# Info 6010 Lesson 3
# Asset Security
# Domain 2
# and Security Assessments & Testing
# Domain 6

Revision 2

Information Security Management & Network Security Architecture

FANSHAWE

# Asset Security

Discussion topics

- Information life cycle
- Information classification and protection
- Information ownership
- Protection of privacy
- Asset retention
- Data security controls
- Asset handling requirements

# Information Life Cycle

An asset is, anything of worth to an organization. This includes people, partners, equipment, facilities, reputation, and information.

- **Acquisition**
  - Information is acquired by an organization in only one of two ways: copied from elsewhere or created from scratch.
- **Use**
  - After the information is prepared and stored, it will be read and modified by a variety of users with the necessary access level. CIA needs to be maintained by only allowing the right people to access or modify it.
- **Archival**
  - Information when no longer used regularly needs to be archived before it is finally disposed of.
- **Disposal**
  - Almost all data will be disposed of at some point.  This usually, but not always, means data destruction. Ensure that the appropriate data does in fact get destroyed, and that it is destroyed correctly.

# Information Classification

- Information is rated based on
  - Impact of loss
  - Impact of disclosure
  - Impact if unavailability
- Classification ensures data is protected in the most cost effective manner
- Classification indicates level of CIA

# Information Classification

- Each level of classification should have its own handling requirements and procedures
  - How users access the data
  - If no longer required, how to dispose of data in a safe manner
- Handling data may require encryption when moving from one location to another
- Using data may require 2 individuals to enter their access codes
- Destroying data may require physical destruction of computer hard drives or simply secure wipe whereby a series of ‘0’ and ‘1’ are written many times to each hard drive sector

# Information Classification

- Military vs. Private Business Classifications
- To classify data an entity must decide on the scheme it will follow to assign classification to its data
- Military classification is can be very different from private business, as always it depends on the organisation.

# Information Classification

- Commercial Classification:
  - Confidential
  - Private
  - Sensitive
  - Public
- Military Classification:
  - Top Secret
  - Secret
  - Confidential
  - Sensitive but unclassified
  - Unclassified

# Information Classification

- Common Commercial Classification Scheme
  - For Office Use Only
  - Proprietary
  - Privileged
  - Private
- Classification scheme customized for each company
  - Ensure each classification is unique and does not overlap
  - Do not create too many classifications
  - Include handling, usage and disposal procedures for each classification
  - Select criteria used to separate data to each classification

# Information Classification

- Classification Controls:
  - Ensure you have strict and granular access controls
  - Encryption while in transit
  - Auditing and monitoring of data usage
  - Separation of duties ensuring there is no collusion between employees
  - Periodic reviews of access control processes
  - Backup and recovery processes
  - Marking and labeling appropriately

# Information Classification

- Data Classification Procedure Steps
  - Define classification levels
  - Criteria for how data is classified
  - Data owner should classify under their responsibility
  - Identify data custodian who will maintain data and security
  - Indicate security controls or protection for each classification
  - Document any exceptions
  - Indicate process for transferring ownership to different custodian
  - Define procedure for declassifying data
  - Integrate in security awareness training program

# Layers of Responsibilities

- Layers of Responsibility
  - Everyone has responsibility
  - Managers and users should have input into best practices, procedures and chosen controls
  - This ensures agreed upon security level is successfully implemented and maintained
  - Specific roles must be assigned such as;
  - Data owner, Data Custodian, System Owner, Process Owner and Security Administrator

# Responsibilities

- Unfortunately people are the weakest link in the Security chain
- Separation of duties and layers of responsibility ensure  a successful security program
- Appropriate level of training and transparency is required for everyone to understand their responsibilities within the company
- Clear structure and chain of command is required

# Responsibilities

- Clear duty descriptions ensure everyone understands their role within the company
- Policies ensure everyone understands expected behaviour.
  - Clearly define acceptable and unacceptable behaviour including reprimand
- Separation of Duties ensures there is no collusion amongst employees
  - Collusion – Two or more employees working together to cause a destructive or fraudulent act against the company

# Responsibilities - CEO

- CEO – Chief Executive Officer
  - Day-to-day management of entire organization
  - Often Chairperson of the Board of Directors and is highest ranking officer in company
  - Oversees companies finances, budget, strategic vision, business plan
  - Decides on partnerships with other vendors
  - Decides how company will differentiate itself from its competitors

# Responsibilities - CFO

- CFO – Chief Financial Officer
  - Day-to-day account and financial activities
  - Responsible for overall financial structure
  - Determines companies current and future financial needs
  - Maintains company capital structure
    - Equity, Cash, Credit, Debt
  - Oversees budget and financial performance metrics
  - Responsible for filing financial statements to regulatory bodies

# Responsibilities - CIO

- CIO – Chief Information Officer
  - Reports to CEO or CFO
  - Responsible for information technology infrastructure
  - Oversee day-to-day technology operations
  - Security policy originating from CEO and CIO helps ensure it is properly implemented

# Responsibilities - CPO

- CPO – Chief Privacy Officer
  - Reports to Chief Security Officer
  - Newer position
  - Oversee appropriate handling and usage of data
  - Familiar with outside regulations and market specific legal requirements
  - Usually an attorney by training

# Security Administration

- Senior management appoints a Security Officer
- Security administration may be a single individual or group of individuals
  - based on size and requirement of company
- Security administration requires clear authority  and reporting structure
- Security officer ensures implementation of security policy
  - Not solely responsible for development of policy

# Responsibilities - CSO

- CSO – Chief Security Officer
  - Responsible for understanding company specific risks and processes used to mitigate these risks
  - Must understand business drivers
  - Responsible for maintaining company Security Program
  - Responsible for compliance with applicable regulations and laws
  - Ensures Business is NOT interrupted in any way

# CISO

- Chief Information Security Officer
- Must have a strong understanding of business processes and objectives
  - Ability to communicate effectively with upper management
  - Understand legal regulations and *security frameworks*
  - Develop and maintain security awareness programs
  - Develop security budget and report to Board of Directors or upper management
  - Respond to security incident or breach

# Responsibilities

- Data Owner
  - Member of management in charge of specific business unit
  - Responsible for specific data subset
  - Has due care responsibility to ensure data/information is not corrupted, destroyed, improperly used or transmitted
  - Responsible for appropriate security controls
  - Responsible for defining appropriate classification, backup requirements, approving access controls and approving any disclosure
  - Responsible for dealing with access violations

# Responsibilities

- Data Custodian
  - Responsible for maintaining and protecting data/information
  - Responsible for performing regular backups ensuring data is available
  - Responsible for retaining data access information
  - Responsible for fulfilling company security requirements assigned to data/information

# Responsibilities

- System Owner
  - Responsible for one or more systems
  - These systems process or hold data/information owned by different individuals
  - Responsible for system purchasing decisions
  - Responsible for ensuring adequate access controls and operating system configurations
  - Ensures systems are properly assessed against any vulnerabilities

# Responsibilities

- Security Administrator
  - Anyone with a root or administrative account to a system
  - Ensures software is properly updated
  - Responsible for day to day system management
  - Ensures company policies are properly implemented at the system level
  - Ensures user access to data/information is done according to security policy

# Responsibilities

- Supervisor
  - Responsible for all user activity and assets created and owned by these users
  - Ensures employees understand their responsibilities
  - Security policy
  - Account information is accurate
  - Take appropriate action when employee role changes
    - Fired
    - Suspended

# Responsibilities

- Change Control Analyst
  - Responsible for approving and rejecting change control requests
  - Must ensure changes will not introduce any vulnerabilities
  - Ensures changes are properly tested and implemented
  - Must understand how various changes impact the following
    - Security
    - Performance
    - Productivity

# Responsibilities

- Data Analyst
  - Ensures data is stored in a fashion that makes sense for the company
  - May design or architect a new system
  - May advise in purchase of new product
  - Works in conjunction with data owners

# Responsibilities

- User
  - Uses data for work-related task
  - Must have required level of access
  - Responsible for following procedural and operational requirements to ensure confidentiality, integrity and availability of data

# Responsibilities

- The Auditor
  - Evaluates security controls within the company
  - Performs internal and external evaluation
  - Performs unbiased, independent and comprehensive evaluation of company
  - Using third party (outside company) ensures ‘unbiased’ review

# Responsibilities

- Why So Many Roles?
- Company business processes are complex
  - Not everyone is familiar with all processes and requirements
- A  system administrator should not be making decisions how to implement security and what assets to secure.
  - This direction should be given by management
- A managerial position should not be implementing security countermeasures.
  - This should be done by qualified technical individuals

# Retention Policies

FANSHAWE

# Retention Policies

- How long should an organisation retain data?
  - For as long as they need it.
  - To comply with laws and regulations.
- Developing a retention policy is a must.
  - What data do we keep?
  - How long do we keep this data?
  - Where do we keep this data?

# How We Retain

- In order for retained data to be useful, it must be accessible in a timely manner.
  - **Taxonomy** A taxonomy is a scheme for classifying data. T
  - **Classification** The sensitivity classification of the data will determine the controls we place on it both while it is in use and when it gets archived.
  - **Normalization** Retained data will come in a variety of formats, The original data needs to be tagged so that it is searchable.
  - **Indexing** Retained data must be searchable if we are to quickly pull out specific items of interest, this can be done by building indexes.

# eDiscovery

- Discovery of electronically stored information (ESI), or *e-discovery*, is the process of producing for a court or external attorney all ESI pertinent to a legal proceeding.
- The Electronic Discovery Reference Model (EDRM) identifies eight steps, though they are not necessarily all required, nor are they performed in a linear manner:
  1. **Identification** of data required under the order.
  2. **Preservation** of this data to ensure it is not accidentally or routinely destroyed while complying with the order.
  3. **Collection** of the data from the various stores in which it may be.
  4. **Processing** to ensure the correct format is used for both the data and its metadata.
  5. **Review** of the data to ensure it is relevant.
  6. **Analysis** of the data for proper context.
  7. **Production** of the final data set to those requesting it.
  8. **Presentation** of the data to external audiences to prove or disprove a claim.

# Data Remanence

- **Data remanence** is the residual physical representation of information that was saved and then erased in some fashion.
- If the media does not hold confidential or sensitive information, overwriting or deleting the files may be the appropriate course of action.

# Media Control

- When media is erased (cleared of its contents), it is said to be **sanitized**
- Media can be sanitized in several ways:
- **Overwriting** with a pattern designed to ensure that the data formerly on the media are not practically recoverable.
- **Degaussing:** magnetic scrambling of the patterns on a tape or disk that represent the information stored there.
- **Encryption** quickly and securely render data unusable. To render the data unrecoverable, the system simply needs to securely delete the encryption key.
- **Physical Destruction** (shredding, crushing, burning)

# Media Management

- Proper media management requires the following tasks:
  - **Tracking (audit logging)** who has custody of each piece of media at any given moment
  - This creates the same kind of audit trail as any audit logging activity—to allow an investigation to determine where information was at any given time, who had it, and, for particularly sensitive information, why they accessed it
  - This enables an investigator to focus efforts on particular people, places, and time, if a breach is suspected or known to have happened

# Media Management

- Effectively implementing access controls
  - Restrict who can access each piece of media to only those people defined by the owner of the media/information on the media
  - Enforce the appropriate security measures based on the classification of the media/information on the media
  - Certain media, due to the physical type of the media, and/or the nature of the information on the media, may require “special handling”
- Access controls will include
  - **physical** (locked doors, drawers, cabinets, or safes)
  - **technical** (access and authorization control of any automated system for retrieving contents of information in the library)
  - **administrative** (the actual rules for who is supposed to do what to each piece of information)

# Media Management

- **Tracking** the number and location of backup versions (both onsite and offsite)
  - This is necessary to ensure proper disposal of information when the information reaches the end of its lifespan; to account for the location and accessibility of information during audits; and to find a backup copy of information if the primary source of the information is lost or damaged
- Documenting the history of changes to media
  - For example when a particular version of a software application kept in the library has been deemed obsolete, this fact must be recorded so the obsolete version of the application is not used unless that particular obsolete version is required

# Media Management

- **Ensuring environmental** conditions do not endanger media
  - Each media type may be susceptible to damage from one or more environmental influences
  - For example, all media formats are susceptible to fire, and most are susceptible to liquids, smoke, and dust
  - Magnetic media formats are susceptible to strong magnetic fields
  - Magnetic and optical media formats are susceptible to variations in temperature and humidity

# Media Management

- **Ensuring media integrity**
  - Verifying each piece of media remains usable, and transferring still-valuable information from pieces of media reaching their obsolescence date to new pieces of media
  - Every type of media has an expected lifespan under certain conditions, after which it can no longer be expected that the media will reliably retain information

# Media Management

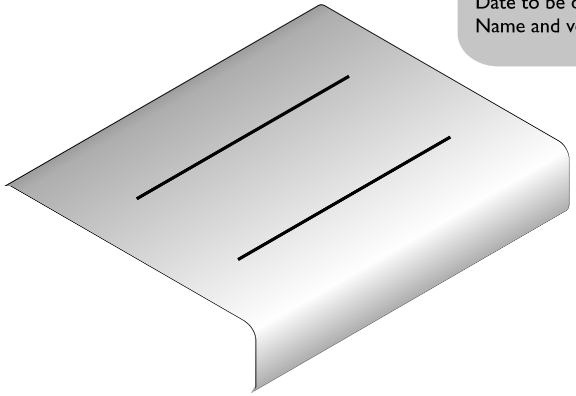
- **Inventorying the media** on a scheduled basis
  - Detect if any media has been lost/changed
  - This can reduce the amount of damage a violation of the other media protection responsibilities could cause by detecting such violations sooner rather than later, and is a necessary part of the media management life cycle by which the controls in place are verified as being sufficient

# Media Management

- **Carrying out secure disposal activities**
  - Disposition includes the lifetime after which the information is no longer valuable and the minimum necessary measures for the disposal of the media/information
  - Secure disposal of media/ information can add significant cost to media management

# Media Management

- **Internal and external labeling** of each piece of media in the library should include
  - Date created
  - Retention period
  - Classification level
  - Who created it
  - Date to be destroyed
  - Name and version



cation level: Confidential
Who created it: Shon Harris
Date to be destroyed: Feb 2012
Name and version: Why Redheads Rule the World

# Protecting Mobile Devices

- Protect mobile devices and the data they hold:
  - Inventory all mobile devices, including serial numbers.
  - Harden the operating system by applying baseline secure configurations.
  - Password-protect the BIOS on laptops.
  - Register all devices with their respective vendors, and file a report with the vendor when a device is stolen.
  - Do not check mobile devices as luggage when flying.
  - Never leave a mobile device unattended,
  - Engrave the device with a symbol or number for proper identification.
  - Use a slot lock with a cable to connect a laptop to a stationary object whenever possible.
  - Back up all data on mobile devices to an organizationally controlled repository.
  - Encrypt all data on a mobile device.
  - Enable remote wiping of data on the device.
- Tracing software can be installed so that your device can “phone home” if it is taken from you.

# Paper Records

Principles to consider when protecting paper records:

- Educate staff on proper handling of paper records.
- Minimize the use of paper records.
- Ensure workspaces are kept tidy so it is easy to tell when sensitive papers are left exposed, and routinely audit workspaces to ensure sensitive documents are not exposed.
- Lock away all sensitive paperwork as soon as you are done with it.
- Prohibit taking sensitive paperwork home.
- Label all paperwork with its classification level. Ideally, also include its owner’s name and disposition (e.g., retention) instructions.
- Conduct random searches of employees’ bags as they leave the office to ensure sensitive materials are not being taken home. **Not legal everywhere!**
- Destroy unneeded sensitive papers using a crosscut shredder. For very sensitive papers, consider burning them instead.

# Safes

- Safes are used to store backup data tapes, original contracts, or other types of valuables. The safe should be penetration resistant and provide fire protection. The types of safes an organization can choose from are:
  - **Wall safe** Embedded into the wall and easily hidden
  - **Floor safe** Embedded into the floor and easily hidden
  - **Chests** Stand-alone safes
  - **Depositories** Safes with slots, which allow the valuables to be easily slipped in
  - **Vaults** Safes that are large enough to provide walk-in access
- Combination lock should be changed periodically, need to know or access basis.
- The safe should be in a visible location, so anyone who is interacting with the safe can be seen.

# Data Leakage

- Data leakage will happen! Leaks of personal information can cause large financial losses. The costs include:
  - Investigating the incident and remediating the problem
  - Contacting affected individuals to inform them about the incident
  - Penalties and fines to regulatory agencies
  - Contractual liabilities
  - Mitigating expenses (such as free credit monitoring services for affected individuals)
  - Direct damages to affected individuals

# Data Leak Prevention

- **Data leak prevention (DLP)** aimed at preventing the loss of sensitive information. By focusing on the:
- location, classification and monitoring of information at rest, in use and in motion, to stop the numerous leaks of information that occur each day.
- The successful implementation of this DLP requires significant preparation and diligent ongoing maintenance.
- Those implementing the solution must take a strategic approach that addresses risks, impacts and mitigation steps, along with appropriate governance and assurance measures

# Info 6010 Lesson 3
# Security Assessment and Testing
# Domain 6

Revision 2

Information Security Management &Network and Security Architecture

FANSHAWE

# Security Assessment and Testing

Discussion topics:

- Internal, external, and third-party audits
- Vulnerability testing
- Penetration testing
- Log reviews
- Synthetic transactions
- Code review and testing
- Misuse case testing
- Interface testing
- Account management
- Backup data verification
- Disaster recovery and business continuity
- Security training and security awareness
- Key performance and risk indicators
- Analyzing and reporting
- Management review and approval

# Assessment, Test and Audit Strategies

- Assessment, Test and Audit – may mean different things to different people.
- Often these words are used interchangeably!
- What is the goal?
  - Define a scope of what is to be assessed/tested or audited.

# Information System Security Audit Process

1. **Determine the goals**, because everything else hinges on this.

2. **Involve the right business unit leaders** to ensure the needs of the business are identified and addressed.

3. **Determine the scope**, because not everything can be tested.

4. **Choose the audit team**, which may consist of internal or external personnel, depending on the goals, scope, budget, and available expertise.

5. **Plan the audit** to ensure all goals are met on time and on budget.

6. **Conduct the audit** while sticking to the plan and documenting any deviations therefrom.

7. **Document the results**, because the wealth of information generated is both valuable and volatile.

8. **Communicate the results** to the right leaders in order to achieve and sustain a strong security posture.

# Internal Audits

- Data is one of an organization’s most valuable asset; it has also become its most vulnerable, hence internal audits are invaluable.
- Ideally, every organization should have an internal audit team capable of performing whatever audits are required.
- Internal staff are familiar with the inner workings of the organization and are flexible; as they can be redeployed as appropriate.

- Disadvantages of internal staff is they may lack a breath of knowledge.
- There is the potential for conflicts of interest, if the auditors believe that their bosses or coworkers may be adversely affected by a negative report.
- Potential conflict of interests if the team has an agenda to pursue.

# External Audits

- An *external audit* (sometimes called a second-party audit) is one conducted by (or on behalf of) a business partner and are tied to contracts.
- Once the contract is in place, the client organization could demand access to people, places, and information to verify that the security provisions are being met by the contractor.

# Third-Party Audits

- Engaging a third party to audit the information systems' security is often a requirement for compliance to regulations and standards.
- Advantages:
  - External/ third party auditors are probably more experienced.
  - Third-party auditors are unaware of the internal dynamics and politics of the target organization.
  - This means that they have no favorites or agendas other than the challenge of finding flaws.
  - Likely to be more objective than internal staff as they were not involved in implementing the controls and therefore not likely to overlook or subconsciously impede the search for defects in those controls.
- Disadvantage of hiring an external team is cost.

# Test Coverage

- *Test coverage* is a measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage.
- It is too costly and time consuming to test everything unless it is a requirement in a safety-critical system.
- Develop a schedule that will test all of the controls over an extended period of time – eventually everything is covered.

# Auditing Technical Controls

- A *technical control* is a security control implemented through the use of an IT asset. This asset is usually some sort of software that is configured in a particular way.
- Audit a technical controls, is testing its ability to mitigate the risks that were identified in the risk management process.

# Vulnerability Testing

The goals of the assessment are to:

- Evaluate the true security posture of an environment.
- Identify as many vulnerabilities as possible, with honest evaluations and prioritizations of each.
- Test how systems react to certain circumstances and attacks, to learn not only what the known vulnerabilities are, but also how the unique elements of the environment might be abused (e.g. SQL injection attacks, buffer overflows, and process design flaws that facilitate social engineering).
- Before the scope of the test is decided and agreed upon, the tester must explain the testing ramifications. Vulnerable systems could be knocked offline by some of the tests, and production could be negatively affected by the loads the tests place on the systems.

# Penetration Testing

- *Penetration testing* is the process of simulating attacks on a network and its systems at the request of the owner, senior management.
- It employs a set of procedures and tools designed to test and possibly bypass the security controls of a system.
- The goal is to measure an organization’s level of resistance to an attack and to uncover any weaknesses within the environment.

# War Dialing

- Allows attackers and administrators to identify available modems.
- Specially written program tools can be used to dial a large bank of phone numbers.
- Tools log valid data connections and attempt to identify the system.
- War dialing enables an attacker to find all the modems that provide remote access into a network

# Other Vulnerability Types

- **Kernel flaws** Any flaw in the kernel that can be reached by an attacker, if exploitable, gives the attacker the most powerful level of control over the system.
- **Buffer overflows** Poor programming practices, or bugs in libraries, allow more input than the program has allocated space to store it.
- **Symbolic links:** if a program follows a symbolic link (a stub file that redirects the access to another place) and the attacker can compromise the symbolic link, then the attacker may be able to gain unauthorized access. (Symbolic links are used in Unix and Linux systems.)
- **File descriptor attacks** File descriptors are numbers many operating systems use to represent open files in a process. Certain file descriptor numbers are universal, meaning the same thing to all programs. If a program makes unsafe use of a file descriptor, an attacker may be able to cause unexpected input to be provided to the program, or cause output to go to an unexpected place with the privileges of the executing program.
- **Race conditions** Race conditions exist when the design of a program puts it in a vulnerable condition before ensuring that those vulnerable conditions are mitigated. Examples include opening temporary files without first ensuring the files cannot be read or written to by unauthorized users or processes, and running in privileged mode or instantiating dynamic load library functions without first verifying that the dynamic load library path is secure.. An example of a race condition is a time-of-check/time-of-use attack.
- **File and directory permissions** Many attacks rely on inappropriate file or directory permissions—that is, an error in the access control of some part of the system, on which a more secure part of the system depends.

# Postmortem Review

- It is important that the team gather after the completion of a project to review things that should be improved for the next time
  - Should be a structured event in which someone leads the meeting(s) and someone takes notes
- Objectively view and identifying issues that could be improved upon the next time around

# Log Reviews

- Enable appropriate level of auditing to ensure all required events are tracked.
- Audit logs can become very large and unmanageable quickly.
  - Log management tools required to administer log information.
- Audit logs must be reviewed by a human to be valuable.
- Audit logs are protected and only Administrators have access.
  - Hacker tampering, User accidental or deliberate deletion
- Audit log retention policies provide adequate protection
  - Security logs overwriting daily may not be ideal.

# Auditing & Logging

- System Level Events
  - System Performance
  - Logon Attempts
  - Logon ID
  - Date and Time of each Logon attempt
  - Account Lockout Events
  - Privileged Use (Administrator Level Tools or Applications)
  - Operating System configuration file changes
  - Privileged Use (Devices)
  - Privileged Use (Applications)

# Auditing & Logging

- Keystroke Monitoring
  - Active user key logging
    - Stores every key pressed by user
  - Usually done in special circumstances
  - Can be used by hackers to gain passwords
  - Privacy and legal considerations if done without authorization

# Auditing & Logging

- Protecting Audit Data and Log Files
  - Only Administrators should have access to audit data
  - Should protect against accidental corruption, deletion or alteration
  - Should implement appropriate retention policy
    - Backup and store Audit and Log information for period of time
  - Confidentiality and Integrity of log files is priority
    - May be used in court of law

# Preventing Log Tampering

Log files are among the first artifacts that attackers will use to attempt to hide their actions. Make it infeasible, or at least very difficult, for attackers to successfully tamper with the log files. The following are the top five steps we can take to raise the bar for the bad folks:

- **Remote logging** Putting the log files on a separate box will require the attackers to target that box too.
- **Simplex communication** Some high-security environments use one-way (or simplex) communications between the reporting devices and the central log repository.
- **Replication** make multiple copies and keep them in different locations.
- **Write-once media** If one of the locations to which you back up your log files can be written to only once, you make it impossible for attackers to tamper with that copy of the data.
- **Cryptographic hash chaining** each event is appended the cryptographic hash of the preceding event. This creates a chain that can attest to the completeness and the integrity of every event in it.

# Synthetic Transactions

- A Synthetic transaction is generated by a script rather than a person.
  - Are predictable and can be very regular, because their behaviours are scripted.
- Real user monitoring (RUM) is a passive way to monitor the interactions of real users with a web application or system. It uses agents to capture metrics such as delay, jitter, and errors from the user’s perspective.

# Misuse Case Testing

- Misuse case testing evaluates software from the attackers perspective.
- Defining the test cases – think of all the different approaches an attacker would use.

# Code Reviews

- Test software using a systematic examination of the instructions that comprise a piece of software, performed by someone other than the author of that code.

# Testing Types

- Testing provides  assurance that the software is working as expected
  - There are different types of tests software should go through because there are different potential flaws we will be looking for
- The following are common testing approaches:
- Unit testing
  - Individual component in a controlled environment
  - Programmers validate data structure, logic, and boundary conditions.

# Testing Types

- Integration testing
  - Verifying that components work together as outlined in design specifications.
- Acceptance testing
  - Ensuring that the code meets customer requirements.
- Regression testing
  - After a change to a system takes place, retesting to ensure functionality, performance, and protection.

# A Code Review Process

1. Identify the code to be reviewed.
2. The team leader organizes the inspection and makes sure everyone has access to the correct version of the source code, along with all supporting artifacts.
3. Everyone prepares for inspection by reading through the code and making notes.
4. All the obvious errors are collated offline (not in a meeting) so as not to waste time in the meeting.
5. If the code is ready for inspection, then the meeting goes ahead.
6. The code is displayed/shared. Everyone discusses bugs, design issues, and anything else that comes up about the code. A scribe (not the author of the code) writes everything down.
7. At the end of the meeting, everyone agrees on a “disposition” for the code:
   - Passed: Code is good to go
   - Passed with rework: Code is good so long as small changes are fixed
   - Re-inspect: Fix problems and have another inspection
8. After the meeting, the author fixes any mistakes and checks in the new version.
9. If the disposition of the code in step 7 was passed with rework, the team leader checks off the bugs that the scribe wrote down and makes sure they’re all fixed.

# Interface Testing

- Modern software systems are extremely complex and interrelated.
  - Complex systems often rely on multiple independent components.
- *Interface testing* is the systematic evaluation of a given set of these exchange points. This assessment should include both known good exchanges and known bad exchanges in order to ensure the system behaves correctly at both ends of the spectrum.
- Application programming interfaces, API’s, define interactions between systems, they must be tested as:
  - They are critical to business operations
  - They introduce potentially serious security issues.

# Auditing Administration Controls

FANSHAWE

# Auditing Administrative Controls

- Administrative controls are implemented through policies or procedures

**Account Management:**

- Usually part of regulatory requirement
- Work flow process for
  - Creation of new accounts
  - Removal of accounts no longer required
    - Terminated employees, contract employees
- Provisioning
  - Data for new account pulled from Human Resource data
    - Authoritative source
  - All user identity attributes stored in an *identity repository*
    - *Meta-directory or virtual directory*

# Account Management

- Federation
    - Several companies interact to share customer information
    - Airline, car rental, hotel
    - Federated identity
    - Allows user to be authenticated across multiple systems and enterprises

# Access Control Practices

- Operational tasks which must be performed on a regular basis to maintain security policy
  - Deny access to Unknown, Anonymous or Unauthorized Users
  - Limit and monitor use of Administrator and Power User Accounts
  - Suspend or Lock Accounts after unsuccessful login attempts
  - Remove obsolete user account
  - Suspend inactive account after 30 to 60 days
  - Enforce strict access criteria
  - Enforce need-to-know and least privilege principles

# Access Control Practices

- Limit and monitor global access rules
- Ensure User ID’s are not job descriptive (i.e. Backup)
- Disable unneeded Operating System features and services
- Enforce regular Password Change (especially Administrator accounts)
- Enforce Password Complexity requirements (All accounts)
- Enforce Account expiry of temporary accounts
- Enable appropriate Auditing of accounts, devices and file usage
- Ensure appropriate Log retention policy
- Protect Log Integrity and Confidentiality

# Access Control Monitoring

- Intrusion Detection System - IDS
  - Process specifically designed to detect unauthorized access, use or attack vector against a network resource
- Looks for unusual patterns or activity
- Alerts on non-normal behaviour
- Two types of Intrusion Detection Systems
  - NIDS - Network Intrusion Detection System
  - HIDS - Host Intrusion Detection System

# Backup Verification

Having a backup does not mean that it is usable.

- **Testing Data Backups**
- *Develop scenarios* that capture specific sets of events that are representative of the threats facing the organization.
- *Develop a plan* that tests all the mission-critical data backups in each of the scenarios.
- *Use automation* to minimize the effort required by the auditors and ensure tests happen periodically.
- *Minimize impact on business* processes of the data backup test plan so that it can be executed regularly.
- *Ensure coverage* so that every system is tested, though not necessarily in the same test.
- *Document the results* so you know what is working and what needs to be worked on.
- *Fix or improve* any issues you documented.

# Disaster Recovery & Business Continuity Plan Testing

- DR & BCP should be tested regularly
  - Environments continually change
  - Processes may change
  - Technology changes
  - Each time a plan is tested, errors, omissions or required additions are discovered
  - Responsibility of testing the plan should be given to an individual or group of individuals who will have sole responsibility of maintaining and testing the plan
  - Maintenance should be incorporated into change control processes within the company

# Business Plan Testing

- Tests and recovery drills should be performed at least once per year
  - Prepare personnel for what they may face
  - Untested plan has ‘zero’ confidence
- Decide what is to be tested and when
- Decide what hardware, resources, personnel and procedures will be tested

# DR & Business Plan Testing

- Most companies cannot shutdown for a day to test, therefore this should be done in smaller pieces or at certain times (after business hours)
- Initial drills should not include everyone, but rather smaller groups until everyone learns their responsibilities
  - BPC team should expect problems and confusion

# Business Plan Testing

- BCP may include additional plans specific to business unit or process
- Business resumption plan
  - recreate business processes
- Continuity of operations plan
  - order of succession, roles and authority
- IT contingency plan
  - System, network, communication and applications
- Crisis communications plan
  - Internal and external communication structure

# Business Plan Testing

- **Checklist**
  - In this test copies of BCP are given to all functional managers within business units
  - Functional managers must review and ensure all processes have been included and are accurate
  - Any changes, omissions are given back to BCP team for incorporation of master BCP

# Business Plan Testing

- **Structured Walk Through**
  - Representatives from each business unit or functional area come together to review the plan
  - Group reviews scope, goals and assumptions
  - Group reviews reporting structure
  - Group evaluates testing, maintenance and training requirements
  - Group steps through different threat scenarios to ensure accuracy

# Business Plan Testing

- **Tabletop exercises** (TTXs) are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation.
- TTXs can happen at an executive level (e.g., CEO, CIO, CFO) or at a team level (e.g., security operations center [SOC]), or anywhere in between.
- A facilitator guides participants through a discussion of one or more scenarios.

# Business Plan Testing

- **Simulation**
  - This test requires more planning and personnel
  - All employees (operational, functional and support) come together and practice executing plan based on specific threat scenario
  - Scenario is used to test reaction of each unit
  - Test would include resources available during actual disaster
  - Test stops at relocation phase

# Business Plan Testing

- **Parallel test**
  - Some systems are moved to recovery site and processing takes place
  - Results are compared to primary site processing output
  - This testing locates process deficiencies

# Business Plan Testing

- **Full-Interruption Test**
  - Most intrusive test
  - Primary site is shutdown and all processing moves to recovery site
  - Recovery teams prepare alternate site
  - Processing takes place at alternate site
    - Only with available resources at recovery site
  - Full drill, requires much planning and is most costly to company
  - This test presents most risk to company and can severely impact company if not planned properly

# Security Training and Security Awareness Training

- Cyber incident response plan
  - Malware or hacker intrusion
- Occupant emergency plan
  - Personnel safety and evacuation procedure

# Business Plan Training

- Employees should have other training
  - First aid
  - How to use fire extinguisher
  - Evacuation procedures
  - Crowd control
  - Emergency communication
  - Proper equipment shutdown procedures

# Business Plan Training

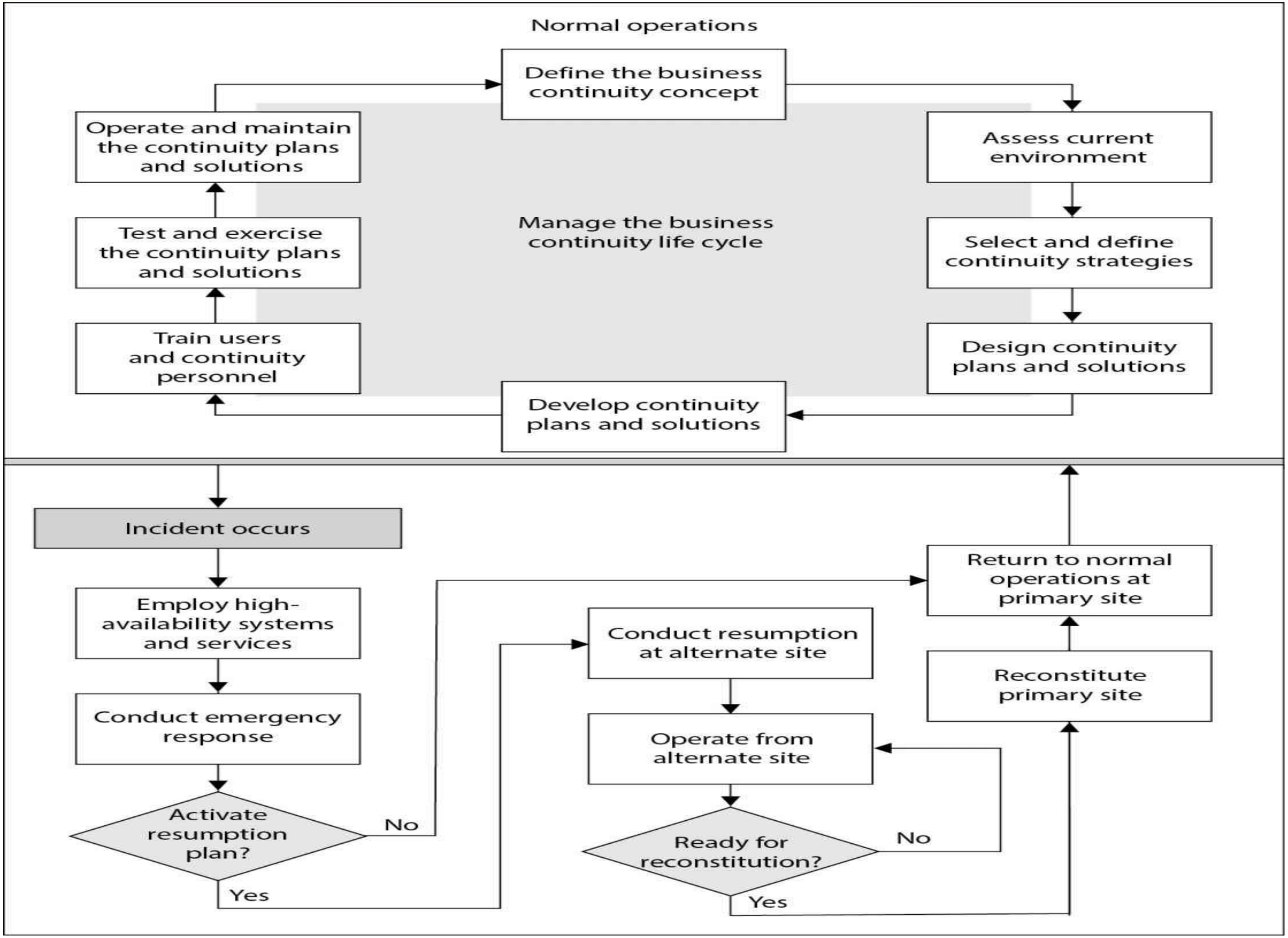
- Emergency response
- Protection of life is primary goal of any response procedure
- All personnel should know their exit routes
- One individual should in be in charge of contacting authorities
- One individual should be in change of communication with external groups (Press)
- Other consequences should be addressed
  - Vandalism
  - Looting
  - Theft

# Maintain Business Plan

- Companies are living entities
  - Processes change
  - People change
  - Technology changes
- BCP could quickly become out of date
- Company will have a false sense of security

# Maintain Business Plan

- Companies can take the following actions to ensure their plans are maintained
  - BCP is part of every business decision
  - BCP maintenance should be included in job description
  - Include BCP maintenance in employee evaluation
  - Perform internal audits that include BCP
  - Perform regular drills
  - Integrate BCP into change management process

Normal operations
Define the business continuity concept
Assess current environment
Select and define continuity strategies
Design continuity plans and solutions
Develop continuity plans and solutions
Train users and continuity personnel
Test and exercise the continuity plans and solutions
Operate and maintain the continuity plans and solutions
Manage the business continuity life cycle
Incident occurs
Employ high-availability systems and services
Conduct emergency response
Activate resumption plan?
No
Yes
Conduct resumption at alternate site
Operate from alternate site
Ready for reconstitution?
No
Yes
Reconstitute primary site
Return to normal operations at primary site

# Social Engineering

- Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim’s natural tendencies and emotional reactions.

# Key Performance and Risk Indicators

- A **key risk indicator** (KRI) is a measure used in management to indicate how risky an activity is. ... It differs from a **key performance indicator** (KPI) in that the latter is meant as a measure of how well something is being done while the former is an **indicator** of the possibility of future adverse impact.

# Reporting

- Clear report writing is critical as the professional needs to communicate with both technical and nontechnical audiences.

**Analyzing Results**

- Determine what has happened, what is the impact and what if anything should be done about it.
- The goal of this analysis process is to move logically from facts to actionable information.
- The next step is writing the report.

# Writing Technical Reports

- **Executive Summary** Preface it with a hard-hitting summary of key take-aways.
- **Background** Describe the scope of the event and explain the conducted of the experiment/test/assessment/audit in the first place.
- **Methodology** Describe the process by which you conducted the study. List the personnel who participated, dates, times, locations, and any parts of the system that were excluded (and why).
- **Findings** You should group your findings to make them easier to search and read for your audience.
- **Recommendations** This section should mirror the organization of the Findings and provide the next steps from your analysis.
- **Appendices** You should include as much raw data as possible, but you certainly want to include enough to justify your recommendations

# Management Review and Approval

- A management review is a formal meeting of senior organizational leaders to determine whether the management systems are effectively accomplishing their goals. In the context of the CISSP, we are particularly interested in the performance of the ISMS (Information Security Management System) which is defined in the ISO27000 series of standards.
- These standards define a Plan-Do-Check-Act loop, as used by ISO and follows the cycle of continuous improvement.
- Senior management will decide to either approve the recommendations in their entirety, approve it with specific changes, reject the recommendation, or send the ISMS team back to either get more supporting data or redesign the options.

# Homework

- Read the relevant chapter in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Depending on which edition you have the relevant sections will be in different places – so use the index.

- Then identify and do the practice m/c questions relating to this subject.

# Questions?