Domain 1: Security & Risk Management

CISSP Cheat Sheet Series

CIA Triad
- Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and confidential business information.
- Integrity: Ensuring the accuracy and completeness of information and adherence to the correct procedures for its processing.
- Availability: Ensuring timely and reliable access to and use of information by authorized users.

Risk Management
- No risk can be completely avoided.
- Risks can be minimized and controlled to avoid impact of damages.
- Risk management is the process of identifying, examining, measuring, mitigating, or transferring risk.

Risk Frameworks
- ISO 17799 & 2700 Series
- COBIT & COSO
- OCTAVE
- ITIL

Risk Terminology
- Asset: Anything of value to the company.
- Vulnerability: A weakness; the absence of a safeguard.
- Threat: Things that could pose a risk to all or part of an asset.
- Threat Agent: The entity which carries out the attack.
- Exploit: An instance of compromise.
- Risk: The probability of a threat materializing.

Risk Management Life Cycle
- Categorize, Classify & Evaluate Assets
- Analyze: Qualitative vs Quantitative
- Mitigate / Response: Reduce, Transfer, Accept

Risk Management Constraints
- Time, budget
- Statement of organization
- Statement of priorities
- Statement of importance
- Statement of accountability

The 6 Steps of the Risk Management Framework
- Categorize
- Select
- Implement
- Asses
- Authorize
- Monitor

Threat Identification Models
- S.T.R.I.D.E.
  - Spoofing - Tampering - Repudiation - Information Disclosure - Denial of Service - Escalation of Privilege
- D.R.E.A.D.
  - Damage - Reproducibility - Exploitability - Affected - Discoverability
- M.A.R.T.
  - Mitigate - Accept - Reject - Transfer

Disaster Recovery / Business Continuity Plan
- Continuity plan goals
- Statement of importance
- Statement of priorities
- Statement of organization responsibility
- Statement of urgency and timing
- Risk assessment
- Risk acceptance / mitigation

Types of Law
- Criminal law
- Civil Law
- Administrative Law
- Comprehensive Crime Control Act (1964)
- Computer Fraud and Abuse Act (1986)
- Computer Security Act (1987)

Threats & Countermeasures
- Security Awareness Training
- Mandatory Vacations
- Job Rotation
- Intrusion Alarms
- Antivirus Software
- Database Shadowing
- Antivirus Solutions
- Business Continuity Plans
- Server Clustering
- Database Shadowing
- Antivirus Solutions
- Business Continuity Plans

Risk Management Frameworks
- Layering
- Abstractions
- Data Hiding
- Encryption

Data classification
- Entails analyzing the data that the organization retains, determining its importance and value, and then assigning it to a category.

Risk Management
- Operational Plan
- Confidentiality
- Business Continuity Plan
- Smart Cards Encryption
- Encryption Awareness Training
- Mandatory Vacations
- Job Rotation
- Intrusion Alarms
- Audit Trails
- Antivirus Solutions
- Server Clustering
- Database Shadowing
- Antivirus Solutions
- Business Continuity Plans
- Server Clustering
- Database Shadowing
- Antivirus Solutions
- Business Continuity Plans

Risk Acceptance
- Only authorized users are accessing and using the system accordingly.

Security Operations
- Software Development Security

Intellectual Property
- Copyright
- Trademarks
- Patents
- Trade Secrets
- Licensing