**Module 1 – An Introduction to Information Security:**

* Information Security: The business function of protecting organizational information assets from harm; directly includes data, information, and systems; indirectly includes physical facilities & people.
* TRIAD Security Principles: Three core principles that underpins all information security activities.
  + Confidentiality: Prevent unauthorized access of data, information or systems; only those who are authorized should be able to access data/information/systems.
  + Integrity: Prevent unauthorized modification of data, information, or systems; only those who are authorized to create, modify, or delete data/information/systems should be allowed to do so.
  + Availability: Prevent disruption of service and productivity for user of data, information, or systems; data, information, and systems should be accessible for the users when needed.

**Module 2 – Information Security Requirements, Blueprints & Architectures:**

* Requirements of Security Solutions:
  + Functional Requirements: For defining security behavior of the IT product or system.
  + Assurance Requirements: For establishing confidence that the security function will perform as intended.
  + Organizational & Business Requirements: Security must address the business requirements, not just a blanket where one size fits all.
* Security Blueprint Solutions:
  + Blueprints: Used to identify, develop and design security requirements for a particular business solution: Portal, Enterprise Resource Planning (ERP), Supply Chain, Customer Relationships Management (CRM), Manufacturing, etc.
  + Not all aspects of a particular blueprint will apply but all should be considered.
  + Security Blueprints: Tailored security best practices that, in total, form a comprehensive security policy program and technical architecture.
    - Composed of several security domains, that at a minimum, are mapped from the ISO 270002 standard.
  + Infrastructure Blueprints: Individual security blueprints reflect tailored requirements meeting the organization’s specific requirements; influenced by legal, regulatory, business, and IT drivers.

**Module 3 – Policy & Support:**

* Policy:
  + Documents and communicates management’s goals and objectives.
  + Defines the organization’s response to laws, regulations, and standards of due care.
  + Builds a foundation for a comprehensive and effective security program.
  + Defines what assets and principles the organization considers valuable.
  + Identifies organization goals and objectives.
  + Protects the company and employees from ‘surprises’.
  + Gives authority to security activity.
  + Provides for personal responsibility/accountability.
  + Provides a basis for interpreting or resolving conflicts that might arise.
  + Defines the elements, functions, and scope of security team.
  + Ensures that all employees and contractors are aware of organizational policy.
  + Written documentation for incident response and enforcement.
  + Provides for exception handling, rewards, discipline.
* Policy Infrastructure: Once an overall organizational security policy has been approved by the governing body of the organization, it is necessary to develop a supporting infrastructure of control objectives.
  + This framework may include other functional policies such as email and internet use policy, remote access policy, and fraud policy.
* Policy Implementation: From policies come the supporting elements: standards, procedures, baselines and guidelines; these will enforce the security policy principles on every business process and system.
  + Standards: Hardware and software mechanisms and products.
    - Examples: Specific anti-virus software, specific access control system, specific firewall system, and published guidelines (e.g. ISO 27002) adopted by an organization as a standard.
  + Procedures: Step by step required actions.
    - Examples: User registration, contracting for security purposes, information system material destruction, and incident response.
  + Baselines: Establishes the implementation methods for security mechanisms and products; platform unique.
    - Examples: Configurations for intrusion detection systems and configurations for access control systems.
  + Guidelines: Recommended actions.
    - Examples: Government recommendations, security configuration recommendations, ISO 27002, organizational guidelines, and product/system evaluation criteria.

**Module 4 – Organizational Roles & Responsibilities For Information Security:**

* Organizational Roles and Responsibilities:
  + For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.
  + Organizations must assign security related functions to designated employees.
  + Responsibilities to consider include:
    - Executive Management: Assigned overall responsibility for asset protection.
    - Information Systems Security Professionals: Responsible for the design, implementation, management, and review of the organization’s security policies, standards, baselines, procedures, and guidelines.
  + The owners are responsible for:
    - Ensuring that appropriate security, consistent with the organization’s security policy, is implemented in their information systems.
    - Determining appropriate sensitivity or classification levels; determining access privileges.
  + Custodian: A function who has “custody” of the system/databases, not necessarily belonging to them, for any period of time. Usually network administration or operations.
  + Users: Responsible to use resources and preserve availability, integrity, and confidentiality of assets – responsible to adhere to security policy.
  + IS/IT Function: Responsible for implementing and adhering to security policies.
  + Information Systems Auditor: Responsible for:
    - Providing independent assurance to management on the appropriateness of the security objectives.
    - Determining whether the security policy, standards, baselines, procedures, and guidelines are appropriate and effective to comply with the organization’s security objectives.
    - Identifying whether the objectives and controls are being achieved.

**Module 5 – Human Resource Procedures and InfoSec:**

* Hiring Procedures: Background checks, following up on references, verification of educational records, and signing employment agreements (non-disclosure, business ethics including telephone and Internet usage, etc.).
  + If low level checks are done at initial hiring – be alert for need for further checks if internal movement within company to higher level classification.
  + Hiring must be coordinated with Human Resources department (not just local manager).
    - Use standard checklists for hiring interviews.
    - Cover points such as keys, ID card, passwords, equipment loaned out to employee (laptops, cell phones, pagers).
* Termination Procedures: Use standard checklists for termination interviews; ensures all access cards and tools are returned.
  + Remove user access immediately upon departure; suspension/disciplinary procedures.
* Good Practices: Job descriptions and defined roles and responsibilities; least privilege / need to know; job rotation; mandatory vacations.
  + Separation of Duties: Forces collusion in order to manipulate the system for unauthorized purposes.
* Security Awareness:
  + Awareness: Provides employees with a reminder of their security responsibilities.
  + Training: Provides skills needed to perform the security functions in their jobs.
  + Education: Provides decision-making, and security management skills that are important for the success of an organization’s security program.
* Raising the Collective Awareness:
  + Variety of methods – videos, newsletters, posters, briefings, key-chains, trinkets, etc.
  + Motivate personnel to comply with requirements.
  + To be effective, the campaign must be creative and frequently changed.
  + Should reward practices such as protecting the physical area and equipment, protecting passwords, and reporting security violations.
* Providing Training Material & Courses:
  + Training should be focused on security-related job skills.
  + Specify and address security requirements of the organization.
  + Increase the ability to hold employees accountable for their actions.
  + Specialized or technical training is needed for specific personnel, such as configuring firewalls or conducting audits.
* Information System Security Education:
  + Education that is more in-depth is typically targeted for information systems security professionals in order to gain expertise.
  + Normally this is accomplished through external programs and should be regarded as part of career development.

**Module 6 – Information Classification:**

* Information Classification Objectives:
  + Ensure that information assets receive an appropriate level of protection.
  + Provide security classifications that will indicate the need and priorities for security protection.
  + Minimize risks of unauthorized information alteration.
  + Avoid unauthorized disclosure; maintain competitive edge; protect legal tactics; comply with privacy laws, regulations and industry standards.
* Information Classification Benefits:
  + Awareness among employees and customers of the organization’s commitment to protect information.
  + Identification of critical information.
  + Identification of sensitivity to modification; enables focus on integrity controls.
  + Sensitive to the need to protect confidential information.
    - Understanding of value of information; meeting legal requirements.
* Information Classification Examples:
  + FOUO: For official use only.
  + Financially sensitive
  + Sensitive management
  + Proprietary: Competitive edge
  + Private: Records about individuals, trade secrets, etc.
* Information Classification:
  + Information is classified by the Information Owner or designate.
    - Accurate classification depends on the ability and knowledge of the classifier.
    - Must be aware of regulations and customer and business expectations.
    - Classification must be done in a consistent manner; often the decisions can be somewhat arbitrary.
    - All classified items must be clearly labeled.
    - Classification process must include manner for declassifying and destroying material.
  + All data handled by the organization must be reviewed for classification: paper, magnetic, video and audio recordings, facsimile, scratch paper, etc.
  + Consider the following as part of classification: Exclusive possession (trade secret, etc.), utility (usefulness), cost of creation/recreation, liability (for protection), convertibility/negotiability (EFT, etc), & operational impact (if unavailable).

**Module 7 – Risk Management:**

* Risk Management Definitions:
  + Asset: A resource (physical or logical) that is valued by the organization.
  + Threat: Any potential danger to information or an information system.
  + Threat Agent: The source that has the potential of causing a threat.
  + Exposure: Instance of being exposed to losses from a threat.
  + Vulnerability: An information system weakness that could be exploited.
  + Attack: An action intending harm by exploiting a vulnerability.
  + Countermeasures and Safeguards: An entity that mitigates the potential risk.
  + Risk: Likelihood of an unwanted event occurring.
  + Residual Risk: The portion of risk that remains.
* Risk Management: A discipline for living with the possibility that future events may cause harm; reduces risks by defining and controlling threats and vulnerabilities.
  + Total Risk: Threats, vulnerability, and asset value.
  + Residual Risk: Total Risk – Countermeasures.
* Risk Management Control Objectives:
  + Risk levels in the red area indicate immediate action should be taken to reduce the risk.
  + Risk levels in the orange area indicate that actions should be planned and initiated to reduce the risk.
  + Risk levels in the yellow area indicate these should be monitored and prepared to respond if they are realized.
  + Risk levels in the green area indicate no specific actions need to be taken.
* How Much Security is Enough?: This decision is the balance between the cost to protect an asset against the level of acceptable risk.
  + To determine the answer to this question, we must understand the:
    - Adversary, means, motives, and opportunity.
    - Asset value
    - Threats
    - Vulnerabilities
    - Resulting Risk
    - Countermeasures
    - Risk Tolerance

**Module 8 – Risk Analysis:**

* Purpose of Risk Analysis:
  + Identify the threats to business processes and information systems.
  + Justify the implementation of specific countermeasures to mitigate risk.
* Importance of Risk Analysis: It is important in order to ensure that the resources and policy of an organization are directed appropriately.
  + Focus:
    - To identify the areas of risk to an organization or functional area.
    - To identify special circumstances that may need better controls – regulatory and financial areas.
* Additional Benefits of Risk Analysis: May be applicable to the business continuity process, insurance and liability, implementing countermeasures, new controls and procedures, and legitimizing security awareness programs.
* Risk Analysis Key Factors: Obtain Management Support:
  + Define and approve purpose and scope of Risk Assessment Team.
  + Select team members.
  + State official authority and responsibility of team.
  + Have Management review findings and recommendations.
* Suggested Team Members:
  + Information System Security
  + IT & Operations management
  + System and network administrators
  + Internal audit
  + Physical security
  + Business process and information owners
  + Advisors (Human Resources, Legal, Emergency Measures Coordinator, Safety Officers)
* Preliminary Security Evaluation:
  + Identify vulnerabilities related to natural disasters, environment (work scene), facility, access controls, and data processing controls.
  + Review existing security measures; document findings.
  + Obtain management review and approval.

**Module 9 - Threats:**

* Threat Examples: Include, but are not limited to:
  + Unauthorized access
  + Hardware failure
  + Utility failure
  + Loss of key personnel
  + Human errors
  + Neighboring hazards
  + Tampering
  + Disgruntled employees
* Emerging Threats Factor: Risk Assessment must also include emerging threats:
  + New technology
  + Change in culture
  + Unauthorized use of technology (i.e., wireless technologies, rogue modems, PDAs – Personal Digital Assistants, unlicensed software)
* Input Sources to Identify Threats: Includes, but is not limited to:
  + Users
  + System administrators
  + Auditors
  + Security Officers
  + Operations
  + Facility records
  + Community records
  + Government records
  + Watchdog alerts (CERT/CC, Bugtraq, etc.)

**Module 10 – Types of Risk Analysis:**

* Quantitative Risk Analysis:
  + Attempts to assign independently objective numeric values (e.g., monetary values) to the elements of the risk assessment and to the assessment of potential losses.
  + When all elements (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty and probability) are quantified, the process is considered to be fully quantitative.
  + Difficulties:
    - Purely quantitative risk analysis can be difficult to achieve – quantitative measure must be applied to qualitative elements.
    - Usually requires substantial time and personnel resources to complete the quantitative process.
  + Three Primary Steps:

1.) Estimate potential losses

2.) Conduct a threat analysis

3.) Determine annual loss expectancy

* + Step 1 – Estimate Potential Losses:
    - SLE (Single Loss Expectancy): Asset Value ($) \* Exposure Factor (%)
    - Exposure Factor: Percentage of asset loss when threat is successful.
    - Types of Loss to Consider:
      * Physical destruction/theft of assets
      * Loss of data
      * Theft of information
      * Indirect theft of assets
      * Delayed processing
  + Step 2 – Conduct Threat Analysis:
    - ARO (Annual Rate of Occurrence): Number of exposures or incidents that could be expected per year.
    - Likelihood of an unwanted event happening.
  + Step 3 – Determine Annual Loss Expectancy:
    - Combine potential loss and rate/year
    - Magnitude of risk = Annual Loss Expectancy
    - Guide: Security measures & amount to spend
    - ALE (Annualized Loss Expectancy): SLE (Single Loss Expectancy) \* ARO (Annualized Rate of Occurrence).
* Qualitative Risk Analysis:
  + Scenario oriented; does not attempt to assign absolute numeric values to components; purely qualitative risk analysis is possible.
  + Rank seriousness of threats and sensitivity of assets; qualitative grades such as blank (no effect), low, medium or high.
    - Perform a carefully reasoned risk assessment.
  + Scenarios: Match threats to assets via scenarios.
    - Describe Range of Threats: Potential act; assets subject to loss.
    - Procedure:
      * Write scenario for each major threat.
      * Functional managers credibility/practicality review.
      * Evaluate use of safeguards.
    - Test Scenarios: Based on test results, document findings
      * Current/planned protection
      * Remaining deficiencies
    - Scalability: Limited security study – 2 or 3 one-page scenarios; broad study hundreds of scenarios.
    - Advantages: Communication, identifying security strengths and vulnerabilities, and evaluating safeguards.
* Remedial Selection Measures:
  + Risk Reduction: Provide countermeasures to reduce the risk and strengthen the security posture.
  + Risk Transference: Transfer risk to another party (Ex: Insurance).
  + Risk Acceptance: Accepting the risk and absorbing the cost when and if it occurs.
  + Risk Avoidance: Decide not to continue with the activity or not to support the situation that causes the risk.

**Module 11 – Computer Crime & the Law:**

* Information Security Related Legal Issues:
  + Three types of harm usually addressed in computer crime laws:
    - Unauthorized access
    - Unauthorized alteration, destruction, or disclosure of information
    - Insertion of malicious programming code
* Computer Crime Categories:
  + Computer Assisted Crime: Criminal activities that are not unique to computers, but merely use computers as tools to assist the criminal endeavor (e.g., fraud, embezzlement).
  + Computer Targeted Crime: Crimes directed at computers, networks and the information stored on these systems (e.g., denial of service, sniffers, attacking passwords).
  + Computer is Incidental: The Computer is Incidental in the criminal activity (e.g., customer lists for traffickers).
* Computer Crimes and Related Laws:
  + Computer-related crimes and abuses e.g., denial of service
  + Malware
  + Software piracy
  + Illegal content issues (child pornography)
  + Wire fraud and mail fraud
  + Lack of computer crime legislation has led to prosecution through traditional laws
* Computer Crime Law Issues:
  + Antiquated Laws: The Computer Fraud and Abuse Act (CFAA) is a United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization.
  + Defining electronic information or data
  + Unlawful destruction of data or denial of service
  + Using a computer to commit, aid, or abet crime
  + Defining intellectual property
  + Complex legal definitions of technical issues
  + Private sector lack of reporting
  + Sentencing guidelines

**Module 12 – Legal Considerations for Security in the United States:**

* Information Security Legal Issues:
  + Electronic Contracts & Non-Repudiation:
    - Uniform Electronic Transactions Act (UETA): Only applies to transactions related to business, commercial (including consumer) and governmental matters.
      * Electronic Record: Means a record created, generated, sent, communicated, received, or stored by electronic means.
      * Electronic Signature: Means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
    - Non-Repudiation: Cannot successfully dispute the validity of a contract on the basis of the authenticity of the signature when it is in electronic form.
  + Encryption:
    - Import: Some countries restrict the importation of cryptographic technology.
      * Citizens can anonymously communicate with each other, preventing any external party from monitoring them.
      * Encrypted transactions may impede external entities to control the conducting of business.
    - Export: As of 2009, non-military cryptography exports from the U.S. are controlled by the Department of Commerce’s Bureau of Industry and Security. Some restrictions still exist, even for mass market products, particularly with regard to export to “rogue states” and terrorist organizations.
  + Intellectual Property:
    - Patent: Grants the owner a legally enforceable right to exclude others from practicing the invention covered; it protects novel, useful and non-obvious inventions.
    - TrademarkTM: Any word, name, symbol, color, sound, product, shape, device or combination of these used to identify goods & distinguish them from those made or sold by others.
    - Copyright©: Covers the expression of ideas rather than the ideas themselves – “original works of authorship”.
    - Trade Secret: Proprietary business or technical information which is confidential and protected as long as it’s owner takes certain security precautions.
  + Internet Restrictions:
    - 1st Amendment Rights: These protections extend to the Internet; however, the U.S. government has censored sites in the past and they are increasing in number to this day.
    - Beginning in 2015, a series of legislation and court rulings has been impacted (much without any fanfare or publicity) the ability for individuals and organizations to produce and distribute content free without restriction via the Internet (See Cybersecurity Information Sharing Act (CISA), 2016 Gallaudet University in conjunction with ADA law).
  + Personal Data Privacy:
    - Data privacy is not highly legislated or regulated in the U.S.
      * No all-encompassing law regulating the acquisition, storage, or use of personal data in the U.S. – fractured by type of data and industry.
      * Health Insurance Portability and Accountability Act of 1996 (HIPAA)
      * Children’s Online Privacy Protection Act of 1998 (COPPA)
      * Fair and Accurate Credit Transactions Act of 2003 (FACTA)
    - The European Union has the General Data Protection Regulation in force since May 25, 2018.
  + Corporate Liability:
    - Due Care: It is the concept that corporate officers and others with fiduciary responsibilities must meet certain requirements to ensure corporate security. The term is derived from “duty of care”.
    - Due Diligence: The act of gathering the necessary information so the best decision-making activities can take place.
    - Due Care vs. Due Diligence:
      * Due Care:
        + Taking responsibility for security
        + Demonstrating that responsibility is taken
        + Planning for threats and vulnerabilities
        + Documenting the process
      * Due Diligence:
        + Implementing controls
        + Ensuring controls are monitored and updated
        + Having a team that assesses all threats and evaluates loss
        + Reviewing adequacy of threat analysis
        + Ongoing risk assessment and documentation
    - Negligence vs. Fraud:
      * Legally recognized obligation
      * Perform to a standard of conduct
      * Protect others from unreasonable risks
      * Failure to conform to a required standard
      * Proximate causation
      * Resulting injury is actual loss or damage to another
      * Fraud: Criminally prosecutable and requires a demonstration of willful intent and it is a much hard legal hurdle to clear.
    - Negligence:
      * Liability and the failure to institute appropriate information security measures may result in:
        + The Organization and Board of Directors may be held liable (individually and personally)
        + Board of Directors fiduciary responsibility to stockholders to protect assets of corporation.
      * Corporation may be liable to others
      * Under doctrines of civil law, not criminal law.
  + Net Neutrality:
    - In the U.S. on June 11, 2018, the repeal of the FCC’s rules took effect, despite a U.S. Senate vote to uphold the regulation.
    - Without Net Neutrality, internet service providers in the U.S. MAY have the ability to manipulate or limit Internet access to certain websites while favoring others.
    - For example, Comcast or AT&T could cap available bandwidth for Netflix customers attempting to stream video.
    - Question: Does MAY = WILL?

**Module 13 – Specific Regulations:**

* 3 Categories of U.S. Security Regulations:
  + Broadly Applicable Regulations
  + Industry-Specific Regulations
  + Key State Regulations
* Broadly Applicable Regulations:
  + Sarbanes-Oxley Act (SOX): Enacted in 2002, the Sarbanes-Oxley Act is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. It was enacted after the high-profile Enron and WorldCom financial scandals of the early 2000s. It is administered by the Securities and Exchange Commission, which publishes SOX rules and requirements defining audit requirements and the records businesses should store and for how long.
    - Affects U.S. public company boards, management and public accounting firms.
    - The Act is organized into 11 titles:

1.) Public Company Accounting Oversight

2.) Auditor Independence

3.) Corporate Responsibility

4.) Enhanced Financial Disclosures

5.) Analyst Conflicts of Interest

6.) Commission Resources and Authority

7.) Studies and Reports

8.) Corporate and Criminal Fraud Accountability

9.) White-Collar Crime Penalty Enhancements

10.) Corporate Tax Returns

11.) Corporate Fraud Accountability

* + Payment Card Industry Data Security Standard (PCI DSS): The PCI DSS is a set of requirements for enhancing security of payment customer account data. It was developed by the founders of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa to help facilitate global adoption of consistent data security measures. PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
    - Retailers, credit card companies, anyone handling credit card data.
    - 6 Objectives and 12 Requirements:
      * Objective 1: Build and Maintain a Secure Retail Point of Sale System
      * Requirement 1: Install and maintain a firewall configuration to protect cardholder data
      * Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
      * Objective 2: Protect Cardholder Data
      * Requirement 3: Protect stored cardholder data
      * Requirement 4: Encrypt transmission of cardholder data across open, public networks
      * Objective 3: Maintain a Vulnerability Management Program
      * Requirement 5: Use and regularly update anti-virus software
      * Requirement 6: Develop and maintain secure systems and applications
      * Objective 4: Implement Strong Access Control Measures
      * Requirement 7: Restrict access to cardholder data by business need-to-know
      * Requirement 8: Assign a unique ID to each person with computer access
      * Requirement 9: Restrict physical access to cardholder data
      * Objective 5: Regularly Monitor and Test Networks
      * Requirement 10: Track and monitor all access to network resources and cardholder data
      * Requirement 11: Regularly test security systems and processes
      * Objective 6: Maintain an Information Security Policy
      * Requirement 12: Maintain a policy that addresses information security
  + Gramm-Leach-Bliley (GLB) Act:
    - Financial Modernization Act of 1999: The GLB Act includes provisions to protect consumers’ personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, the Safeguards Rule and pretexting provisions.
    - Financial institutions (banks, securities firms, insurance companies), as well as companies providing financial products and services to consumers (including lending, brokering or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts).
    - 3 Parts:
      * The Financial Privacy Rule: Requires financial institutions to give customers privacy notices that explain its information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information.
      * The Safeguards Rule: Requires all financial institutions to design, implement and maintain safeguards to protect the confidentiality and integrity of personal consumer information.
      * Pretexting Provisions: Protect consumers from individuals and companies that obtain their personal financial information under false pretenses, including fraudulent statements and impersonation.
  + Electronic Fund Transfer Act (EFT): Enacted in 1978, this law protects consumers engaging in electronic fund transfers from errors and fraud. It carries out the purposes of the Electronic Fund Transfer Act, which establishes the basic rights, liabilities, and responsibilities of EFT consumers of financial institutions that offer these services. EFTs include ATM transfers, telephone bill-payment services, point-of-sale terminal transfers in stores and preauthorized transfers from or to a consumer’s account (such as direct deposit and Social Security payments). Effective August 2010, a new provision states that institutions may not impose dormancy, inactivity or service fees for pre-paid products, such as gift cards, nor can they have an expiration date of less than five years.
    - Affects Financial institutions that hold consumer accounts or provide EFT services, as well as merchants and other payees.
    - Regulation E includes the following provisions:

1.) Definition of access device (debit cards, PINs, phone transfers, bill payment codes, private label cards).

2.) Consumer acceptance of device (either through a request for the device or validation of an unsolicited device).

3.) Financial institution responsibilities, such as disclosure requirements and records retention.

4.) Consumer rights and responsibilities, such as procedures for reporting lost or stolen access devices and notifying the institution of an error.

5.) Rules for preauthorized debits and electronic check transactions.

6.) Error resolution process.

7.) Unauthorized EFTs.

* + Children’s Online Privacy Protection Act (COPPA): Took effect in 2000. Applies to the online collection of personal information from children under 13. Monitored by the Federal Trade Commission (FTC), the rules limit how companies may collect and disclose children’s personal information. They codify what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children’s privacy and safety online.
    - Operators of commercial Web sites and online services directed to children under 13 that collect personal information from children, as well as general audience Web sites with actual knowledge they are collecting personal information from children.
  + Fair and Accurate Credit Transaction Act (FACTA): Passed in December 2003, FACTA is an amendment to the Fair Credit Reporting Act that is intended to help consumers avoid identity theft. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in the legislation. The Act also says businesses in possession of consumer information or information derived from consumer reports must properly dispose of the information.
    - Credit bureaus, credit reporting agencies, financial institutions, any business that uses a consumer report and creditors. As defined by FACTA, a creditor is anyone who provides products or services and bill for payment.
  + Federal Rules of Civil Procedure (FRCP): In place since 1938, the FRCP discovery rules govern court procedures for civil lawsuits. The first major revisions, made in 2006, make clear that electronically stored information is discoverable, and they detail what, how and when electronic data must be produced. As a result, companies must know what data they are storing and where it is; they need policies in place to manage electronic data; they need to follow these policies; and they need to be able to prove compliance with these policies, in order to avoid unfavorable rulings resulting from failing to produce data that is relevant to a case.

**Module 14 – Industry Specific Regulations:**

* Industry-Specific Regulations:
  + Federal Information Security Management Act (FISMA): Enacted in 2002, FISMA requires federal agencies to implement a program to provide security for their information and information systems, including those provided or managed by another agency or contractor. It is Title III of the E-Government Act of 2002.
    - Requirements:
      * Periodic risk assessments.
      * Policies and procedures based on these assessments that cost-effectively reduce information security risk and ensure security is addressed throughout the life cycle of each information system.
      * Subordinate plans for information security for networks, facilities, etc.
      * Security awareness training for personnel.
      * Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices and controls, at least on an annual basis.
      * A process to address deficiencies in information security policies.
      * Procedures for detecting, reporting and responding to security incidents.
      * Procedures and plans to ensure continuity of operations for information systems that support the organization’s operations and assets.
  + North American Electric Reliability Corp. (NERC) Standards: The current set of 83 NERC standards were developed to establish and enforce reliability standards for the bulk-power system of North America, as well as protect the industry’s critical infrastructure from physical and cyber threats. These overall standards became mandatory and enforceable in the U.S. on June 18, 2007. Critical Infrastructure Protection (CIP) elements of the reliability standard have been subsequently updated, most recently in 2009. CIP standards include identification and protection of both physical assets and digital (“cyber”) systems.
  + Title 21 Electronic Records: Part 11, as it is commonly called, was issued in 1997 and is monitored by the U.S. Food and Drug Administration. It imposes guidelines on electronic records and electronic signatures in an effort to uphold their reliability and trustworthiness.
    - Any business subject to FDA compliance.
    - Requirements:
      * Use of validated existing and new computerized systems.
      * Secure retention of electronic records and instant retrieval.
      * User-independent, computer-generated, time-stamped audit trails.
      * System and data security, data integrity and confidentiality through limited authorized access to systems and records.
      * Use of secure electronic signatures for closed and open systems.
      * Use of digital signatures for open systems.
      * Use of operational checks.
      * Use of device checks.
      * Determination that the people who develop, maintain or use electronic systems have the education, training and experience to perform their assigned task.
  + Health Insurance Portability and Accountability Act (HIPAA): Enacted in 1996, (supplemented in 2003, 2009, & 2013) HIPAA is intended to improve the efficiency and effectiveness of the health care system. As such, it requires the adoption of national standards for electronic health care transactions and code sets, as well as unique health identifiers for providers, health insurance plans and employers.
    - Recognizing that electronic technology could erode the privacy of health information, the law also incorporates provisions for guarding the security and privacy of personal health information. It does this by enforcing national standards to protect:
      * Individually identifiable health information, known as the Privacy Rule.
      * The confidentiality, integrity and availability of electronic protected health information, known as the Security Rule.
    - Requirements:
      * Electronic Transaction and Code Sets Standards: Requires every provider who does business electronically to use the same health care transactions, code sets and identifiers. This rule is administered by The Centers for Medicare & Medicaid Services.
      * Privacy Rule: Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. The rule permits the disclosure of personal health information needed for patient care and other important purposes. This rule is administered by the Office for Civil Rights.
      * Security Rule: Specifies a series of administrative, physical and technical safeguards for covered entities to use to assure the confidentiality, integrity and availability of electronic protected health information. This rule is administered by the Office for Civil Rights.
      * National Identifier Requirements: Requires that health care providers, health plans and employers have standard national numbers that identify them on standard transactions. This rule is administered by The Centers for Medicare & Medicaid Services.
      * Enforcement Rule: Provides standards for enforcing all the Administration Simplification Rules.
  + The Health Information Technology for Economic and Clinical Health Act (HITECH): Part of the American Recovery and Reinvestment Act of 2009, the HITECH Act significantly modifies HIPAA by adding new requirements concerning privacy and security for patient health information. It widens the scope of privacy and security protections available under HIPAA, increases the potential legal liability for non-compliance and provides for more enforcement.
    - Introduces the concept of “Business Associates”.
    - Requirements:
      * Expansion of HIPAA security standards to “business associates,” including people and organizations (typically subcontracts) that perform activities involving the use or disclosure of individually identifiable health information, such as claims processing, data analysis, quality assurance, billing, and benefit management, as well as those who provide legal, accounting, or administrative functions.
      * Increased civil penalties for “willful neglect.”
      * Data breach notification requirements for unauthorized uses and disclosures of “unsecured PHI.” These notification requirements are similar to many state data breach laws related to personally identifiable financial information data.
      * Stronger individual rights to access electronic medical records and restrict the disclosure of certain information.
      * New limitations on the sale of protected health information, marketing and fundraising communications.
  + The Chemical Facility Anti-Terrorism Standards Regulation

**Module 15 – State Specific Regulations:**

* State Regulations:
  + Mass Data Protection Law: This Massachusetts law – which went into effect March 2010 – works to protect the state’s residents against fraud and identity theft. It requires that any business that stores or uses personally identifiable information about a Massachusetts resident develop a written, regularly audited plan to protect this information. It takes a risk-based approach – rather than a prescriptive one – to information security. That means it directs businesses to establish a security program that takes into account the business size, scope, resources, nature and quantity of data collected or stored and the need for security rather than requiring the adoption of every component of a stated program.
  + Nevada Personal Information Data Privacy Encryption Law: In January 2010, Nevada was the first state to enact a data security law that mandates encryption for customers’ stored and transported personal information.

**Quiz Questions:**

1. Truncating, masking, or hiding part of an employees social security number on a printed pay sub would be an example of which foundational information security concept?
   1. Accuracy
   2. Availability
   3. Integrity
   4. Confidentiality
2. Establishing a control on a sales transaction database so that only an authorized sale associates can modify data they previously created would be an example of which foundational information security concept?
   1. Accuracy
   2. Integrity
   3. Availability
   4. Confidentiality

1. Which of the cornerstone principals of information security focus on the prevention of disruption of service?
   1. Accuracy
   2. Integrity
   3. Availability
   4. Confidentiality

1. Which of the IT Security Requirements focuses on establishing measurements that the IT security functions will be performed as intended?
   1. Strategic Requirements
   2. Functional Requirements
   3. Benchmarking Requirements
   4. Assurance Requirements

1. Sarah works in the IT Department for ABC Corp developing and implementing technical solutions in the information systems of the company. In her job, Sarah performs which of type of information security requirement?
   1. Strategic Requirements
   2. Functional Requirements
   3. Benchmarking Requirements
   4. Assurance Requirements
2. The notion that corporate offices must adhere to maintaining a certain level of security for the organization and the organizational assets in their control is known as:
   1. Due Cause
   2. Due Diligence
   3. Due Care
   4. Due Process

1. A legally recognized obligation that is not performed by a corporate officer who is responsible for said obligation and results in harm is:
   1. Due Care
   2. Negligence
   3. Due Diligence
   4. Fraud

1. SOX applies to all of the following organizations EXCEPT...
   1. ExxonMobil
   2. Auburn University Federal Credit Union
   3. Citi Bank
   4. Intel

1. Which of the following is TRUE?
   1. Gramm-Leach requires public universities to protect and management personally identifiable student data
   2. HiTech requires any business entity that stores, manages, or transfer heathcare data to comply with HIPAA
   3. PCI-DSS legislation requires all publically traded companies to conduct risk assessments
   4. SOX only applies to financial institutions and brokage firms with more than $400 million in assets
2. When a manager fails to exercise due diligence, it most likely can be considered...
   1. Dereliction of Duty
   2. Liable
   3. Negligence
   4. Fraud

**Quiz Answers:**

1.) D.

2.) B.

3.) C.

4.) D.

5.) B.

6.) C.

7.) B.

8.) A.

9.) B.

10.) C.