

# Thor's Quick Sheets - CC® Domain 1

## Contents

Information Security, IT Security, and Cybersecurity .....	2
CIA Triad: Confidentiality, Integrity, and Availability .....	2
IAAA: Identification, Authentication, Authorization, and Accountability .....	2
Privacy.....	3
Risk Management .....	3
Access Control Categories and Types .....	4
Ethics and Governance vs. Management.....	4
Laws and Regulations.....	4
Information Security Governance: Values, Vision, Mission, and Plans .....	5



# Thor's Quick Sheets – CC® Domain 1

## Information Security, IT Security, and Cybersecurity

**Information Security:** Protects all types of information (e.g., paper documents, voice data).

**IT Security:** Protects hardware, software, and data (e.g., computers, networks).

**Cybersecurity:** Protects internet-accessible IT systems.

## CIA Triad: Confidentiality, Integrity, and Availability

### Confidentiality:

- Keep data secret and inaccessible to unauthorized users.
- Use encryption, secure transport protocols, strong passwords, and access controls.
- Threats: Cryptanalysis, social engineering, key loggers, IoT vulnerabilities.

### Integrity:

- Ensure data remains unaltered.
- Use cryptography, checksums, message digests, and digital signatures.
- Threats: Data alterations, code injections, cryptanalysis attacks.

### Availability:

- Ensure data is accessible to authorized users when needed.
- Use IPS/IDS, patch management, redundancy, SLAs.
- Threats: DDOS, application and component failures.

### DAD: Disclosure, Alteration, and Destruction

- **Disclosure:** Unauthorized access to information.
- **Alteration:** Unauthorized changes to data.
- **Destruction:** Data or systems are destroyed or inaccessible.

## IAAA: Identification, Authentication, Authorization, and Accountability

### Identification:

- Methods: Username, ID number, SSN.
- Example: "I am Thor."

### Authentication:

- **Prove Identity:** Use multi-factor authentication.
  - **Type 1:** Knowledge factors (passwords, PIN).
    - Strong, complex passwords.
    - Policy: Minimum length, regular updates, no reuse.
    - Key stretching and clipping levels to enhance security.
  - **Type 2:** Possession factors (ID, smart card).
  - **Type 3:** Biometric factors (fingerprint, iris scan).
    - **Types:** Physiological (fingerprint) and behavioral (typing rhythm).
    - **Errors:**
      - **FRR:** False rejection of authorized users.
      - **FAR:** False acceptance of unauthorized users.
      - **CER:** Optimal balance of FRR and FAR.



# Thor's Quick Sheets – CC® Domain 1

- **Important Considerations**
  - **Privacy Concerns:** Biometrics reveal personal info.
  - **Security Risks:** Biometrics can be spoofed.
  - **Data Breaches:** Much harder to replace biometric data than passwords.
- **Authorization:**
  - **Principles:** **Least privilege** and **need-to-know**.
  - **DAC:** User discretion for access.
  - **MAC:** Labels and clearance levels.
    - **Labels:** Objects have Labels assigned to them; the subject's clearance must dominate the object's label.
    - **Clearance:** Subjects have Clearance assigned to them.
  - **Content-Based Access Control:** Access is provided based on the attributes or content of an object.
  - **RBAC:** Roles determine access.
  - **ABAC:** Attributes and conditions control access.
  - **Context-Based Access Control:** Access to an object is controlled based on certain contextual parameters.
  - **Content-Based Access Control:** Access is provided based on the attributes or content of an object.
- **Accountability:**
  - **Trace Actions to Identity:** Ensures non-repudiation.
  - **Audit Trails:** Logs to track actions.
  - **Non-repudiation:** Proof of actions taken by users.

## Privacy

### Privacy:

- Freedom from observation or disturbance.
- Protection from unauthorized intrusion.

### Rights:

- Privacy is a human right.
- Protection of Personally Identifiable Information (PII).

### Regulations:

- US: Patchwork of laws, inconsistent coverage.
- EU: Strict regulations on data collection, usage, and storage.

## Risk Management

**Phases of Risk Management: Identification, Assessment, Response and Mitigation, Monitoring**

### Risk Formula:

- $\text{Risk} = \text{Threat} * \text{Vulnerability (Likelihood)}$ .
- $\text{Total Risk} = \text{Threat} * \text{Vulnerability} * \text{Asset Value}$ .
- $\text{Residual Risk} = \text{Total Risk} - \text{Countermeasures}$ .

### Components:

- **Threat:** Potentially harmful incident.
- **Vulnerability:** Weakness allowing threat exploitation.



# Thor's Quick Sheets – CC® Domain 1

- **Due Diligence:** Research before implementation.
- **Due Care:** Implementing security measures.

## Risk Assessment:

- **Qualitative Analysis:** Likelihood and impact of risks.
- **Quantitative Analysis:** Cost-based risk evaluation.
- **Risk Responses:** Accept, mitigate, transfer, avoid.
- **Risk Rejection:** Never acceptable.

## Key Indicators:

- **KGI:** Measures goal achievement.
- **KPI:** Measures performance.
- **KRI:** Metrics indicating risk exposure.

## Access Control Categories and Types

### Categories:

- **Administrative Controls:** Policies, training.
- **Technical Controls:** Firewalls, encryption.
- **Physical Controls:** Locks, guards.

### Types:

- **Preventative:** Stop actions (firewalls).
- **Detective:** Identify actions (IDS).
- **Corrective:** Fix issues (patches).
- **Recovery:** Restore systems (backups).
- **Deterrent:** Discourage actions (signs).
- **Compensating:** Substitutes for primary controls.

## Ethics and Governance vs. Management

**ISC2 Code of Ethics:** Protect society, act honorably, provide competent service, advance the profession.

**Computer Ethics:** Do not harm, steal, or snoop with computers. Respect intellectual property.

**Governance:** Set objectives, monitor performance, define risk appetite.

**Management:** Plan and execute activities to meet objectives.

## Laws and Regulations

### Types:

- **Criminal Law:** Punish and deter societal harm.
- **Civil Law:** Compensate victims.
- **Administrative Law:** Government regulations (HIPAA).
- **Private Regulations:** Contractual compliance (PCI-DSS).
- **Customary Law:** Based on traditions.
- **Religious Law:** Based on beliefs.



# Thor's Quick Sheets – CC® Domain 1

## Key Regulations:

- **HIPAA:** US health information privacy.
- **ECPA:** Protects electronic communications.
- **PATRIOT Act:** Expands law enforcement capabilities.
- **CFAA:** Prosecutes computer crimes.
- **GDPR:** EU data protection, strict adherence required.

## Information Security Governance: Values, Vision, Mission, and Plans

### Principles:

- **Values:** Ethics and beliefs.
- **Vision:** Aspirations.
- **Mission:** Purpose and motivation.
- **Strategic Objectives:** Goals and plans.
- **Action & KPIs:** Actions, Recourses, Outcomes, Owners, and Timeframes.

### Documentation:

- **Policies:** High-level mandates.
- **Standards:** Specific technology use.
- **Guidelines:** Recommendations.
- **Procedures:** Detailed instructions.

