Thor's Study Guide - CISSP® Domain 2

Contents

Thor's Study Guide – CISSP® Domain 2

Introduction to Domain 2

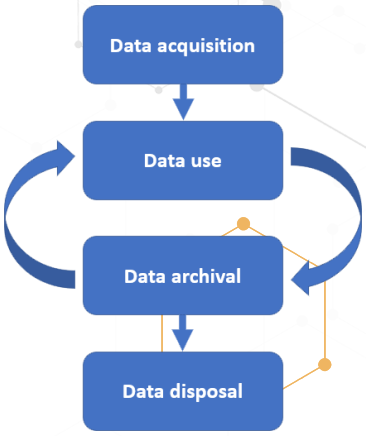
In this domain we cover:

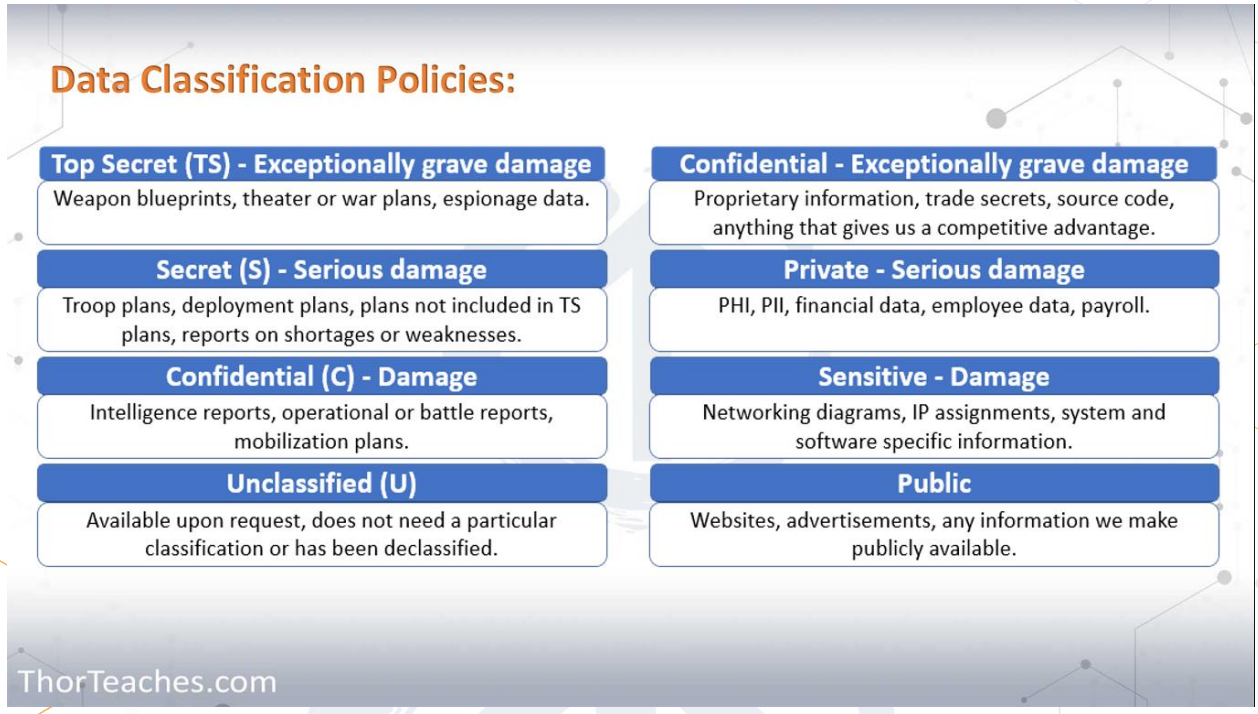
- **The Information Life Cycle.**
- **Information and Asset Classification:**
  How we classify our data, so we know what to protect and how? How do we store and inventory the data?
- **Ownership (Data owners, System owners, and Data custodians):**
  Who owns the data and what are the different roles?
- **Protect Privacy:**
  How do we protect data privacy?
  Memory and data remanence.
- **Appropriate Retention:**
  We keep data as long as it is useful or required, whichever is longest.
- **Data Security Controls:**
  How we protect our data in motion, at rest, and in use and how we securely destroy hardware.
- **Handling Requirements (e.g., markings, labels, storage):**
  How we label, store, and inventory our data so we can properly dispose of it when it is no longer needed.

This domain is the smallest both in the concepts it covers and the percentage of the weighted exam questions (10%).

The Information Life Cycle

- **Data acquisition.**
  - The information is either created or copied from another location.
  - Make it useful, index it, and store it.
- **Data use.**
  - How do we ensure the data is kept confidential, the integrity is intact, and it is available when needed (The CIA triad).
- **Data archival.**
  - Retention required by law, or the data will be used later.
  - Archival vs. backup.
- **Data disposal.**
  - How do we dispose properly of the data once it is no longer useful and required?





Data Classification Policies

- **Labels**: ***Objects have Labels*** assigned to them.
  - The label is used to allow Subjects with the right clearance to access them.
  - Labels are often more granular than just "Top Secret" they can be "Top Secret – Nuclear."

- **Clearance**: ***Subjects have Clearance*** assigned to them.
  - A formal decision on a subject's current and future trustworthiness.
  - The higher the clearance, the more in-depth the background checks should be (always in military, not always in the corporate world).
- **Formal Access Approval:**
  - Document from the data owner approving access to the data for the subject.
  - Subject must understand all requirements for accessing the data and the liability involved if compromised, lost, or destroyed.
  - Appropriate Security Clearance is required as well as the Formal Access Approval.
- **Need to know:**
  - Just because you have access does not mean you are allowed the data.
  - You need a **valid** reason for accessing the data. If you do not have one you can be terminated/sued/jailed/fined.

- Leaked information about Octomom Natalie Suleman cost 15 Kaiser employees fines or terminations because they had no valid reason for accessing her file.
- We may never know who actually leaked the information. It may not be one of the 15, but they violated HIPAA by accessing the data.

- **Least privilege:** Users have the minimum necessary access to perform their job duties.

Sensitive Information and Media Security

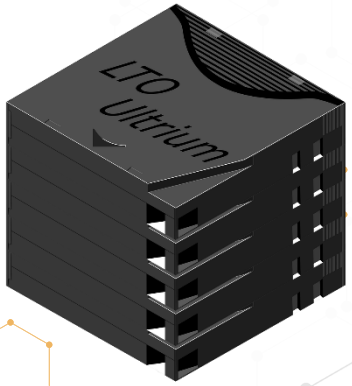
- **Sensitive information**
  Any organization has data that is considered sensitive for a variety of reasons.
  *We want to protect the data from Disclosure, Alteration and Destruction (**DAD**).*

  - **Data has 3 States:** We want to protect it as well as we can in each state.
    - **Data at Rest** (Stored data): This is data on disks, tapes, CDs/DVDs, USB sticks.
      - ☐ We use disk encryption (full/partial), USB encryption, tape encryption (avoid CDs/DVDs).
      - ☐ Encryption can be hardware or software encryption.
    - **Data in Motion** (Data being transferred on a network).
      - ☐ We encrypt our network traffic, end to end encryption, this is both on internal and external networks.
    - **Data in Use:** (We are actively using the files/data, it can't be encrypted).
      - ☐ Use good practices: clean desk policy, print policy, allow no 'shoulder surfing', may be the use of view angle privacy screen for monitors, locking computer screen when leaving workstation.

  - **Data handling:**
    - Only trusted individuals should handle our data; we should also have policies on how, where, when, why the data was handled. Logs should be in place to show these metrics.
  - **Data storage:**
    - Where do we keep our sensitive data? It should be kept in a secure, climate-controlled facility, preferably geographically distant or at least far enough away that potential incidents will not affect that facility too.

- ☐ Many older breaches were from bad policies around tape backups.
- ☐ Tapes were kept at the homes of employees instead of at a proper storage facility or in a storage room with no access logs and no access restrictions (often unencrypted).

- **Data retention:**
  - Data should not be kept beyond the period of usefulness or beyond the legal requirements (whichever is greater).
  - Regulation (HIPAA or PCI-DSS) may require a certain retention of the data (1, 3, 7 years, or infinity).
  - Each industry has its own regulations and company policies may differ from the statutory requirements.
  - Know your retention requirements!



Data, system, mission ownership, custodians, and users

Each role is unique and has certain responsibilities to ensure our data is safe.

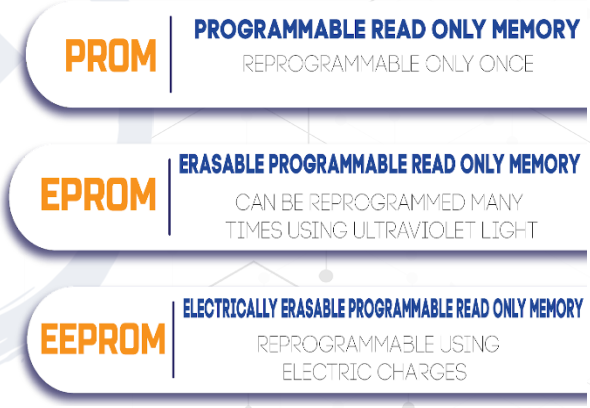
- **Mission/business owners:**
  - Senior executives make the policies that govern our data security.
- **Data/information owners:**
  - Management level, they assign sensitivity labels and backup frequency.
  - This could be you or a data owner from HR, payroll, or other departments.
- **Data custodians:**
  - These are the technical hands-on employees who do the backups, restores, patches, and system configuration. They follow the directions of the data owner.
- **System owner:** Management level and the owner of the systems that house the data.
  - Often a data center manager or an infrastructure manager.
- **Data controllers and data processors:**
  - Controllers create and manage sensitive data in the organization (HR/Payroll)
  - Processors manage the data for controllers (Outsourced payroll).
- **Security Administrators:**
  - Responsible for firewalls, IPS' (Intrusion Prevention Systems), IDS' (Intrusion Detection Systems), security patches, create accounts, and assign access to the data following the data owners' directions.
- **Supervisors:**
  - Responsible for user behavior and assets created by the users. Directly responsible for user awareness and needs to inform the security administrator if

there are any changes to user employment status, user access rights, or any other pertinent changes to an employees' status.

- **Users:**
  - These are the users of the data. User awareness must be trained; they need to know what is acceptable and what is not acceptable, and the consequences for not following the policies, procedures, and standards.
- **Auditors:**
  - Responsible for reviewing and confirming our security policies are implemented correctly, we adhere to them, and that they provide the protection they should.

Memory and Data Remanence

- **Data Remanence:** Data left over after normal removal and deletion of data.
- **Memory**: Is just 0s (off) and 1s (on); switches representing bits.
  - **ROM:**
    - **ROM** (Read Only Memory) is nonvolatile (retains memory after power loss); most common use is the BIOS.
      - **PROM** (Programmable read only memory)
      - **EPROM** (Erasable programmable read only memory)
      - **EEPROM** (Electrically erasable programmable read only memory)



    - **PLD** (Programmable logic devices) are programmable after they leave the factory (EPROM, EEPROM and flash memory). Not PROM.

- **Cache Memory:** L1 cache is on the CPU (fastest), L2 cache is connected to the CPU, but is outside it.
- **RAM** (Random Access Memory) is volatile memory. It loses the memory content after a power loss (or within a few minutes). This can be memory sticks or embedded memory.
  - **SRAM and DRAM**:
    - **SRAM** (Static RAM): Fast and expensive. Uses latches to store bits (Flip-Flops).
      - Does not need refreshing to keep data, keeps data until power is lost. This can be embedded on the CPU.
    - **DRAM** (Dynamic RAM) Slower and cheaper. Uses small capacitors.

SRAM

SDRAM

- Must be refreshed to keep data integrity (100-1000ms).
- This can be embedded on graphics cards.
- **SDRAM**: (Synchronous DRAM):
  - → What we normally put in the motherboard slots for the memory sticks.
  - → DDR (Double Data Rate) 1, 2, 3, 4 SDRAM.

- **Firmware and SSDs (Solid State Drives).**
  - **Firmware:**
    - This is the BIOS on a computer, router or switch; the low-level operating system and configuration.
    - The firmware is stored on an embedded device.
    - PROM, EPROM, EEPROM are common firmware chips.
  - **Flash memory:**
    - Small portable drives (USB sticks are an example); they are a type of EEPROM.
  - **SSD drives** are a combination of EEPROM and DRAM, can't be degaussed.
    - To ensure no data is readable we must use ATA Secure Erase or/and destruction of SSD drives.

Data Destruction

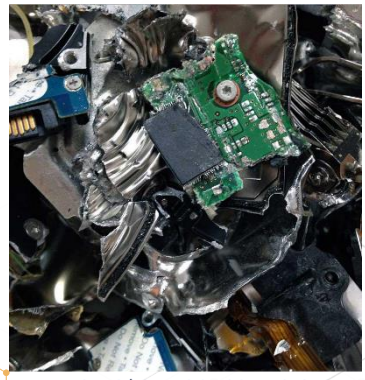
When we no longer need a certain media, we must dispose of it in a manner that ensures the data can't be retrieved. This pertains to both electronic media and paper copies of data.

- **Paper disposal** – It is highly encouraged to dispose of ANY paper with any data on it in a secure manner. This also has standards and cross shredding is recommended. It is easy to scan and have a program re-assemble documents from normal shreds like this one.
- **Digital disposal** – The digital disposal procedures are determined by the type of media.
  - **Deleting, formatting, and overwriting (Soft destruction):**
    - **Deleting** a file just removes it from the table; everything is still recoverable.
    - **Formatting** does the same, but it also puts a new file structure over the old one. Still recoverable in most cases.
    - **Overwriting** (Clear) is done by writing 0s or random characters over the data.
    - **Sanitization** is a process of rendering target data on the media infeasible for a given level of recovery effort.

- **Purge** is removing sensitive data from a system or device to a point where data recovery is no longer feasible even in a laboratory environment.

- **Degaussing** destroys magnetic media by exposing it to a very strong magnetic field. This will also most likely destroy the media integrity.

- **Full physical destruction is safer than soft destruction:**
  - **Disk crushers** do exactly what their name implies: they crush disks (often used on spinning disks).
  - **Shredders** do the same thing as paper shredders do; they just work on metal. These are rare to have at normal organizations, but you can buy the service.
  - **Incineration, pulverizing, melting, and acid** are also (very rarely) used to ensure full data destruction.


Crushed/shredded hard disk fragments.

It is common to do multiple types of data destruction on sensitive data (both degaussing and disk crushing/shredding).

Data Security Controls and Frameworks

- We use standards, baselines, scoping and tailoring to decide which controls we use, and how we deploy them.
- Different controls are deployed for data at rest and data in motion.
- Some of the standards and frameworks used could be PCI-DSS, ISO27000, OCTAVE, COBIT, or ITIL.
- **Scoping** is determining which portion of a standard we will deploy in our organization.
  - We take the portions of the standard that we want or that apply to our industry and determine what is in scope and what is out of scope for us.
- **Tailoring** is customizing a standard to your organization.
  - This could be, we will apply this standard, but we use a stronger encryption (AES 256bit).
- **Certification**: A system, and the security measures to protect it, meet the security requirements set by the data owner or by regulations/laws.
- **Accreditation**: The data owner accepts the certification and the residual risk. This is required before the system can be put into production.

Data protection

- **Digital Rights Management (DRM)** - Uses technology and systems to protect copyrighted digital media.
    - Encryption – Regional DVDs.
    - Permissions management and limiting access.
    - Serial numbers, limit installations, expiry dates, IP addresses, geolocation, VPN.
    - Copy restrictions: Copy, edit, saving, screenshots, screen recording, printing.
    - Persistent authentication and audit trails.
    - Tracking – watermarks or meta data embedded in files.
- **Cloud Access Security Broker (CASB)** – on-premises or cloud software between our users and our cloud applications.
    - Monitors user activity, warns admins about possible malicious/dangerous actions, malware prevention, protects against shadow IT, and enforces security policy compliance.
- **Data Loss Prevention (DLP)**
    - Loss vs. leak.
    - Data in use, in motion, and at rest.
    - Network and endpoint DLP.

What we covered in the second CBK Domain:

- **In this domain, we covered how we classify our data, how objects have labels and subjects have clearance.**
- **The different roles of mission, data and system owner, custodians, and users.**
- **The 3 different states of data (at rest, in use, or in motion).**
- **We looked at volatile and non-volatile memory, the different types of each and where they are used.**
- **How we ensure there is no data remanence and destroying our media properly to not expose the data on it.**