Welcome to the First Chapter.

Domain 1: What we will be covering.

- This chapter is **VERY** important because:
  Every other knowledge domain build on top of this chapter.
  This is the **foundation.**

- **We will cover:**
  The differences between Information security, IT Security, and Cybersecurity.
  The CIA triad and IAAA.
  Privacy.
  Risk and incident management.
  Access control.
  Governance, management, laws, and regulations.
  The ISC2 ethics.

Information Security, IT Security, and Cybersecurity:

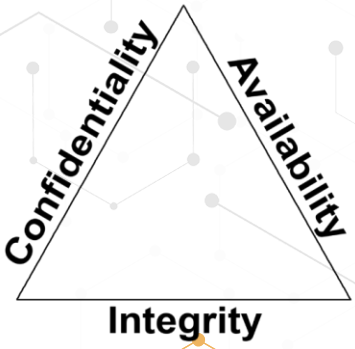
- **Information Security** is all our information:
  Paper documents, voice information, data, the knowledge people have, …
- **IT Security** is all our hard/software, and data:
  Computers, servers, networks, hardware, software, firmware, and data being processed, stored, and communicated.
- **Cybersecurity** is everything from IT Security that is accessible from the internet.

The CIA Triad: Confidentiality, Integrity and Availability:

- **This is the foundation of IT/IS security.**
  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 encryption 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)

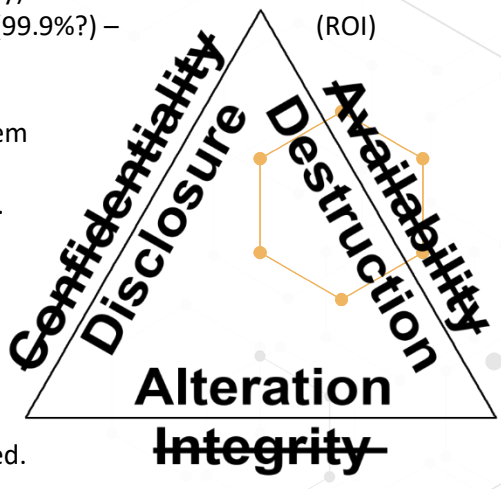
Threats:

- 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.).

Something you know - Type 1 Authentication:

- Passwords, pass phrase, PIN etc., also called Knowledge factors.
- The subject uses these to authenticate their identity, if they know the secret, they must be who they say they are.
- This is the most commonly used form of authentication, and a password is the most common knowledge factor.
- The user is required to prove knowledge of a secret in order to authenticate.
- Variations include both longer ones formed from multiple words (a passphrase) and the shorter purely numeric PINs (personal identification number) commonly used for cash machines (ATM's).
- It is the weakest form of authentication and can easily be compromised.
- Secret questions like "Where were you born?" are poor examples of a knowledge factor, it is known by a lot of people and can often be researched easily.
  - Sarah Palin had her email account hacked during the 2008 US Presidential campaign using her secret questions. Since she used basic ones (high school and birthday, …) the hackers could easily find that information online, he reset her password with the information and gained full control of her email account.

- **Passwords:**
  - It is always easier to guess or steal passwords than it is to break the encryption.
  - We have password policies to ensure they are as secure as possible.

- → They should contain minimum length, upper/lower case letters, numbers, and symbols, they should not contain full words or other easy to guess phrases.
- → They have an expiration date, password reuse policy and minimum use before users can change it again.
- → Common and less secure passwords often contain:
  - The name of a pet, child, family member, significant other, anniversary dates, birthdays, birthplace, favorite holiday, something related to a favorite sports team, or the word "password".
  - Winter2023 is not a good password, even if it does fulfil the password requirements.

- **Key Stretching** – Adding 1-2 seconds to password verification.
- If an attacker is brute forcing a password and needs millions of tries it will become an unfeasible attack.
- **Brute Force Attacks** (Limit number of wrong logins):
- Uses the entire key space (every possible key), with enough time any ciphertext can be decrypted.
- Effective against all key based ciphers except the one-time pad, it would eventually decrypt it, but it would also generate so many false positives the data would be useless.
- **Clipping Levels:** Clipping levels are in place to **prevent administrative overhead**.
  - → It allows authorized users who forget or mistype their password to still have a couple of extra tries.
  - → It prevents password guessing by locking the user account for a certain timeframe (an hour), or until unlocked by an administrator.

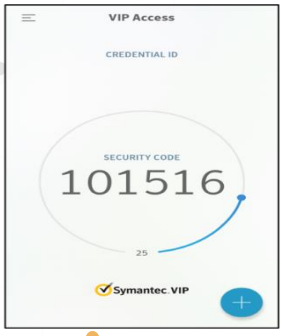
- **Password Management:**
  - We covered some password requirements, here are the official recommendations by the U.S. Department of Defense and Microsoft.
    - → Password history = set to remember 24 passwords.
    - → Maximum password age = 90 days.
    - → Minimum password age = 2 days (to prevent users from cycling through 24 passwords to return to their favorite password again).
    - → Minimum password length = 14 characters.
    - → Passwords must meet complexity requirements = true.
    - → Store password using reversible encryption = false.

Something you have - Type 2 Authentication:

- ID, passport, smart card, token, cookie on PC, these are called Possession factors.
    - The subject uses these to authenticate their identity, if they have the item, they must be who they say they are.
    - Simple forms can be credit cards, you have the card, and you know the pin, that is multifactor authentication.
    - Most also assume a shared trust, you have your passport, it looks like you on the picture, we trust the issuer, so we assume the passport is real.

- **Single-Use Passwords:**
    - Having passwords which are only valid once makes many potential attacks ineffective, just like one-time pads.
    - While they are passwords, it is something you have in your possession, not something you know.
    - Some are one-time-pads with a challenge-response or just a pin or phase sent to your phone or email you need to enter to confirm the transaction or the login.
    - Most users find single use passwords extremely inconvenient.
- They are widely implemented in online banking, where they are known as TANs (Transaction Authentication Numbers).
    - Most private users only do a few transactions each week, the single-use passwords has not led to customers refusing to use it.
        - → It is their money; they actually care about keeping those safe.
- **Smart Cards and Tokens** (contact or contactless):
    - They contain a computer circuit using an ICC (Integrated Circuit Chip).
    - **Contact Cards** - Inserted into a machine to be read.
        - → This can be credit cards you insert into the chip reader or the DOD CAC (Common Access Card).
    - **Contactless Cards** - can be read by proximity.
        - → Key fobs or credit cards where you just hold it close to a reader.
        - → They use a RFID (Radio Frequency Identification) tag (transponder) which is then read by a RFID Transceiver.

TOTP tokens
Hardware
Software



- **Magnetic Stripe Cards:**
  - → Swiped through a reader, no circuit.
  - → Very easy to duplicate.

- **Tokens:**
  - HOTP and TOTP can be either hardware or software based.
  - Cellphone software applications are more common now.
    - → **HOTP (HMAC-based One-Time Password):**
      - Shared secret and incremental counter, generate code when asked, valid till used.
    - → **TOTP (Time-based One-Time Password):**
      - Time based with shared secret, often generated every 30 or 60 seconds, synchronized clocks are critical.

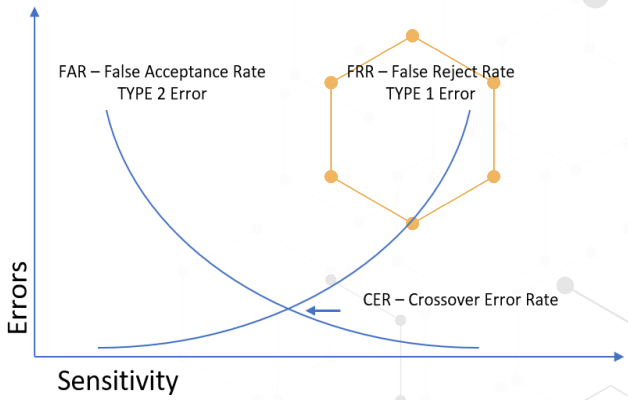
Something you are - Type 3 Authentication (Biometrics):

- Fingerprint, iris scan, facial geometry etc., these are also called realistic authentication.
  - The subject uses these to authenticate their identity, if they are that, they must be who they say they are.
  - Something that is unique to you, this one comes with more issues than the two other common authentication factors.
  - We can allow unauthorized people into our facilities or systems if we accept someone by mistake. (False Accept)
  - We can prevent our authorized people from entering our facilities if we refuse them by mistake. (False Reject).

Fingerprint reader, with keypad.
This is multifactor authentication.

Errors for Biometric Authentication:

- **FRR (False rejection rate)**
  Type 1 error:
  - Authorized users are rejected.
  - This can be too high settings - 99% accuracy on biometrics.



- **FAR (False accept rate) Type 2 error:**
  - Unauthorized user is granted access.
  - This is a very serious error.
- We want a good mix of FRR and FAR where they meet on the graph is the **CER (Crossover Error Rate)**, this is where we want to be.

Biometric identifiers are often categorized as physiological and behavioral characteristics.

- **Physiological Characteristics** uses the shape of the body, these do not change unless a drastic event occurs.
  - Fingerprint, palm veins, facial recognition, DNA, palm print, hand geometry, iris recognition, retina, and odor.
- **Behavioral Characteristics** uses the pattern of behavior of a person, these can change, but most often revert back to the baseline.
  - Typing rhythm, how you walk, signature and voice.

Issues with Biometric Authentication:

- We also need to respect and protect our employee's privacy:
  - Some fingerprint patterns are related to chromosomal diseases.
  - Iris patterns could reveal genetic sex, retina scans can show if a person is pregnant or diabetic.
- Hand vein patterns could reveal vascular diseases.
- Most behavioral biometrics could reveal neurological diseases, etc.
- While passwords and smart cards should be safe because you keep them a secret and secure, biometrics is inherently not and something others can easily find out.
- Attackers can take pictures of your face, your fingerprints, your hands, your ears and print good enough copies to get past a biometric scan.
- It is possible to copy fingerprints from your high-resolution social media posts if you do a peace sign like the one on the right here.

- How you type, sign your name and your voice pattern can be recorded, also not too difficult to cheat biometrics if it is worth the effort.
- Some types are still inherently more secure, but they are often also more invasive.
- Lost passwords and ID cards can be replaced with new different ones, biometrics can't.
- Which should make us question even more the mass collection of biometric data.
  - When Home Depot loses 10 million credit card numbers it is bad, but they can be reissued.
  - The US Office of Personnel Management got hacked and lost 5.6 million federal employees' fingerprints.

- The FBI has a database with 52 million facial images and Homeland Security and U.S. Customs and Border Patrol is working on adding the iris scans and 170 million foreigner fingerprints to the FBI's database.
- The compromises of the future will have much more wide-reaching ramifications than the ones we have seen until now.

- **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 later when we cover DAC, MAC, RBAC, ABAC, and RUBAC.

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.

DAC (Discretionary Access Control) - Often used when Availability is most important:

- Access to an object is assigned at the discretion of the object owner.
- The owner can add, remove rights, commonly used by most OS's'.
- Uses DACL's (Discretionary ACL), based on user identity.

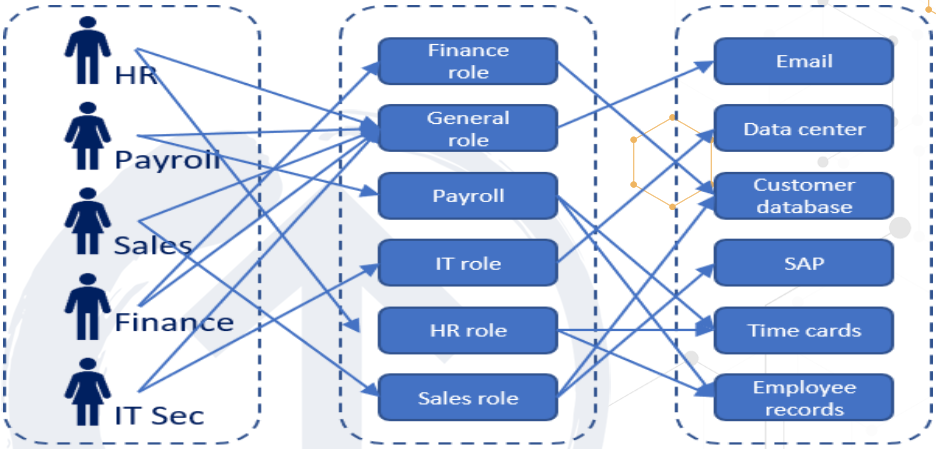
MAC (Mandatory Access Control) - Often used when Confidentiality is most important:

- Access to an object is determined by labels and clearance, this is often used in the military or in organizations where confidentiality is very important.
- **Labels**: Objects have Labels assigned to them; the subject's clearance must dominate the object's label.
  - The label is used to allow Subjects with the right clearance access them.
  - Labels are often more granular than just "Top Secret", they can be "Top Secret – Nuclear".

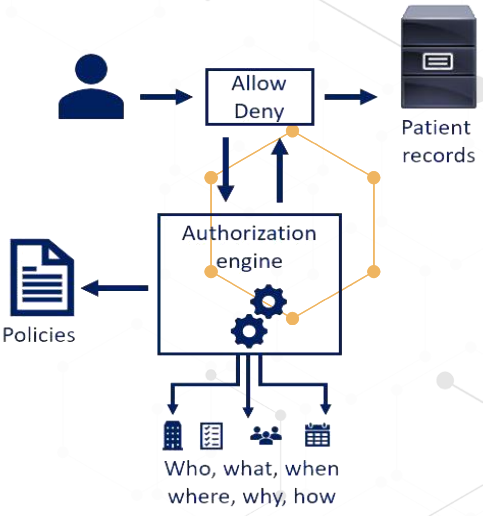
- **Clearance**: Subjects have Clearance assigned to them.
  - Based on a formal decision on a subject's current and future trustworthiness.
  - The higher the clearance the more in depth the background checks should be.

RBAC (Role-Based Access Control) - Often used when Integrity is most important:

- Policy neutral access control mechanism defined around roles and privileges.



- A role is assigned permissions, and subjects in that role are added to the group, if they move to another position they are moved to the permissions group for that position.
- It makes administration of 1,000's of users and 10,000's of permissions much easier to manage.
- The most commonly used form of access control.
- If implemented right, it can also enforce separation of duties and prevent authorization/privilege creep.
  - We move employees transferring within the organization from one role to another and we do not just add the new role to the old one.



ABAC (Attribute-Based Access Control):

- Access to objects is granted based on subjects, objects, AND environmental conditions.
- Attributes could be:

- *Subject* (user) – Name, role, ID, clearance, etc.
- *Object* (resource) – Name, owner, and date of creation.
- *Environment* – Location and/or time of access, and threat levels.

- Expected to be used by 70% of large enterprises within the next 5 years, versus around 25% today.
- Can also be referred to as policy-based access control (PBAC) or claims-based access control (CBAC).

Context-Based Access Control:

- Access to an object is controlled based on certain contextual parameters, such as location, time, sequence of responses, access history.
- Providing the username and password combination followed by a challenge and response mechanism such as CAPTCHA, filtering the access based on MAC addresses on wireless, or a firewall filtering the data based on packet analysis are all examples of context-dependent access control mechanisms.

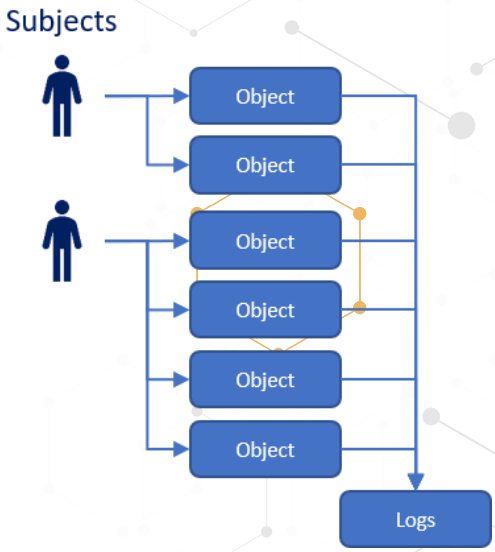
Content-Based Access Control:

- Access is provided based on the attributes or content of an object, then it is known as a content-dependent access control.
- In this type of control, the value and attributes of the content that is being accessed determine the control requirements.
- Hiding or showing menus in an application, views in databases, and access to confidential information are all content-dependent.

- **Accountability** (often referred to as Auditing):

Traces an Action to a Subject's Identity:

- Proves who performed given action, it provides non-repudiation.
- Group or shared accounts are never OK, they have zero accountability.
- Uses audit trails and logs, to associate a subject with its actions.



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.

Privacy:

- **Privacy is a human right.**

  A definition of Privacy:

  1. The state or condition of being free from being observed or disturbed by other people.
  2. Freedom from unauthorized intrusion.

- You as a citizen and consumer have the right that your Personally Identifiable Information (PII) is being kept securely.
- US privacy regulation is a patchwork of laws, some overlapping and some areas with no real protection.
- EU Law – Strict protection on what is gathered, how it is used and stored.

Risk Management:

- **Risk Management - Identification:**

  *Risk = Threat * Vulnerability (or likelihood).*
  *We can also use Risk = Threat * Vulnerability * Impact.*

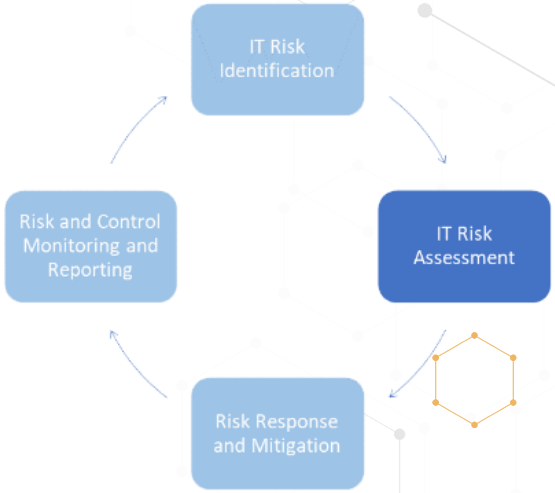
  *Total Risk = Threat * Vulnerability * Asset Value.*
  Residual Risk = Total Risk – Countermeasures.

- **Threat** – A potentially harmful incident.
- **Vulnerability** – A weakness that can allow the Threat to do harm.
- **Due Diligence:** Doing the research before implementation.
  DD – Do Detect
- **Due Care:** It is the implementation. **DC - Do Correct**
- **The Risk Management lifecycle is iterative**.

  Identify our Risk Management team.
  What is in and what is out of scope?
  Which methods are we using?
  Which tools are we using?
  What are the acceptable risk levels, which type of risk appetite do we have in our enterprise?
  Identify our assets.
  - Tangible: Physical hardware, buildings, anything you can touch.
  - Intangible: Data, trade secrets, reputation, etc.

- **Risk Assessment.**

  Quantitative and Qualitative Risk Analysis.
  Uncertainty analysis.
  Everything is done using cost-benefit analysis.
  Risk Mitigation/Risk Transference/Risk Acceptance/Risk Avoidance.
  Risk Rejection is **NEVER** acceptable.
  We assess the current countermeasures.
  - Are they good enough?
  - Do we need to improve on them?
  - Do we need to implement entirely new countermeasures?



- **Qualitative vs. Quantitative Risk Analysis.**

  For any Risk analysis we need to identify our assets. What are we protecting?
  Qualitative Risk Analysis – How likely is it to happen and how bad is it if it happens?
  Quantitative Risk Analysis – What will it actually cost us in $? This is fact-based analysis, Total $ value of asset, math is involved.

- **Qualitative Risk Analysis with the Risk Analysis Matrix.**
- **Let's pick an asset, a laptop.**

  How likely is one to get stolen or left somewhere?
  I would think possible or likely.
  How bad is it if it happens?
  That really depends on a couple of things:
  - Is it encrypted?
  - Does it contain classified or PII/PHI content?

Likelihood \ Consequences	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Possible	L	M	H	H	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Where the L, M, H, E is for your organization can be different from this.
L = Low, M = Medium, H = High, E = Extreme Risk

Let's say it is likely and a minor issue, that puts the loss the high-risk category. It is normal to move high and extreme on the quantitative risk analysis. If mitigation is implemented, we can maybe move the risk level to "Low" or "Medium".

A risk category to group similar risks.
The risk breakdown structure identification number.
A brief description or name of the risk to make the risk easy to discuss.

The impact (or consequence) if event actually occurs rated on an integer scale.
The probability or likelihood of its occurrence rated on an integer scale.
The Risk Score (or Risk Rating) is the multiplication of Probability and Impact, and is often used to rank the risks.
Common mitigation steps (e.g. within IT projects)

Category	Name	Risk #	Probability	Impact	Mitigation	Contingency	Risk Score after Mitigation	Action By	Action When

- Identify
- Analyze
- Plan Response
- Monitor
- Control

- **Quantitative Risk Analysis**

  This is where we put a number on our assets and risks.
  We find the asset's value: How much of it is compromised, how much one incident will cost, how often the incident occurs and how much that is per year.
  - Asset Value (**AV**) – How much is the asset worth?
  - Exposure factor (**EF**) – Percentage of Asset lost?
  - Single Loss Expectancy (**SLE**) = (**AV** x **EF**) – What does it cost if it happens once?
  - Annual Rate of Occurrence (**ARO**) – How often will this happen each year?
  - Annualized Loss Expectancy (**ALE**) – This is what it costs per year if we do nothing.
  - Total Cost of Ownership (**TCO**) – The mitigation cost: upfront + ongoing cost (Normally Operational

Let's look at a few examples.

- Asset Value **(AV)** = The Laptop ($1,000) + PII ($10,000) per loss.
- Exposure factor **(EF)** = It is a 100% loss, it is gone.
- Single Loss Expectancy **(SLE)** = **(AV x EF)** = Loss per laptop is $11,000 x 100%.
- Annual Rate of Occurrence **(ARO)** = The organization loses 25 Laptops Per Year.
- Annualized Loss Expectancy **(ALE)** = The annualized loss is $275,000
- Total Cost of Ownership **(TCO)** = $100,000

- **Types of risk responses:**

  Accept the Risk – We know the risk is there, but the mitigation is more costly than the cost of the risk (Low risks).

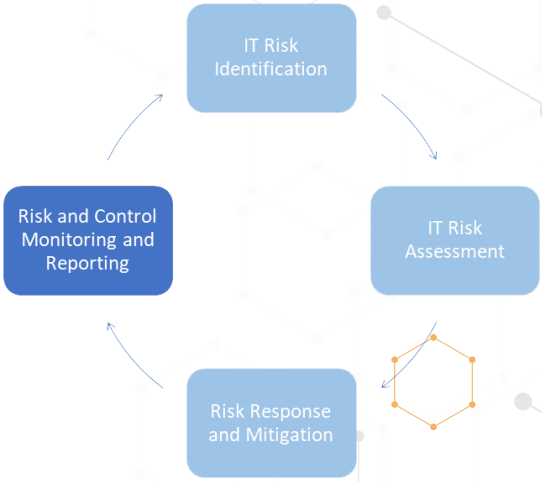
Mitigate the Risk (Reduction) – The laptop encryption/wipe is an example – acceptable level (Leftover risk = Residual).
Transfer the Risk – The insurance risk approach.
Risk Avoidance – We don't issue employees laptops (if possible) or we build the data center in an area that doesn't flood.
Risk Rejection – You know the risk is there, but you are ignoring it. This is **never** acceptable. (You are liable).
Secondary Risk – Mitigating one risk may open up another risk.

- **KGI (Key Goal Indicator):**
  Define measures that tell management, after the fact—whether an IT process has achieved its business requirements.
- **KPI (Key Performance Indicators):**
  Define measures that determine how well the IT process is performing in enabling the goal to be reached.
- **KRI (Key Risk Indicators):**
  Metrics that demonstrate the risks that an organization is facing or how risky an activity is.
  They are the mainstay of measuring adherence to and establishing enterprise risk appetite.
  Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.
  KRI give an early warning to identify potential event that may harm continuity of the activity/project.

- **Risk Response and Mitigation**
  Risk mitigation, transference, acceptance, or avoidance.
  We act on senior management choices, which they made based on our recommendations from the assessment phase.
  Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?
  Update the risk register, with the mitigations, and the risk responses.

- **Risk and Control Monitoring and Reporting**

  The process is ongoing, we have to keep monitoring both the risk and the controls we implemented.
  This is where we could use the KRIs (Key Risk Indicators)
  We would also use KPIs (Key Performance Indicators)
  It is normal to do the Risk Management lifecycle on an annual basis and do out-of-cycle Risk Management on critical items.



Access Control Categories and Types:

- **Access Control Categories:**

  Administrative (Directive) Controls:
  - Organizational policies and procedures.
  - Regulation.
  - Training and awareness.

  Technical (Logical) Controls:
  - Hardware/software/firmware – Firewalls, routers, encryption.

  Physical Controls:
  - Locks, fences, guards, dogs, gates, bollards.

- **Access Control Types:**

  Access Control Types (Many can be multiple types – On the exam look at question content to see which type it is).
  - **Preventative:**
    - Prevents action from happening – Least privilege, drug tests, IPS, firewalls, encryption.
  - **Detective:**
    - Controls that Detect during or after an attack – IDS, CCTV, alarms, anti-virus.
  - **Corrective:**
    - Controls that Correct an attack – Anti-virus, patches, IPS.
  - **Recovery:**
    - Controls that help us Recover after an attack – DR Environment, backups, HA Environments.
  - **Deterrent:**
    - Controls that Deter an attack – Fences, security guards, dogs, lights, Beware of the dog signs.
  - **Compensating:**
    - Controls that Compensate – When other controls are impossible or too costly to implement.

The Ethics of your organization and (ISC)²:

- **ISC² Code of Ethics**

  You agree to this before the exam, and the code of ethics is **very testable**. Understand the preamble and the 4 ethics canons, but they should not be a substitute for the ethical judgment of the professional.

  Code of Ethics Preamble:
  - The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
  - Therefore, strict adherence to this code is a condition of certification.

  Code of Ethics Canons:
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principles.
  - Advance and protect the profession.

  Computer Ethics Institute:
  - Thou shalt not use a computer to harm other people.
  - Thou shalt not interfere with other people's computer work.
  - Thou shalt not snoop around in other people's computer files.
  - Thou shalt not use a computer to steal.
  - Thou shalt not use a computer to bear false witness.
  - Thou shalt not copy or use proprietary software for which you have not paid.
  - Thou shalt not use other people's' computer resources without authorization or proper compensation.
  - Thou shalt not appropriate other people's' intellectual output.
  - Thou shalt think about the social consequences of the program you are writing or the system you are designing.
  - Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

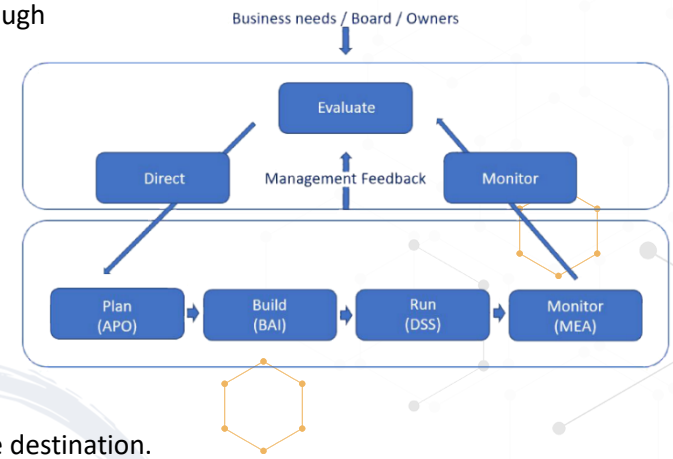
- **Your Organization's Ethics:**

  You need to know the Internal Code of Ethics of your organization
  If you don't, how can you adhere to it?

Governance vs. Management:

Governance – This is C-level Executives.

- 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.

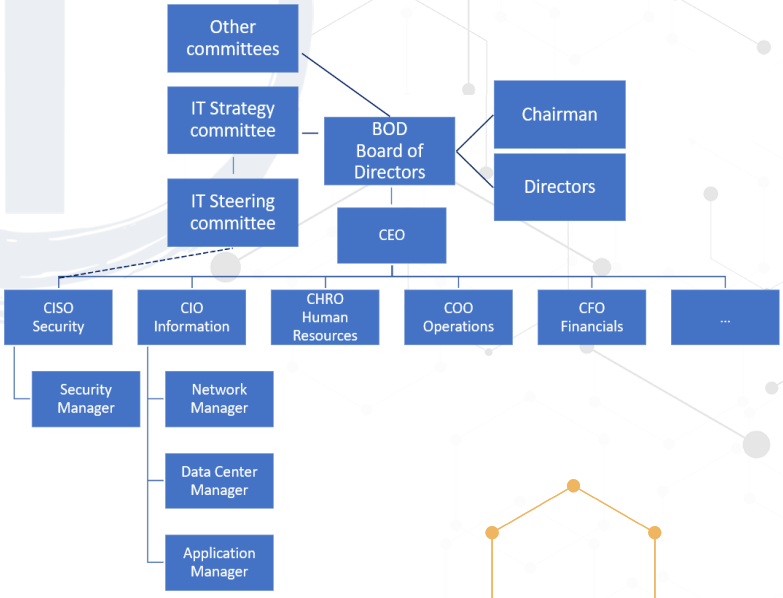


Management – How do we get to the destination.

- 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.

- **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.



Laws and Regulations:

- 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.

- **Rules, Regulations and Laws:**

HIPAA: 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.

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.

- **GDPR**

  GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
  It does **not** matter where we are based, if we have customers in EU/EEA we have to adhere to the GDPR.
  Violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.
  Restrictions: Lawful Interception, national security, military, police, justice system
  Right to access: Data controllers must be able to provide a free copy of an individual's data if requested.
  Personal data: Covers a variety of data types including: Names, Email Addresses, Addresses, Unsubscribe confirmation URLs that contain email and/or names, IP Addresses.
  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.

Information Security Governance: Values, vision, mission, and plans:

- **Security governance principles.**

  Values:
  - What are our values? Ethics, Principles, Beliefs.

  Vision:
  - What do we aspire to be? Hope and Ambition.

  Mission:
  - Who do we do it for? Motivation and Purpose.

  Strategic Objectives:
  - How are we going to progress? Plans, goals, and sequencing.

Action & KPIs:

- What do we need to do and how do we know when we achieved it? Actions, Recourses, Outcomes, Owners, and Timeframes.

Policies – Mandatory.

- High level, non-specific.
- They can contain "Patches, updates, strong encryption"
- They will not be specific to "OS, encryption type, vendor Technology"

Standards – Mandatory.

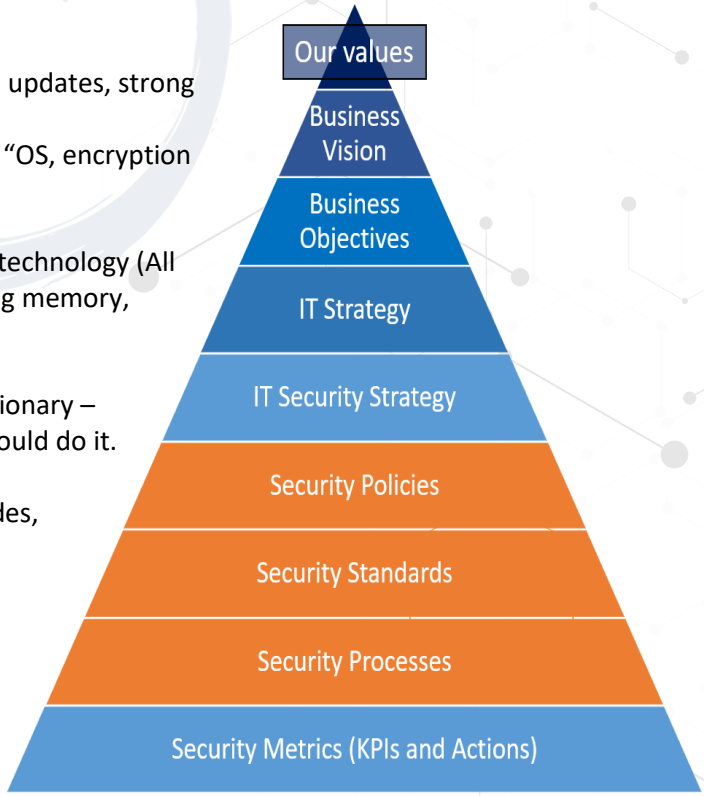
- Describes a specific use of technology (All laptops are W10, 64bit, 8gig memory, etc.)

Guidelines – non-Mandatory.

- Recommendations, discretionary – Suggestions on how you would do it.

Procedures – Mandatory.

- Low level step-by-step guides, specific.
- They will contain "OS, encryption type, vendor Technology"



➢ Domain 1: What we covered.

- This chapter is **VERY** important because:
  Every other knowledge domain build on top of this chapter
  This is the **foundation.**

- **We talked about:**
  The differences between Information Security, IT Security, and Cybersecurity.
  The CIA triad and IAAA.
  Privacy.
  Risk and incident management.
  Access control.
  The (ISC)² ethics.
  Governance, management, laws, and regulations.