CISSP
PROCESS GUIDE

V.18

After passing the CISSP exam, and for the purpose of benefiting others with the knowledge and experienced I gained during my study term, I have summarized the main basic concepts in a general overview. I am hoping this consolidation of core concepts and processes would benefit those interested in becoming members of the CISSP study group and the community.

The intention of this document is to be supplementary, not a replacement for officially published study guides and books. I may have added multiple definitions of the same process or procedure due to the varying definitions from different resources such as the Official CBK, Sybex, NIST publications, SANS papers, or the AIO Shon Harris books. If you encounter any conflicts, please refer to the latest Official CISSP CBK. Being a CISSP candidate you should fully understand CISSP concepts, methodologies and their implementations within the organization.

Please do not try any short cut when it comes to reading books and gaining knowledge. This quick reference should be utilized as a fast recap of security concepts. It's important that you read Official CISSP books first and then use these notes to get a recap of what you have read. I wish you good luck for the CISSP exam.

Fadi Sodah (aka madunix) CISSP CISA CFR ICATE
https://www.linkedin.com/in/madunix/
https://www.experts-exchange.com/members/madunix.html

Corporate Governance:

Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly.

- Auditing supply chains
- Board and management structure and process
- Corporate responsibility and compliance
- Financial transparency and information disclosure
- Ownership structure and exercise of control rights

Governance, Risk and Compliance (GRC):

The process of how an organization manages its information resources. This process usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions. It is designed to ensure the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated.

Areas of focus for IT Governance:

- Strategic alignment
- Value delivery
- Resource management
- Risk management
- Performance management

Governance vs. Management:

- Oversight vs. Implementation
- Assigning authority vs. authorizing actions
- Enacting policy vs. enforcing
- Accountability vs. responsibility
- Strategic planning vs. project planning
- Resource allocation vs. resource utilization

Note: Governance: (What do we need to accomplish). Governance typically focuses on the alignment of internal requirements, such as corporate policies, business objectives, and strategy. Management: (How)

The Importance of Following Infosec Standards:

Creating and using common, proven practices is an important part of a successful information security program. Not only do standards support proactive management and efficient risk mitigation, adopting and consistently following a standard can bring additional benefits to any organization.

• TRUST & CONFIDENCE. When organizations obtain certifications that demonstrate compliance, they create a sense of trust and confidence among employees and third parties with whom they interact.

• BETTER RESULTS. When you speak the same jargon, results are more productive, effective, and cohesive. E.g., vendor assessments can be smoother and faster with a formal infosec program in place.

• COMPETITIVE ADVANTAGE. Developing a formal infosec program and obtaining certification boosts client and stakeholder confidence in how infosec risks are managed and aligned with their own risk appetite.

• CORPORATE RESPONSIBILITY. Holding an infosec certification can help organizations demonstrate due diligence and due care, which are mandatory requirements for company officers and essential for mitigating corporate negligence.

Note: Information security standards offer best practices and share expert information. These standards allow organizations to adopt, tailor, and implement a valuable infosec program without having to hire fulltime experts, reinventing the wheel, and learning by trial and error, which is costly, time consuming and dangerous.

Challenges of implementing and maintaining standards:

• Time: Implementing and maintaining information security standards is not a one-time project. Rather, it is a process that requires dedicated, qualified personnel, support from senior leadership, and continuous monitoring and improvement. A successful effort will require buy-in from the entire organization.

• Cost: Standards can be expensive to implement and just as costly to maintain. In the case of ISO 27001, for example, in addition to the time and effort necessary to meet the standard requirements, organizations must budget for annual audit fees, which can be substantial.

• Buy-in: Senior leadership buy-in and program ownership at the C-level are critical elements for an organization to deploy an information security program effectively. The information security team must share metrics, report the effectiveness of the program, and demonstrate its value and strategic alignment with the organization's business objectives to maintain senior leadership support.

• Change management: In general, everyone appreciates the value of securing information until it requires a change. Security teams implementing standards are challenged to strike a delicate balance between security and convenience.

• Continuous improvement: Standards have life cycles. When a standard is updated, it is the responsibility of all compliant organizations to be aware of the updates and implement them by specified dates, or as soon as possible if a time line is not mandated. In some cases, a standard might become obsolete, and a new standard must be researched and presented to senior leadership for approval for implementation.

Main security requirements and their subcomponents:

- Network Security
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
- Identity Management
  - Authentication
  - Authorization
  - Accountability
  - Revocation
- Privacy
  - Data Privacy
  - Anonymity
  - Pseudonimity
  - Unlinkability
- Trust
  - Device Trust
  - Entity Trust
  - Data Trust
- Resilience
  - Robustness against attacks
  - Resilience against failures

CIA-AP:

• Confidentiality: The capability of limiting information access and disclosure to authorized clients only.
• Integrity: The capability of preserving the structure and content of information resources.
• Availability: The capability of guaranteeing continuous access to data and resources by authorized clients.
• Authenticity: The capability of ensuring that clients or objects are genuine.
• Privacy: The capability of protecting all information pertaining to the personal sphere of users.

Authorization approval procedure:

• Formalized
• Approval by the direct manager, data owner, security professional
• Access permissions follow the principle of least privilege
• Balance security with the need for access
• Avoid allowing too much privilege — Conflicts of interest
• Remove privilege when no longer needed

Business Impact Assessment (BIA):

A systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of exploitation, disaster, accident or emergency.

Key Metrics to establish BIA:

• SLO • RPO • MTD • RTO • WRT • MTBF • MTTR • MOR

Business Impact Assessment:

- Identify Priorities
- Identify Risk
- Likelihood Assessment
- Impact Assessment
- Resource prioritization

Note: Risk can never be mitigated to zero (there is no such thing as "no risk" or "perfect security")

Business Impact Analysis:

- Identify critical functions
- Identify critical resources
- Calculate MTD for resources
- Identify threats
- Calculate risks
- Identify backup solutions

Business Impact Analysis:

- Select individuals to interview for data gathering
- Create data-gathering techniques
- Identify critical business functions
- Identify resources these functions depend upon
- Calculate how long these functions can survive without these resources
- Identify vulnerabilities and threats
- Calculate the risk for each different business function
- Document findings and report them to management

Business Continuity Planning (BCP):

- Project Initiation
- Business Impact Analysis
- Recovery Strategy
- Plan design and development
- Implementation
- Testing
- Continual Maintenance

BCP (NIST 800-34):

- Develop planning policy;
- BIA
- Identify preventive controls
- Create contingency strategies
- Develop contingency plans
- Test
- Maintenance

WHY - Business Continuity Planning (BCP):

- Provide an immediate and appropriate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Work with outside vendors and partners during the recovery period
- Reduce confusion during a crisis
- Ensure survivability of the business
- Get "up and running" quickly after a disaster

DRP vs. BCP:

- BCP - Corrective Control
- DRP - Recovery Control
- Both BCP and DRP - fall under the category of Compensating Control
- BCP – is not a preventive control as it can NOT prevent a disaster
- BCP - helps in the continuity of organization function in the event of a disaster
- BCP - maintaining critical functions during a disruption of normal operations
- DRP - recovering to normal operations after a disruption

Business Continuity Planning (BCP):

- Continuity Policy
- Business Impact Assessment (BIA)
- Identify Preventive Controls
- Develop Recovery Strategies
- Develop BCP
- Exercise/Drill/Test
- Maintain BCP

DR Team:

- Rescue Team: Responsible for dealing with the immediacy of the disaster – employee evacuation, crashing the server room, etc.
- Recovery Team: Responsible for getting the alternate facility up and running and restoring the most critical services first.
- Salvage Team: Responsible for the return of operations to the original or permanent facility (reconstitution) – (get us back to the stage of normalcy)

Business Continuity Planning (BCP) Documents:

- Continuity of planning goals
- Statement of importance and statement of priorities
- Statement of Organizational responsibilities
- Statement of Urgency and Timing
- Risk assessment, Risk Acceptance, and Risk mitigation document
- Vital Records Program
- Emergency Response Guidelines
- Documentation for maintaining and testing the plan

DRP/BCP document plan should be:

- Created for an enterprise with individual functional managers responsible for plans specific to their departments
- Copies of the plan should be kept in multiple locations
- Both Electronic and paper copies should be kept
- The plan should be distributed to those with a need to know
- Most employers will only see a small portion of the plan

Business Continuity Planning (BCP):

- Project scope and planning
  - •• Business Organization Analysis
  - •• BCP team selection
  - •• Resource Requirements
  - •• Legal and regulatory requirements
- Business impact assessment
  - •• Identify priorities
  - •• Risk Identification
  - •• Likelihood Assessment
  - •• Impact Assessment
  - •• Resource Prioritization
- Continuity planning
  - •• Strategy Development
  - •• Provisions and Processes
  - •• Plan Approval
  - •• Plan Implementation
  - •• Training and Education
- Approval and implementation
  - •• Approval by senior management (APPROVAL)
  - •• Creating an awareness of the plan enterprise-wide (AWARENESS)
  - •• Maintenance of the plan, including updating when needed (MAINTENANCE)
  - •• Implementation

Development of Disaster Recovery Plan (DRP):

- Plan Scope and Objectives
- Business Recovery Organization (BRO) and Responsibilities (Recovery Team)
- Major Plan Components - format and structure
- Scenario to Execute Plan
- Escalation, Notification and Plan Activation
- Vital Records and Off-Site Storage Program
- Personnel Control Program
- Data Loss Limitations
- Plan Administration

Disaster Recovery Plan (DRP) procedures:

- Respond to disaster in accordance with a pre-defined disaster level
- Assess damage and estimate time required to resume operations
- Perform salvage and repair

Elements of Recovery Strategies:

- Business recovery strategy
  - Focus on the recovery of business operations
- Facility & supply recovery strategy
  - Focus on facility restoration and enable alternate recovery site(s)
- User recovery strategy
  - Focus on people and accommodations
- Technical recovery strategy
  - Focus on the recovery of IT services
- Data recovery strategy
  - Focus on the recovery of information assets

The eight R's of a successful Recovery Plan:

- Reason for planning
- Recognition
- Reaction
- Recovery
- Restoration
- Return to Normal
- Rest and Relax
- Re-evaluate and Re-document

Disaster Recovery Program:

- Critical Application Assessment
- Backup Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

Post-Incident Review:

The purpose is how we get better; after a test or disaster has taken place:

- Focus on how to improve
- What should have happened?
- What should happen next?
- Not who´s fault it was; this is not productive

Continuity Planning:

Normally applies to the mission/business itself; Concerns the ability to continue critical functions and processes during and after an emergency event.

Contingency Planning:

Applies to information systems, and provides the steps needed to recover the operation of all or part of the designated information system at an existing or new location in an emergency.

Business Continuity Plan (BCP):

BCP focuses on sustaining an organization's mission/business process during and after a disruption. It May be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allows.

Occupant Emergency Plan (OEP):

It outlines first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of the personnel, the environment, or property.

Cyber Incident Response Planning (CIRP):

It's A type of plan that normally focuses on detection, response, and recovery to a computer security incident or event. It establishes procedures to address cyber-attacks against an organization's information system(s).

Information System Contingency Plan (ISCP):

It provides established procedures for the assessment and recovery of a system following a system disruption. Provides key information needed for system recovery, including roles and responsibilities, inventory info, assessment procedures, detailed recovery procedures, and testing of a system.

Continuity of Operations Plan (COOP):

It focuses on restoring an organization's mission essential function of an alternate site and performing those functions for up to 30 days before returning to normal operations.

Disaster Recovery Plan (DRP):

Applies to major physical disruptions to service that deny access to the primary facility infrastructure for an extended period. An information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. Only addresses information system disruptions that require relocation.

The risks to the organization found in:

- Financial
- Reputational
- Regulatory

Risk Analysis:

- Analyzing the environment for risks
- Creating a cost/benefit report for safeguards
- Evaluating threat

Elements of risk:

- Threats
- Assets
- Mitigating factors

Risk Analysis methodology:

- CRAMM (CCTA Risk Analysis and Management Method)
- FMEA (Failure modes and effect analysis methodology)
- FRAP (Facilitated Risk Analysis Process)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- PUSH
- Spanning Tree Analysis
- SOMAP (Security Officers Management and Analysis Project)
- VAR (Value at risk)

RMF CSIAAM: (NIST 800-37)

The risk management framework (RMF) encompasses a broad range of activities to identify, control, and mitigate risks to an information system during the system development life cycle. One of the activities is the development of an ISCP. Implementing the risk management framework can prevent or reduce the likelihood of the threats and limit the consequences of risks. RMF include:

- Categorize the information system and the data
- Select an initial set of baseline security controls
- Implement the security controls and describe how the controls are employed
- Assess the security controls
- Authorize systems to be launched
- Monitor the security controls

Risk Management Process: (FARM)

- Framing risk
- Assessing risk
- Responding to risk
- Monitoring risk

Risk management Policy Document:

• Objectives of the policy and rationale for managing risk
• Scope and charter of information risk management
• Links between the risk management policy and the organizations strategic and corporate business plans-Extent and range of issues to which the policy applies
• Guidance on what is considered acceptable risk levels
• Risk management responsibilities
• Support expertise available to assist those responsible for managing risk
• Level of documentation required for various risk-management related activities, e.g., change management
• A plan for reviewing compliance with the risk management policy
• Incident and event severity levels
• Risk reporting and escalation procedures, format and frequency

Risk Management Life Cycle:

• Continuously monitoring
• Evaluating
• Assessing and reporting risk.

Risk management:

• Risk Assessment — Identify Assets, Threats Vulnerabilities
• Risk Analysis — Value of Potential Risk
• Risk Mitigation — Responding to Risk
• Risk Monitoring — Risk is forever

Risk management entails evaluating:

• Threats
• Vulnerabilities
• Countermeasures

Methodologies of Risk Assessment:

- Prepare for the assessment.
- Conduct the assessment:
  - Identify threat sources and events.
  - Identify vulnerabilities and predisposing conditions.
  - Determine the likelihood of occurrence.
  - Determine the magnitude of impact.
  - Determine risk.
- Communicate results.
- Maintain assessment.

Preparing Risk Assessment:

- Purpose of the assessment
- The scope of the assessment
- Assumptions and constraints associated with the assessment
- Sources of information to be used as inputs to the assessment
- Risk model and analytic approaches

Risk Assessment (NIST 800-30):

- System / Asst. Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation

Damage assessment:

• Determining the cause of the disaster is the first step of the damage assessment
• How long it will take to bring critical functions back online
• Identifying the resources that must be replaced immediately
• Declare a disaster

Damage assessment:

- Determine the cause of the disaster.
- Determine the potential for further damage.
- Identify the affected business functions and areas.
- Identify the level of functionality for the critical resources.
- Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated MTD values to restore operations, then a disaster should be declared and BCP should be put into action.

Note:

• The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.
• The final step in a damage assessment is to declare a disaster.
• The decision to activate a disaster recovery plan is made after damage assessment and evaluation is completed.

Configuration Management:

• Plan
• Approve Baseline
• Implement
• Control Changes
• Monitor
• Report
• Repeatable

Configuration Management:

- Configuration Identification
- Configuration Control
- Configuration Status Accounting
- Configuration Audit

Change Management:

- Request for a change to take place
- Approval of the change
- Documentation of the change
- Tested and presented
- Implementation
- Report change to management

Change Management:

- Request
- Review
- Approve
- Schedule
- Document

Change Management:

- Request
- Evaluate
- Test
- Rollback
- Approve
- Document
- Determine Change Window
- Implement
- Verify
- Close

Data Contamination Controls:

To ensure the integrity of data, there are two types of controls: input and output controls. Input controls consist of transaction counts, dollar counts, hash totals, error detection, error correction, resubmission, self-checking digits, control totals, and label processing. Output controls include the validity of transactions through reconciliation, physical-handling procedures, authorization controls, verification with expected results, and audit trails.

Phases of DITSCAP and NIACAP accreditation:

- Definition
- Verification
- Validation
- Post Accreditation

The Systems Development Life Cycle:

• Initiation (considers value, sensitivity, regulatory compliance, classification, etc. of application/data).
• Define Functional Requirements (documents user and security needs).
• Design Specifications (system architecture/software designed).
• Development/Implementation/Testing (source code and test cases generated, quality/reliability addressed).
• Documentation/Program Controls (controls related to editing data, logging, version, control, integrity checks, etc.).
• Certification/Accreditation (independently testing data/code ensuring requirement are met, data validation, bounds checking, sanitizing, management's authorization for implementation).
• Production/Implementation (systems are live).

SDLC:

• Project initiation and planning
• Functional requirements definition
• System design specifications
• Development and implementation
• Documentation and common program controls
• Testing and evaluation control, (certification and accreditation)
• Transition to production (implementation)

Note: The system life cycle (SLC) extends beyond the SDLC to include two:
• Operations and maintenance support (post-installation).
• Revisions and system replacement.

SDLC:

- Request/Gather information
  - •• Security risk assessment
  - •• Privacy risk assessment
  - •• Risk-level acceptance
  - •• Informational, functional, and behavioral requirements
- Design
  - •• Attack surface analysis + Threat modeling
- Develop
  - •• Automated CASE tools + Static analysis
- Test/Validation
  - •• Dynamic analysis + Fuzzing + Manual Testing
  - •• Unit, integration, acceptance, and regression testing
- Release/Maintenance
  - •• Final security review

Note: Fuzz testing used to describe the use of known bad or randomized inputs to determine what unintended results may occur.

SDLC 10 phases:

- Initiation- Identifying the need for a project
- System Concept Development- Defining the project scope and boundaries
- Planning- Creating the project management plan
- Requirements Analysis- Defining user requirements
- Design- Creating a Systems Design Document that describes how to deliver the project
- Development- Converting the design into a functional system
- Integration and Test- Verifying that the system meets the requirements
- Implementation- Deploying the system into the production environment
- Operations and Maintenance- Monitoring and managing the system in production
- Disposition - Migrating the data to a new system and shutting the system down

The Cloud Secure (SDLC)

- Defining
- Designing
- Development
- Testing
- Secure Operations
- Disposal

Insecure code practices:

- Comments in source code
- Lack of error handling
- Overly verbose error handling
- Hard-coded credentials
- Race conditions
- Unauthorized use of functions/unprotected APIs
- Hidden elements
- Sensitive information in the DOM
- Lack of code signing

Systems Development Life Cycle:

• Initiation: During the initiation phase, the need for a system is expressed and the purpose of the system is documented.
• Development/Acquisition: During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed.
• Implementation/Assessment: After system acceptance testing, the system is installed or fielded.
• Operation/Maintenance: During this phase, the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.
• Disposal: Activities conducted during this phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

Security Considerations in SDLC:

- Prepare a Security Plan
- Initiation
  - Survey & understand the policies, standards, and guidelines
  - Identify information assets (tangible & intangible)
  - Define information classification & the protection level (security categorization)
  - Define rules of behavior & security
  - Conduct preliminary risk assessment
- Development/Acquisition
  - Determine Security Requirements
  - Conduct risk assessment
  - Perform cost/benefit analysis
  - Incorporate Security Requirements into Specifications
  - Security planning (based on risks & CBA)
  - Obtain the System and Related Security Activities
  - Develop security test
- Implementation
  - Install/Turn on Controls
  - Security Testing
  - Perform Security Certification & Accreditation of the target system.
- Operation/Maintenance
  - Security Operations and Administration
  - Operational Assurance
  - Audits and Continuous monitoring
  - Configuration management & performs change control
- Disposal
  - Information transfer or destruction
  - Media Sanitization
  - Dispose of hardware

Systems Development Life Cycle:

- Conceptual definition
- Functional requirements determination
- Control specifications development
- Design review
- Code review walk-through
- System test review
- Maintenance and change management

Forensic

The forensic investigation process must demonstrate that information handling procedures and actions performed did not alter the original data throughout the custody chain. This may include:

- Recording the name and contact information of those charged with maintaining a chain of custody
- Details of the timing of the event
- Purpose of moving the data
- Identification of evidence through recording of serial numbers and other details
- Sealing the evidence with evidence tape
- Documenting the location of storage
- Documenting the movement of the information

Concepts unique to the forensic analysis:

- Authorization to collect information
- Legal defensibility
- Confidentiality
- Evidence preservation and evidence security
- Law enforcement involvement

Forensic Process:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Generic Computer Forensic Investigation Model:

- Pre-process
- Acquisition and preservation
- Analysis
- Presentation
- Post-process

E-discovery Process:

- Information Governance
- Identification
- Preservation
- Collection
- Processing
- Review
- Analysis
- Production
- Presentation

CSIRT:

Organizations will often form a cybersecurity incident response team (CSIRT) to help identify and manage information security incidents. The individuals that make up the CSIRT are trained in proper collection and preservation techniques for investigating security incidents. National Institute of Standards and Technology Special Publication (NIST SP) 800-61r2 identifies the following models for organizing such a team.

• Central team One team handles incidents on behalf of the entire organization.

• Distributed team For larger or geographically dispersed organizations, it may be more appropriate to have individual CSIRTs for different segments of the organization or different geographic locations.

• Coordinating team An overarching central team can be added to provide guidance and coordination among distributed teams.

CSIRT Tools:

The CSIRT has a number of tools they can use to help handle security incidents. Keeping the toolkit up-to-date will contribute to the CSIRT working optimally. The following table lists a few common examples.

• The Sleuth Kit (TSK) / Cross-platform
• EnCase / Windows
• Forensic Toolkit (FTK) / Windows
• Forensics Explorer / Windows
• SANS Investigative Forensic Toolkit (SIFT) / Ubuntu (Linux)
• Digital Forensics Framework (DFF) / Cross-platform
• Computer Online Forensic Evidence Extractor (COFEE) / Windows
• WindowsSCOPE / Windows
• HashMyFiles / Windows
• Volatility / Windows, Linux
• TestDisk / Cross-platform
• Wireshark / Cross-platform

Data Classification Scheme:

- Identify custodian
- Specify evaluation criteria
- Classify and label each resource
- Document any exceptions
- Select security controls
- Specify the procedures for declassifying
- Create enterprise awareness program

Data Classification:

- Scope (value, Age)
- Classification Controls
- Assurance
- Marking and labeling

Classify Information:

- Specify the classification criteria
- Classify the data
- Specify the controls
- Publicize awareness of the classification controls

Classification program:

- Define classification level
- Identify owner
- Determine security level
- Develop a procedure to declassifying

Data Classification Procedures:

- Define classification levels.
- Specify the criteria that will determine how data are classified.
- Identify data owners who will be responsible for classifying data.
- Identify data custodian who will be responsible maintaining data and sec. level.
- Indicate the security controls, protection mechanisms, required for each class level
- Document any exceptions to the previous classification issues.
- Indicate the methods that can be used to transfer custody of info to diff owner.
- Create a procedure to periodically review the classification and ownership.
- Communicate any changes to the data custodian.
- Indicate procedures for declassifying the data.
- Integrate these issues into the security-awareness program

The goal of Incident Handling and Response Planning:

- Detects compromises as quickly and efficiently as possible.
- Responds to incidents as quickly as possible.
- Identifies the cause as effectively as possible.

Purpose of incident response:

- Restore normal service
- Minimize impact on business
- Ensure service quality and availability are maintained

Incident Response:

- Triage (assesses the severity of the incident and verify)
- Investigation (contact law enforcement)
- Containment (limit the damage)
- Analysis
- Tracking

Incident Response:

- Preparation
- Detection -- Identification
- Response -- Containment
- Mitigation
- Reporting -- Report to Sr. Management
- Recovery -- Change Management & Configuration. Management
- Remediation -- RCA & Patch M. & Implement controls
- Lessons Learned -- Document and knowledge transfer

Incident Response:

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Post Incident Review/Lesson learned

Incident Handling Steps: NIST 800-61

- Preparation People
- Identification Identify
- Containment Containers
- Eradication Ending
- Recovery Real
- Lessons Learned Lives

Incident response process: PIC-ERL

- Preparation
- Identification
    - Detection/analysis
    - Collection
- Containment
- Eradication
- Recovery
- Post-incident
    - Lessons learned
        - Root cause analysis
    - Reporting and documentation

Note: Gap analysis includes reviewing the organization's current position/performance as revealed by an audit against a given standard.

Incident Response Process:

- Plan for and identify the incident.
- Initiate incident handling protocols.
- Record the incident.
- Evaluate and analyze the incident.
- Contain the effects of the incident.
- Mitigate and eradicate the negative effects of the incident.
- Escalate issues to the proper team member, if applicable.
- Recover from the incident.
- Review and report the details of the incident.
- Draft a lessons-learned report.

Incident Response Plans Models

•• Compliance Driven

- Designed to evaluate a response after the fact.
- Reflects an approach from an audit and compliance (HIPAA, GLBA, PCI-DSS).
- Security engineers and analysts do not refer to them during an incident, except possibly in retrospective reports.

•• Technical Driven

- Elaborate playbooks that communicate techniques for data analysis and are often unwieldy and intentionally vague about accountability.
- Developed by security or network engineers, but can be frustrating when evaluating a response to reports to the Board of Directors or executives.

•• Coordinated (Compliance Driven + Technically Driven)

- Provides a framework for activities where they are more ambiguous: between teams and roles. The coordinated plan describes communication and authority so they are not in question during an incident, but also allows the expertise of a team to be applied without micromanagement by the plan.

Incident Response Plans:

A usable IR plan is dynamic enough to address many incidents, but simple enough to be useful. Some characteristics of a plan are:

• Brief During an incident, there is little time to read and understand large documents and find highlighted portions that may be relevant.

• Clear Incidents are complex and often, are not well understood in the beginning.

• Resilient Rigid and prescriptive incident response plans can fail when key participants are absent.

• Living This is not just a plan to be reviewed and (potentially) updated once annually.

Incident investigation methodology:

- Analysis and Imaging
- Dead box forensics
- Volatile data collection
- Server handling
- Endpoint imaging
- Live system handling (Volatile data collection)
- Write-block
- Controlled forensic boot (Volatile data considerations)

Vulnerability management:

- Inventory
- Threat
- Asses
- Prioritize
- Bypass
- Deploy
- Verify
- Monitor

Vulnerability Assessment:

- Collect
- Store
- Organize
- Analysis
- Report

Consideration of vulnerability scanning

- Time to run a scan
- Protocols used
- Network topology
- Bandwidth limitations
- Query throttling
- Fragile systems/non-traditional assets

Information Security Continuous Monitoring:

- Define
- Establish
- Implement
- Analyze
- Respond
- Review
- Update
- Repeat

Threat Modelling:

- Assessment scope
- System Modeling
- Identify Threat
- Identify Vulnerability
- Exam Threat history
- Impact
- Response

Threat modeling: (STRIDE)

- Spoofing: Attacker assumes the identity of the subject
- Tampering: Data or messages are altered by an attacker
- Repudiation: Illegitimate denial of an event
- Information Disclosure: Information is obtained without authorization
- Denial of Service: Attacker overload system to deny legitimate access
- Elevation of Privilege: Attacker gains a privilege level above what is permitted

Generic Threat Modeling:

- Assessment Scope
- System Modeling
- Identify Threats
- Identify Vulnerabilities
- Examining the Threat History
- Evaluation of Impact on the Business
- Developing a Security Threat Response Plan

Change control:

- Implement changes in a monitored and orderly manner.
- Changes are always controlled
- Formalized testing
- Reversed/rollback
- Users are informed of changes before they occur to prevent loss of productivity.
- The effects of changes are systematically analyzed.
- The negative impact of changes in capabilities, functionality, performance
- Changes are reviewed and approved by a CAB (change approval board).

Problem Management:

- Incident notification
- Root cause analysis
- Solution determination
- Request for change
- Implement solution
- Monitor/report

Vulnerability assessment and PT testing:

- Scope
- Information gathering
- Vulnerability detection
- Information analysis and planning
- Penetration testing
- Privilege escalation
- Result analysis
- Reporting
- Cleanup

Note: Vulnerability assessments should be done on a regular basis to identify new vulnerabilities. VA scanners usually don't have more than a Reading privilege.

Botnet

- A Botnet is a number of different devices connected together and controlled as a group without the owners knowledge.
- The botnet owner can control the botnet using command an control (C&C) software.
- The word "botnet" is a combination of the words "robot" and "network."

Information systems auditor:

• Audits information security activities for compliance; Verifies adherence to security objectives, policies, procedures, standards, regulations, and related requirements.
• Verifies whether information security activities are managed and operated to ensure achievements of state security objectives.
• Provides independent feedback to senior management.

Auditing uses:

• Record review
• Adequacy of controls
• Compliance with policy
• Detect malicious activity
• Evidence of persecution
• Problem reporting and analysis

Audit:

The systematic process by which a competent, independent person objectively obtains and evaluates the evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards. Audit: Evaluate security controls - Report on their effectiveness - Recommend improvements

Audit plan:

• Define audit objectives
• Define the audit scope
• Conduct audit
• Refine the audit process

Audit Process:

- Determine goals
- Involve right business unit leader
- Determine Scope
- Choose audit Team
- Plan audits
- Conduct audit
- Document result
- Communicate result

Audit Report:

- Purpose
- Scope
- Results discovered or revealed by the audit
- Problems, events, and conditions
- Standards, criteria, and baselines
- Causes, reasons, impact, and effect
- Recommended solutions and safeguards

IT security audit is designed to find:

- Malfunctioning controls
- Inadequate controls
- Failure to meet target standards/guidelines

Capability Maturity Model (IRDMO):

- Initial Stage - unpredictable, poorly controlled, and reactive
- Repeatable Stage - characterized for projects, repeatable
- Defined Stage - characterized by the entire organization and is proactive.
- Managed Stage - quantitatively measured and controlled
- Optimizing the Stage - continuous improvement. (Budget)

Capability Maturity Model (IRDMO):

• Level 1: Initial - The software development process is characterized as ad-hoc. Success depends on individual effort and heroics.
• Level 2: Repeatable -Basic project management (PM) processes are established to track performance, cost, and schedule.
• Level 3: Defined - Tailored software engineering and development processes are documented and used across the organization.
• Level 4: Managed - Detailed measures of product and process improvement are quantitatively controlled.
• Level 5: Optimizing - Continuous process improvement is institutionalized.

Information Systems Security Engineering (ISSE) Process:

• Discover Information Protection Needs; ascertain the system purpose. Identify information asset needs protection.
• Define System Security Requirements; Define requirements based on the protection needs.
• Design System Security Architecture; Design system architecture to meet security requirements.
• Develop Detailed Security Design; Based on security architecture, design security functions and features of the system.
• Implement System Security; Implement designed security functions and features into the system.
• Assess Security Effectiveness; Assess the effectiveness of ISSE activities.

Patch management:

- Inventory
- Allocate Resources
- Pursue updates
- Test
- Change Approval
- Deployment plan
- Rollback plan
- Deploy and verify the updates with policy requirements
- Document

Patch management:

- Patch Information Sources
- Prioritization
- Scheduling
- Testing
- Installation
- Assessment
- Audit
- Consistency
- Compliance

Patch management:

- Evaluate
- Test
- Approve
- Deploy
- Verify

Required for accountability:

- Identification
- Authentication
- Auditing

Policy:

- Organizational (or Master) Policy
- System-specific Policy
- Issue-specific Policy

Software-Defined Everything (SDx)

Extension of virtualization that abstracts an application or function from its underlying hardware, separating the control and data planes and adding programmability. Beginning with software-defined networking (SDN), SDx now encompasses software defined storage (SDS), software-defined computing, software-defined security, and software-defined data centers (SDDC), among others.

Software-Defined networking (SDN):

- Application
- Control
- Infrastructure

Software-Defined networking (SDN):

- Network administrators can adjust network traffic on the fly.
- They provide you with the ability to better detect network traffic anomalies.
- They add a higher level of complexity to the network that requires special skills.

OECD:

Organization for Economic Cooperation and Development (OECD) suggests that privacy laws include:

- Collection limitation principle
- Data quality principle
- Purpose specification principle
- Use limitation principle
- Security safeguards principle
- The openness principle

Social Engineering:

It's important for any user to understand social engineering and their tactics. Additionally, by understanding the underlying principles, it becomes easier to avoid being tricked by them. The following sections introduce these principles.

- Authority
- Intimidation
- Consensus / Social Proof
- Scarcity
- Urgency
- Familiarity/Liking
- Trust

API – formats:

- Representational State Transfer (REST) - is a software architecture style, consisting of guidelines and best practices for creating scalable web services.
- Simple Object Access Protocol (SOAP) - is a protocol specification for exchanging structured information in the implementation of web services in computer networks

Media control:

- Accurately and promptly mark all data storage media
- Ensure proper environmental storage of the media
- Ensure the safe and clean handling of the media
- Log data media to provide a physical inventory control

Enterprise Security Architecture (ESA):

- Presents a long-term, strategic view of the system
- Unifies security controls
- Leverages existing technology investments

Third Party Contracts:

- NDA/NDC
- Regulatory Compliance
- Incident notification
- SLA/SLC

Evaluate the Third party:

- On-Site Assessment
- Document Exchange and Review
- Process/Policy Review

Security Policy:

- Define the scope
- Identify all assets
- Determine level of protection
- Determine personal responsibility
- Develop consequences for noncompliance

Common Criteria CC:

- PP - what the customer needs
- ST - what Vendor provides
- TOE - The actual product
- EAL - Rating which provides Evaluation and Assurance

Note: The EAL is a measure of how thoroughly the security features the product vendor claims the product offers have been tested and reviewed, and by whom. The EAL does not offer any true measure of how well those security features will work in a production environment, whether those features are preferable to other features offered by competing products, or whether the product is "good."

EAL: FSM2S2F

- EAL1 - Functionally tested (lowest rating)
- EAL2 - Structurally tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed (medium rating)
- EAL5 - Semi-formally designed and tested
- EAL6 - Semi-formally verified, designed and tested
- EAL7 - Formally verified, designed and tested (highest rating)

Documentation:

All documentation should be subject to an effective version control process as well as a standard approach to marking and handling; and conspicuously labeled with classification level, revision date and number, effective dates, and document owner.

Cryptography:

- Privacy
- Authentication
- Integrity
- Non-repudiation

Data archiving:

• Format
• Regulatory requirements
• Testing

RUM vs Synthetic:

• RUM harvests information from actual user activity, making it the most realistic depiction of user behavior.
• Synthetic monitoring approximates user activity, but is not as exact as RUM

Before selecting a Security Monitoring Tool type:

• It should collect information from numerous sources.
• It should be able to inter-operate with other systems, such as a help desk or change management program.
• It should comply with all relevant laws and industry regulations.
• It should offer scalable reporting so you get both a high-level and low-level perspective on your security

Security information and event management (SIEM):

• Correlation
• Compliance
• Alert

Tasks may be performed automatically for you with tools such as SIEMs:

- Filter out unnecessary or duplicate data
- Combine sources
- Synchronize events logged in different sources
- Normalize data formats
- Store data securely
- Data Collection, Analysis, and Correlation

SIEM on Cloud ....the benefits are

- No capital expenditure
- No need to invest on premise machines
- No need to invest in technical support for hardware
- No installation charges
- Only fine tuning
- Upgrades rolled out automatically by the cloud provider

Software requirements:

- Informational model
- Functional model
- Behavioral model

Attacks Phase:

- Gaining Access
- Escalating Privileges
- System Browsing
- Install Additional Tools
- Additional Discovery

API Security:

- Use same security controls for APIs as for any web application on the enterprise.
- Use Hash-based Message Authentication Code (HMAC).
- Use encryption when passing static keys.
- Use a framework or an existing library to implement security solutions for APIs.
- Implement password encryption instead of a single key-based authentication.

Key Performance Indicator KPI based on:

- BIA
- Effort to implement
- Reliability
- Sensitivity

Note: SLAs are often a subset of KPI

Security Programs Metrics:

- KPI looks backward at historical performance
- KRI looks forward, show how much risk exists that may jeopardize the future security of the organization.

Software Protection Mechanisms:

- Security Kernels
- Processor privilege states
- Security controls for buffer overflow
- Controls for incomplete parameter check and enforcement
- Memory protection
- Covert channel controls
- Cryptography
- Password protection techniques

Software Acquisition:

- Planning
- Contracting
- Monitoring
- Acceptance
- Follow on

Endpoint Protection:

- Built-in firewall functionality.
- Intrusion detection system (IDS) /intrusion prevention system (IPS) functionality.
- Data loss prevention (DLP) functionality.
- Application whitelisting / blacklisting functionality.
- Full disk encryption.
- Management interfaces for configuration of each endpoint or groups of endpoints.
- A centralized in-house server for distributing malware signature updates.

Note: A discovery tool is a primary component of a DLP solution. This might be employed for purposes of identifying and collecting pertinent data.

Prevent SQL Injection (SQLi):

- Perform Input Validation
- Limit Account Privileges
- Use Stored Procedures

In a SQL injection attack, an attacker could:

- Harvest and crack password hashes
- Delete and modify customer records
- Read and write system files

Injection attacks:

SQL injection attack consists of insertion or "injection" of a SQL query via the input
• HTML injection is a type of injection issue that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page
• Command injection is an attack in which the goal is the execution of arbitrary commands on the host operating system via a vulnerable application
• Code injection allows the attacker to add his own code that is then executed by the application.

Wireless and RF Vulnerabilities:

• Evil Twin
• Karma Attack
• Downgrade attack
• Dauth. Attack
• Fragmentation Attack
• Credential Harvesting
• WPS Implementation Weakness
• Bluejacking
• Bluesnarfing
• RFID Cloning
• Jamming
• Repeating

Basic MALWARE Analysis:

• Malware assessment
• String analysis
• Dependency analysis
• Encountering files with wiped logical data
• Sandbox analysis
• Online malware scanner / sandbox

Security of Logs:

• Control the volume of data
• Event filtering or clipping level determines the amount of log
• Auditing tools can reduce log size
• Establish procedures in advance
• Train personnel in pertinent log review
• Protect and ensure unauthorized access
• Disable auditing or deleting/clearing logs
• Protect the audit logs from unauthorized changes
• Store/archive audit logs securely

The four tiers are named as follows:

• Tier I: Basic Data Center Site Infrastructure
• Tier II: Redundant Site Infrastructure Capacity Components
• Tier III: Concurrently Maintainable Site Infrastructure
• Tier IV: Fault-Tolerant Site Infrastructure

Storage Area Network (SAN) security issues

SANs are high-speed networks that combine a variety of storage technologies, including tapes, disk arrays, and optical drives to provide network-attached storage to appear as if it is local. These devices can usually support disk mirroring, sharing data between servers across networks, and backup/restore operations.

• Storage Area Network access control

Authentication / Authorization / Encryption / Availability

• Fiber Channel Storage Area Network attacks

Session hijacking / LUN masking attacks / Man In The Middle Attack (MITM) / name server pollution / WWN spoofing / zone hopping / switch attack

• Internet Small Computer System Interface attacks

Man-in-the-middle Attack / Internet Simple Name Server Domain Hopping / Authentication Attack.

WLAN attacks:

- Confidentiality Attacks
  - Traffic Analysis
  - Eavesdropping
  - Man-in-the-Middle Attack
  - Evil Twin AP
- Access Control Attacks
  - War Driving
  - Rogue Access Point
  - MAC addresses spoofing
  - Unauthorized Access
- Integrity Attacks
  - Session Hijacking
  - Replay Attack
  - Frame Injection Attack
- Availability Attacks
  - Denial-of-Service Attack
  - Radiofrequency (RF) Jamming
  - Beacon Flood
  - Associate/Authentication Flood
  - De-authentication & Disassociation
  - Queensland DoS / Virtual carrier-sense attack
  - Fake SSID
  - AP theft
- Authentication Attack
  - Dictionary & Brute force attack

Authentication and Authorization Protocols:

- SAML:
  - Authentication and Authorization/Enterprise
  - Single sign-on for enterprise users
- SPML:
  - Account Provisioning/Account Management, SPML paired with SAML
- XACML:
  - Control policies
- OAuth:
  - Resource Access integrated with OpenID
  - API authorization between applications
- OpenID:
  - Authentication and Authorization/Commercial/Mobile App
  - Single sign-on for consumers

OAuth Flow:

- Ask for a request token
- Get Temporary credentials
- Exchange for an access token

Basic TCB function:

- Process activation
- Execution domain switching
- Memory protection
- I/O operation

Memory Manager:

- Relocation
- Protection
- Sharing
- Logically Organization
- Physical Organization

Memory Protection:

- DEP (Data Execution Prevention)
- ASLR (Address Space Layout Randomization)
- ACL (Access Control List)

Memory Protection:

- Segmentation
- Paging
- Protection keying

The Life Cycle of any Process:

- Plan and organize
- Implement
- Operate and maintain
- Monitor and evaluate

Fire extinguishers:

- Class A - used for ordinary combustibles, paper, wood, cardboard, etc.
- Class B - used for flammable liquids, gasoline, kerosene, oil, etc.
- Class C - used in electrical equipment, appliances, wires, etc.
- Class D - used for combustible metals, magnesium, titanium, potassium, etc.

Attacks (Mitigation):

- Eavesdropping (encryption)
- Cyber-squatting (Secure your domain registration)
- SPAM (email filtering)
- Teardrop (patching)
- Overlapping fragment (not allowing fragments to overwrite)
- Source routing Attack (block source-routed packets)
- SYN flood Attack (vendor support in securing network stack)
- Spoofing (patching, firewalls, strong authentication mechanisms)
- Session hijacking (encryption, regular re-authentication)

Facility Attacks

- Piggybacking
- Fence jumping
- Dumpster diving
- Lockpicking
- Lock bypass
- Egress sensor
- Badge cloning

Data exfiltration:

- Covert channels
- File sharing services

Man-in-the-middle:

- ARP spoofing
- ICMP redirect
- DHCP spoofing
- NBNS spoofing
- Session hijacking
- DNS poisoning

Isolating CPU processes:

- Encapsulation of objects
- Time multiplexing of shared resources
- Naming distinctions
- Virtual memory mapping

Security mechanisms:

- I/O operations
- Process activation
- Domain switching
- Memory protection
- Hardware management

Capture Security Requirement:

- Threat modeling
- Data classification
- Risk assessments

Data removal:

- Erasing - delete operation
- Clearing - overwriting operation
- Purging - more intensive form of clearing by repetition
- Declassification - purge media to be suitable for use for the secure environment
- Sanitization - a combination of a process that removes data from a system or media
- Degaussing - use of a strong magnetic field
- Destruction - crushing, Incineration, Shredding, disintegration

Emergency-Response Guidelines include:

- Immediate response procedures
- List of the individuals who should be notified of the incident
- Secondary response procedures that first responders should take

ISC2 - Code of Ethics:

- Protect Society, Commonwealth Infrastructure
- Act honorably, honestly, justly, responsibly and legally
- Provide diligent, competent service to the Principles
- Advance and protect the profession

Background checks:

- Credit History
- Criminal History
- Driving Records
- Drug and Substance Testing
- Prior Employment
- Education, Licensing, and Certification Verification
- Social Security Number Verification and Validation
- Suspected Terrorist Watch List

Hacking Website: (Deface Websites)

- SQL injection
- XSS / CSRF
- Remote file inclusion
- Local file inclusion
- DDOS
- Exploiting vulnerability
- Directory traversal
- Command injection

Penetration Test: D En V E R

• Discovery - Obtain the footprint and information about the target.
• Enumeration - Perform ports scans and resource identification.
• Vulnerability mapping - Identify vulnerabilities in systems and resources.
• Exploitation - Attempt to gain unauthorized access by exploiting the vulnerabilities.
• Report - Report the results to management with suggested countermeasures

Main sections defined by the standard as the basis for penetration testing execution:

• Pre-engagement Interactions
• Intelligence Gathering
• Threat Modeling
• Vulnerability Analysis
• Exploitation
• Post Exploitation
• Reporting

Penetration Test:

• Goal
• Recognizance
• Discovery
• Exploitation
• Brute-Force
• Social Engineering
• Taking Control
• Pivoting
• Evidence
• Reporting
• Remediation

Penetration Testing:

- External testing
- Internal testing
- Blind testing - Limited information on the PT team
- Double-blind testing - No information to the internal security team
- Targeted testing - Both internal and PT team aware.

Penetration Testing:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

Penetration Testing:

- Performing basic reconnaissance to determine system function
- Network discovery scans to identify open ports
- Network vulnerability scans to identify unpatched vulnerabilities
- Web application vulnerability scans to identify web application flaws
- Use of exploit tools to automatically attempt to defeat the system security
- Manual probing and attack attempts

Penetration Testing Techniques:

- Wardriving/dialing
- Eavesdropping
- Network sniffing
- Physical security testing
- Social engineering

Penetration Testing Rules of Engagement:

• Identifies and fines the appropriate testing method(s) and techniques with exploitation of the relevant devices and/or services
• While scope defines the start and the end of an engagement, the rules of engagement define everything in between

Rules of engagement (ROE)

• Introduction
• Logistics
• Communication
• Targets
• Execution
• Reporting
• Signatures

There are a few elements that are common to most effective pen testing reports:

- Preparation:
    - •• Identify the objectives and purpose of the penetration test.
    - •• Consider how best to address the audience you are writing to.
    - •• Ensure that you can place all relevant events in the context of time.
- Content:
    - •• Detail the test methodology you used in your tests.
    - •• Detail the results of each test, identifying specific assets and vulnerabilities that you id
- Provide your analysis and interpretation of the results.
- Suggest remediation techniques to employ.
- Formatting:
    - •• Format your report to comply with all of the applicable government regulations and with standards.
    - •• Write in clear, practical language. Avoid technical jargon.
    - •• Format your report with groups and sections to enhance readability.
- Reviewing:
    - •• Proofread your document before sending it out.
    - •• Ask another expert to provide a second opinion on the report before sending it out.

Enumeration:

- Extracting usernames using emails IDs, default passwords
- Extracting usernames using SNMP
- Extracting information using DNS zone transfer, Finger OS, and ports

Firewall:

- 1st generation: Packet filtering firewalls.
- 2nd generation: application (proxy) firewalls
- 3rd generation: state full packet firewalls
- 4th generation: dynamic filtering
- 5th generation: kernel proxy

Firewall Logs:

- Connections permitted or denied
- IDS activity
- Address translation audit trail
- User activity
- Cut-through-proxy activity
- Bandwidth usage
- Protocol usage

Fire suppression:

- Wet systems - constant water supply;
- Dry systems - valve releases when stimulated by heat;
- Pre-action systems - water held back until detectors activate;
- Deluge systems - sprinkler heads in an open position;

Threats to the DNS Infrastructure:

• Footprinting
• Denial-of-Service Attack
• Data modification
• Redirection
• Spoofing

Attacks against DNS servers:

• Zone transfer: Information gathering shortcut
• Zone poisoning: Breach primary server and alter the zone file to the corrupt domain
• Cache poisoning: Send false answers to cache servers until they store them
• Reflection DoS: Send bogus requests into a chain of servers that do recursive queries

Reduce XSS:

• Data validation
• Data Sanitization
• Cookies security
• Output Escaping

The PCI Data Security Standard goals:

• Build and Maintain a Secure Network
• Protect Cardholder Data
• Maintain a Vulnerability Management Program
• Implement Strong Access Control Measures
• Regularly Monitor and Test Networks
• Maintain an Information Security Policy

Note: PCI DSS allows for cardholder information at rest to be secured with either tokenization or encryption, but the use of one is mandatory.

Outsourcing:

• Ensuring that the organization has appropriate controls and processes in place to facilitate outsourcing.
• Ensuring that there are appropriate information risk management clauses in the outsourcing contract.
• Ensuring that a risk assessment is performed for the process to be outsourced.
• Ensuring that an appropriate level of due diligence is performed prior to contract signature.
• Managing the information risk for outsourced services on a day to day basis
• Ensuring that material changes to the relationship are flagged and new risk assessments are performed as required.
• Ensuring that proper processes are followed when relationships are ended.

Mobile devices are prime vectors for data loss; areas the professional should focus on:

• Secure communications
• Antimalware
• Strong authentication
• Passwords
• Control 3rd party software
• Separate secure mobile gateways
• Lockdown, audits
• Penetration tests
• Mobile security policy

Basic Types of Mobile Threats:

• Denial of service Deny or degrade service to users. Jamming of wireless communications, overloading networks with bogus traffic, ransomware, theft of mobile devices or mobile services.

• Geolocation Physical tracking of users. Passively or actively obtaining accurate three-dimensional coordinates of target, possibly including speed and direction.

• Information disclosure Unauthorized access to information or services. Interception of data in transit, leakage or exfiltration of users, app, or enterprise data, tracking of user location, eavesdropping on voice or data communications, surreptitiously activating the phone's microphone or camera to spy on the user.

• Spoofing Impersonating something or someone. Email or SMS message pretending to be from the boss or colleague (social engineering); a fraudulent Wi-Fi access point or cellular base station mimicking a legitimate one.

• Tampering Modifying data, software, firmware, or hardware without authorization. Modifying data in transit, inserting tampered hardware or software into the supply chain, repackaging legitimate apps with malware, modifying network or device configuration (e.g., jailbreaking or rooting a phone).

Regression and Acceptance Testing include:

- Test fixed bugs promptly.
- Watch for side effects of fixes.
- Write a regression test for each bug fixed.
- If two or more tests are similar, determine which is less effective and get rid of it.
- Identify tests that the program consistently passes and archive them.
- Focus on functional issues, not those related to design.
- Make changes (small and large) to data and find any resulting corruption.
- Trace the effects of the changes on program memory.

Data Retention policy in cloud:

- Regulation
- Data mapping
- Data Classification
- Procedures
- Monitoring and maintenance

Retention policies should address:

- Storage
- Retention
- Destruction / Disposal

8 steps Data retention:

- Evaluate Statutory Requirements, Litigation obligations, and business needs
- Classify types of records
- Determine retention periods and destruction policies
- Draft and justify record retention policy
- Train staff
- Audit retention and destruction practices
- Periodically review policy
- Document policy, implementation, training, and audits

System engineering management:

- Decision Analysis
- Technical Planning
- Assessment Requirements
- Configuration, Interface
- Technical Data
- Risk Management

Cyber Kill Chain:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

Cybersecurity Framework:

• Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

• Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

• Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

• Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

• Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

Attacks (1):

• Passive Attacks – hard to detect because the attacker is not affecting the protocol. Examples are Eavesdropping, network sniffing, and capturing data as it passes, used to gather data prior to an active attack.

• Active Attacks – Altering messages, modifying system files, and masquerading are examples because the attacker is actually doing something.

• Ciphertext Attacks - The attacker obtains ciphertext of several messages, with each message being encrypted using the same encryption algorithm. Attacker's goal is to discover the key. Most common attacks are easy to get ciphertext, but hardest attack to be successful at.

• Known-Plaintext Attack - The attacker has the ciphertext of several messages, but also the plaintext of those messages. The goal is to discover the key by reverse-engineering and trial/error attempts

• Chosen Plaintext Attack - The attacker not only has access to the ciphertext and associated plaintext for several messages, he also chooses the plaintext that gets encrypted. More powerful than a known-plaintext attack because the attacker can choose specific plaintext blocks to encrypt, ones that might yield more info about the key.

• Chosen-Ciphertext Attack: Attacker can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. This is a harder attack to carry out, and the attacker would need to have control of the system that contains the cryptosystem

• Adaptive Attacks: Each of the attacks has a derivative with the word adaptive in front of it. This means that an attacker can carry out one of these attacks, and depend on what is gleaned from the first attack, the next attack can be modified. This is the process of reverse-engineering or cryptanalysis attacks.

Attacks (2):

• Birthday attack: a Cryptographic attack that exploits the math behind the birthday problem in the probability theory forces collisions within hashing functions.

• Brute force attacks: continually tries different inputs to achieve a predefined goal. Brute force is defined as “trying every possible combination until the correct one is identified".

• Buffer overflow: Too much data is put into the buffers that make up a stack. Common attacks vector are used by hackers to run malicious code on a target system.

• Cross-site scripting: refers to an attack where vulnerability is found on a website that allows an attacker to inject malicious code into a web application

• Dictionary attacks: Files of thousands of words are compared to the user’s password until a match is found.

• DNS poisoning: Attacker makes a DNS server resolve a hostname into an incorrect IP address

• Fraggle attack: A DDoS attack type on a computer that floods the target system with a large amount of UDP echo traffic to IP broadcast addresses.

• Pharming: redirects a victim to a seemingly legitimate, yet fake, web site

• Phishing: type of social engineering with the goal of obtaining personal information, credentials, credit card number, or financial data. The attacker's lure, or fish, for sensitive data through various different methods

• Mail Bombing: This is an attack used to overwhelm mail servers and clients with unrequested e-mails. Using e-mail filtering and properly configuring email relay functionality on mail servers can be used to protect this attack.

Attacks (3):

• Ping of Death: A DoS attack type on a computer that involves sending malformed or oversized ICMP packets to a target.

• Replay attack: a form of network attack in which a valid data transmission is maliciously or fraudulently repeated with the goal of obtaining unauthorized access.

• Replay Attack: an attacker capturing the traffic from a legitimate session and replaying it to authenticate his session

• Session hijacking: If an attacker can correctly predict the TCP sequence numbers that the two systems will use, then she can create packets containing those numbers and fool the receiving system into thinking that the packets are coming from the authorized sending system. She can then take over the TCP connection between the two systems.

• Side-channel attacks: Nonintrusive and are used to uncover sensitive information about how a component works, without trying to compromise any type of flaw or Weakness. A noninvasive attack is one in which the attacker watches how something works and how it reacts to different situations instead of trying to "invade" it with more intrusive measures. side-channel attacks are fault generation, differential power analysis, electromagnetic analysis, timing, and software attacks.

• Smurf attack: A DDoS attack type on a computer that floods the target system with spoofed broadcast ICMP packets.

• Social engineering: An attacker falsely convinces an individual that she has the necessary authorization to access specific resources.

Attacks (4):

• Spoofing at Login: an attacker can use a program that presents to the user with a fake login screen, which often tricks the user into attempting to log on

• SYN flood: DoS attack where an attacker sends a succession of SYN packets with the goal of overwhelming the victim system so that it is unresponsive to legitimate traffic.

• TOC/TOU attack: Attacker manipulates the “condition check” step and the “use” step within the software to allow for unauthorized activity.

• War dialing: war dialer inserts a long list of phone numbers into war dialing program in hopes of finding a modem to gain unauthorized access.

• Wormhole attack: This takes place when an attacker captures packets at one location in the network and tunnels them to another location in the network for a second attacker to use against a target system.

• Denial-Of-Service (Dos) Attack: An attacker sends multiple service requests to the victim’s computer until they eventually overwhelm the system, causing it to freeze, reboot, and ultimately not be able to carry out regular tasks.

• Man-In-The-Middle Attack: An intruder injects herself into an ongoing dialog between two computers so she can intercept and read messages being passed back and forth. These attacks can be countered with digital signatures and mutual authentication techniques.

• Teardrop: This attack sends malformed fragmented packets to a victim. The victim’s system usually cannot reassemble the packets correctly and freezes as a result. Countersues to this attack is to patch the system and use ingress filtering to detect these packet types.

Power:

• Blackout: Generator
• Brownout: (UPS) Uninterruptible Power Supply
• Surge: Surge protector
• Spike: Surge protector
• Noise: Power conditioner
• Clean power: No solution is needed

Security Mode:

• Dedicated security mode (All users can access all data).
• System high-security mode (on a need-to-know basis, all users can access limited data).
• Compartmented security mode (on a need-to-know basis, all users can access limited data as per the formal access approval).
• Multilevel security mode (on a need-to-know basis, all users can access limited data as per formal access approval and clearance).

Code Repository Security:

• System security
• Operational security
• Software security
• Secure communications
• File system and backups
• Employee access
• Maintaining security
• Credit card safety

Common vulnerabilities and threats of Security Architecture:

- Poor memory management
- Covert channels (storage and timing)
- Insufficient system redundancy
- Poor access control
- Hardware failure
- Misuse of privileges
- Buffer overflows
- Memory attacks
- DoS
- Reverse engineering,
- Hacking,
- Emanations
- State attacks (race conditions)

A honeypot can be used

- Gathering threat intelligence
- Distracting attackers
- Delaying attackers

Sensitivity vs. Criticality:

- Sensitivity describes the amount of damage that would be done should the information be disclosed
- Criticality describes the time sensitivity of the data. This is usually driven by the understanding of how much revenue a specific asset generates, and without that asset, there will be lost revenue

Hashing:

- MDS Message-Digest Algorithm - 128-bit digest
- SHA - 160-bit digest
- HAVAL
- RIPEMD-160
- Birthday attacks possible

Symmetric Algorithms:

- Data Encryption Standard (DES)
- 3DES (Triple DES)
- Blowfish
- Twofish
- International Data Encryption Algorithm (IDEA)
- RC4, RCS, and RCG
- Advanced Encryption Standard (AES)
- Secure and Fast Encryption Routine (SAFER)
- Serpent
- CAST

Asymmetric Algorithms:

- RSA - factoring the product of two large prime numbers
- Diffie-Hellmann Algorithm
- EI Gamal- discrete logs
- Elliptic Curve Cryptography (ECC)

Methods of Cryptanalytic Attacks:

- Cipher text-Only Attack (Only Ciphertext)
- Known Plaintext (Both Plaintext and Ciphertext available)
- Chosen Plaintext (Known algorithm, Adaptive where Plaintext can be changed)
- Chosen Ciphertext (Known algorithm, Adaptive where Ciphertext can be changed)

Security Concepts:

• Need-to-Know (access only to what's needed to perform task/job).
• Separation of Duties (one person cannot execute all steps of critical processes or engage in a malicious activity without collusion).
• Monitor special privileges (audit logs for system operators /administrators/data center employees ensure privileged users cannot circumvent security policy, should not have access to their logged activity, conduct background investigations).
• Job rotation (reduces collusion).
• Information lifecycle: (creation, use, destruction of data, information/data owner helps safeguard data by classifying and determining its criticality and sensitivity).

Black/White List (BL/WL):

• The blacklist is an explicit deny.
• The whitelist is an implicit deny.
• The blacklist = "If you are on the list then you are NOT allowed in."
• The whitelist = "If you are NOT on the list then you are NOT allowed in."

RAID:

Some of the RAID protection options are:
• RAID0 – Striped
• RAID 1 withstands failure of one drive within one of the mirrored pairs. The number of required drives is twice the amount required to store data.
• RAID2 - Hamming Code requires either 14 or 39 disks
• RAID3 - Striped Set with Dedicated Parity (Byte Level)
• RAID4 - Striped Set with Dedicated Parity (Block Level)
• RAID 5 protection is also available. Data blocks are striped horizontally across the members of a RAID 5 group, and each member owns some data tracks and some parity tracks.
• RAID 6 protects data with failures of up to 2 drives per RAID group.
• RAID1+0 - striped set of mirrored disks

Client-based vulnerabilities, Client system should have:

- Licensed as running
- Current antivirus and antimalware
- HIDS
- Strong encryption
- Limited accounts without administrative privileges
- Continuous monitoring
- Hardened mobile devices

Server-based vulnerabilities, Server system should:

- Determine how remote access will be established
- Check configuration management be performed
- Control data flow

Wireless Attack:

- Rogue AP
- Interference
- Jamming
- Evil Twin
- War Driving
- War Chalking
- IV attack
- WEP/WPA attacks

Secure configuration of Hardware devices:

- Secure build
- Secure initial configuration
- Host hardening - remove all non-needed
- Host Patching
- Host lockdown
- Secure ongoing configuration, maintenance

RFID Attacks:

- RFID Counterfeiting
- RFID Sniffing
- Tracking
- Denial of Service
- Spoofing
- Repudiation
- Insert Attacks
- Replay Attacks
- Physical Attacks
- Viruses

RFID attacks:

- Eavesdropping/Skimming
- Traffic Analysis
- Spoofing
- Denial of Service Attack/Distributed Denial of Service Attack
- RFID Reader Integrity
- Personal Privacy

Attacks on VLAN:

• MAC Flooding Attack
• 802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack
• Double-Encapsulated 802.1Q/Nested VLAN Attack
• ARP Attacks
• Multicast Brute Force Attack
• Spanning-Tree Attack
• Random Frame Stress Attack

Methods for defeating a switch:

• MAC Spoofing Set the MAC address of a NIC to the same value as another
• MAC Flooding Overwhelm the CAM table of the switch so it coverts to hub mode
• ARP Poisoning Inject incorrect information into the ARP caches of two or more endpoints.

Most important elements that record state data on network devices:

• Routing tables
• CAM tables
• NAT tables
• DNS cache
• ARP cache

Positive/Negative Test:

• Positive Test - Work as expected (Output as per given input - goes as per plan)
• Negative Test - Even unexpected inputs are handled gracefully with tools like Exception Handlers

Artificial Intelligence (AI):

- Expert Systems
- Artificial Neural Networks
- Real Neural Networks
- Bayesian Filtering
- Genetic Algorithms and Programming

OWASP threat risk modeling process steps:

- Identify Security Objectives
- Survey the Application
- Decompose it
- Identify Threats
- Identify Vulnerabilities

Logical Security:

- Fail Open/Soft (availability is preserved, but data may not be secure)
- Fail Secure/Closed (data is secure, but availability is not preserved) Physical Security
- Fail Safe/Open (systems are shut down / entrances unlocked - humans are safe)
- Fail Secure/Closed (entrances are locked)
- Failover is a fault tolerance (redundancy) concept. If you have two redundant NICs; a primary and a backup – and the primary fails, the backup is used.

ACID model:

• Atomicity -Is when all the parts of a transaction's execution are either all committed or all rolled back - do it all or not at all
• Consistency - Occurs when the database is transformed from one valid state to another valid state. A transaction is allowed only if it follows user-defined integrity constraints.
• Isolation - Is the process guaranteeing the results of a transaction are invisible to other transactions until the transaction is complete.
• Durability- Ensures the results of a completed transaction are permanent and can survive future system and media failures; that is, once they are done, they cannot be undone.

Database Model should provide:

• Transaction persistence
• Fault tolerance/recovery
• Sharing
• Security controls

Threats to a DBMS include:

- Aggregation (combining data to form sensitive information)
- Bypass attacks (avoiding controls to access information)
- Compromising database views (modifying/accessing restricted views)
- Concurrency (processes running at the same time without proper locks)
- Contamination (corruption)
- Deadlocking (denying users who access information at the same time)
- DoS (preventing authorized access)
- Improper modification (accidental/intentional)
- Inference (deducing restricted information by observation)
- Interception of data
- Server access
- Polymorphism
- Polyinstantiation
- TOC/TOU (malicious changing data at a certain time)
- Web security issues
- Unauthorized access

Aggregation vs. Inference:

Inference (understand business, risk analysis, interview owner); by combining multiple reports or source of information, you succeed in guessing or making up new information. Aggregation (understand data and fields); the sum may represent a level of security higher than each of the parts. Be aware of these terms:

- Polyinstantiation: Prevents inference attacks
- Database Views: Constrained interfaces, restrictive interface
- Context-dependent access control: Content dependent controls
- Noise and perturbation: Addresses inference attacks
- Cell suppression: A technique used against the inference

Noise and perturbation: A technique of inserting bogus information in the hopes of misdirecting an attacker or confusing the matter enough that the actual attack will not be fruitful.

Tokens - "Synchronous" vs "Asynchronous":

• Synchronous Dynamic Password Tokens Hardware tokens that create synchronous dynamic passwords are time-based and synchronized with an authentication server. They generate a new password periodically, such as every 60 seconds. This does require the token and the server to have accurate time.
• Asynchronous Dynamic Password Tokens does not use a clock. Instead, the hardware token generates passwords based on an algorithm and an incrementing counter. When using an incrementing counter, it creates a dynamic one-time password that stays the same until used for authentication. Some tokens create a one-time password when the user enters a PIN provided by the authentication server into the token.

Token Usage: (NIST 800-63)

• Single-token authentication
• Multi-token authentication

Types of tokens for e-authentication: (NIST 800-63)

• Memorized Secret Token
• Pre-registered Knowledge Token
• Look-up Secret Token
• Out of Band Token
• Single-factor (SF) One-Time Password (OTP) Device
• Single-factor (SF) Cryptographic Device
• Multi-factor (MF) Software Cryptographic Token
• Multi-factor (MF) One-Time Password (OTP) Device
• Multi-factor (MF) Cryptographic Device

Token Threats:

• Something you have may be lost, damaged, stolen from the owner or cloned by the Attacker.
• Something you know may be disclosed to an Attacker. The Attacker might guess a password or PIN.
• Something you are may be replicated.

Token Threat Mitigation Strategies:

• Multiple factors make successful attacks more difficult to accomplish.
• Physical security mechanisms may be employed to protect a stolen token from duplication.
• Imposing password complexity rules may reduce the likelihood of a successful guessing attack.
• System and network security controls may be employed to prevent an Attacker from gaining access to a system or installing malicious software.
• Periodic training may be performed to ensure the Subscriber understands when and how to report compromise (or suspicion of compromise) or otherwise recognize patterns of behavior that may signify an Attacker attempting to compromise the token.
• Out of band techniques may be employed to verify proof of possession of registered devices (e.g., cell phones).

Token Threat/Attack: (NIST SP800-63)

• Theft - Use multi-factor tokens which need to be activated through a PIN or biometric.
• Duplication - Use tokens that are difficult to duplicate, such as hardware cryptographic tokens.
• Discovery - Use methods in which the responses to prompts cannot be easily discovered.
• Eavesdropping
  •• Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
  •• Use tokens that generate authenticators based on a token input value.
  •• Establish tokens through a separate channel.
• Offline cracking
  •• Use a token with a high entropy token secret
  •• Use a token that locks up after a number of repeated failed activation attempts.
• Phishing or pharming - Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
• Social engineering - Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator.
• Online guessing - Use tokens that generate high entropy authenticators.

Key States and Transitions: (NIST 800-57)

• The pre-activation state: The key has been generated, but not yet authorized for use
• The active state: The key may be used to cryptographically protect information
• The deactivated state: The crypto period of the key is expired, but the key still needs to perform cryptographic operations
• The destroyed state: The key is destroyed here
• The compromised state: The key is released or determined by an unauthorized entity
• The destroyed compromised state: The key is destroyed after a compromise or the compromise is found after the key is destroyed

Key management:

• Secure generation of keys
• Secure storage of keys
• Secure distribution of keys
• Secure destruction of keys

Secure Key Management:

• Key Generation: How, when, and on what devices keys are generated
• Key Derivation Constructing cryptographic keys from other keys and variables
• Key Establishment: Two parties algorithmic computation of keying material Secure wrapping and sending keys from one device to another
• Key Storage: Secure storage of keys (frequently encrypted using 'key encryption keys') and in what type of device(s)
• Key Lifetime: How long a key should be used before being destroyed (zeroized)
• Key Zeroization: the Secure destruction of key material
• Accounting: Identifying, tracking and accounting for the generation, distribution, and destruction of key material between entities

Key issues with Identity Services:

• APIs: While IAM vendors offer connectors to the most common cloud services, they are unlikely to provide all the connectors you need.
• Authorization Mapping: There are many possible ways to specify authorization rules, such as by role vs. by attribute.
• Audit: In-house systems can be linked with log management and SIEM systems to produce compliance reports and provide monitoring and detection of security events.
• Privacy: Users, user attributes, and other information are often pushed outside your corporate network and into one or more cloud data repositories.
• Latency: Propagating rule changes from internal IAM to cloud IAM can take some time. Latency is a subject to discuss with both your IAM provider and cloud service provider.
• Privileged User Management: This has been a problem for a long time, and the cloud adds a new wrinkle. Historically privileged users were all employees, and if things went pear-shaped you could handle it as an HR event. In the cloud that breaks down.
• App Identity: Once you have the user logged in you might still need to verify the application they are using — or perhaps there is no user at all, just middleware.
• Mobile: mobile connections to cloud services occur outside of the boundaries of normal.
• Identity Store Location: If companies are moving their applications and data to cloud services, will they also move existing identity stores?

Due Diligence vs. Due Care:

• Due Diligence - "Researching" -- Investigating and understanding risks
• Due Diligence – “Doing” all the necessary tasks required to maintain the due care
• Due Care - "Doing" -- Developing policies and procedures to address risk
• Due Care is to act responsibly

Security:

Security is a continuous process, not a one-shot project. The security life cycle or the security wheel is a continuous process that consists of several consequent phases (stages). The word cycle indicates the continuous and endless nature of such process. The ISO 27001 defines the cycle of the information security management system ISMS as PCDA: Plan-Do-Check-Act.

Cohesion vs. Coupling

• Co_H_esion -> H stands for HIGH: How many different types of tasks a module can carry out; Object should perform similar functions NOT separate functions; High cohesion is better for security as it is less dependent on other functions
• Coup_L_ing -> L stands for LOW: The level of interaction between objects to carry out its tasks; Lower (Loosely coupled) coupling means better design as objects is self-dependent. It is easier to troubleshoot and update; High (Tightly Couple) is not a good design as the object is dependent on other objects to perform its tasks; Low coupling is better for security as it will communicate with other functions or objects

General Data Backup Considerations:

• The scope of Backups/ Total size
• Importance
• Security
• Frequency of change
• Recovery time
• Testing the Integrity of Backups

Considerations for Security Controls include:

• Accountability (can be held responsible)
• Auditability (can it be tested?)
• A trusted source (source is known)
• Independence (self-determining)
• Consistently applied
• Cost-effective
• Reliable
• Independence from other security controls (no overlap)
• Ease of use
• Automation
• Sustainable
• Secure
• Protects confidentiality, integrity, and availability of assets
• Can be "backed out" in the event of an issue
• Creates no additional issues during operation
• Leaves no residual data from its function

Training and Awareness (NIST 800-16):

• Training that teaches people the drills that will enable them to perform their jobs more effectively
• Awareness programs that set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure

Project Management Quick Reference:

• The work package is the LOWEST level on a WBS.
• The WBS doesn't show the order of the work packages or any dependencies between them.
• WBS Dictionary – Detailed description of the WBS component
• Cost Benefit: Looking at how much your quality activities will cost
• Stakeholders are ONLY the interested entities that are internal or external to the organization.
• Project life cycle approach is Project governance and is described in the project management plan.
• Risk and uncertainty are greatest at the start of the project.
• Analysis of project forecasts (including time and cost) is also part of Performance Reporting.
• Risk appetite is the degree of uncertainty an entity is willing to take on in anticipation of a reward.
• Risk tolerance is the degree, amount, or volume of risk that an organization or individual will withstand.
• Risk threshold refers to measures along the level of uncertainty or the level of impact at which a stakeholder may have a specific interest.
• Positive and negative risks are commonly referred to as opportunities and threats.
• Project risk could exist at the moment a project is initiated.
• The procurement SOW describes the prospective sellers if they are capable of providing the products, services, or results.
• PMO manages the methodologies, standards, overall risks/opportunities, metrics, and interdependencies between projects at the enterprise level. Supportive, Controlling and Directive are the types of PMO structures in organizations.
• UNILATERAL: this is a special class of contract in which the seller doesn't have to explicitly accept the offer in order for a contract to be established. This is a unilateral contract, and the best example is a purchase order (PO)
• Force Majeure Risks, such as Earthquakes, Floods, Acts of Terrorism, Etc., should be covered under Disaster Recovery Procedures instead of Risk Management.

Quality of Service Metrics:

- Availability
- Outage Duration
- Mean Time Between Failures (MTBF)
- Capacity Metric
- Performance Metrics
- Reliability Percentage Metric
- Storage Device Capacity Metric
- Server Capacity Metric
- Instance Startup Time Metric
- Response Time Metric
- Completion Time Metric
- Mean Time to Switchover Metric
- Mean Time System Recovery Metric
- Scalability Component Metrics
- Storage Scalability Metric
- Server Scalability Metric

Contracts with third parties include:

• Agreement that the vendor will comply with applicable information security and privacy laws and regulations.
• Information security and privacy safeguards.
• Right-to-audit
• Notification in the event of a data breach.
• Where the data will be accessed, stored, and/or processed. It is important to know the specific locations and ensure that the vendor will notify the primary entity if there is a need to add, change, or remove a location.
• Data return or destruction when a contract terminates.
• Employee background checks/employment verification.
• Expectations for employee training.
• The ability of the vendor to subcontract work.
• Business continuity/disaster recovery plans. Within what time frame must the vendor's function be operational in the event of a disaster?

Identity and Access Management (IAM) Lifecycle:

• Provisioning: Applying appropriate rights to users for files/folders
• Review: Periodic monitoring of existing rights for the continued need
• Revocation: Removal of rights when no longer needed or warranted

Phases of IAM:

• Provisioning and de-provisioning
• Centralized directory services
• Privileged user management
• Authentication and access management

A comprehensive and effective security intelligence process can produce:

• Faster detection and remediation of threats.
• Improved regulatory compliance.
• Reduction of fraud, theft, and data leakage.
• Reduction of effort needed to provide security and deal with fallout related to breaches.
• The ability to detect potential weaknesses before an exploit actually occurs.

Security Intelligence Collection Lifecycle:

• Planning and direction
• Collection
• Processing
• Analysis and production
• Dissemination and integration

Cloud Service Models:

• Software as a Service (SaaS)
  •• Provider's applications run in the cloud
  •• Clients use thin apps (like a browser) to access SaaS
• Platform as a Service (PaaS)
  •• Client apps deployed into and running in the cloud
• Infrastructure as a Service (IaaS)
  •• Processing, storage, and network services
  •• Client controls operating systems and host configurations

Note: You remain accountable and responsible – regardless of any cloud service used.

Popular services:

• IaaS: Amazon EC2, Windows Azure, Rackspace (backup)
• PaaS: Google App Engine, Cloud Foundry, force.com
• SaaS: Office 365, Dropbox, salesforce.com, Google Apps
• Cloud management: CloudStack, OpenStack

Evaluating Cloud Service Security:

• What is the security of the facility running the servers?
• Is client data encrypted? If so, what encryption method is being used?
• Is the cloud provider's internal system segregated from its internet-facing cloud servers?
• Does the provider have a security audit they can share with us?
• What safeguards do they employ on their web service interface and/or API?
• Do they back up their data regularly and perform test restores for proper disaster recovery?
• What general data breach and protection policies are in place?
• Is client data shared with any third parties?

Securing the Infrastructure:

The internal information technology (IT) infrastructure must be secure before you can securely extend IT into a cloud.....
Securing the Infrastructure
• Framework for Governance
• Risk Management
• The Security Program
• Data Protection
• System and Data Management
• Security Awareness Training
• User Provisioning
• Monitoring and Enforcement
• Incident Response

Virtualization Risks:

• VM Sprawl
• Sensitive Data within a VM
• Security of Offline and Dormant VMs
• Security of Pre-Configured (Golden Image) VM / Active VMs
• Lack of Visibility Into and Controls Over Virtual Networks
• Resource Exhaustion
• Hypervisor Security
• Unauthorized Access to Hypervisor
• Account or Service Hijacking Through the Self-Service Portal
• The workload of Different Trust Levels Located on the Same Server
• Risk Due to Cloud Service Provider API

Cloud computing impacts four areas of governance and risk management:

• Governance includes the policy, process, and internal controls that comprise how an organization is run.
• Enterprise risk management includes managing overall risk for the organization, aligned with the organization's governance and risk tolerance.
• Information risk management covers managing the risk to information, including information technology.
• Information security is the tools and practices to manage risk to information.

Cloud security – general areas of concern:

- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit
- Information Management and Data Security
- Portability and Interoperability
- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security as a Service

ENISA Cloud Security document:

- LOSS OF GOVERNANCE; CSP does not commit to the necessary task
- VENDOR LOCK-IN, the high cost of moving to a different vendor
- ISOLATION FAILURE: one tenant influences another.
- COMPLIANCE RISKS: i.e. Audit impossible, or no evidence
- MANAGEMENT INTERFACE COMPROMISE
- DATA PROTECTION; protection cannot be demonstrated
- INSECURE OR INCOMPLETE DATA DELETION
- MALICIOUS INSIDER: i.e. Cloud provider or auditor

Cloud Storage security:

- Encryption
- Authentication
- Authorization

Security in Cloud Computing:

- Data segregation
- Identity Management
- Availability Management
- Vulnerability Management
- Access Control Management

Steps to take on the cloud to avoid vendor lock-in:

- Do your due diligence
- Plan early for an exit
- Design your application to be loosely coupled
- Maximize portability of your data
- Consider a multi-cloud strategy
- Implement DevOps tools and processes

Notice: A poorly crafted contract can lead to vendor lock-in

12 critical issues to cloud security:

- Data Breaches
- Weak Identity, Credential, and Access Management
- Insecure APIs
- System and Application Vulnerabilities
- Account Hijacking
- Malicious Insiders
- Advanced Persistent Threats (APTs)
- Data Loss
- Insufficient Due Diligence
- Abuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Issues

Cloud Risk:

• Privileged user access
• Regulatory compliance
• Data Location
• Data Segregation
• Recovery
• Long-term viability

Cloud API Security Concern:

A cloud API is basically used to integrate applications in order to enhance the cloud experience and provide inter-cloud compatibility. They are broadly classified into two categories: in-process APIs and remote APIs.

• Ensuring proper security measures to safeguard hypervisor to any sort of security threat.
• Careful assessment of the security practices as implemented by the cloud service providers need to be done before adopting any of them
• Proper SLAs between the customer and the CSP, defining the organizations' security requirements that need to be addressed.
• APIs in use need to be looked after and screened carefully. In the current scenario, most of the organizations prefer an integration of security techniques with their service models. They should be aware of the security implications associated with the usage of these cloud services. Reliance on weak APIs may jeopardize the security of important organizational data.

SLA in Cloud:

- Availability (e.g. 99.99% during work days, 99.9% for nights/weekends)
- Performance (e.g. Maximum response times)
- Security/privacy of the data (e.g. Encrypting all stored and transmitted data)
- Disaster Recovery expectations (e.g. Worse case recovery commitment)
- Location of the data (e.g. Consistent with local legislation)
- Access to the data (e.g. Data retrievable from a provider in readable format)
- Portability of the data (e.g. Ability to move data to a different provider)
- The process to identify problems and resolution expectations (e.g. Call center)
- Change Management process (e.g. Changes – updates or new services)
- Dispute mediation process (e.g. escalation process, consequences)
- Exit Strategy with expectations on the provider to ensure a smooth transition

Note: The uptime and availability requirements are a key component of the service level agreement (SLA).

Preparing for Cloud Use:

- Framework for Cloud Governance
- Planning for Cloud use
- Security controls for Cloud use
- Security Awareness Training for Cloud Users
- Performing due diligence on intended Cloud Service Providers (CSPs)

The CSP Agreement:

- Required services, service levels, uptime, redundancy, recovery
- Confidentiality / Non-Disclosure / Ownership / Access
- Compliance guarantees with notification and penalties for violations
- Breach / Incident detection, notification, response, and remediation
- Prudent management of the CSP business
- Monitoring, auditing, inspections, maintaining metrics, reports

Essential characteristics of Cloud:

- Resource pooling. Multiple customers
- On-demand self-service. Unilateral provisioning
- Broad network access. Network and client
- Rapid elasticity. Speedy provisioning and deprovisioning
- Measured Service. Pay per use

MDM solutions include:

- Device enrollment and authentication.
- Remote locks and wipe.
- Locating devices through GPS and other technologies.
- Pushing out OS, app, and firmware updates to devices.
- Preventing root access or jailbreaking of the device.
- Constructing an encrypted container on devices in which to keep sensitive organization data.
- Restricting certain features and services based on access control policies.

Threats in BYOD Environments:

- De-perimeterization
- Unpatched and insecure devices
- Strained infrastructure
- Forensic complications
- Lost or stolen devices

Management Controls for Privacy and Data Protection measures:

- Separation of Duties
- Training
- Authentication and Authorization procedures
- Vulnerability Assessments
- Backup and Recovery processes
- Logging
- Data-retention control
- Secure disposal

Note: Log data should be protected at least at the same sensitivity level as the systems from which it was collected.

Data Protection (How To...)

- Physical Security — Locked doors, security guards, access controls
- Network Security - Authentication, authorization, auditing, firewalls, IDS/IPS
- System Security — Patching, AV, configuration controls, approved applications
- Application Security — Secure coding, code review, design standards
- User Security - Policies, training, provisioning, monitoring, enforcement
- Administrator Security - Policies, supplemental training, provisioning, monitoring, specialized auditing, enforcement

Frameworks:

• Zachman Framework - not specific to security architecture
• Sherwood Applied Business Security Architecture (SABSA) Framework - Chain of traceability
• IT Infrastructure Library (ITIL) - service strategy, service design, service transition, service operations, and continuous service improvement. Processes to allow for IT service management developed by the United Kingdom's Office of Government Commerce
• TOGAF: Model and methodology for the development of enterprise architectures developed by The Open Group
• Six Sigma: Business management strategy that can be used to carry out process improvement
• Capability Maturity Model Integration (CMMI): Organizational development for process improvement developed by Carnegie Mellon

SOC:

SOC reports most commonly cover the design and effectiveness of controls for a 12-month period of activity with continuous coverage from year to year to meet user requirements from a financial reporting or governance perspective. In some cases, a SOC report may cover a shorter period of time, such as six months. A SOC report may also cover only the design of controls at a specified point in time for a new system/service or for the initial examination (audit) of a system/service.
• SOC1: Focused on Financial Controls
• SOC2: Focused on CIA and Privacy -- Private
• SOC3: Focused on CIA and Privacy -- Public
Note: the ISO 27001 certification is for the information security management system (ISMS), the organization's entire security program. The SAS 70 and SSAE 16 are audit standards for service providers and include some review of security controls but not a cohesive program (and the SAS 70 is outdated); The SOC reports are how SSAE 16 audits are conducted. The SOC 1 is for financial reporting; the SOC 2, Type 2 is to review the implementation (not design) of controls; and the SOC 3 is just an attestation that an audit was performed.

SOC 1:

• The purpose of a SOC 1 report scope should cover the information systems (both manual and automated) processes that are utilized to deliver the services under review. There are two types of SOC 1 reporting options:
•• SOC 1 Type 1: A design of controls report. This option evaluates and reports on the design of controls put into operation as of a point in time.
•• SOC 1 Type 2: Includes the design and testing of controls to report on the operational effectiveness of controls over a period of time (typically 12 months).

SOC 2:

• The purpose of a SOC 2 report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and/or privacy.
•• SOC 2 Type 1: Reports concern policies and procedures that were placed in operation at a specific moment in time.
•• SOC 2 Type 2: Reports concern policies and procedures over a period of at least – systems must be evaluated (normally 6 – 12 months in duration).
This generally makes SOC 2 type 2 reports more comprehensive and useful than type I reports when considering a possible service provider's credentials.

SOC 2 framework includes 5 key sections:

• Security - The system is protected against unauthorized physical and logical access.
• Availability - The system is available for operation and use as committed or agreed.
• Processing Integrity - System processing is complete, accurate, timely, and authorized.
• Confidentiality - Information designated as confidential is protected as committed or agreed.
• Privacy - Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice

Information Security Strategies:

• Strategic planning – Long-term (3 to 5 years) and must be aligned with business objectives.
• Tactical planning – Short-term (6 to 18 months) used to achieve specific goals. May consist of multiple projects
• Operational and project planning – Specific plans with milestones, dates, and accountabilities provide communication and direction for project completion

Confinement, Bounds, and Isolation:

• Confinement- restricts a process to reading from and writing to certain memory locations.
• Bounds - are the limits of memory a process cannot exceed when reading or writing.
• Isolation - is the mode a process runs in when it is confined through the use of memory bounds.

Ports:

• DNS – TCP/53, UDP/53
• LDAP – TCP/389, UDP/389, X.500
• NetBIOS – TCP/137,138, UDP/135,139
• CIFS/SMB – TCP/445, Samba (Unix)
• SMTP – TCP/25, ESMTP
• TFTP – UPD/69
• FTP – TCP (20-DATA, 21-CONTROL)
  •• Secure FTP with TLS (Encrypted FTP)
  •• SFTP (SSH FTP – Not an FTP but SSH used for file transfer)
  •• FTP over SSH (Tunnel FTP traffic over SSH)
  •• Active mode (PORT mode) – Sever initiates the data connection
  •• Passive mode (PASV mode) – Client initiates the data connection

Scanning Types:

• DISCOVERY SCANNING: A discovery scan can be performed with very simple methods, for example, by sending a ping packet (ping scanning) to every address in a subnet. More sophisticated methods will also discover the operating system and services of a responding device.
• COMPLIANCE SCANNING: A compliance scan can be performed either from the network or on the device (for instance, as a security health check). If performed on the network, it will usually include testing for open ports and services on the device.
• VULNERABILITY SCANNING: A vulnerability scan can either test for vulnerability conditions or try an active exploitation of the vulnerability. A vulnerability scan can be performed in a non-disruptive manner or under acceptance of the fact that even a test for certain vulnerabilities might affect the target's availability or performance.

DevOps

DevOps and cloud computing work together to help organizations bring new services and applications to market more quickly, at less cost. DevOps is about streamlining the development, while cloud offers on-demand resources, automated provisioning, and easy scaling, to accommodate application changes. Many DevOps tools can be acquired on-demand in the cloud or as part of a larger cloud platform. To support hybrid cloud deployment (workloads with an ability to move between clouds), enterprises should select DevOps platforms with an interface to the cloud providers they will use. DevOps promotes lean and agile delivery of quality software that adds value to business and customers.
DevOps reference:
• Plan and measure
• Develop and test
• Release and deploy
• Monitor and optimize

DevOps Principles:

- Develop and test against production-like systems
- Deploy with repeatable, reliable processes
- Monitor and validate the operational quality
- Amplify feedback loops

DevOps Practices:

- Release planning
- Continuous integration
- Continuous delivery
- Continuous testing
- Continuous monitoring and feedback

Note: DevOps and cloud computing work together to help organizations bring new services and applications to market more quickly, at less cost. DevOps is about streamlining the development, while cloud offers on-demand resources, automated provisioning, and easy scaling, to accommodate application changes. Many DevOps tools can be acquired on-demand in the cloud or as part of a larger cloud platform. To support hybrid cloud deployment (workloads with an ability to move between clouds), enterprises should select DevOps platforms with an interface to the cloud providers they will use.

Markup Language:

• GML: Generalized Markup Language - a Top level markup language
• SGML: Standardized Generalized Markup Language - Derived from GML
• SPML: Service Provisioning Markup Language -Allows exchange of provisioning data between systems. SPML: XML based format for exchanging user and resource information and controlling provisioning.
• SAML: Security Assertion Markup Language - Standard that allows the exchange of Authentication and Authorization data to be shared between security domains. SAML can expose the system to poor identification or authorization. SAML: provides an XML-based framework for exchanging security-related information over networks.
• XACML: Extensible Access Control Markup Language - Used to express security policies and access rights provided through web services and applications
• XML: Can include tags to describe data as anything desired. Databases from multiple vendors can import and export data to and from an XML format, making XML a common language used to exchange information. XML is vulnerable to injection attacks. XML is a universal format for storing information.

Networking Hardware:

• Modems (converts digital to analog/analog to digital signals)
• Hubs (operate at the physical layer, retransmit signals)
• Repeaters (operate at the physical layer, re-amplify signals)
• Bridges (operate at layer 2, filters traffic)
• Switches (operate at layer 2, forwards broadcasts and frames)
• Routers (forwards packets)

Identity as a Service IDaaS:

Identity as a Service (IDaaS) is an authentication infrastructure that is built, hosted and managed by a third-party service provider. IDaaS can be thought of as single sign-on (SSO) for the cloud. This can provide benefits including integration with cloud services and remove overhead for maintenance of traditional on-premise identity systems, but it can also create risk due to the third-party control of identity services and reliance on an offsite identity infrastructure. An IDaaS solution via a cloud provider usually includes the following:

- Single sign-on
- Provisioning
- Password management
- Access governance

Benefits of Identity as a Service IDaaS:

- SSO authentication
- Federation
- Granular authorization controls
- Administration
- Integration with internal directory services
- Integration with external services

SSO Technologies:

- Kerberos
- SESAME
- LDAP
- Microsoft Active Directory

Life Cycle of Evidence:

- Collection and Identification
- Storage, preservation, and transportation
- Presentation in court
- Return of the evidence

Equipment Life Cycle:

- Defining requirements
- Acquiring and implementing
- Operations and maintenance
- Disposal and decommission

Cloud Data Life Cycle:

- Create: Creation is the generation of new digital
- Store: Storing is the act committing the digital data
- Use: Data is viewed, processed, or otherwise used
- Share: Information is made accessible to others
- Archive: Data leaves active use and enters long-term storage
- Destroy: Data is permanently destroyed

Factors effective Biometrics Access Control System:

- Accuracy
- Speed/Throughput
- Data storage requirements
- Reliability
- Acceptability

Downsides biometric:

- User acceptance
- Enrollment timeframe
- Throughput
- Accuracy over time

Availability other concepts:

- Usability
- Accessibility
- Timeliness
- Reliability

Confidentiality other concepts:

- Sensitivity
- Discretion
- Criticality
- Concealment
- Secrecy
- Privacy
- Seclusion
- Isolation

Content-Distribution Network (CDN) benefits:

- On-demand scaling
- Cost efficiency
- Locality of Content
- Security Enhancement
- Filter out DDOS attacks

Drawbacks multilayer protocols:

- Covert channels are allowed
- Filters can be bypassed
- Logically imposed network segment boundaries can be overstepped

Covert channels include:

- Transmitting data over a rarely used port that the firewall does not block.
- Concealing data in the headers of TCP/IP packets
- Breaking the data up into multiple packets to be sent at different
- Transmitting data over a shared resource that is not typically used as a communication channel
- Transmitting encrypted data that cannot be inspected as it leaves the network.

Benefits multilayer protocols:

- A wide range of protocols can be used
- Encryption
- Flexibility and resiliency

MPLS feature:

- Traffic engineering
- Better router performance
- Built-in tunneling

Two main MPLS routing protocols:

- Label Distribution Protocol (LDP) - No Traffic Engineering
- Resource Reservation Protocol with Traffic Engineering (RSVP-TE)

Label Switched Path (LSP) MPLS Router Roles/Positions are:

• Label Edge Router (LER) or "Ingress Node" - The router that first encapsulates a packet inside an MPLS LSP; Also the router that makes the initial path selection.
• Label Switching Router (LSR) or "Transit Node" - A router that only does MPLS switching in the middle of an LSP.
• Egress Node - The final router at the end of an LSP, which removes the label.

Generic Routing Encapsulation (GRE) Tunnel

Tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an internet protocol network.

Defense-in-depth strategy:

- Developing security policies, procedures
- Addressing security throughout the lifecycle
- Implementing a network topology has multiple layers
- Providing logical separation between the corporate and network devices
- Employing a DMZ network architecture
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant)
- Disabling unused ports and services
- Restricting physical access to network and devices.
- Restricting user privileges
- Considering the use of separate authentication mechanisms and credentials
- Using modern technology
- Implementing security controls
- Applying security techniques
- Expeditiously deploying security patches
- Tracking and monitoring audit trails

Physical Security:

• Protecting life is the primary goal of physical security
• Physical security helps prevent operational interruptions
• The primary goal of the physical program is facility access control
• Arrange barriers in layers with progressive security closer to center/highest protective area
• Conduct a security risk/vulnerability assessment to identify threats (natural and man-made) to assets and impacts of the loss
• During assessment address security control during/after hours, access control, surveillance, policies/procedures, BCP, etc.
• Apply defense in depth

Industrial control system key-components (ICS):

• Control Loop
• Human-Machine Interface (HMI)
• Remote Diagnostics and Maintenance Utilities

Major control components of industrial control systems (ICS):

• Control Server
• SCADA Server or Master Terminal Unit (MTU)
• Remote Terminal Unit (RTU)
• Programmable Logic Controller (PLC)
• Intelligent Electronic Devices (IED)
• Human-Machine Interface (HMI)
• Data Historian
• Input / Output (IO) Server

Platform vulnerabilities in industrial control systems (ICS):

- Platform Configuration Vulnerabilities
- Platform Hardware Vulnerabilities
- Platform Software Vulnerabilities
- Platform Malware Protection Vulnerabilities

Developing a Comprehensive Security Program for ICS:

- Obtain senior management buy-in
- Build and train a cross-functional team
- Define charter and scope
- Define specific ICS policies and procedures
- Define and inventory ICS assets
- Perform a risk and vulnerability assessment
- Define the mitigation controls
- Provide training and raise security awareness for ICS staff

ICS are addressed in NIST 800-82 Guide to Industrial Control Systems (ICS) Security

General types of viruses:

- File Infectors – Infects program or object files.
- Boot sector infectors – Attach or replace boot records
- System Infectors – Attaches to system files or system structure
- Companion virus – Does not physically touch the target file
- Email Virus – Aware of the email system.
- Multipartite – Reproduces in more than one way
- Macro Virus – Uses macro programming of the app. Infect data files
- Script Virus – Standalone files that can be executed by an interpreter
- Script host – .vbs as host to script virus.

Big Data:

Data collections that is so large and complex that they are difficult for traditional database tools to manage. Businesses are often prompted to restructure their existing architecture to handle it.

Big Data:

Cloud Secure Alliance (CSA) has categorized the different security and privacy challenges into four different aspects of the Big Data ecosystem. These aspects are Infrastructure Security, Data Privacy, Data Management and, Integrity and Reactive Security. Each of these aspects faces the following security challenges, according to CSA:

- Infrastructure Security
  - Secure Distributed Processing of Data
  - Security Best Actions for Non-Relational Data-Bases
- Data Privacy
  - Data Analysis through Data Mining Preserving Data Privacy
  - Cryptographic Solutions for Data Security
  - Granular Access Control
- Data Management and Integrity
  - Secure Data Storage and Transaction Logs
  - Granular Audits
  - Data Provenance
- Reactive Security
  - End-to-End Filtering & Validation
  - Supervising the Security Level in Real-Time

Common threats to Big Data:

- Breach of privacy
- Privilege escalation
- Repudiation
- Forensic complications

Secure life cycle for big data

The life cycle of big data has six main stages: creation and discovery, access and data flow, process, share, store, and destroy.

• The key challenges in creation and discovery are:
  •• Identifying all endpoints in the network that contribute the data.
  •• Identifying intellectual property and determining the value and business impact of each data in the big data cluster.
  •• Defining data provenance.

• The security challenges in access and data flow are:
  •• Implementing security in distributed programming frameworks.
  •• Implementing granular access controls (sensitive data vs. user role).
  •• Defining security controls for non-relational data sources.
  •• Identifying end-to-end data flow.

• Security challenges while data processing are:
  •• Implementing scalable, privacy and security during data mining and data analytics.
  •• Implementing granular data audits.

• The security challenges while sharing data are:
  •• Implementing granular data audits.
  •• Implementing reactive security to secure the integrity of data.

• The security challenges while storage data are:
  •• Implementing secure data storage and transaction data logs and files.

• Data disposal is the most crucial stage in the life cycle of big data. Data in the wrong hands may be catastrophic. Organization-level security policies to implement secure data disposal methods and removal of access rights on employee/user exit interviews should be in place to ensure the data is available only to authorized users.

Challenges of current Big Data:

• There are limited levels of protection in the majority of distributed systems computations.
• Security solutions are not being able to tackle the demand with several non-relational databases constantly
• There is a lack of appropriate security processes for the transfer of automated data.
• System updates, audits, patches are not always carried out.
• Information coming in should be constantly validated, to ensure its credibility and accuracy
• The attack on systems that contain sensitive information of the customers can put the customers at risk.
• Some organizations do not deploy any kind of access controls to differentiate between the confidentiality
• Monitoring and tracking of systems are difficult with the current scale of Big Data application.

Artificial Intelligence, Machine Learning and Deep Learning:

• Artificial intelligence: Any technique which enables computers to mimic human behavior
• Machine Learning: Subset of AI techniques which use statistical methods to enable machines to improve with experiences.
• Deep Learning: Subset of ML, which make the computation of multi-layer neural networks feasible.

The IoT architecture:

• The perception layer
• The network layer
• The application layer

IoT Characteristics:

- Existence
- Sense of self
- Connectivity
- Interactivity
- Dynamicity
- Scalability
- Limitations of Computational
- Limitations of Resources

The IoT building block consists of five main modules:

- Sensor Module
- Processing Module
- Actuation Module
- Communication Module
- Energy Module

OWASP Top 10 IoT Vulnerabilities (2014):

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption/Integrity Verification
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

IoT Device Security Challenges:

• IoT products may be deployed in insecure or physically exposed environments
• Security is new to many manufacturers and there is limited security planning in development methodologies
• Security is not a business driver and there are limited security sponsorship and management support in the development of IoT products
• There is a lack of defined standards and reference architecture for secure IoT development
• There are difficulties recruiting and retaining requisite security skills for IoT development teams, including architects, secure software engineers, hardware security engineers, and security testing staff
• The low price point increases the potential adversary pool
• Resource constraints in embedded systems limit security options

Guidance for Secure IoT Development:

• Secure Development Methodology
• Secure Development and Integration Environment
• Identity Framework and Platform Security Features
• Establish Privacy Protections
• Hardware Security Engineering
• Protect Data
• Secure Associated Apps
• Protect Interfaces/APIs
• Provide Secure Update Capability
• Implement Secure Authn/z
• Establish Secure Key Management
• Provide Logging Mechanisms
• Perform Security Reviews

IoT Security (BEST PRACTICES):

•Make hardware tamper resistant
•Provide for firmware updates/patches
•Perform dynamic testing
•Specify procedures to protect data on device disposal
•Use strong authentication
•Use strong encryption and secure protocols
•Minimize device bandwidth
•Divide networks into segments
•Protect sensitive information
•Encourage ethical hacking and vulnerability disclosure
•Institute an IoT Security and Privacy Certification Board

Securing the Internet of Things: (Seven Steps to Minimize IoT Risk in the Cloud)

• Secure Cloud Infrastructure
• Leverage Standards-Based Best Practices
• Design for Security
• Secure IoT Devices
• Secure Device Connections
• Secure IoT Services and Apps
• Secure Users and Access

Product vendors/developers should consider steps below to improve IoT security:

• Secure web/desktop/mobile applications with proper authentication and authorization.
• If feasible, Implement and enable 2-factor authentications by default, it will considerably improve IoT device security.
• Follow secure coding methods and always perform input validation to avoid Cross-site scripting (XSS), SQL injection and Buffer Overflow (BoF) vulnerabilities. Follow hyperlinks to understand more about these vulnerabilities.
• Enforce an effective password policy
• Use captcha, account lockout policy methods to avoid brute force attacks.
• Vendors should provide security updates including details on security fixes, the impact of the vulnerability and provide simple steps to deploy security updates.
• If feasible, always use encryption for communication.
• Ensure regular backups (at least two or more data) in a secure place.
• Avoid information disclosure. i.e avoid publishing customer's data
• While adding new features to the product, vendors should make sure it will not create or be used as a security hole.
• Vendors should think on ease of use vs security
• Apply OWASP Top 10 IoT Vulnerabilities should be addressed, while IoT design and development.

Types of tests that can be employed for IoT device developments:

• Static Application Security Testing (SAST)
• Dynamic Application Security Testing (DAST)
• Interactive Application Security Testing (IAST)
• Attack Surface and Vectors
• 3rd Party Library
• Fuzzing
• Customized per threat vector

IoT Forensics Challenges:

- The Investigation Framework
- Diversity of Devices
- IoT Constraints
- Lack of Standardization
- Improper Evidence Handling
  - Evidence identification, collection, and preservation
  - Evidence analysis and correlation
- Securing the Chain of Custody

Attacks in IoT:

- Node Tampering / Node Compromised
- Denial of Service (DoS)
- Distributed DoS
- Device Spoofing
- The Breach of Privacy
- Malware
- Application-based Attacks
- Man in the Middle Attacks

NIST (1):

- NIST 800-12 NIST Handbook Intro to Computer Security
- NIST 800-13 Telecomm Security Guidelines for Telecomm Mgmt. Network
- NIST 800-14 Generally Accepted Principles and Practices Securing Information
- NIST 800-18 AUP / Rules of Behavior
- NIST 800-30 Risk Management/Assessments
- NIST 800-34 Contingency Planning
- NIST 800-37 Risk Management Framework
- NIST 800-40 Creating a Patch and Vulnerability Management Program
- NIST 800-41 Guidelines on Firewalls and Firewall Policy
- NIST 800-44 Guidelines on Securing Public Web Servers

NIST (2):

- NIST 800-45 Guidelines on Electronic Mail Security
- NIST 800-47 Security Guide for Interconnecting IT Systems
- NIST 800-48 Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST 800-50 Building an IT Security Awareness and Training Program
- NIST 800-53 Security and Privacy Controls for Federal Information Systems
- NIST 800-54 Border Gateway Protocol Security
- NIST 800-55 Security metrics IS
- NIST 800-57 Recommendation for Key Management
- NIST 800-60 Guide for Mapping Types of Information and Information
- NIST 800-61 Computer Security Incident Handling
- NIST 800-63 Electronic Authentication
- NIST 800-64 Security Considerations in SDLC
- NIST 800-66 Healthcare privacy issues
- NIST 800-86 Guide to Integrating Forensic Techniques into IR
- NIST 800-82 Guide to Industrial Control Systems (ICS) Security
- NIST 800-83 Guide to Malware Incident Prevention and Handling
- NIST 800-86 Guide to Integrating Forensic Techniques into Incident Response
- NIST 800-88 Media Sanitization
- NIST 800-94 IDS/1PS
- NIST 800-100 IS Handbook
- NIST 800-115 IS Security Testing and Assessment
- NIST 800-119 Guidelines for Secure Deployment of IPv6
- NIST 800-122 Protect PII
- NIST 800-137 Information Security Continuous Monitoring (ISCM)
- NIST 800-145 Cloud computing

ISO:

- ISO 7498: OSI Model
- ISO 27000: ISMS-Overview and Vocabulary
- ISO 27001: ISMS-Requirement
- ISO 27002: Code of practice
- ISO 27003: ISMS implementation
- ISO 27004: Measurement and metrics framework
- ISO 27005: Risk management
- ISO 27006: Certification body requirements
- ISO 27007: ISMS-Auditing
- ISO 27008: Information Security Control
- ISO 27011: ISMS guideline telecom organization
- ISO 27014: Governance of information security
- ISO 27017: Use of cloud services
- ISO 27018: Cloud privacy protection overview
- ISO 27031: Communications technology readiness for business continuity
- ISO 27032: Cyber Security Resilience
- ISO 27034: Security applications
- ISO 27035: Security incident management
- ISO 27037: Covers identifying, gathering, and preserving digital evidence.
- ISO 27799: Directives on protecting personal health information
- ISO 31000: Risk Management Framework
- ISO 22301: BCM - Business continuity
- ISO 15408: Common Criteria
- ISO 28000: Supply Chain Management
- ISO 42010: Systems and Software Engineering Architecture description
- ISO 14443: Smart card standardizations

IEEE:

- IEEE 802.11: Wireless LANs
- IEEE 802.15: Wireless PANs
- IEEE 802.16: Broadband Wireless MANs
- IEEE 802.20: Mobile Broadband Wireless Access

ISO 27002 includes:

- Security Policy
- Organization and Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisitions, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Important FISMA Features:

- Periodic risk assessments.
- Policies and procedures based on assessments.
- Qualitative risk rating-data-driven security model.
- Subordinate plans for information security for networks, facilities, and other subsystems.
- Security awareness training for personnel.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and controls at least annually.
- A process to address deficiencies in information security policies (POAM).
- 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.

Important HIPAA Features:

• Electronic Transaction and Code Sets Standards: Requires the same health care transactions, code sets, and identifiers.
• 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.
• Security Rule: Specifies administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity and availability of electronic protected health information.
• National Identifier Requirements: Requires that health care providers, health plans, and employers have standard national numbers that identify them on standard transactions.
• Enforcement Rule: Provides standards for enforcing all the Administrative Simplification Rules.

Important HITECH Features:

• Expansion of HIPAA security standards to "business associates" that perform activities involving the use or disclosure of individually identifiable health information.
• Increased civil penalties for "willful neglect."
• Data-breach notification requirements for unauthorized uses and disclosures of "unsecured PHI."
• Stronger individual rights to access electronic medical records and restrict the disclosure of certain information.
• New limitations on the sale of protected health information, as well as marketing and fundraising communications.

EU Data Protection Directive Features:

• Notice: Data subjects should be given notice when their data are being collected.
• Purpose: Data should only be used for the purpose stated.
• Consent: Data should not be disclosed without the subject's consent.
• Security: Collected data should be kept secure from any potential abuses.
• Disclosure: Data subjects should be informed as to who is collecting their data.
• Access: Data subjects should be allowed to access their data and make corrections to any inaccurate data.
• Accountability: Data subjects should have an available method to hold data collectors accountable for following these six principles above.

COBIT 5.0:

• Principle 1: Meeting Stakeholder Needs
• Principle 2: Covering the Enterprise End to End
• Principle 3: Applying a Single, Integrated Framework
• Principle 4: Enabling a Holistic Approach
• Principle 5: Separating Governance from Management

ITIL Benefits:

• Increased user and customer satisfaction with IT services.
• Improved service availability, directly leading to increased business profits and revenue.
• Financial savings from reduced rework, lost time, improved resource management and usage.
• Improved time to market for new products and services.
• Improved decision-making and optimized risk.

CIS

The Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber Defense (CSC) is a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.

- Basic CIS Controls
    - Inventory and Control of Hardware Assets
    - Inventory and Control of Software Assets
    - Continuous Vulnerability Management
    - Controlled Use of Administrative Privileges
    - Secure Configuration for Hardware and Software for Mobile Devices, Laptops, Workstations and Servers
    - Maintenance, Monitoring and Analysis of Audit Logs

- Foundational CIS Controls
    - Email and Web Browser Protections
    - Malware Defenses
    - Limitation and Control of Network Ports, Protocols and Services
    - Data Recovery Capabilities
    - Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
    - Boundary Defense
    - Data Protection
    - Controlled Access Based on the Need to Know
    - Wireless Access Control
    - Account Monitoring and Control

- Organizational CIS Controls
    - Implement a Security Awareness and Training Program
    - Application Software Security
    - Incident Response and Management
    - Penetration Tests and Red Team Exercises

TOGAF

The structure of the TOGAF documentation reflects the structure and content of an Architecture Capability within an enterprise.

• PART I: (Introduction)- This part provides a high-level introduction to the key concepts of enterprise architecture and,in particular, the TOGAF approach. It contains the definitions of terms used throughout TOGAF and release notes detailing the changes between this version and the previous version of TOGAF.

• PART II: (Architecture Development Method) - This part is the core of TOGAF. It describes the TOGAF Architecture Development Method (ADM), a step-by-step approach to developing an enterprise architecture.

• PART III: (ADM Guidelines and Techniques) - This part contains a collection of guidelines and techniques available for use in applying TOGAF and the TOGAF ADM.

• PART IV: (Architecture Contenf Framework) - This part describes the TOGAF content framework, including a structured meta-model for architectural artifacts,. The use of re-usable architecture, building blocks, and an overview of typical architecture deliverables.

• PART V: (Enterprise Continuum & Tools) - This part discusses appropriate taxonomies and tools to, categorize and store the outputs of architecture activity within an enterprise.

• PART VI: (TOGAF Reference Models) - This part provides a selection of architectural reference models, which includes the TOGAF Foundation Architecture, and the Integrated Information Infrastructure Reference Model (III-RM).

• PART VII: (Architecture Capability Framework) - This part discusses the organization, processes, skills, roles, and responsibilities required to establish and operate an architecture function within an enterprise.

SABSA

SABSA is comprised of a series of integrated frameworks, models, methods, and processes used independently, or as a holistic integrated enterprise solution, including:

- Business Requirements Engineering Framework (known as Attributes Profiling)
- Risk and Opportunity Management Framework
- Policy Architecture Framework
- Security Services-Oriented Architecture Framework
- Governance Framework
- Security Domain Framework
- Through-life Security Service Management & Performance Management Framework

Conclusions/Recommendations:

• Your role is a RISK ADVISOR
• Do not FIX problems: Consult/advise
• Who is responsible for security?
• How much security is enough?
• All decisions start with risk management: cost-benefit analysis
• In the exam read the question fully, sometimes twice if the writing is twisted;, mark the keywords from the question; Read all answers the first time; Eliminate options with a clear wrong answer. Read questions carefully and understand the real problem and answer accordingly.
• Get your mind into the zone of thinking from the correct perspective.
• Keep in mind the CISSP process
• Think like a manager
• If you study by yourself, you will always see your material from the same perspective; I recommend choosing a study group.
• Check CISSP references www.isc2.org/Certifications/References (link that has some suggested references for the CBK - CISSP)
• Measure your progress through quizzes and practice exams, be aware don't go by the score try to fill your gaps
• Read up on what others have done by checking https://community.isc2.org/ and other study groups such as SNT FB, reddit or others.

REFERENCES

- *The Official (ISC)2 Guide to the CISSP CBK, Fourth Edition ((ISC)2 Press)*
- *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 7th Edition*
- *CISSP Official (ISC)2 Practice Tests*
- *CISSP All-in-One Exam Guide, Seventh Edition*
- *The Official (ISC)2 Guide to the CCSP CBK*
- *(ISC)2 presentation isc2.org*
- *CISM CRM – ISACA isaca.com*
- *Cloud Secure Alliance (CSA)*
- *Sybextestbanks.wiley.com*
- *Cccure.org (CCCURE)*
- *Isc2.org community*
- *Issa.org (ISSA)*
- *Cloudsecurityalliance.org*
- *NIST publications*
- *Cyber Security First Responder CFR – Logical Operations*
- *SANS documentation*
- *EC-Council*
- *CCSP Certified Cloud Security Professional, Presentation - Kelly Handerhan*
- *CISSP Certified Information Systems Security Professional, Kelly Handerhan*
- *IBM Cloud Services ibm.com*
- *Security Cloud Guidance V4*
- *Uncategorized*
    - *https://safecode.org/publications/*
    - *https://www.merlot.org/merlot/InformationTechnology.htm*
    - *(IJACSA) International Journal of Advanced Computer Science and Applications*
    - *http://www.diocc.com/artificial-intelligence-training.html*
    - *INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES May 2017*
    - *Hacking Internet of Things (IoT) A Case Study on DTH Vulnerabilities*
    - *CSA Launches Best Practices for Mitigating Risks in Virtualized Environments*
    - *ISSUES REGARDING SECURITY PRINCIPLES IN CLOUD COMPUTING*
    - *Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products (IoT Working Group | Future-proofing the Connected World)*
    - *ZHOU, Jun et al. Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications*
    - *https://www.researchgate.net/publication/316867894*
    - *http://www.pentest-standard.org*
    - *https://www.experts-exchange.com/articles/32132/Better-Security-in-the-Cloud.html*
    - *https://www.experts-exchange.com/articles/31793/Vulnerability-Assessments-versus-Penetration-Tests.html*
    - *https://www.experts-exchange.com/articles/31763/Incident-Handling-and-Response-Plan.html*
    - *https://www.experts-exchange.com/articles/31744/Cloud-Security-Threats-Risks-and-Concerns.html*
    - *https://www.experts-exchange.com/articles/32316/What-Gives-SIEM-a-Good-Name.html*
    - *https://www.isc2.org/Certifications/References*
    - *https://www.studynotesandtheory.com/*
    - *https://www.facebook.com/groups/InformationAudit/*
    - *https://www.facebook.com/groups/1525346961013038/*
    - *https://www.cybrary.it/*
    - *https://github.com/DoGByTe-ZN/infosec-resources4all/*
    - *https://www.linkedin.com/groups/8592316*