CISSP

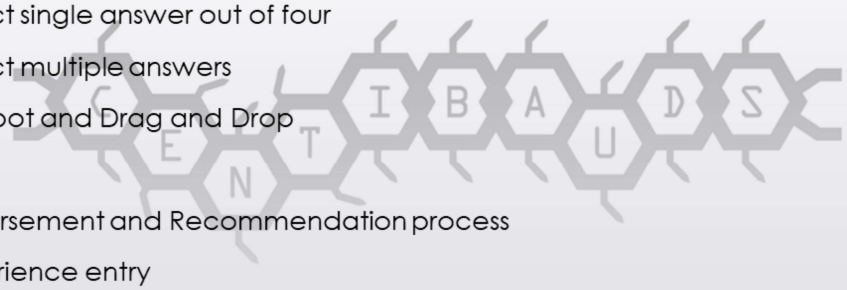
Aitizaz Uddin Syed (M.Engg, CISSP, CISSP-ISSAP, CCSP, CRISC, GICSP, TOGAF)

Overview of the CISSP Exam

- CISSP CAT (Computerized Adaptive Testing)
- 100-150 Questions
- Passing score is 70% or 700/1000
- scored (i.e., operational items) or unscored (i.e., pre-test questions)
- 3 attempts in 12 months period. Max 30 days wait after 1st attempt
- Peace of Mind Option

During Exam and Post-Exam

- Select single answer out of four
- Select multiple answers
- Hotspot and Drag and Drop



- Endorsement and Recommendation process
- Experience entry
- Maintain CPE points

Exam Objectives

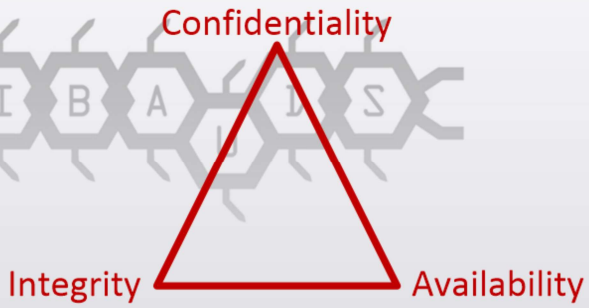
- Domain 1: Security and Risk Management 16%
- Domain 2: Asset Security 10%
- Domain 3: Security Architecture and Engineering 13%
- Domain 4: Communication and Network Security 13%
- Domain 5: Identity and Access Management (IAM) 13%
- Domain 6: Security Assessment and Testing 12%
- Domain 7: Security Operations 13%
- Domain 8: Software Development Security 10%

Domain 1
Security and Risk Management

CHAPTER 1
Security Governance Through Principles and Policies

Cyber Security

- What is Cyber Security?
- CIA Triad
  - Confidentiality
  - Integrity
  - Availability



Confidentiality

- Sensitivity
- Discretion
- Concealment (Security through Obscurity)
- Secrecy
- Privacy
- Seclusion
- Isolation

- **Common control for Confidentiality: Encryption**

Integrity

- Accuracy
- Truthfulness
- Validity
- Accountability
- Responsibility
- Completeness
- Comprehensiveness

- **Common control for Integrity: Hashing**

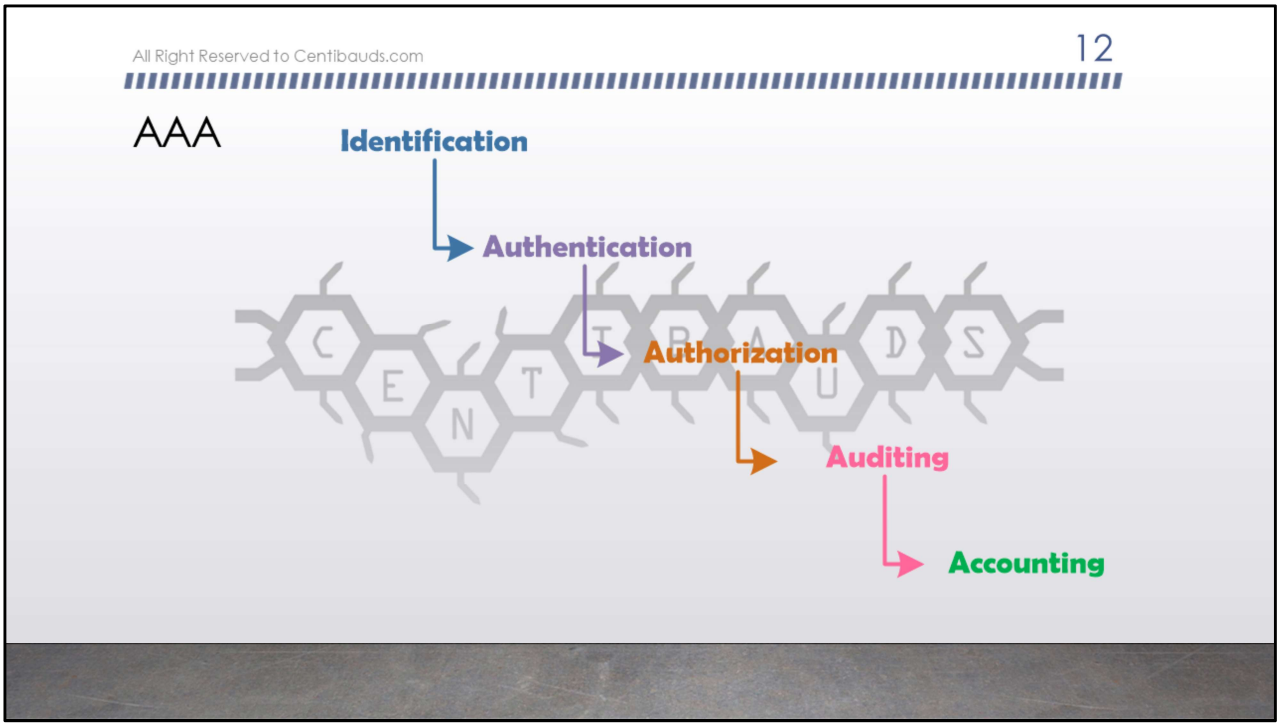
Availability

- Usability
- Accessibility
- Timeliness

- **Common control for Availability: Redundancy, Backup, Assurance**

Some other related terms

- OT has Triad in reverse order
- Disclosure, Alteration, Destruction
- Balance between Overprotection and access enablement
- Authenticity
- **Non-repudiation**
- AAA i.e. Authentication Authorization and Accounting (or Auditing)

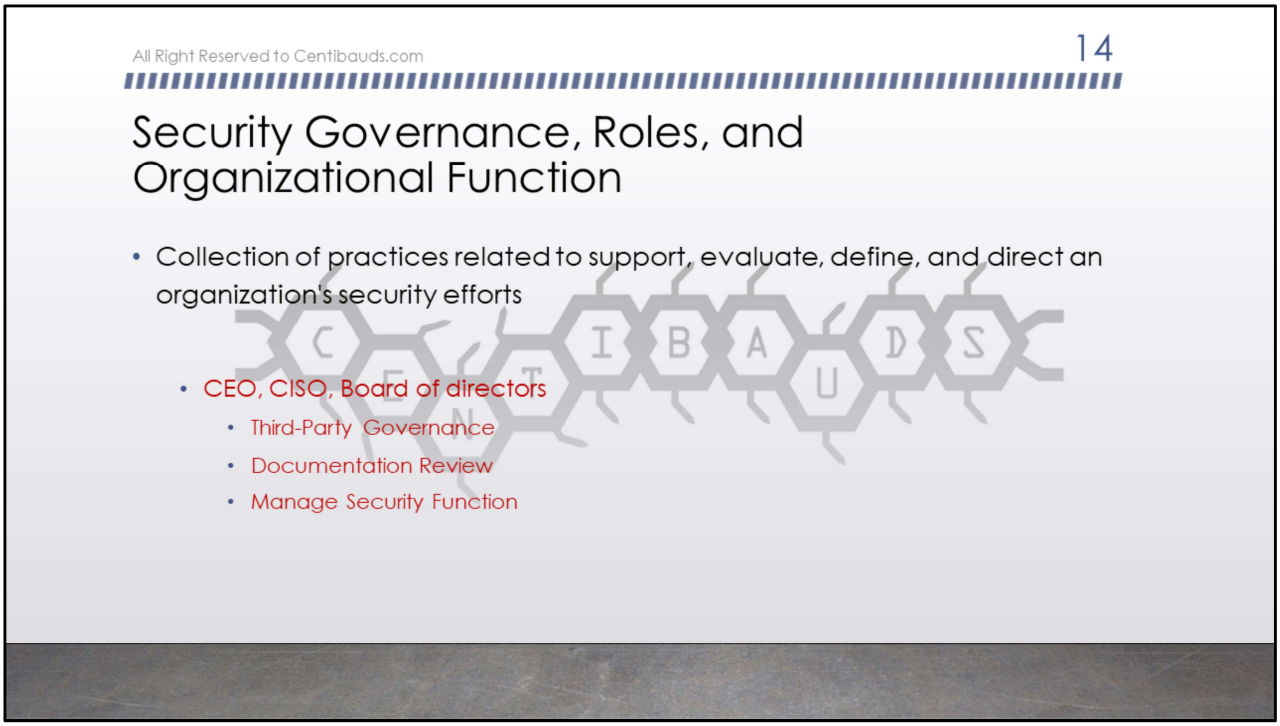


-Auditing involves monitoring (all technical aspects)
-Accounting is to bring in security policy rules and make someone accountable (Non technical aspect)
-Accounting leads a way to nonrepudiation, forensics and evidence development

Some other Terms

- Defense in depth (Defense in Diversity)
  - Abstraction
  - Data Hiding
  - Encryption (Obscurity)
- Due Care vs Due Diligence
- Prudent man rule (Circumstantial action)

-Due care: Obligation
-Due diligence: Making an extra mile effort
-From Cyber security perspective Due care is necessary action and Due Diligence is maintaining record/evidence
-Prudent man rule is set by judicial system enabling empathy and circumstantial actions

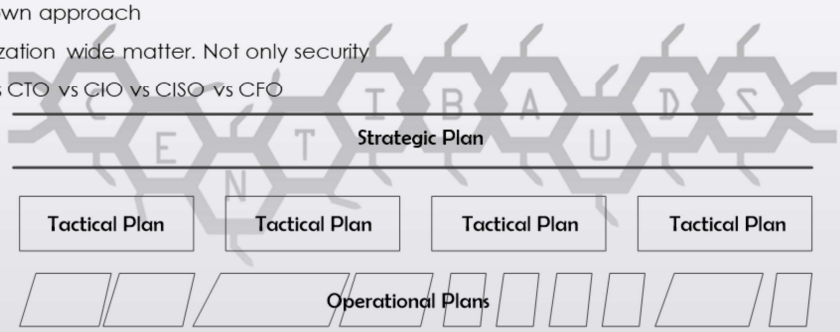


-Third party governance is oversight of law, regulation, obligation, contractual obligation, licensing OR outsource security matters
-Openly document share from peers to evaluate
-Collection of documents and evidence maintenance. Some may give Authorize to operate

Governance
-Define KPIs, levels and thresholds; Any function should return financial benefit to organization, financial benefit to client, automate a process, or develop knowledge base
-Non-quantifiable no benefit. Put value on process is what security function demands
-Non-tangible having value matters organization most

Security Governance, Roles, and Organizational Function (contd..)

- Top-Down approach
- Organization wide matter. Not only security
- CEO vs CTO vs CIO vs CISO vs CFO



- Processes of Divestiture, Resource reduction, Mergers, Acquisitions

-CISO responsible for security
-CEO main decision maker
-CTO ensure technology contribute smoothly for the business requirement
-CIO information as an asset contribute to organization business objectives
-CFO financial objectives to organization requirements and business deliverables

Security Governance, Roles, and Organizational Function (contd..)

- Processes of Services Outsourcing
  - 3rd party assessments (On-Site, Documentation Exchange, Process/Policy Review, 3rd party financial AICPA audit and SOC reports)
  - SLAs, SLR, MOUs
- Organizational Roles and Responsibilities
  - Senior Manager
  - Security Professional
  - Asset Owner
  - Custodian
  - User
  - Auditor

-Define how document will be shared
-Senior Manager ultimate responsible bearing last sign, sign policy etc.
-Security Professional: Write policy and suggest policy procedure; Focus on protection
-Custodian is liaised responsibility of CIA

Security Control Frameworks

- **Standard VS Framework**
- **Certification VS Accreditation**

- ISO/IEC 27000
  - **Standard** to implement ISMS
  - ISMS is to implement CIA across the defined Scope
  - Why ISMS?
    - Competitive advantage
    - Cost Benefit
    - Legal, regulations, obligations
    - Improve organization processes and structure
  - Process is done in PDCA cycle

-ISO22301 BC in normal situation
-ISO31000 Risk Assessment

NIST Special Publication (SP) 800 Series

- NIST Cybersecurity Framework (CSF), formalized in NIST SP 800-53
- NIST Risk Management Framework (RMF) formalized in NIST SP 800-37

Control Objectives for Information and Related Technologies (COBIT)

- Framework enhances IT services for business processes from governance perspective
- Acquired by ISACA
- Follow six principles or priorities:
  - Provide Stakeholder Value
  - Holistic Approach
  - Dynamic Governance System
  - Governance Distinct from Management
  - Tailored to Enterprise Needs
  - End-to-End Governance System
- Can be used for auditing and gap assessment
- ITIL is somewhat similar to COBIT but it develops ITSM and focuses on IT management perspective (Not particularly Risk driven)

Example

-Contextual Security Architecture develops Business requirement or Business Driver, its associated security attributes such as (Confidentiality, Integrity, Availability, Privacy etc.) and risks identified in business risk profile

-Conceptual Security Architecture develops Security Services Architecture highlighting high-level security services such as (access control, encryption, logging etc.) and how security services contribute to mitigation of risk

-Logical Security Architecture specifies the design blueprint of the security services in the form of LLD, security policies, procedures, and standards etc.

-Physical Security Architecture maps technology and physical/virtual entities such as (Firewall, AV solution, perimeter walls etc.) required for security services

-Component Security Architecture covers deep down configuration and management aspect of the security services such as (ACLs, policies config, backup approach etc.)

-Operational Security Architecture focuses on operational aspects such as monitoring, incident response, auditing, compliance

Payment Card Industry Data Security Standard (PCI DSS)

- Advises 12 requirements in 6 objectives

1. Build and protect a secure Network:
   - Install and maintain firewall
   - Remove default configuration, credentials, settings
2. Protect Card holder data
   - Data at rest
   - Data in motion
3. Create vulnerability management program
   - Use, update and maintain Anti Virus
   - Build and maintain secure applications

Payment Card Industry Data Security Standard (PCI DSS) (contd..)

4. Apply strong access control measures
   - Limit access to cardholder data
   - Unique identification for access control
   - Restrict physical access
5. Regularly monitor and Test network
   - Monitor and track network access
   - Test security system and processes regularly
6. Create information security policy
   - Establish functional information security policy

Payment Card Industry Data Security Standard (PCI DSS) (contd..)

- Terms
  - Qualified Security Assessors (QSA)
  - Self Assessment Questionnaire (SAQ)
  - Attestation of Compliance (AoC)
  - Report of Compliance (RoC)
- PCI DSS Levels
  - Level 1: 6 million plus transactions per year external audit by QSA submitted to attain AoC
  - Level 2: 1 million to 6 million transaction per year internal audit RoC submitted to attain AoC
  - Level 3: 20,000 to 1 million transaction per year SAQ filling and submission to attain AoC
  - Level 4: Less then 20,000 transaction is a merchant that should take PoS from certified and approved bank

The Open Group Architecture Framework (TOGAF)

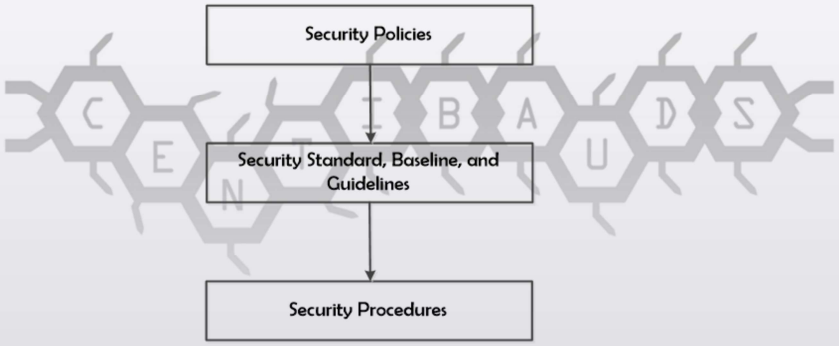
- Framework to enable Enterprise Architecture (EA) and Enterprise Architecture Development Method (ADM)
- Framework for designing, planning, implementing , and governing enterprise architecture
- ADM introduces formal methodology to embed architecture enablement

ADM

Federal Risk and Authorization Management Program (FedRAMP)

- U.S federal agencies cyber security rules for Cloud Service Providers (CSPs)
- Key elements:
  - Security standardization
  - Authorization process
  - Continuous monitoring
  - Reuse of authorizations
  - Collaboration
  - Three impact levels of breach
  - Compliance framework

Security Policy, Standards, Procedures, and Guidelines



Threat Modeling (TM)

- Security process where potential threats are identified, categorized, and analyzed
  - Proactive TM: Start in preliminary stages and proceed onwards
  - Reactive TM: Later stages on developed product; Involves threat hunting and testing

Threat Modeling Process

- Identifying Threats (Asset, Attack, Software oriented)
- Categorize Threats based on models (STRIDE, PASTA, Natural, Man made)
  - Microsoft Threat categorization model of STRIDE (Spoofing, Tampering, Repudiation, Info Disclosure, DoS, Elevation of privilege)
  - Process for Attack Simulation and Threat Analysis (PASTA) is 7 stage model
- Diagramming Potential Attacks (UEBA, UML, Cyber Kill Chain)
- Performing Reduction Analysis (Trust Boundaries, Dataflow Paths, Input Points, Privileged Operations, Security Stance and Approach)
- Response OR Damage potential (Impact)
- Risk Assessment= Impact x Likelihood (Risk Matrix, DREAD)

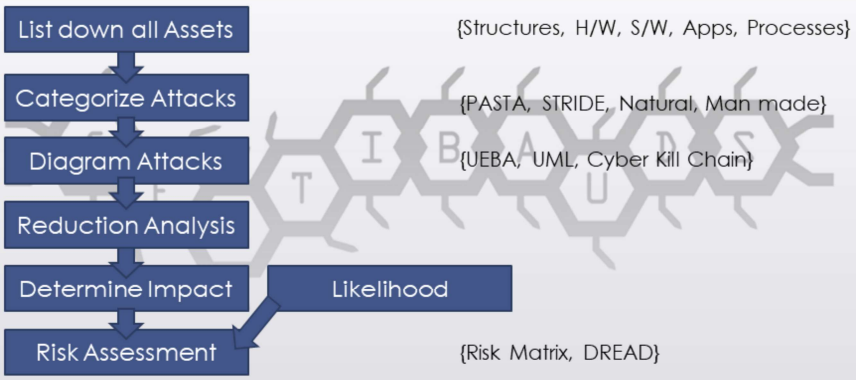
Threat Modeling (contd..)

- Perform rating, ranking, and/or %age
- DREAD
  - Damage Potential [1 to 10]
  - Reproducibility [1 to 10]
  - Exploitability [1 to 10]
  - Affected Users [1 to 10]
  - Discoverability [1 to 10]

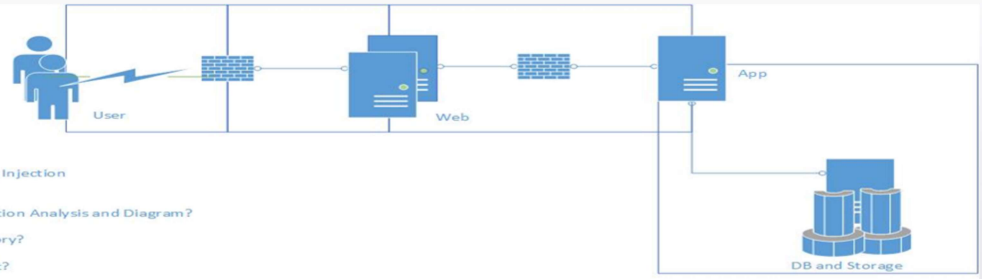
Risk Matrix

Probability \ Impact	H	M	L
H	HH	HM	HL
M	MH	MM	ML
L	LH	LM	LL

Threat Modeling (contd..)



Threat Modelling Example 1



1) SQL Injection

Reduction Analysis and Diagram?

Category?

Impact?

Probability if WAF at Web and Input Validation at APP?

Probability if NO WAF at Web and Input Validation at APP?

Probability \ Impact	H	M	L
H	HH	HM	HL
M	MH	MM	ML
L	LH	LM	LL

D R E A D

Threat Modelling Example 2

2) Abuse case

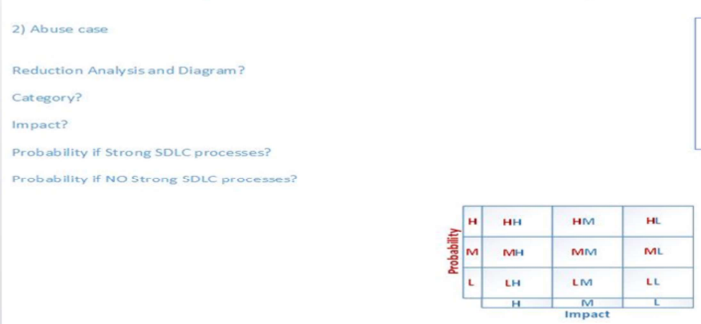
Reduction Analysis and Diagram?

Category?

Impact?

Probability if Strong SDLC processes?

Probability if NO Strong SDLC processes?



Probability \ Impact	H	M	L
H	HH	HM	HL
M	MH	MM	ML
L	LH	LM	LL

D
R
E
A
D

Supply Chain Risk Management

- Supply chain and 3rd party risk assessment
  - Sign-off and Buy-in at every component
  - Commercial-off-the-shelf COTs
  - Trust level developed
  - Normalized SLA and SLR

Supply Chain Risk Management (contd..)

- Silicon Root of Trust – Achieves Authentication, Confidentiality, and Integrity
  - Tamper resistant
  - Secure boot
  - Cryptographic function
  - Remote attestation
- Physically Unclonable Function – Achieves Authentication and Integrity
  - Unique fingerprint and identifier that can't be replicated
  - Challenge response method
- Software Bill of Material
  - List of software used by components and systems to address known vulnerabilities
  - Achieves compliance, transparency, security and management

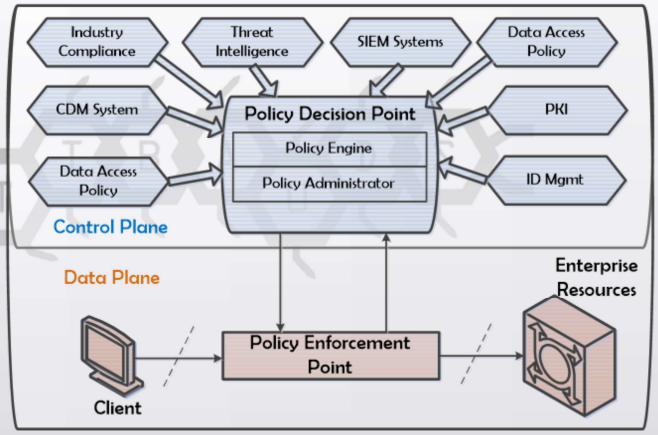
-SRoT, TPM and HSM are similar topic will be discussed onwards
-Biggest difference between PUF and SRoT is PUF generates and maintain its unique keys unlike SRoT stores a provided key

Zero Trust Architecture (NIST 800-207)

- Zero Trust Architecture (ZTA) is developed to address the challenges of perimeter less communication
- Restrict unauthorized access and enforce granular access
- Principles of ZTA:
  - Every entity is a resource
  - All communication is secured irrespective of location
  - Per session base access
  - Granular Attribute based Access Control driven by Risk Assessment and dynamic policy
  - Monitor and measure integrity and security posture of associated assets
  - Authenticate before granting access
- Untrustworthiness of any aspect of network

Zero Trust Architecture (contd..)

- Components of ZTA
- Abstract architecture
  - Agent/Gateway
  - Microperimeter
  - Portal Based
  - Sandboxing



-PDP is divided into Engine that drives all the decision logic and take all the feeds. It has a Trust logic and Trust algorithm
-Enforcement point makes decision to allow and deny
-Continuous Diagnostics and mitigation (patching and vulnerability mitigation)