CISSP
PROCESS GUIDE

V.13

CISSP PROCESS GUIDE

By

Fadi SODAH, CISSP

(a.k.a. ***madunix****)*

Powered by

CISSP Exam Preparation - Study Notes and Theory - Facebook Study Group

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 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 Official CISSP CBK. Being a CISSP candidate you should fully understand CISSP concepts, methodologies and their implementations within the organization.

If you find this document useful and the information valuable, please consider making a donation to help defray the costs of the bandwidth and hosting services required to distribute it. Every little bit helps. To make a contribution, please go to: https://www.studynotesandtheory.com/single-post/Donations

-Fadi Sodah

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*
- *CISM CRM - ISACA*
- *Sybextestbanks.wiley.com*
- *Cloudsecurityalliance.org*
- *NIST documentations/papers*
- *SANS documentations/papers*
- *CCSP Certified Cloud Security Professional, Presentation - Kelly Handerhan*
- *CISSP Certified Information Systems Security Professional, Presentation - Kelly Handerhan*
- *IBM Cloud Services*
- *Cisco Systems*

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

5x 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. Management: How

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

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 plan
- 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 from a disaster
- BCP helps in continuity of organization function in the event of a disaster

Business Continuity Planning (BCP):

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

Team:

•Rescue Team: Responsible for dealing with the immediacy of 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 Plan should be kept in multiple locations
- Both Electronic and paper copies should be kept
- Plan should be distributed to those with a need to know
- Most employees 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 to 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 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 recovery of IT services
- Data recovery strategy
  - Focus on 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
- Back-Up Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

Post-Incident Review:

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 designated information systems at an existing or new location in an emergency.

Business Continuity Plan (BCP):

Focuses on sustaining an organization's mission/business processed 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 allow.

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 functions at 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 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
- Accessing 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

Methodologies of Risk Assessment:

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

Preparing Risk Assessment:

- Purpose of the assessment
- 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 the 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)

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

SDLC 10x 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 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

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

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 & 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 target system.
• Operation/Maintenance
– Security Operations and Administration
– Operational Assurance
– Audits and Continuous monitoring
– Configuration management & perform change control
• Disposal
– Information transfer or destruction
– Media Sanitization
– Dispose hardware

Forensic:

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

E-discovery:

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

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 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 security-awareness program

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 M. & Configuration. M.
- 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

Vulnerability management:

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

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 identity of 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 overloads 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 or 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 on capabilities, functionality, performance
- Changes are reviewed and approved by a CAB (change approval board).

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 Read privilege. Also VA scanning should be performed within same segment means bypassing firewalls. That is why VA scanners come with multiple LAN ports to scan each subnet local to subnet scanning behind the firewalls will filter ports and critical vulnerabilities may not be detected.

Problem Management:

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

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 stated security objectives.
- Provides independent feedback to senior management.

Auditing uses:

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

Audit:

Systematic process by which a competent, independent person objectively obtains and evaluates 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 audit scope
- Conduct audit
- Refine the audit process

Audit Process:

- Determine goals
- Involve right business unit leader
- Determine Scope
- Choose audit Team
- Plan audit
- 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

Capability Maturity Model: (IRDMO)

- Initial Stage - unpredictable, poorly controlled, and reactive
- Repeatable Stage - characterized for projects, repeatable
- Defined Stage - characterized for the entire organization and is proactive.
- Managed Stage - quantitatively measured and controlled
- Optimizing 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 on security requirements.
- Develop Detailed Security Design; Based on security architecture, design security functions and features for the system.
- Implement System Security; Implement designed security functions and features into the system.
- Assess Security Effectiveness; Assess effectiveness of ISSE activities.

Patch management:

- Inventory
- Allocate Resources
- Pursue updates
- Test
- Change Approval
- Deployment plan
- Rollback plan
- Deploy and verify 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 networking (SDN):

- Application
- Control
- Infrastructure

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 Third party:

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

Security Policy:

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

Common Criteria CC:

- PP - is what customer needs
- ST - is what Vendor provides
- TOE - Actual product
- EAL - is rating which provides Evaluation and Assurance

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

Security information and event management (SIEM):

•Correlation
•Compliance
•Alert

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

Software Protection Mechanisms:

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

Software Acquisition:

- Planning
- Contracting
- Monitoring
- Acceptance
- Follow on

SQL Injection (SQLi):

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

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

Security of Logs:

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

OAuth Flow:

- Ask for request token
- Get Temporary credentials
- Exchange for 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 use the following steps:

- 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 on 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)
- Over lapping 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)

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 secure environment
- Sanitization - combination of 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 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
- Remote file inclusion
- Local file inclusion
- DDOS
- Exploiting vulnerability

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

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 info to the PT team
- Double-blind testing - No information to 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

Enumeration:

- Extracting user names using emails IDs, default passwords
- Extracting user names 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

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 open position;

Threats to the DNS Infrastructure:

- Foot printing
- Denial-of-Service Attack
- Data modification
- Redirection
- Spoofing

Reduce XSS:

- Data validation
- Data Sanitization
- Cookies security
- Output Escaping

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

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 policy should address:

- Storage
- Retention
- Destruction / Disposal

8x 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 topics include:

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

Attacks (1):

•Passive Attacks – hard to detect because the attacker is not effecting 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.

•Cipher text Attacks - The attacker obtains cipher text 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 cipher text, but hardest attack to be successful at.

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

•Chosen Plaintext Attack - The attacker not only has access to the cipher text 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-Cipher text Attack: Attacker can choose different cipher texts 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 depending 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: 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 web site 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 host name 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 attackers 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 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 in 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 Logon: attacker can use a program that presents to the user a fake logon 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 software to allow for unauthorized activity.

•War dialing: war dialer inserts long list of phone numbers into war dialing program in hopes of finding 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 are 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)

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

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 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:

•Blacklist is an explicit deny

•Whitelist is an implicit deny

•Blacklist = "If you are on the list then you are NOT allowed in."

•Whitelist = "If you are NOT on the list then you are NOT allowed in."

RAID:

•RAID 0 - Striped

•RAID 1 - Mirrored

•RAID 2 - Hamming Code requiring either 14 or 39 disks

•RAID 3 - Striped Set with Dedicated Parity (Byte Level)

•RAID 4 - Striped Set with Dedicated Parity (Block Level)

•RAID 5 - Striped Set with Distributed Parity - one drive down, still working

•RAID 6 - Striped Set with Dual Distributed Parity - two drives down, still working

•RAID 1+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 preformed
- Control data flow

Wireless Attack:

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

Secure configuration of HW:

- Secure build
- Secure initial configuration
- Host hardening - remove all non-needed
- Host patching
- Host lock-down
- 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

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 same time without proper locks)
- Contamination (corruption)
- Deadlocking (denying users who access information at 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 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 inference

Note: 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" means with time and "Asynchronous" means without time:

•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

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 good design as 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:

- 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?)
- 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 event of 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

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.
- Ability of the vendor to subcontract work.
- Business continuity/disaster recovery plans. Within what timeframe 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 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

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 within the cloud
- Infrastructure as a Service (IaaS)
  - • Processing, storage, and network services
  - • Client controls operating systems and host configurations

Cloud Storage security:

- Encryption
- Authentication
- Authorization

Security in Cloud Computing:

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

Common Threats in Cloud:

- Data Breaches: Disclosure
- Data Loss: Loss of integrity or destruction
- Account of Service Hijacking: Attacker sniffing or MITM
- Insecure Interfaces/APIs: provided by vendors to access their networks
- DoS/DDos
- Malicious insiders
- Abuse of cloud services: Inherent weakness of any internet service
- Insufficient Due Diligence/Due Care
- Shared Technology Vulnerabilities: multiple tenants brings in risks

Threats Cloud Security:

- Data loss
- Account hijacking
- Insecure API
- DoS
- Extra billing for unused resources
- Inside threats
- Poor security form SP
- Multi-tenancy related breaches

Cloud Risk:

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

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 provider in readable format)
- Portability of the data (e.g. ability to move data to a different provider)
- 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 smooth transition

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

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

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.

The SOC 2 framework includes five 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 a 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 per formed 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 Reference:

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 operational quality
- Amplify feedback loops

DevOps Practices:

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

Markup Language:

•GML: Generalized Markup Language - 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 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
•Extensible Markup Language (XML): Goes beyond describing how to display the data by actually describing the data. 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. Many specific schemas have been created so that companies know exactly what tags are being used for specific purposes. XML is vulnerable to injection attacks. XML is universal format for storing information.

Networking Hardware:

- Modems (converts digital to analog/analog to digital signals)
- Hubs (operate at physical layer, retransmit signals)
- Repeaters (operate at 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:

IDaaS, or Identity as a Service, provides an identity platform as a third-party service. This can provide benefits including integration with cloud services and removing overhead for maintenance of traditional on-premise identity systems, but it can also create risk due to 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

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

Benefits multilayer protocols:

- 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.

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 primary goal of physical security
- Physical security helps prevent operational interruptions
- Primary goal of 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 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

Note: 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 email system.
- Multipartite – Reproduces in more than one way
- Macro Virus – Uses macro programming of app. Infect data files
- Script Virus – Standalone files that can be executed by interpreter
- Script host - .vbs as host to script virus.

Big Data:

Data collections that are 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

NIST:

•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 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	Health care 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 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
•ISO 7498: OSI Model

IEEE:

- IEEE 802.1: Bridging & Management
- 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

CISSP Mindset:

- 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
- Identifying/valuating your assets

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*
- *CISM CRM – ISACA*
- *Cloud Secure Alliance (CSA)*
- *Sybextestbanks.wiley.com*
- *Cloudsecurityalliance.org*
- *NIST documentations/papers*
- *SANS documentations/papers*
- *CCSP Certified Cloud Security Professional, Presentation - Kelly Handerhan*
- *CISSP Certified Information Systems Security Professional, Presentation - Kelly Handerhan*
- *IBM Cloud Services*
- *Cisco Systems*