- **Welcome to the second CBK Domain.**
    - **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, 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 CBK is one of the smaller chapters both in the concepts it covers and the percentage of the exam it makes up (10%).

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."

Military Classification	Business Classification
TOP SECRET	HIGHLY SENSITIVE
SECRET	SENSITIVE
CONFIDENCIAL	INTERNAL
UNCLASSIFIED	PUBLIC

- **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 business).

Data Classification Policies:

- **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.

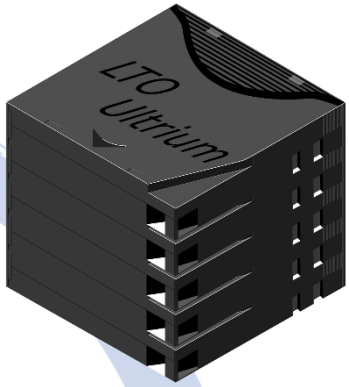
Sensitive information and Media Security:

- **Sensitive Information**
    - **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).

Sensitive information and Media Security:

- **Sensitive information**
  - **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 has unique roles and responsibilities to keep the data safe.

- **Mission/business owner:** Senior executives make the policies that govern our data security.
- **Data/information owner:** Management level, they assign sensitivity labels and backup frequency.
  - This could be you or a data owner from HR, payroll or other departments.
- **System owner:** Management level and the owner of the systems that house the data.
  - Often a data center manager or an infrastructure manager.
- **Data custodian:** These are the technical hands-on employees who do the backups, restores, patches, system configuration. They follow the directions of the data owner.
- **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.
- **Data controllers and data processors:**
  - Controllers create and manage sensitive data in the organization (HR/Payroll)
  - Processors manage the data for controllers (Outsourced payroll)

Memory and Data Remanence:

- **Data Remanence:** Data left over after normal removal and deletion of data.
- **Memory**: Is just 0's (off) and 1's (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) – Can only be written once, normally at the factory.
      - **EPROM** (Erasable programmable read only memory) – Can be erased (flashed) and written many times, by shining an

ultraviolet light (flash) on a small window on the chip (normally covered by foil).

- **EEPROM** (Electrically erasable programmable read only memory) – These are electrically erasable; you can use a flashing program. This is still called read only.
  - The ability to write to the BIOS makes it vulnerable to attackers.
- **PLD** (Programmable logic devices) are programmable after they leave the factory (EPROM, EEPROM and flash memory). Not PROM.

Memory and Data Remanence:

- **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.
      - 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.

Memory and Data Remanence:

- **Firmware and SSD's (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 must 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** is done by writing 0's or random characters over the data.
      - As far as we know there is no tool available that can recover even single pass overwriting (not possible on damaged media).

Data Destruction:

Crushed/shredded hard disk fragments.

- **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.
- It is common to do multiple types of data destruction on sensitive data (both degaussing and disk crushing/shredding).
- While it may not be necessary, it is a lot cheaper than a potential $1,000,000 fine or loss of proprietary technology or state secrets.

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).
- **Classification**: 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 Security Controls and Frameworks:

- **Governance standards and control frameworks:**
  - **PCI-DSS** - Payment Card Industry Data Security Standard (while a standard it is required, more on this one later).
  - **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** – Committee Of Sponsoring Organizations:
    - **Goals** for the entire organization.
  - **ITIL** - Information Technology Infrastructure Library.
    - IT Service Management **(ITSM).**
  - **FRAP** - Facilitated Risk Analysis Process:
    - Analyzes one business unit, application or system at a time in a roundtable brainstorm with **internal** employees. Impact is analyzed, threats and risks prioritized.

Data Security Controls and Frameworks:

- **Governance standards and control frameworks.**
  - **ISO 27000 series**:
    - **ISO 27001:** Establish, implement, control and improve the ISMS. Uses PDCA (Plan, Do, Check, Act)
    - **ISO 27002:** (From BS 7799, 1/2, ISO 17799) Provides practical advice on how to implement security controls. It has 10 domains it uses for ISMS.
    - **ISO 27004:** Provides metrics for measuring the success of your ISMS.
    - **ISO 27005:** Standards-based approach to risk management.
    - **ISO 27799:** Directives on how to protect PHI (Protected Health Information).

What we covered in the second CBK Domain:

- In this 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.
- Finally, we covered data standards and frameworks and how we can scope or tailor them to meet the needs of our organization.