**Lesson 7 – Managing Risk in Information Systems:**

* System Availability: We want 99.99% up-time; to do this we will need to eliminate single points of failure (SPOF)
  + Single Point of Failure (SPOF): Part of a system that can cause entire system to fail; if SPOF fails, the entire system fails.
* System Functions:
  + Manual: Written records; knowledge of process.
  + Automated: System records; little to no knowledge of process.
* Hardware Assets:
  + Computers: Servers, desktop PCs
  + Networking Devices: Routers, switches
  + Network Appliances: Firewalls, spam appliances
  + Information Necessary to Know: Location, manufacturer, model #, hardware components (such as processor and Random Access Memory (RAM)), hardware peripherals (such as add-on network interface cards (NICs)), and Basic Input/Output System (BIOS) version.
* Software Assets:
  + Operating system and applications
  + OS Specifics Should Include: Hardware system where it’s installed, name of the operating system & the latest service pack installed
  + Application Specifics Should Include: Name of the application, version number & a service pack or update information if available
* Personnel Assets:
  + The people working for you; when any function or process depends on a single person, he/she becomes a single point of failure
  + Reduce Risk By: Hiring additional personnel, cross-training & rotating jobs
* Data & Information Assets:
  + Data is protected by access controls and backups
  + Identifying Data Assets: Protect data & ensure methods are available to retrieve data (data warehousing, data mining, etc.)
  + Role of Data in Organization: Value of data often overlooked; classifying is an important step
    - Without classifications…
      * Users may not recognize the value; users may not protect; IT may not backup as often as needed
* Asset & Inventory Management Within the Seven Domains of a Typical IT Infrastructure:
  + Inventory Management: Used to manage hardware inventories
  + Asset Management: Used to manage all types of assets; much more detailed data than an inventory management system
  + Seven Domains of a Typical IT Infrastructure: User domain, workstation domain, LAN domain, LAN-to-WAN domain, WAN domain, remote access domain & system/application domain.
* Identifying Facilities & Supplies Needed to Maintain Business Operations:
  + Identifying mission-critical systems and applications
  + Business impact analysis planning
  + Business continuity planning
  + Disaster recovery planning
  + Business liability insurance planning
  + Asset replacement insurance planning
* BIA Planning Introduction: Identifies impact of sudden loss
  + Define the scope -> identify objectives -> identify mission-critical functions and processes -> map functions and processes to IT systems
  + Identify Assets: First step in risk management; you can’t plan the protection if you don’t know what you’re protecting
    - When do you want to identify a single point of failure? Before it fails or after it fails?
  + Identify Valuable Assets: Ask a system owner how much downtime or data loss they can accept? The answer is usually “none”
    - Then ask: “How much money are you willing to spend?”

**Lesson 8 – Identifying and Analyzing Threats, Vulnerabilities, and Exploits:**

* Threat Assessments: Identifies and evaluates threats
  + Determines impact on confidentiality, integrity & availability
  + Risk = Threat \* Vulnerability:
    - Threat Assessments: Help reduce impact of threats
    - Vulnerability Assessments: Help reduce vulnerabilities
    - Exploit Assessments: Help validate actual threats and vulnerabilities
  + Techniques for Identifying Threats: Reviewing historical data, performing threat modeling, and analogy & comparison with similar situations and activities
  + Internal Threats: Users with unintentional access, users responding to phishing attempts, users forwarding viruses, disgruntled ex-employees, equipment failure, data loss & attacks
  + External Threats: Attacks on public-facing servers, weather conditions and natural disasters
  + Threat Modeling: What system are you trying to protect? Is the system susceptible to attacks? Who are the potential adversaries? How might a potential adversary attack? Is the system susceptible to hardware or software failure? Who are the users? How might an internal user misuse the system?
  + Best Practices for Threat Assessments: Assume nothing, recognizing that things change. Verify that systems operate and are controlled as expected. Limit the scope of the assessment to a single domain at a time. Use documentation and flow diagrams to understand the system you’re evaluating. Identify all possible entry points for the domain you’re evaluating. Consider threats to confidentiality, integrity, and availability. Consider internal and external human threats. Consider natural threats.
* Vulnerability Assessments: Vulnerabilities are any weaknesses in an IT infrastructure.
  + Assessments Identify Vulnerabilities Within an Organization: Servers, Networks & Personnel
  + Entire networks can be vulnerable if access controls aren’t implemented
  + Internal Assessments: Security professionals exploit internal systems to learn about vulnerabilities
  + External Assessments: Personnel outside the company exploit systems to learn about vulnerabilities.
  + Assessing Vulnerabilities: Documentation review, review logs, vulnerability scans, audits and personnel interviews, process and output analysis & system testing
  + Documentation Review:
    - Incidents: Review incident documentation; cause of an incident directly related to a vulnerability.
    - Outage Reports: Investigate outages that affect mission of business; if outage affected bottom line, you can probably identify a vulnerability.
    - Assessment Reports: Review past assessment reports; helps identify common problems and problems that have not been corrected.
  + Intrusion Detection System Outputs: IDS uses logs; logs can be used in assessments
  + Vulnerability Scans & Other Assessment Tools: Identify vulnerabilities -> scan systems and network -> provide metrics -> document results.
  + Audits & Personnel Interviews:
    - Audits performed to check compliance with rules and guidelines
    - VA audits check compliance with internal policies; checks to see if an organization is following the policies that are in place
    - Audits Can Be: Manual, automated, scripted & personnel interviews
  + Process Analysis & Output Analysis:
    - Firewall has five rules – use process analysis
    - Firewall has 100 rules – use output analysis
  + System Testing:
    - Functionality Testing: Defining requirements
    - Access Controls: Verifying user rights and allocations
    - Penetration Testing: Verifying security countermeasures
    - Tests transactions with applications
  + Verifying Rights & Permissions: Verify user rights and permissions; principle of least privilege.
  + Best Practices for Vulnerability Assessments: Identify assets -> ensure scanners are kept up to date -> perform internal and external checks -> document the results -> provide reports.
* Exploit Assessments:
  + Exploit assessments attempt to exploit vulnerabilities; they simulate an attack to determine if the attack can succeed
  + An Exploit Test:
    - Usually starts with a vulnerability test to determine vulnerabilities
    - Follows with an attempt to exploit the vulnerability
  + Identifying Exploits:
    - Vulnerability Test: Perform a vulnerability test to determine vulnerabilities.
    - Seven Domains: Look at all seven domains of a typical IT infrastructure.
  + Common Exploits: Social engineering, MAC flood attack, TCP SYN flood attack (a common DoS attack), etc.
  + Mitigating Exploits with a Gap Analysis & Remediation Plan:
    - An Exploit Assessment Identifies: Exploits that are mitigated & exploits that are not mitigated
    - Difference represents a gap in security
    - Gap analysis report documents differences
    - Remediation plan often included with gap analysis
  + Implementing Configuration or Change Management:
    - Both help prevent or remediate exploits
    - Configuration Management: Use standards to ensure that systems are configured similarly
    - Change Management: A process that controls changes to systems
  + Verifying & Validating the Exploit Has Been Mitigated:
    - Verify that the exploit has been mitigated in the same way you identified it originally; run a vulnerability scan again & repeat the audit related to the exploit
  + Best Practices for Exploit Assessments:
    - Get permission first; without permission, you are the attacker
    - Identify as many exploits as possible
    - Use a gap analysis for legal compliance
    - Verify that exploits have been mitigated

**Lesson 9 – Identifying and Analyzing Risk Mitigation Security Controls:**

* In-Place Controls:
  + Installed in an operational system
  + Replace in-place controls that don’t meet goals
  + Three Primary Objectives of Controls: Prevent, recover & detect
* Planned Controls:
  + Those that have been approved but not yet installed
  + Identify planned controls before approving others
  + Vulnerabilities that planned controls mitigate still exist
  + Evaluate effectiveness of a planned control through research
* NIST SP 800-53 Control Families:
  + Access Control (AC)
  + Audit and Accountability (AU)
  + Awareness and Training (AT)
  + Configuration Management (CM)
  + Contingency Planning (CP)
  + Identification and Authentication (IA)
  + Incident Response (IR)
  + Maintenance (MA)
  + Media Protection (MP)
  + Personnel Security (PS)
  + Physical and Environment Protection (PE)
  + Planning (PL)
  + Program Management (PM)
  + Risk Assessment (RA)
  + Security Assessment and Authorization (CA)
  + System and Communications Protection (SC)
  + System and Information Integrity (SI)
  + System and Services Acquisition (SA)
* Functional Controls: Controls based on function being performed
  + Preventive: Hardening, patching
  + Detective: Audit trails, IDS
  + Corrective: Backups, file recovery
* Procedural Control Examples: Policies and procedures, security plans, insurance and bonding, background and financial checks, data loss prevention program, awareness training, rules of behavior & software testing
* Technical Control Examples: Login identifier, session timeout, system logs and audit trails, data range and reasonableness checks, firewalls and routers, encryption and public key infrastructure (PKI)
* Firewalls & Routers: Filters traffic – access control lists (ACLs)
* Using Digital Signatures:
  + Creating Digital Signatures: Message hashed (77), hash encrypted with sender’s private key, and the digital signature is included with the message.
  + Validating Digital Signatures: The hash is decrypted with sender’s public key; if decryption is successful, it must have been encrypted with private key.
* Physical Control Examples: Locked doors, guards, CCTV, fire detection and suppression, water detection HVAC (temperature and humidity detection/control) & electrical grounding and circuit breakers

**Lesson 10 – Planning Risk Mitigation Throughout Your Organization:**

* Where Should Your Organization Start with Risk Mitigation?:
  + Identify Assets: High, medium & low
  + Identify and analyze threats and vulnerabilities
  + Evaluate the controls to determine what controls to implement
* Scope of Risk Management: Critical business operations, customer service delivery, mission-critical business systems, applications, and data access, seven domains of a typical IT infrastructure & information systems security gap
* Identifying CBFs: Making a purchase, receiving funds & shipping products
* Understanding/Assessing Impact of Legal and Compliance Issues:
  + Compliance is a mitigation control
  + Assessing the Impact of Compliance Issues: Identify what compliance issues apply to organization & assess impact of issues on business operations
* Legal Requirements, Compliance Laws, Regulations, and Mandates:
  + Health Insurance Portability and Accountability Act (HIPAA)
  + Sarbanes-Oxley Act (SOX)
  + Federal Information Security Management Act (FISMA)
  + Family Educational Rights and Privacy Act (FERPA)
  + Children’s Internet Protection Act (CIPA)
  + Payment Card Industry Data Security Standard (PCI DSS)
  + Compliance Issues: CIPA requires a TPM; other laws may require other controls
* Assessing How Security Countermeasures/Safeguards Can Assist with Risk Mitigation:
  + Controls are implemented at a point in time to reduce the risks at that time
  + A Control Will Attempt to Mitigate Risk by: Reducing the impact of threats to an acceptable level & reducing a vulnerability to an acceptable level
  + Risk assessment (RA) is a point-in-time assessment
* Identifying Risk Mitigation and Risk Reduction Elements: Account management controls, access controls, physical access, personnel policies, security awareness and training
* Performing a Cost-Benefit Analysis:
  + Compare cost of control to cost of risk if it occurs
  + Calculating Projected Benefits: loss before control – loss after control = projected benefits
  + Determining if Control Should be Used: projected benefits – cost of control = control value
* Risk Mitigation Best Practices:
  + Review Historical Documentation: Although risks change, many of the threats and vulnerabilities will be the same
  + Include Both a Narrow and Broad Focus: Identify specific risks and mitigation strategies and broaden the focus to include the entire organization
  + Ensure That Governing Laws are Identified: If you don’t know what laws apply, you won’t be in compliance.
  + Redo RAs When a Control Changes: If a control changes, the original RA is no longer valid
  + Include a Cost-Benefit Analysis: CBAs provide justification for controls and help determine their value

**Lesson 11 – Turning Your Risk Assessment into a Risk Mitigation Plan:**

* Creating a Risk Mitigation Plan: Complete a risk assessment, identify costs, perform a cost-benefit analysis (CBA) & implement a plan
  + High-Level Review of Risk Assessment: Identify and evaluate relevant threats, identify and evaluate relevant vulnerabilities, identify and evaluate countermeasures & develop mitigating recommendations
* Reviewing Risk Assessment Countermeasures:
  + In-Place Countermeasures
  + Planned Countermeasures
  + Approved Countermeasures
  + Overlapping Countermeasures
* Calculating Costs: Initial purchase, facility, installation, training, etc.
  + Look for hidden costs
  + Is extra power required to eliminate a single point of failure?
* Time to Implement: Simple configurations can be implemented in a shorter time period; complex configurations require more planning and time
* Operational Impact:
  + Tradeoff with Security: The more secure a system, the harder it is to use; the easier it is to use, the less secure it is.
  + Firewall implicit deny philosophy
* Prioritizing Risk Elements:
  + Threat/Vulnerability Matrix: Determine likelihood and impact
  + Prioritize countermeasures
* Performing a Cost-Benefit Analysis:
  + Identify losses you expect before, or without, a countermeasure
  + Identify the losses you expect after implementing the countermeasure
  + Calculating Projected Benefits: Loss before countermeasure – loss after countermeasure = projected benefits
  + Determining Value of Countermeasure: Projected benefits – cost of countermeasure = countermeasure value
* CBA Report Elements: Recommended countermeasure, risk to be mitigated, annual projected benefits, initial costs, annual or recurring costs, a comparison of the costs and benefits & a recommendation
* Implementing a Risk Mitigation Plan:
  + Stay Within Budget: Ensure costs calculated accurately
  + Stay on Schedule: Use tools to manage project
* Monitoring Implementation: Use project management tools
* Implementation Challenges: Scope and cost overruns; stay within budget and on schedule
  + Ineffective Countermeasures: Ensure countermeasures work as expected
* Following Up on the Risk Mitigation Plan: Ensure countermeasures are implemented (POAM); ensure security gaps have been closed.
* Risk Management Best Practices:
  + Stay Within Scope: Should not go outside the scope of the RA
  + Redo CBAs if New Costs are Identified: Ensure data is accurate
  + Prioritize Countermeasures: Prioritize based on importance
  + Include current countermeasures in analysis; when scoring countermeasures, ensure that current countermeasures are considered
  + Control Costs and Schedule: Costs should stay within the allocated budget
  + Follow Up: Implement approved countermeasures; ensure countermeasures mitigate the risk.

**Lesson 12 – Mitigating Risk with a Business Impact Analysis:**

* What is a Business Impact Analysis?:
  + A study used to identify the impact that can result from disruptions in the business
  + Focuses on the failure of one or more critical IT functions
  + Terms:
    - **Maximum Acceptable Outage (MAO)**
    - **Critical Business Functions (CBFs)**
    - **Critical Success Factors (CSFs)**
* Seven Steps of Contingency Planning: Develop the contingency planning policy statement, conduct the BIA, identify preventive controls, develop contingency strategies, develop an IT contingency plan, ensure plan testing, training, and exercises & ensure plan maintenance
* Dimensions of a BIA: Identify the business impact of IT disruptions
  + Mission-critical IT systems and components
  + Does not analyze all IT functions
  + Stakeholders identify mission-critical systems
  + Compliance issues often drive BIA
  + Inputs into the Business Continuity Plan (BCP) and Risk Assessment (RA)
* Defining Scope of a BIA:
  + Define BIA scope early in the process
  + Scope defines the boundaries of the plan
  + Scope is affected by the size of the organization
    - Small Organizations: Scope could include entire organization
    - Large Organizations: Scope could include only certain areas, department, divisions
  + Purchase phase and shipment phase
* Objectives of BIA:
  + Identify critical business functions (CBFs)
  + Identify critical resources
  + Identify Maximum Acceptable Outage (MAO) and impact
    - Direct and indirect costs
  + Identify recovery requirements
* Balancing Costs: Cost to recover & cost of disruption; consider the direct and indirect costs
* Steps Involved in Implementing a BIA: Identify the environment, identify stakeholders, identify CBFs, identify critical resources, identify maximum downtime, identify recovery priorities & develop the BIA report
* Identifying Mission-Critical Business Functions and Processes:
  + Mission-Critical Functions Are:
    - Any functions considered to be vital
    - Derived from critical success factors (CSFs)
    - Successful CSFs result in performing CBFs
    - Key processes -> critical success factors -> critical business functions
    - Experts have key information regarding mission-critical functions
* BIA Best Practices: Start with clear objectives, maintain focus on objectives, use a top-down approach, vary data collection methods, plan interviews and meetings in advance, avoid the quick solution, use normal project management methods & consider the use of technology resources

**Past Questions:**

1. What is NOT an example of unintentional threat?
   1. Malware written and run by a “script kiddie” just to see what he could do destroys a company’s information database.
   2. A swine flu epidemic causes a massive reduction in the labor force that maintains a company’s systems.
   3. The server for an Internet-based business crashes.
   4. An employee enters important data incorrectly on a day when he accidentally leaves his glasses at home.
2. What is a security policy?
   1. An access control.
   2. A high-level overview of security goals.
   3. Principle of need to know.
   4. Principle of least privilege.
3. When does a threat/vulnerability pair occur?
   1. When an attacker exploits an unintentional threat.
   2. When a vulnerability exploits a threat.
   3. When a threat exploits a vulnerability.
   4. When a threat creates a loss.
4. What is one source of risk reduction?
   1. Eliminating the threat/vulnerability pair.
   2. Eliminate the threat.
   3. Increasing the rate of the occurrence.
   4. Reducing the impact of the loss.
5. When risk is reduced to an acceptable level, the remaining risk is referred to as \_\_\_\_\_.
   1. Low-impact risk.
   2. Acceptable risk.
   3. Remaining risk.
   4. Residual risk.
6. HIPAA requires that your insurance company sets standards for the protection of your data and the systems that handle that data’s \_\_\_\_\_\_\_\_.
   1. Storage, use, and transmission
   2. Storage, use, and backups
   3. Creation, management, and storage
   4. Creation, use, and transmission
7. When your bank or credit card company sends you a notification of changes in how it collects or shares data, it is sending that notification in compliance with \_\_\_\_\_\_\_\_.
   1. Financial Privacy Rule
   2. Safeguards Rule
   3. Due Process
   4. FERPA
8. When a fiduciary does not exercise due diligence, it can be considered \_\_\_\_\_\_\_.
   1. Negligence
   2. Due Process
   3. Reasonable Doubt
   4. Promissory Estoppel
9. What is the purpose of a separation of duties?
   1. To ensure no single person controls an entire process.
   2. To reduce fraud and embezzlement.
   3. To define acceptable use for IT systems and data.
   4. To encourage collusion.
10. Which is NOT a regulatory or legal statute for compliance that exists to assess and improve security?
    1. PCI DSS
    2. SOX
    3. HIPAA
    4. FERPA
11. After it’s data breach Equifax Inc. suffered a loss of public trust. This would best illustrate which of the following:
    1. Intangible Loss
    2. Negligence
    3. Compliance
    4. Fraud
12. XYZ Corp. IT staff has applied all of the proper patches to its public-facing web server. Controls are in place to minimize the risk that the server can be successfully compromised. Finally, the IT staff has fully tested and approved the current server configuration. Based on this scenario, which of the following statements is TRUE:
    1. The patches applied to the server should not be installed on the production server.
    2. The controls that are in place are insufficient.
    3. Residual risk exists with respect to the XYZ Corp web server.
    4. The IT staff of XYZ Corp. should not have approved the configuration of the server.
13. Who is responsible for residual risk?
    1. Senior Management
    2. IT Staff
    3. End Users
    4. Security Staff
14. Which is NOT a step in risk management process?
    1. Eliminate Risk
    2. Assess Risk
    3. Evaluate Controls
    4. Implement Controls
15. Your credit card company sends you a notification of changes in how it collects or shares data, it is sending that notification in compliance with which of the following?
    1. Financial Privacy Rule
    2. Safeguards Rule
    3. PCI-DSS
    4. SOX
16. A risk management team determines that cost of a new firewall monitoring appliance is greater than the anticipated loss should a threat/vulnerability pair occur related to a firewall compromise. What recommendation to management should the risk management team make regarding the new firewall monitoring appliance?
    1. Purchase the new appliance and explain to management that all risk must be mitigated as much as possible.
    2. Do not purchase the new appliance and accept the risk.
    3. Purchase the new appliance and implement it immediately to further mitigate the risk.
    4. Purchase the new appliance but only implement the control after a point in time when the risk is determined to be lower then the current level.
17. What is NOT a benefit of a qualitative risk analysis?
    1. Generally relies on expert opinions.
    2. Supports the development of accurate cost models for controls.
    3. Can be completed quickly.
    4. Is framed on categories that are easy to understand.
18. Which of the following is a TRUE statement regarding HIPAA?
    1. The Omnibus Rule extends HIPAA compliance to businesses that are not directly involved in providing healthcare.
    2. The Hi-Tech Rule extends HIPAA compliance to businesses that are not directly involve in providing healthcare.
    3. The Show Cause Rule of HIPAA requires healthcare providers to notify patients when their data is shared with 3rd parties.
    4. The Administrative Rule of HIPAA requires all healthcare providers to complete an annual risk assessment.

**Answers to Past Questions:**

1. A.
2. B.
3. C.
4. D.
5. D.
6. A.
7. A.
8. A.
9. A.
10. A.
11. A.
12. C.
13. A.
14. A.
15. A.
16. A.
17. B.
18. B.
19. A.