CISSP

LAST MINUTE STUDY GUIDE

DOMAIN 2
ASSET SECURITY

JULY 2025

MOS

CISSP Domain 2: Asset Security

Section 2.1: Understand and Apply Information Classification and Ownership

What is Information Classification?

Information classification is the structured process of identifying, evaluating, labeling, and protecting data based on its sensitivity, regulatory requirements, value to the organization, and potential impact if compromised.

Without proper classification, organizations cannot:

- Apply the correct level of security controls
- Comply with legal and contractual requirements
- Prevent data misuse, breaches, or unintentional exposure

Objectives of Classification

Objective	Description
Confidentiality	Ensure sensitive information is not disclosed to unauthorized parties.
Integrity	Prevent tampering or unauthorized modification of data.
Availability	Ensure access to important data is maintained when needed.
Compliance	Meet legal/regulatory requirements (GDPR, HIPAA, PCI-DSS, SOX, etc.)
Operational Security	Maintain internal security processes to avoid insider threats and human error.
Competitive Edge	Safeguard trade secrets, pricing strategies, customer lists, and IP from competitors.

Key Terms & Definitions

Term	Definition

Asset	Anything valuable to an organization – data, people, devices, software, services
Data Owner	The person responsible for defining classification and determining access
Data Custodian	Implements and manages controls to protect data
User	Uses the data within the scope of authorization
Sensitivity	Degree of impact if data is disclosed, altered, or unavailable
Criticality	Importance of the data to operations and mission success

Types of Information Classification Systems

1. Government/Military Classification (Mandatory Access Control)

Based on federal policy, classified by levels of **national security impact**:

Level	Description
Top Secret	Extremely sensitive information; unauthorized disclosure causes "exceptionally grave damage" to national security
Secret	Unauthorized disclosure causes "serious damage" to national security
Confidential	Unauthorized disclosure causes "damage" to national security
Unclassified/Public	No damage if released; may still require control (e.g., FOIA compliance)

2. Commercial/Enterprise Classification (Discretionary Access Control)

Level	Description
Confidential	Sensitive internal information (e.g., financials, legal documents)
Private/Internal Use Only	Business-impacting information like employee data, project plans
Sensitive	May be personal or regulated (e.g., PII, PHI, cardholder data)

Public	Approved for external release (e.g., press releases, marketing material)

Organizations may create hybrid models depending on their sector, geography, and applicable regulations.

Classification Process Lifecycle

1. **Identify Data and Assets**
    - Conduct a full data inventory: structured (databases) and unstructured (emails, docs).
    - Tagging tools, DLP scanners, and manual reviews help locate data.
    - Understand *where* and *how* data flows through systems (data flow diagrams).
2. **Assign an Owner**
    - A senior employee (not IT) who understands the business use case of the data.
    - Owner must be able to define risk tolerances, impact if lost, and required access restrictions.
3. **Determine Sensitivity & Criticality**
    - Analyze what happens if the data is exposed, deleted, or altered.
    - Use Business Impact Analysis (BIA) and Risk Assessment inputs.
4. **Label Data**
    - Labels must be visible and standardized: e.g., "CONFIDENTIAL - INTERNAL HR USE ONLY".
    - Use metadata tagging, header/footer markings, and color-coding (e.g., Red for Confidential).
5. **Apply Controls Based on Classification**
    - Examples include:
        - **Confidential**: encrypted storage, 2FA, strict access control, audit trails

- **Public**: no restriction, but integrity protection (e.g., signed checksums)

- Controls should follow data wherever it resides (on-prem, cloud, mobile).

6. **Review & Update Classification Regularly**
   - Classification may change over time: e.g., embargoed product data becomes public post-launch.
   - Set review cycles (e.g., annual) and automatic triggers (e.g., retention expiry, re-orgs).

Access Control Enforcement by Classification

Control Type	Description
MAC (Mandatory Access Control)	Admin-defined labels; users cannot change access rules (e.g., Top Secret)
DAC (Discretionary Access Control)	Data owner defines access list (e.g., SharePoint permissions)
RBAC (Role-Based Access Control)	Access based on job roles (e.g., Finance can view salary data)
ABAC (Attribute-Based Access Control)	Contextual: user location, time, device, project (used in Zero Trust models)

Real-World Scenarios

Scenario 1:

A marketing intern sends an unreleased press release to a blogger. The information was labeled "Internal – Do Not Distribute". What classification process failed?

- **Answer**: Failure in access enforcement, likely no training, and poor label visibility.

Scenario 2:

A VP wants unrestricted access to all HR records. How do you handle this as a security architect?

- **Answer**: Apply least privilege and consult HR data owner. Even seniority does not override need-to-know policies.

Responsibilities of Key Roles

Role	Duties
Data Owner	Defines classification, approves access, sets retention, requests audits
Data Custodian	Maintains backups, configures ACLs, updates classification labels
System Owner	Oversees systems that store/process data, manages OS/application-level security
User	Uses data per policy, reports suspicious activity
Privacy Officer	Ensures data handling aligns with privacy laws and corporate policies
Compliance Officer	Audits classification policy adherence, especially in regulated sectors (e.g., finance, healthcare)

Memory Aids & Mnemonics

- **CLASS**: Classification Lifecycle =
    - **C**reate Inventory
    - **L**abel Data
    - **A**ssign Owner
    - **S**et Controls
    - **S**chedule Review
- **POLAR**: What to consider when classifying
    - **P**rivacy
    - **O**perational Impact
    - **L**egal Risk
    - **A**ccess Requirements
    - **R**etention Duration

Exam Triggers from This Section

- "Who defines the classification?" → **Data Owner**
- "What type of control is used in military environments?" → **MAC**
- "Which role is responsible for technical enforcement of controls?" → **Custodian**
- "Which principle is violated if a user accesses more than required?" → **Least Privilege**
- "What is the best way to label unstructured documents?" → **Visible headers/footers and metadata tags**

Section 2.2: Determine and Maintain Information and Asset Ownership

2.2.1 What Is Asset Ownership?

Every information asset—whether it's a database, an email archive, or a physical report—must have a designated owner who is accountable for how that asset is used, secured, stored, and eventually disposed of.

Who Is the "Owner" of Data?

Not necessarily the creator. Not IT.

- Typically, the business unit leader who understands the value and purpose of the asset.
- E.g., Payroll records → HR Director is the data owner, not the payroll tool vendor.

Core Responsibilities of a Data Owner

Responsibility	Description
Classification	Determines how sensitive data is (e.g., Public, Private, Confidential)
Access Approval	Authorizes who can access the data and at what level
Protection Level	Decides what security controls are needed (e.g., encryption, ACLs)

Compliance Alignment	Ensures the data is handled in accordance with laws/regulations
Retention & Disposal	Defines how long data is kept and when/how it should be destroyed

Important Distinction:
Ownership ≠ Custody. A custodian maintains technical controls. The owner defines policies and oversight.

2.2.2 What Is Data Custodianship?

The **data custodian** implements and enforces the policies defined by the data owner.

Function	Role of Custodian
Technical Access	Configure and manage access control lists (ACLs)
Data Protection	Apply encryption, backups, monitoring, patching
Logging & Reporting	Maintain audit trails for who accessed/modified the data
Data Recovery	Ensure business continuity and disaster recovery plans are in place

2.2.3 Key Roles Compared

Role	Function
Data Owner	Assigns classification, defines retention, approves access
Data Custodian	Implements technical controls, manages backups
User	Uses data responsibly, reports issues
System Owner	Owns the infrastructure (servers, applications)
Security Officer	Oversees enforcement of security policies
Auditor	Verifies data is handled according to policy

2.2.4 Defining Ownership Through Policies

Organizations should define ownership responsibilities via:

- **Data Classification Policy**
- **Access Control Policy**
- **Acceptable Use Policy**
- **Information Lifecycle Management Policy**

These should be backed by awareness training, automated DLP solutions, and enforcement processes.

2.3 Information and Asset Retention

Now we move into a major sub-area closely related to ownership:

2.3.1 What Is Data Retention?

Data retention refers to the strategic and policy-based decision of how long to keep specific types of data and what procedures to follow for its eventual disposal.

Not all data should be kept forever. Excessive retention creates:

- **Legal liability** (discoverability in lawsuits)
- **Compliance risk** (GDPR fines for storing longer than needed)
- **Storage cost & attack surface**

Data Retention Policies Should Include:

1. **Data Type** – Personal data, financial, medical, source code, logs
2. **Retention Period** – e.g., HR records = 7 years, CCTV footage = 30 days
3. **Storage Location** – Cloud, backup tape, data warehouse
4. **Access Control** – Who can access it during retention
5. **Secure Disposal Method** – Based on classification (see 2.4)

Retention Standards & Regulations

Standard/Regulation	Retention Requirement

SOX (Sarbanes-Oxley)	7 years for financial records
HIPAA	6 years for health data
GDPR	Only as long as necessary (no fixed duration, must be justifiable)
PCI DSS	1 year for audit logs, 3 months must be immediately available
Company IP	May retain indefinitely, but with strict controls

2.4 Information Lifecycle & Secure Disposal

2.4.1 Information Lifecycle Stages

Stage	Description
Create	New data is generated or collected
Store	Stored in secure environments (cloud, DB, backup)
Use	Accessed, edited, analyzed; governed by access controls
Share	Transmitted internally or externally (with encryption, DLP)
Archive	Moved to long-term storage; rarely accessed
Destroy	Secure deletion, wiping, or shredding after retention ends

2.4.2 Secure Disposal Methods

Media Type	Recommended Disposal
Paper	Cross-cut shredding, incineration
Hard Drives	Degaussing, overwriting (DoD 5220.22-M), physical destruction
Flash Drives	Cryptographic erasure or physical destruction
Cloud Data	API-based deletion followed by cloud provider's sanitization process
Memory (RAM)	Automatically cleared on shutdown (but consider hibernation data)

Tip: Always maintain a **certificate of destruction** for legal and audit trail purposes.

2.4.3 Data Sanitization Techniques

Technique	Description	Best Used When
Clearing	Remove data with standard OS delete commands	Reuse within trusted environment
Purging	Overwrite using tools like DBAN or DoD wipe utilities	Medium sensitivity data reuse
Degaussing	Magnetic field disrupts drive platters	Bulk HDD disposal
Destruction	Physical destruction (drill, shred, melt)	Highly sensitive or end-of-life assets

Exam Tip: Don't Confuse These

Term	Definition
Erasure	Making data unreadable by overwriting
Deletion	Logical removal; data can often be recovered
Sanitization	Comprehensive process of ensuring data is unrecoverable
Shredding	Physical destruction of media (paper or hardware)

Privacy Protection, Data Residency, and Asset Handling in Complex Environments

2.5 Protect Privacy

Protecting privacy means ensuring personally identifiable information (PII), sensitive personal data, and other private records are collected, processed, stored, and disposed of in accordance with legal, ethical, and organizational obligations.

2.5.1 What is PII?

Personally Identifiable Information (PII) is any data that can be used to identify an individual either directly or indirectly.

Examples:

Direct Identifiers	Indirect Identifiers
Full Name	IP Address

Passport Number	GPS Coordinates
National ID Number	Date of Birth
Biometric Data	Purchase Behavior

2.5.2 Sensitive PII (SPII) & Special Categories

Some jurisdictions treat specific **types of PII as extra sensitive, requiring explicit consent and stronger controls.**

Region	Special Data Types
GDPR (EU)	Health, biometrics, sexual orientation, political views
HIPAA (US)	Personal Health Information (PHI)
PCI DSS	Cardholder data (PAN, CVV)

2.5.3 Privacy Principles (OECD & GDPR-Aligned)

Principle	Meaning
Notice	Users must be informed when their data is collected
Consent	Data collection must be voluntary unless exempted
Purpose Limitation	Collected for specific, explicit purposes
Data Minimization	Collect only what's strictly necessary
Accuracy	Ensure data is current and correct
Storage Limitation	Data retained only as long as needed
Integrity and Confidentiality	Protect data against loss or misuse
Accountability	Data controllers must prove compliance

2.5.4 Privacy Roles in Organizations

Role	Description
Data Controller	Determines the purpose and means of processing PII
Data Processor	Acts on behalf of the controller (e.g., cloud vendor)

Data Subject	The individual whose data is collected
DPO (Data Protection Officer)	Oversees privacy compliance, mandatory under GDPR for large-scale sensitive data processing

2.5.5 Privacy by Design (PbD) & Privacy by Default

- **PbD**: Embed privacy into system architecture from the beginning.
- **PbD Default**: Settings should be private unless user opts in to share.

Example: Social media profile visibility is set to "Friends Only" by default—not Public.

2.5.6 Privacy Breach Handling

- **Detect**: DLP alerts, anomaly detection
- **Contain**: Quarantine affected systems
- **Report**: Notify Data Protection Authorities (e.g., within 72 hours under GDPR)
- **Notify**: Inform impacted data subjects with actionable steps

Legal impact varies by jurisdiction; breach notification laws differ globally.

2.6 Ensure Appropriate Asset Handling

2.6.1 Protecting Data Across States

Data State	Description	Protection Methods
At Rest	Stored on disk or backup	Full-disk encryption, access control, volume encryption
In Transit	Moving across networks	TLS, VPN, encrypted APIs
In Use	Active in memory or processing	Encrypted memory, secure enclaves, access logging

2.6.2 Handling Media Securely

1. Media Labeling

- Apply classification labels (e.g., "Confidential") on USBs, printed docs, HDDs.

- Use color codes, barcodes, or RFID tagging for tracking.

2. Storage of Media

- Lock physical drives in safes or racks
- Secure server rooms and offsite media vaults (fire-resistant, humidity-controlled)

3. Transport of Media

- Always use tamper-proof, logged, secure carriers for sensitive data
- Chain of custody logs must be maintained
- Prefer electronic over physical transmission when possible

2.6.3 Remanence and Residual Risk

Remanence = residual data remaining after deletion or formatting
Threat: Skilled attackers may recover sensitive data from "deleted" media.

Controls:

- Use secure wipe tools
- Purge with DoD-standard software (7-pass overwrite)
- Destroy drives with crushers or shredders

2.6.4 BYOD & Mobile Asset Security

BYOD (Bring Your Own Device) introduces flexibility but increases risk.

Risk	**Control**
Data leakage via untrusted apps	MDM solutions, containerization
Lost/stolen devices	Full disk encryption, remote wipe
Unauthorized cloud sync	Disable third-party storage apps

Acceptable Use Policies (AUP) and **Mobile Device Policies** must:

- Define who can use personal devices
- Set security baselines (encryption, screen lock, antivirus)
- Enforce device registration and compliance

2.6.5 Asset Handling in Cloud & Outsourced Environments

Concern	Control
Data sovereignty	Host data in compliant regions
Shared responsibility	Understand split between org and CSP
Loss of visibility	Use CASB tools, require audit logs
Vendor lock-in	Ensure data portability in contracts
Deletion & sanitization	Demand verifiable deletion processes

Remember: Even if you outsource the process, you **don't outsource accountability** under law or compliance frameworks.

Intellectual Property, Licensing, Logging, and Asset Management

2.7 Identify and Support Intellectual Property (IP) Requirements

Organizations must protect intellectual property (IP) to maintain their competitive advantage, compliance posture, and brand integrity.

2.7.1 What Is Intellectual Property (IP)?

IP refers to intangible creations of the mind that carry commercial value and are legally protected.

IP Type	Description
Trade Secrets	Confidential business info (e.g., algorithms, formulas, internal processes)
Copyrights	Legal rights over original creative works (e.g., code, documentation, graphics)
Patents	Exclusive rights for inventions (granted after formal registration)
Trademarks	Brand identity elements like logos, slogans, and product names

2.7.2 Handling Copyrighted Content

What you CAN'T do without permission:

- Reproduce licensed training videos or books
- Copy code libraries into your proprietary code
- Distribute open-source components without honoring license terms

2.7.3 Software Licensing Models

License Type	Description
Proprietary (Commercial)	Must be purchased; vendor retains IP rights (e.g., Microsoft Office)
Freeware	Free to use but not to modify (e.g., Adobe Reader)
Shareware	Try-before-you-buy; limited time use
Open Source	Free to use, modify, and distribute (under conditions)
Copyleft (e.g., GPL)	Derivative works must also be open source
Creative Commons	Used for content, not software (multiple levels of permission)

Understand how each type affects your ability to use, modify, and distribute content/software.

2.7.4 Digital Rights Management (DRM)

DRM controls are implemented to prevent unauthorized duplication or distribution of licensed materials.

Mechanism	Use Case
License keys	Software activation
Copy protection	Media access control
Online validation	Enforce usage limits (e.g., number of devices)

Organizations should ensure DRM solutions don't interfere with user productivity or incident response capabilities.

2.7.5 Legal Risks of Violating IP

Violation	Consequences
Using pirated software	Lawsuits, malware exposure, audit failure
Breaching OSS licenses	Forced release of proprietary code (under GPL)
IP theft (e.g., ex-employee leaking source code)	Civil/criminal penalties

2.8 Establish Asset Handling Requirements

2.8.1 Asset Management Lifecycle

Phase	Action
Acquisition	Inventory assigned with unique ID
Deployment	Configuration baseline applied (e.g., Group Policy, CIS hardening)
Usage	Tracked and monitored; access controlled
Maintenance	Patches, upgrades, backups applied
Decommissioning	Sanitized and removed from inventory; disposal certificate issued

ASSET MANAGEMENT LIFECYCLE

2.8.2 Asset Inventory Controls

- Maintain up-to-date asset inventory: hardware, software, cloud, virtual, mobile
- Include:
    - Owner
    - Serial Number
    - Configuration baseline
    - OS version, patch level
    - Classification level
    - Location

Tooling Examples:

- CMDBs (ServiceNow, BMC Remedy)
- Endpoint Detection & Response (EDR) tools
- Network scans to detect rogue/unmanaged devices

2.8.3 Logging and Monitoring

Objective	Explanation
Integrity	Logs must be tamper-proof (e.g., immutable or signed)
Accountability	Capture who did what, when, and how
Forensics	Logs are critical evidence in incident response
Compliance	PCI DSS, SOX, HIPAA all require audit logging

Include:

- Asset provisioning logs
- Change management logs
- Incident and exception logs
- Decommissioning logs (with sanitization confirmation)

2.8.4 Protection of Asset Metadata

Even asset metadata (e.g., device IP, OS type, installed software) can be exploited if leaked.

Threat	Exploitable By
Open ports & firmware version	Attackers scanning for vulnerabilities
Device names (e.g., FINANCE-PC01)	Helps attackers map targets
Software inventory	Enables license compliance audits or exploit targeting

- Enforce RBAC for inventory systems.
- Avoid exposing inventory reports via email or SharePoint

2.8.5 Example Policy Inclusions

- **Who is authorized** to handle sensitive assets
- **Labeling requirements** per classification level
- **Chain of custody logs** for movement of media or devices
- **Acceptable Use** rules (e.g., USB policy, BYOD terms)
- **Escalation procedures** for lost/stolen assets

Final Thoughts

Domain 2 is the heart of data governance, where trust, control, and responsibility converge. It emphasizes that security isn't just about protecting systems—it's about safeguarding the value embedded in assets throughout their lifecycle.

The Core Principle:

"You can't secure what you don't classify, own, and track."

Foundation Pillars of Domain 2:

1. **Data Classification** – Label data based on its sensitivity and value. The more critical the data, the tighter the controls.
2. **Ownership** – Every asset needs a clearly defined owner, not just someone who maintains it. Owners make policy decisions.
3. **Privacy Protection** – Understand and enforce privacy laws (GDPR, HIPAA) and embed privacy by design into all data handling.
4. **Retention & Disposal** – Keep data only as long as necessary, and dispose of it securely to prevent data remanence.
5. **Handling & Protection** – Whether at rest, in transit, or in use, data must be protected using appropriate encryption, access controls, and monitoring.
6. **Special Environments** – Cloud, BYOD, and outsourced ecosystems introduce complexity—know your risks and your responsibilities.
7. **IP & Licensing** – Respect intellectual property, manage licenses legally, and avoid legal landmines like pirated or misused software.
8. **Asset Inventory & Logging** – Maintain up-to-date records of your assets, and ensure all actions on them are monitored and auditable.

Thank You

Want to learn CISSP? Get trained for just ₹4,999/- at MoS!

MINISTRY OF MOS SECURITY

WWW.MINISTRYOFSECURITY.CO