Welcome to the first CBK Domain.

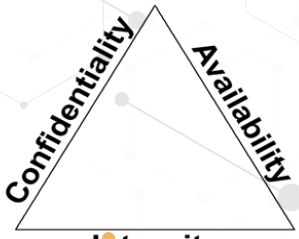
In this domain we cover:

- **Confidentiality, Integrity, and Availability concepts.**
  We want the right balance; our data needs to be secure, while keeping its integrity intact and availability high.
- **Security Governance Principles.**
  What and how we grant data access to people, the frameworks we use for it, and defense in depth.
- **Legal and Regulatory Issues.**
  The laws and regulations we must adhere to, types of evidence, how we handle it, intellectual property
- **Professional Ethics**
  The ISC2 Code of Ethics and corporate code of ethics.
- **Security Policies, Standards, Procedures and Guidelines**
  How we use policies, standards, guidelines, procedures, baselines what each does.
- **Risk Identification, Assessment, Response, Monitoring and Reporting**
  How we determine the quantitative and qualitative risks to our assets and types of attackers.
- **BCP and BIA**
  The considerations for our BCP (Business Continuity Plan) and our BIA (Business impact analysis).

This domain is highly weighted on the exam (15%) and is the foundation of everything. Every other knowledge domain builds on top of this chapter.

Confidentiality, Integrity and Availability

- **The CIA Triad (*sometimes referred to as AIC*)**
  - **Confidentiality**
    - This is what most people think IT Security is.
    - We keep our data and secrets secret.
    - We ensure no one unauthorized can access the data.
  - **Integrity**
    - How we protect against modifications of the data and the systems.
    - We ensure the data has not been altered.
  - **Availability**
    - We ensure authorized people can access the data they need, when they need to.

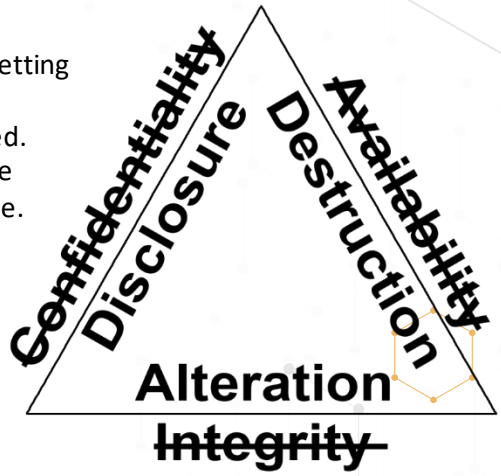


- **Confidentiality**, Integrity and Availability.
  - **We use:**
    - Encryption for **data at rest** (for instance AES256), full disk encryption.
    - Secure transport protocols for **data in motion**. (SSL, TLS or IPSEC).
    - Best practices for **data in use** - clean desk, no shoulder surfing, screen view angle protector, PC locking (automatic and when leaving).
    - Strong passwords, multi-factor authentication, masking, access control, need-to-know, least privilege.
  - **Threats:**
    - Attacks on your encryption (cryptanalysis).
    - Social engineering.
    - Key loggers (software/hardware), cameras, Steganography.
    - IoT (Internet of Things) – The growing number of connected devices we have pose a new threat, they can be a backdoor to other systems.

- Confidentiality, **Integrity** and Availability.
  - **We use:**
    - Cryptography (again).
    - Check sums (This could be CRC).
    - Message Digests also known as a hash (This could be MD5, SHA1 or SHA2).
    - Digital Signatures – non-repudiation.
    - Access control.
  - **Threats:**
    - Alterations of our data.
    - Code injections.
    - Attacks on your encryption (cryptanalysis).

- Confidentiality, Integrity and **Availability.**
  - **We use:**
    - IPS/IDS.
    - Patch Management.
    - Redundancy on hardware power (Multiple power supplies/UPS's/generators), Disks (RAID), Traffic paths (Network design), HVAC, staff, HA (high availability) and much more.
    - SLA's – How much uptime do we want (99.9%?) – (ROI)
  - **Threats:**
    - Malicious attacks (DDOS, physical, system compromise, staff).
    - Application failures (errors in the code).
    - Component failure (Hardware).

- **Disclosure, Alteration, and Destruction**
  - The opposite of the CIA Triad is DAD.
    - **Disclosure** – Someone not authorized getting access to your information.
    - **Alteration** – Your data has been changed.
    - **Destruction** – Your data or systems have been destroyed or rendered inaccessible.



IAAA (Identification and Authentication, Authorization and Accountability):

- **Identification**
  - Your name, username, ID number, employee number, SSN etc.
  - "I am Thor".
- **Authentication**
  - "Prove you are Thor". – Should **always** be done with multi-factor authentication!
    - **Something you know - Type 1** Authentication (passwords, pass phrase, PIN, etc.).
    - **Something you have - Type 2** Authentication (ID, passport, smart card, token, cookie on PC, etc.).
    - **Something you are - Type 3** Authentication (and Biometrics) (Fingerprint, iris scan, facial geometry, etc.).
- **Authorization**
  - What are you allowed to access?
  - We use Access Control models. What and how we implement depends on the organization and what our security goals are.
  - More on this in Domain 5 - Identity and Access Management (DAC, MAC, RBAC, RUBAC)

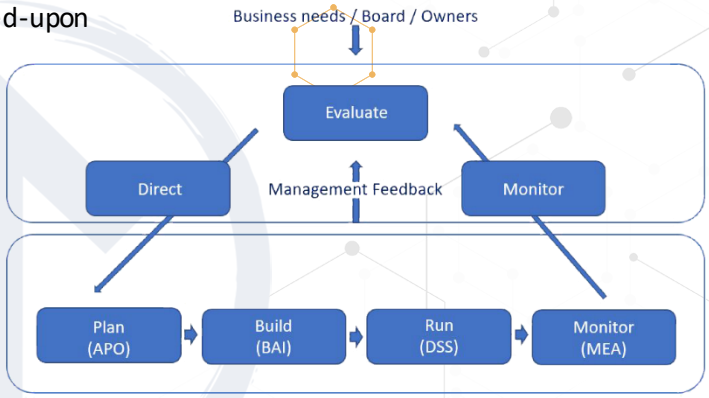
- **Accountability** (also often referred to as Auditing)
  - Trace an Action to a Subject's Identity:
    - Prove who/what a given action was performed by (non-repudiation).

Security Governance Principles

- **Least Privilege and Need to Know.**
  - **Least Privilege** – (Minimum necessary access) Give users/systems exactly the access they need, no more, no less.
  - **Need to Know** – Even if you have access, if you do not need to know, then you should not access the data.

- **Non-repudiation.**
  - A user cannot deny having performed a certain action. This uses both Authentication and Integrity.
- **Subject and Object.**
  - **Subject** – (Active) Most often users, but can also be programs – Subject manipulates Object.
  - **Object** – (Passive) Any passive data (both physical paper and data) – Object is manipulated by Subject.
  - Some can be both at different times, an active program is a subject; when closed, the data in program can be object.

- **Governance vs. Management**
  - **Governance** – This is C-level Executives (Not you).
    - Stakeholder's needs, conditions and options are evaluated to define:
      - Balanced agreed-upon enterprise objectives to be achieved.
      - Setting direction through prioritization and decision making.
      - Monitoring performance and compliance against agreed-upon direction and objectives.
      - Risk appetite – Aggressive, neutral, adverse.

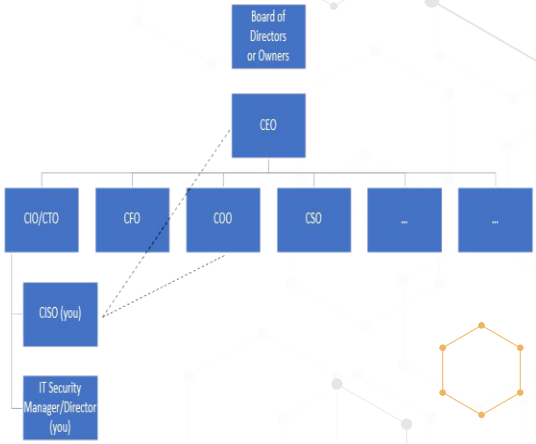


  - **Management** – How do we get to the destination (This is you).
    - Plans, builds, runs, and monitors activities in alignment with the direction set by the governance to achieve the objectives.
    - Risk tolerance – How are we going to practically work with our risk appetite and our environment.

- **Top-Down vs. Bottom-Up Security Management and Organization structure.**
  - **Bottom-Up:** IT Security is seen as a nuisance and not a helper, often changes when breaches happen.
  - **Top-Down:** IT leadership is on board with IT Security, they lead and set the direction. (The exam).

- **C-Level Executives (Senior Leadership) – *Ultimately Liable.***
  - **CEO:** Chief Executive Officer.
  - **CIO:** Chief Information Officer.
  - **CTO:** Chief Technology Officer.
  - **CSO:** Chief Security Officer.

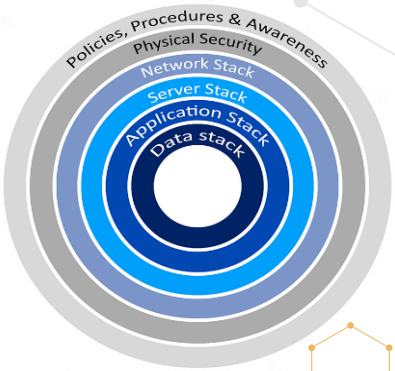
- **CISO:** Chief Information Security Officer.
- **CFO:** Chief Financial Officer.
- Normal organizations obviously have more C-Level executives, the ones listed here you need to know.



- **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** – 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 analyzed, threats and risks prioritized.
  - **ISO 27000 series**:
    - **ISO 27001:** Establish, implement, control and improvement of 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** (Information Security Management Systems).
    - **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).

Links on all these as well as ones from previous slides in the "Extras" lecture.

- **Defense in Depth** – Also called Layered Defense or Onion Defense.
  - We implement multiple overlapping security controls to protect an asset.
  - This applies both to physical and logical controls.
    - To get to a server, you may have to go through multiple locked doors, security guards, man traps.
    - To get to the data, you may need to get past firewalls, routers, switches, the server, and the applications security.
    - Each step may have multiple security controls.
  - No single security control secures an asset.
  - By implementing Defense in Depth, you improve your organization's Confidentiality, Integrity, and Availability.



Legal and Regulatory Issues

- *There are a handful types of laws covered on the exam and important to your job as an IT Security Professional.*
  - **Criminal Law:**
    - "Society" is the victim and proof must be "Beyond a reasonable doubt".
    - Incarceration, death, and financial fines to "Punish and deter".
  - **Civil Law** (Tort Law):
    - Individuals, groups or organizations are the victims and proof must be "the majority of proof".
    - Financial fines to "Compensate the victim(s)".
  - **Administrative Law** (Regulatory Law):
    - Laws enacted by government agencies (FDA Laws, HIPAA, FAA Laws, etc.)
  - **Private Regulations**:
    - Compliance is required by contract (For instance PCI-DSS).
  - **Customary Law:**
    - Mostly handles personal conduct and patterns of behavior and it is founded in traditions and customs of the area or region.
  - **Religious Law:**
    - Based on the religious beliefs in that area or country, they often include a code of ethics and moralities which are required to be upheld.

- **Liability:**
  - If the question is who is ULTIMATELY liable, the answer is Senior Leadership. This does not mean you are not liable; you may be, that depends on Due Care. Who is held accountable? Who is to blame? Who should pay?

- **Due Diligence and Due Care:**
  - Due Diligence – The research to build the IT Security architecture of your organization, best practices and common protection mechanisms, research of new systems before implementing.
  - Due Care – Prudent person rule – What would a prudent person do in this situation?
    - *Implementing the IT Security architecture, keep systems patched. If compromised: fix the issue, notify affected users (Follow the Security Policies to the letter).*
  - **Negligence** (and gross negligence) is the opposite of Due Care.
    - If a system under your control is compromised and you can prove you did your Due Care, you are most likely not liable.
    - If a system under your control is compromised and you did NOT perform Due Care, you are most likely liable.

- **Evidence:**

  How you obtain and handle evidence is VERY important.
  - **Types of evidence:**
    - **Real Evidence:** Tangible and physical objects in IT Security: Hard disks, USB drives – NOT the data on them.
    - **Direct Evidence:** Testimony from a firsthand witness, what they experienced with their 5 senses.
    - **Circumstantial Evidence:** Evidence to support circumstances for a point or other evidence.
    - **Collaborative Evidence:** Supports facts or elements of the case: not a fact on its own, but support other facts.
    - **Hearsay:** Not first-hand knowledge – normally inadmissible in a case.
      - **Computer-generated records** - For us, that means log files are considered hearsay, but case law and updates to the Federal Rule of Evidence have changed that.

        Rule 803 provides for the admissibility of a record or report that was:

        "made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation."
  - **Best Evidence Rule** – The courts prefer the best evidence possible.
    - Evidence should be accurate, complete, relevant, authentic, and convincing.
  - **Secondary Evidence** – This is common in cases involving IT.
    - Logs and documents from the systems are considered secondary evidence.

- **Evidence Integrity** – It is vital that the evidence's integrity cannot be questioned.
  - We do this with hashes. Any forensics is done on copies and never the originals.
  - We check hash on both original and copy before and after the forensics.
- **Chain of Custody** – This is done to prove the integrity of the data; that no tampering was done.
  - Who handled it?
  - When did they handle it?
  - What did they do with it?
  - Where did they handle it?

- **Reasonable Searches:**
  - The Fourth Amendment to the United States Constitution protects citizens from unreasonable search and seizure by the government.
  - In all cases, the court will determine if evidence was obtained legally.
  - Exigent circumstances apply if there is an immediate threat to human life or of evidence destruction.
  - Your organization needs to be very careful when ensuring that employees are made aware in advance that their actions are monitored, that their equipment, and maybe even personal belongings, can be subjected to searches.

- **Entrapment and Enticement:**
  - **Entrapment** (Illegal and unethical): When someone is persuaded to commit a crime they had no intention of committing and is then charged with it.
  - **Enticement** (Legal and ethical): Making committing a crime more enticing, but the person has already broken the law or at least has decided to do so.
    - Honeypots can be a good way to use Enticement.
      - If there is a gray area in some cases between Entrapment and Enticement, it is ultimately up to the jury to decide which one it was.
      - Check with your legal department before using honeypots. They pose both legal and practical risks.

- **Intellectual Property:**
  - **Copyright ©** - (Exceptions: first sale, fair use).
    - Books, art, music, software.
    - Automatically granted and lasts **70 years after creator's death or 95 years after creation by/for corporations.**
  - **Trademarks ™** and **®** (Registered Trademark).
    - Brand names, logos, slogans – Must be registered, is valid for 10 years at a time, can be renewed indefinitely.
  - **Patents: Protects inventions for 20 years** (normally) –
    - **Cryptography algorithms can be patented.**

- Inventions must be:
  - **Novel** (New idea no one has had before).
  - **Useful** (It is actually possible to use and it is useful to someone).
  - **Nonobvious** (Inventive work involved).
- **Trade Secrets.**
  - You tell no one about your formula, your secret sauce. If discovered, anyone can use it; you are not protected.
- **Attacks on Intellectual Property:**
  - **Copyright.**
    - Piracy - Software piracy is by far the most common attack on Intellectual Property.
    - Copyright infringement – Use of someone else's copyrighted material, often songs and images.
  - **Trademarks.**
    - Counterfeiting – Fake Rolexes, Prada, Nike, Apple products – Either using the real name or a very similar name.
  - **Patents.**
    - Patent infringement – Using someone else's patent in your product without permission.
  - **Trade Secrets.**
    - While an organization can do nothing if their Trade Secret is discovered, *how* it is done can be illegal.
  - **Cyber Squatting** – Buying a URL you know someone else will need (gray area legally).
  - **Typo Squatting** – Buying a URL that is VERY close to real website name (Can be illegal in certain circumstances).

- **Privacy:**
  - You as a citizen and consumer have the right that your Personally Identifiable Information (PII) is being kept securely.
    - There are a number of Laws and Regulations in place to do just that.
  - US privacy regulation is a patchwork of laws, some overlapping, and some areas with no real protection.
  - EU Law – Very pro-privacy, strict protection on what is gathered, how it is used and stored.
    - There are a lot of large lawsuits against large companies for doing what is legal in the US (Google, Apple, Microsoft, etc.)
- **Rules, Regulations and Laws you should know for the exam (US):**
  - **HIPAA** (Not HIPPA) – Health Insurance Portability and Accountability Act.
    - Strict privacy and security rules on handling of PHI (Protected Health Information).

- **Security Breach Notification Laws.**
  - NOT Federal, all 50 states have individual laws, know your state.
- **Electronic Communications Privacy Act (ECPA):**
  - Protection of electronic communications against warrantless wiretapping.
  - The Act was weakened by the Patriot Act.
- **PATRIOT Act of 2001:**
  - Expands law enforcement electronic monitoring capabilities.
  - Allows search and seizure without immediate disclosure.
- **Computer Fraud and Abuse Act (CFAA) – Title 18 Section 1030:**
  - Most commonly used law to prosecute computer crimes.
- **Gramm-Leach-Bliley Act (GLBA):**
  - Applies to financial institutions; driven by the Federal Financial Institutions
- **Sarbanes-Oxley Act of 2002 (SOX):**
  - Directly related to the accounting scandals in the late 90s.
- **Payment Card Industry Data Security Standard (PCI-DSS)**

  Technically not a law, created by the payment card industry.
  - The standard applies to cardholder data for both credit and debit cards.
  - Requires merchants and others to meet a minimum set of security requirements.
  - Mandates security policy, devices, control techniques, and monitoring.
  - NOT Federal, all 50 states have individual laws, know your state.

- **General Data Protection Regulation (GDPR)**
  - **Restrictions:** Lawful Interception, national security, military, police, justice
  - **Personal data –** covers a variety of data types including: Names, Email, IP, and Physical Addresses, Unsubscribe confirmation URLs that contain email and/or names,
    - **Right to access:** Data controllers must be able to provide a free copy of an individual's data if requested.
    - **Right to erasure:** All users have a "right to be forgotten".
    - **Data portability:** All users will be able to request access to their data "in an electronic format".
    - **Data breach notification:** Users and data controllers must be notified of data breaches within 72 hours.
    - **Privacy by design:** When designing data processes, care must be taken to ensure personal data is secure. Companies must ensure that only data is "absolutely necessary for the completion of duties".
    - **Data protection officers:** Companies whose activities involve data processing and monitoring must appoint a data protection officer.