CISSP NetSECWIZ Notes: 2023 - Created by NetSecWiz, CISSP.

Domain 1: Security and Risk Management

Mnemonic Magic

(ISC)2 Ethics: PAPA = Protect, Act, Provide, Advance

RMF: Crime Scene Investigators Always Act Modestly
Categorize, Select, Implement, Assess, Authorize, Maintain.

Due Diligence: Do Detect

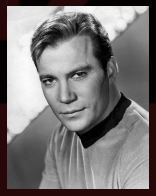
Due Care: Do correct

COBIT: Has IT in it; IT governance.

ITIL: Has IT in it; IT service manager delivery.

Quantitative: Think Like Spock(MATH)

Qualitative: Think Like Kirk(Feeling)



🍺🍺🍺 = 💔😊 **ALE=ARO X SLE: ALE CAUSES AROSLE** 🍺🍺🍺 = 💔😊

ISO: Raging Crackheads Risk Health
Requirements, Code of practice, Risk Management, Health
ISO27001, 27002, 27005, 27799

BCP/DRP: Disastrous Catastrophes Invoke Drastic Damage Planning

Domain 1: Security and Risk Management

Essential Enclave

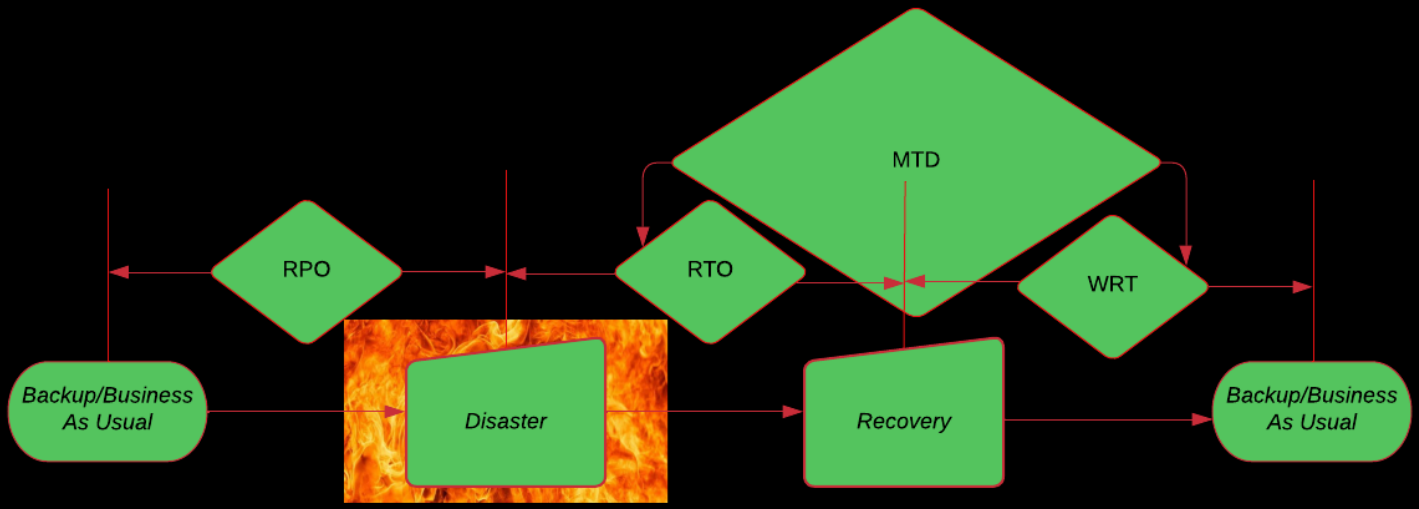
- Guidelines(FYI)
- Procedures(How, Who)
- Standards(What)
- Policies(Why When)
- Business Continuity Management (BCM)
  - Structure, policies, and procedures to create and maintain BCP and DRP
  - Disastrous Catastrophes Invoke Drastic Damage Planning

Business Continuity Plan (BCP) Business	Disaster Recovery Planning (DRP) Technical
Develop Policy	Develop Policy
Conduct BIA	Conduct BIA
Identify Controls	Identify Controls
Develop Contingency Strategies (DRP)	Develop Contingency strategies (DRP)
Develop IT Contingency Plan	Develop IT Contingency Plan
Plan Training	Plan Training
Plan Maintenance	Plan Maintenance

- BCPs contain COOP (Continuity of Operations Plan)
  - Crisis Communications Plan
  - Critical Infrastructure Protection Plan
  - Cyber Incident Response Plan
  - DRP (Disaster Recovery Plan)
  - ISCP (Information System Contingency Plan)
  - Occupant Emergency Plan

Domain 1: Security and Risk Management

- Business Impact Analysis (BIA)
- RPO (Recovery Point Objective): The acceptable amount of data that cannot be recovered
- MTD (Maximum Tolerable Downtime): MTD > RTO + WRT:
  - RTO (Recovery Time Objective): The amount of time to restore the system
  - WRT(Work Recovery Time)
- MTTR (Mean Time to Repair
- MOR (Minimum Operating Requirements)
- WRT (Work Recovery Time)



Domain 1: Security and Risk Management

Challenge Chamber

Professional Ethics

Ethics: Just because something is legal doesn't make it right. Within the ISC context: Protecting information through CIA

ISC2 Code of Ethics Canons

- **Protect society, the commonwealth, and the infrastructure.**
- **Act honorably, honestly, justly, responsibly, and legally.**
- **Provide diligent and competent service to principals.**
- **Advance and protect the profession.**

SLE = AV x EF

ALE= SLE x ARO

Risk Value = Probability * Impact

RTO < MTD

- Legal and Regulatory Issues: Information security professionals must be aware of various laws and regulations that impact their work, such as intellectual property laws, data protection and privacy laws (e.g., GDPR, HIPAA), and governance standards (e.g., ISO 27001).

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

Domain 1: Security and Risk Management

Governance standards and control frameworks.

PCI-DSS - Payment Card Industry Data Security Standard
It is a standard but required if we want to handle or issue credit and debit cards.
OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation. Self Directed Risk Management.
COBIT - Control Objectives for Information and related Technology.
Goals for IT - Stakeholder needs are mapped down to IT related goals. COSO - Goals for the entire organization.
ITIL - Information Technology Infrastructure Library.
IT Service Management (ITSM).

ISO 27000 series:
ISO 27001: Establish, implement, control and improvement of the ISMS. Uses PDCA (Plan, Do, Check, Act)
ISO 27002: Provides practical advice on how to implement security controls
ISO 27004: Provides metrics for measuring the success of your ISMS.
ISO 27005: Standards based approach to risk management.
ISO 27799: Directives to protect PHI (Protected Health Information).

- Risk Assessment Steps:

1. Identify assets and their values: Conduct a comprehensive inventory of assets within the organization and assign them a corresponding value based on their importance and potential impact.
2. Identify threats: Identify potential threats that could exploit vulnerabilities and cause harm to assets.
3. Assess vulnerabilities: Evaluate the weaknesses or vulnerabilities associated with each asset, considering factors such as configuration, access controls, and physical security measures.
4. Estimate the likelihood of threats: Analyze historical data, expert opinions, and industry reports to estimate the likelihood or probability of each identified threat occurring within a given timeframe.
5. Estimate the impact of threats: Assess the potential impact or consequences if a threat is realized, considering factors such as financial loss, operational disruption, reputational damage, and legal implications.
6. Calculate risk levels: Combine the likelihood and impact assessments to assign risk levels to each identified threat, enabling prioritization of mitigation efforts.

Domain 1: Security and Risk Management

- RMM and Levels: Risk Maturity Models (RMMs) evaluate the key indicators and activities of a mature, sustainable, and repeatable risk management process. RMMs typically use a five-level model to assess risk management capability, similar to the Capability Maturity Model (CMM). The levels include:

1. Ad hoc: Initial stage with chaotic risk management processes.
2. Preliminary: Loose attempts at risk management, unique assessments by each department.
3. Defined: Adoption of a common or standardized risk framework across the organization.
4. Integrated: Integration of risk management into business processes, use of metrics to measure effectiveness, consideration of risk in strategic decision-making.
5. Optimized: Risk management focuses on achieving objectives, proactive planning for business success, rather than just reacting to external threats.

- BCP Steps:

1. Project Initiation: Start the BCP project, identify stakeholders, obtain C-level approval, and establish the project structure.
2. Scope the Project: Define the objectives, boundaries, and limitations of the BCP project.
3. Business Impact Analysis: Identify critical systems, functions, and activities, and assess their potential impacts. Determine metrics such as RPO and RTO for each critical component.
4. Identify Preventive Controls: Identify existing and potential preventive controls that can mitigate risks and minimize the impact of disruptions.
5. Recovery Strategy: Develop recovery strategies to restore operations efficiently in the event of a disaster. Consider options such as disaster recovery sites, system restores, or cloud-based solutions.
6. Plan Design and Development: Create a comprehensive BCP document that outlines specific procedures, guidelines, and tools for recovery from different disaster scenarios.
7. Implementation, Training, and Testing: Implement the BCP, provide necessary training to personnel, and regularly test the plan to identify and address any gaps or deficiencies.
8. BCP Maintenance: Continuously review, update, and improve the BCP to ensure its effectiveness as the organization evolves and the threat landscape changes.

Domain 1: Security and Risk Management

Laws

- ITAR, 1976. Defense goods, arms export control act
- FERPA - Education
- GLBA, Graham, Leach, Bliley; credit related PII
- ECS, Electronic Communication Service (Europe); notice of breaches
- Fourth Amendment - basis for privacy rights is the Fourth Amendment to the Constitution.
- 1974 US Privacy Act - Protection of PII on federal databases
- 1980 Organization for Economic Cooperation and Development (OECD) - Provides for data collection, specifications, safeguards
- 1986 (amended in 1996) US Computer Fraud and Abuse Act - Trafficking in computer passwords or information that causes a loss of $1,000 or more or could impair medical treatment.
- 1986 Electronic Communications Privacy Act - Prohibits eavesdropping or interception w/o distinguishing private/public

- Communications Assistance for Law Enforcement Act (CALEA) of 1994 - amended the Electronic Communications Privacy Act of 1986. CALEA requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.

- 1987 US Computer Security Act - Security training, develop a security plan, and identify sensitive systems on govt. agencies.

- 1991 US Federal Sentencing Guidelines - Responsibility on senior management with fines up to $290 million. Invoke prudent man rule. Address both individuals and organizations

- 1996 US Economic and Protection of Proprietary Information Act - industrial and corporate espionage

- 1996 Health Insurance and Portability Accountability Act (HIPPA) amended

- 1996 US National Information Infrastructure Protection Act - Encourage other countries to adopt a similar framework.

- Health Information Technology for Economic and Clinical

- Health Act of 2009 (HITECH) - Congress amended HIPAA by passing this Act. This law updated many of HIPAA's privacy and security requirements.