + Review past risk assessments
  + Match the RA to the management structure
  + Identify assets within the RA boundaries
  + Identify and evaluate relevant threats
  + Identify and evaluate relevant vulnerabilities
  + Identify and evaluate countermeasures
  + Track the results