Domain 1: Security & Risk Management

CISSP Cheat Sheet Series comparitech

CIA Triad

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Note – Encryption (At transit – TLS) (At rest - AES – 256)
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Availability	Ensuring timely and reliable access to and use of information by authorized users.

***Citation:** https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

Achieving CIA - Best Practices

Separation of Duties	Mandatory Vacations	Job Rotation	Least Privileges	Need to know	Dual Control

Availability Measuring Metrics	RTO/MTD/RPO, MTBF, SLA

D.A.D.

Disclosure	Alteration	Destruction
Opposite of Confidentiality	Opposite of Integrity	Opposite of Availability

IAAAA

Identification	Unique user identification
Authentication	Validation of identification
Authorization	Verification of privileges and permissions for authenticated user
Accountability	Only authorized users are accessing and use the system accordingly
Auditing	Tools, processes, and activities used to achieve and maintain compliance

Plans

Type	Duration	Example
Strategic Plan	up to 5 Years	Risk Assessment
Tactical Plan	Maximum of 1 year	Project budget, staffing etc
Operational Plan	A few months	Patching computers Updating AV signatures Daily network administration

Protection Mechanisms

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

- 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

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Solution – Keep risks at a tolerable and acceptable level.
Risk management constraints – Time, budget

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

***Citation:**https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/

Risk Management Frameworks

Preventive Ex ISO 27001	Deterrent Ex ISO 27000	Detective	Corrective	Recovery
Security Policies	Security Personnel	Logs	Alarms	Backups
Security Cameras	Guards	Security Cameras	Antivirus Solutions	Server Clustering
Callback	Security Cameras	Intrusion Detection Systems	Intrusion Detection Systems	Fault Tolerant Drive Systems
Security Awareness Training	Separation of Duties	Honey Pots	Business Continuity Plans	Database Shadowing
Job Rotation	Intrusion Alarms	Audit Trails		Antivirus Software
Encryption	Awareness Training	Mandatory Vacations		
Data Classification	Firewalls			
Smart Cards	Encryption			

Risk Framework Types

- Security and Risk Management
- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

Risk Management Life Cycle

Assessment	Analysis	Mitigation / Response
Categorize, Classify & Evaluate Assets	Qualitative vs Quantitative	Reduce, Transfer, Accept
as per NIST 800-30:	Qualitative – Judgments	Reduce / Avoid
System Characterization	Quantitative – Main terms	Transfer
Threat Identification	AV – Asset Value	Accept / Reject
Vulnerability Identification	EF – Exposure Factor	
Control Analysis	ARO – Annual Rate of Occurrence	
Likelihood Determination	Single Loss Expectancy = AV * EF	
Impact Analysis	Annual Loss Expectancy = SLE*ARO	
Risk Determination	Risk Value = Probability * Impact	
Control Recommendation		
Results Documentation		

Security Governance

- BS 7799
- ISO 17799 & 2700 Series
- COBIT & COSO
- OCTAVE
- ITIL

The 6 Steps of the Risk Management Framework

- **Categorize**
- **Select**
- **Implement**
- **Asses**
- **Authorize**
- **Monitor**

Threat Identification Models

S.T.R.I.D.E.	**S**poofing - **T**ampering - **R**epudiation - **I**nformation Disclosure - **D**enial of Service - **E**scalation of Privilege
D.R.E.A.D.	**D**amage - **R**eproducibility - **E**xploitability - **A**ffected - **D**iscoverability
M.A.R.T.	**M**itigate - **A**ccept - **R**eject - **T**ransfer

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 (1984)
- Computer Fraud and Abuse Act (1986)
- Computer Security Act (1987)
- Government Information Security Reform Act (2000)
- Federal Information Security Management Act (2002)

Intellectual Property

- Copyright
- Trademarks
- Patents
- Trade Secrets
- Licensing