CISSP Certification: CISSP domain 1 & 2

https://www.udemy.com/course/cissp-domain-1-2/

Domain 1: Security and risk management

- This is a **very important topic:**
  - Every knowledge domain builds on top of this chapter.
  - This is the **foundation**.
- 15% of questions on the certification are from this domain.

CIA(NA) triad - Confidentiality, integrity and availability

The **CIA Triad (AIC):**

- **Confidentiality:** what most people think IT security is… But it is much more.
  - Keep our data and secrets secure and secret.
  - We ensure no one unauthorised 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 authorised people can access the data they need, when they need to.
- **Non-repudiation:** the assurance that when an action is taken, it is possible to prove that the action was taken by that person. It combines the pillars of Authentication and Integrity into one concept.
- **Authentication:** Authentication is where all of this comes together. Someone or something is allowed to look at data, and someone or something is allowed to alter the data. Authentication provides the means to determine who is allowed to look at and do what.

Confidentiality - Disclosure

Threats:

- Attacks on your encryption (cryptanalysis).
- Social engineering.
- Keyloggers (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.

We use:

- Encryption for **data at rest** (for instance AES256), full disk encryption. *Data strationed in a database.*
- Secure transportation protocols for **data in motion** (SSL, TLS or IPSEC). *Traversing the network.*

- Best practices for **data in use** - clean desk policy, no shoulder surfing, screen view angle protector, PC locking (automatic and when leaving). *Actively being used on a workstation or server.* It is not actively in use (motion), it is not sitting somewhere (rest) - this data cannot be encrypted. **Training, policies and awareness** are key here. Printed data is also **data in use**!
- Strong passwords, multi factor authentication, masking, access control, need-to-know, least privilege.

Integrity - Alteration

Threats:

- Alterations of our data.
- Code injections.
- Attacks on your encryption (cryptanalysis).

We use:

- Cryptography.
- Check sums (this could be CRC).
- Message Digests also known as hash (SHA3).
- Digital signatures - non-repudiation.
- Access control.

Availability - Destruction

Threats:

- Malicious attacks (DDoS, physical, system compromise, staff).
- Application failures (errors in the code).
- Component failure (hardware).

We use:

- IPS/IDS.
- Patch management.
- Redundancy of hardware power (multiple power supplies / UPS / generators), disks (RAID), traffic paths (Network design), HVAC, staff, HA (High availability) and much more.
- SLAs- how high uptime we want (99,9%?) - ROI.

RPE: Resume producing event: two power cables for all your servers, with 120% load on one UPS, 60% one the other. Shutting down the 120% UPS means the other UPS needs to suddenly carry 120% load. This cannot be done (overload), thus shutting down the servers since the UPS is shutting down.

Put it all together

Finding the **right mix** of CIA is a balancing act. Cornerstone of IT security - finding the RIGHT mix for YOUR organisation. Too much C means A can suffer. Too much I mean A can suffer. Too much A and C / A can suffer.

The **opposite** of the CIA triad is DAD (Disclosure, Alteration and Destruction).

- **Disclosure:** someone not authorised getting access to your information.
- **Alteration:** your data has been changed.
- **Destruction:** your data or systems have been destroyed or rendered inaccessible.

(I)AAA - Identification, Authentication, Authorization and Accountability

Identification: Your name, username, ID number, employee number, SSN,... “I am Fred”. It identifies you.

Authentication: “Prove you are Fred” - should always be done with multi-factor authentication.

- **Type 1** Authentication **: something you know.** (passwords, pass phrase, PIN,...).
- **Type 2** Authentication **: something you have.** (ID, passport, smart card, token, cookie on PC,...).
- **Type 3** Authentication **: something you are.** (and Biometrics) (fingerprint, iris scan, facial geometry).

Authorization: what are you allowed to access?

- **Access Control** methods, what and how we implement depends on the organisation and what our security goals are.
    - **DAC:** Discretionary access control - you can grant rights to a certain folder or file based on who the user is.
    - **MAC:** Mandatory access control - intelligent services / military, least privilege. Exactly enough access to what they are doing - more access = grant access. Confidentiality is important in these industries!
    - **RBAC:** Role-based access control (**most common**).
    - **ABAC:** Attribute access control.
    - **RUBAC:**

Accountability (or Auditing): trace an action to a subject’s identity: prove who / what a given action was performed by (non-repudiation). My IP, my working hours,... bring me back to me changing the data.

IT Security: is **not** the most important part of the organisation, but we span the entire organisation. We enable the organisation to fulfil its mission statement and the business goals.

Security governance principles

Least privilege and Need To Know:

- **Least Privilege:** Minimum necessary access. We give our 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(s).
- **Object:** (Passive) Any passive data (both physical and data). Object is manipulated by Subject.
- Some can be both at different times, an active program is a subject (pulls data from X). When closed - the data in the program can be object.

Governance vs management

Governance: C-level executives (not you).

- Stakeholder needs, conditions and options are evaluated to define:
    - Balanced agreed-upon enterprise objectives to be achieved.
    - Setting direction through prioritisation 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? (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 Organisation structure:

- **Bottom-up:** IT security is seen as a nuisance and not a helper, this often changes when a breach happens.
- **Top-down:** IT leadership is on board with IT security. They lead and set the direction (exam!).

C-level executives (Senior leadership):

- **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.
- **COO:** Chief Operations Officer.

They report to the CEO.

Security governance principles

Governance standards and control frameworks:

- **PCI-DSS:** Payment Card Industry Data Security Standard. Required when you want to handle debit or credit 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 Organisations. **Goals** for the **entire** organisation.
- **ITIL:** Information Technology Infrastructure Library. IT Service Management (**ITSM**).
- **FRAP:** Facilitated Risk Analysis Process. Analysed one business unit, application or system at a time in a roundtable brainstorm with **internal** employees. This impact is analysed, and the threats and risks are prioritised.

ISO series:

- **ISO 27001:** establish, implement, control and improve the ISMS (Information Security Management Systems). Uses PDCA (Plan, Do, Check, Act).
- **ISO 27002:** provides practical advice on how to implement security controls. It has 10 domains it uses for ISMS. *Practical implementation*.
- **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).

Defence In Depth: also called layered defence or onion defence. Peeling one layer away - we have another layer of defence.

- Applies to physical, administrative, and logical controls.
    - To get to a server you may have to go through multiple locked doors, security guards, man traps.
- To get to data you may need to get past firewalls, routers, switches, the server, and applications security.
    - Each step may have multiple security controls.
- No single security control secures an asset.
- By implementing Defence in Depth you improve your organisation's CIA(NA).

Legal and regularly issues

- **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 organisations 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).
- **Private Regulations:** compliance is required by contract (for instance PCI-DSS).
- **Customary Law:** mostly handles personal conduct and patterns of behaviour and it is founded in traditions and customs of the area of 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?** *If you did not include security on a website - you are liable because you did not do your due diligence.*

Due Diligence and Due Care

- **Due Diligence (DD - Do Detect):** the research to build the IT security architecture of your organisation, best practices and common protection. **The research, preparation and practical preparation before implementation, Monitoring and Confirming everything works.** *Detect something is wrong, prepare and fix it with Due Care.*
- **Due Care (DC - Do Care - Do Correct): Implementation.** Prudent person rule - what would a prudent person do in this situation? This is the **actual audit** that will be checked.

Negligence (gross negligence) is the opposite of Due Care.

- If a system under control is compromised and you can prove you did your Due Care, you are most likely **not liable**.
- If a system under 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**.

- **Real evidence:** tangible and physical objects in IT security: hard disks, USB drives, **NOT the data** on them.
- **Direct evidence:** testimony from a first hand witness, what they experienced with their 5 senses.
- **Circumstantial evidence:** evidence to support circumstances for a point or other evidence.
- **Corroborative evidence:** supports facts or elements of the case, not facts on their own but they support other facts.

Hearsay: not first-hand knowledge - normally inadmissible in a case. *Computer-generated records, for us the means log files are considered hearsay. But case law and updates to the Federal Rule of Evidence have changed that.*

Evidence:

- **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. *When doing forensics - **work on a copy**. Hash the copy and the original - if both are still the same after applying changes / forensics to the copy, it is still the same file.*

- **Chain of Custody:** this is done to prove the integrity of the data - no tampering. Who handled it? When did they handle it? What did they do with it? Where did they handle it?

CISSP originates from the USA - thus the context (such as law) will push towards American Law - but overall the rules apply to other countries in the world too as counterparts.

- **Reasonable searches:** fourth amendment to the US constitution protects citizens from unreasonable search and seizure by the government. No search warrant = cannot search the house. Was the evidence obtained legally?
    - **Exception: Exigent circumstances** apply if there is an immediate threat to human life or of evidence destruction.
    - You need to ensure that employees are aware their actions are monitored (and it can be used in any way based on policies / rules). **Do mind privacy laws!!!**

Illegal concepts

- **Entrapment:** illegal and unethical: someone is persuaded to commit a crime they had no intention of committing and is then charged with it. **Not planning on committing a crime** - telling someone to hack a server, if they had no intention on doing that.
- **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 Enticements. **Already planned to commit the crime - you are making it more attractive.** They already hacked the server, you are opening ports or services - such as with honeypots.
- ***Grey area:*** *up to a jury if it is either one of the previous ones.*
- **Honeypots warning:** have a sign-off of your senior mgmt, HR and definitely Legal. They present real legal and practical risks.

Intellectual property

- **Copyright ©:** *exception: first sale, fair use*. Book, art, music, software. Automatically granted and lasts **70 years after creator's death or 95 years after creation by / for corporations.**
- **Trademarks ™:** (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 privacy 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 use 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 organisation can do nothing if their trade secret is discovered, **how** it is done can be illegal. *No real legal protection here*. How they get it may be illegal. *Corporate espionage, for example. The act may be illegal, but if someone knows the "secret" you cannot get it back easily.*
- **Cyber squatting:** buying a URL you know someone else will need (grey area legally). *How is someone going to use it? Overselling a specific URL to a company, for example. Just using the URL yourself is in theory not illegal.*
- **Typosquatting:** buying a URL that is VERY close to the real website name (can be illegal in certain circumstances). *Pretend to be Google - that is illegal! If you use the website for any other reason that is fine, not illegal. Defensive buying: buy all your similarly named domain names.*

Privacy

You as a citizen and consumer have the right that your **Personally Identifiable Information (PII)** is being kept secure.

- **US privacy regulation:** is a patchwork of laws, some overlapping and some areas with no real protection.
- **EU law:** GDPR: 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,...).

PII: unique to you: national identification number, driver's licence number, IP address, Licence plate on your car, Biometric data (fingerprints, arm prints, handwriting), credit card number, birthday, birthplace, genetic information. *If you have them, you can figure out who someone is.*

What is not PII: country, state, city you live in, gender, race, school name you worked at, job title, how much money you make, criminal record.

US regulation

- **HIPAA:** Health Insurance Portability and Accountability Act.
  - Strict privacy, security rules and Breach Notification rule on handling of PHI (Protected Health Information).

- **Security Breach Notification Law:** NOT federal, all 50 states have individual laws.
- **ECPA:** Electronic Communications Privacy Act.
    - 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.
    - *Allows ISPs to hand over private information voluntarily. Eases restriction on obtaining foreign intelligence information for the US.*
- **CFAA: Computer Fraud and Abuse Act - Title 18 Section 1030:**
    - Most commonly used law to prosecute computer crimes.
- **GLBA:** Gramm-Leach-Bliley Act:
    - Applies to financial institutions, driven by the Federal Financial Institutions.
- **SOX:** Sarbanes-Oxley Act of 2002:
    - Directly related to the accountancy scandals in the late 90's.
- **PCI-DSS:** Payment Card Industry - Data Security Standard.
    - Requires merchants and others to meet a minimum set of security requirements.

EU regulations

GDPR: General Data Protection Regulation for all individuals in the EU and the EEA (European Economic Area).

It does not matter where we are based, if we have customers in the EU / EEA we have to adhere to 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.

- Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so.
- **Personal data** covers a variety of data types including: names, email addresses, addresses, unsubscribe confirmation URLs that contain email and / or names, IP addresses.
- **Restrictions:** lawful interception, national security, military, policy and justice.
- **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 (DPO):** companies whose activities involve data processing and monitoring must appoint a DPO.

International standards

OECD: Organisation for Economic Cooperation and Development **privacy guidelines:**

- 30 member nations from around the world, including the US.
- OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued in 1980, updated in 2013.
- *There are no lawful actions if you do not adhere to one principle. Just guidelines.*
- **Collection limitation principle:** *aligns with the GDPR.*
- **Data quality principle:** data should be complete, current and relevant for what is it used for.
- **Purpose specification principle:** subject is told why is the data collected - and what is the purpose + only use it for this purpose.
- **Use limitation principle:** only used with the consent of the subject, or by authority of law. PII enclosed only used for the purpose.
- **Security safeguards principle:** reasonable safeguards to protect data from laws, unauthorised access or disclosure.
- **Openness principle:** open communication about policies of how data is used, identity of organisation and nature of PII collected.
- **Individual participation principle:** should be able which organisations have your data. Correct wrong data, or challenge any requests that are denied.
- **Accountability principle:** comply with measures that are stated in the other principles.

Wassenaar Arrangement: export / import controls for *Conventional Arms and Dual-Use goods* and Technologies.

- 41 countries are part of the arrangement.
- **Cryptography is considered "Dual-Use":**
    - Iran, Iraq, China, Russia and others have import restrictions on strong cryptography.
    - If it is too strong it cannot be broken; they want to be able to spy on their citizens.
    - Companies have to make "country specific" products with different encryption standards.

Third party software, acquisitions and divestiture

We need to ensure their security standards, measures and controls meet the security standards of our organisation.

- **Procurement:** when we buy products or services from a third party, security is included and not an afterthought.
- **SLA: Service Level Agreement:** *99,9% uptime is promised.*
- Industry Standard Attestation should be used: ISO, SOC, PCI-DSS.
    - Right to penetration test or right to audit are often part of agreement.
- **Acquisitions:** your organisation has acquired another.
    - How do we ensure security standards are high enough? Data availability in transition?
- **Divestiture:** your organisation is being split up.
    - How do we ensure no data crosses boundaries it should not? Who gets IT infra?

Ethics

ISC2 Code of Ethics

You agree to this before the exam, and the code of ethics is **very testable**.

There are only four mandatory canons in the code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgement of the professional.

- **Code of Ethics Preamble:** 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 behaviour.
    - Therefore, strict adherence to this code is a condition of certification.
    - *Know you must sign the ethics before the exam - if you break them (Negligence) your certificate might be revoked.*
- **Code of Ethics Canons:** protects society, common good, necessary public trust and confidence, and the infrastructure.
    - Act honourably, honestly, justly, responsibly, and legally.
    - Provide diligent and competent service to principles.
    - Advance and protect the profession.

Computer Ethics Institute

Ten commandments of Computer Ethics:

- 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 authorisation 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.

No exam questions - just handle ethically.

IABs Ethics and the internet: considered **unethical behaviour:**

- seeks to gain unauthorised access to the resources of the internet.
- Disrupt the intended use of the internet.
- Wastes resources (people, capacity, computer) through such actions: *Destroy integrity of computer-based information, or compromise the privacy of users.*

Information security governance

Security governance principles

- **Values:** what are our values? Ethics, Principles, Beliefs.
- **Vision:** what do we aspire to be? Hope and ambition - future?
- **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, resources, outcomes, owners and timeframes.

Plans:

- **Governance:** strategic plan: 3 - 5 years, reviewed annually, long term.
- **Management:** tactical plan: 1 year, acquisitions, hiring, budgets,...
- **Staff:** operational plan: high detail, updated frequently.

Policies - Mandatory: General Management Statements.

- **High level, non-specific**: what is allowed, what is not allowed.
- Influences by our mission and vision.
- Three categories: regulatory, advisory or informational.
    - Regulatory: rules we have to follow based on the industry we are in (HIPAA).
    - Advisory: what types of behaviour are acceptable, or not acceptable (punishments, acceptable use, employment,...).
    - Informational: inform people - talks about our values, mission, vision.
- They can contain “patches, updates, strong encryption”.
- They will **not be** specific to “OS, encryption type, vendor technology” -> **Procedures**.

Standards - Mandatory: Specific Mandatory Controls

- Describes a specific use of technology (all laptops are W10, 64 Bit, 8 GB mem,...).

Guidelines - non-Mandatory: Recommendations / best practices

- Recommendations, discretionary - suggestions on how you could implement it.

Procedures - Mandatory: step-by-step instructions

- Low level step-by-step guides, specific.
- They will contain “OS, encryption type, vendor technology”.

Baselines (Benchmarks) - Mandatory:

- Benchmarks for server hardening, apps, network. Minimum requirements, we can implement stronger if needed.

Personnel security

Users often pose the largest security risk.

- **Awareness:** change user behaviour. This is what we want, we want them to change their behaviour.
- **Training:** provides users with a skillset - this is nice, but if they ignore the knowledge, it does nothing.
    - **Pre-training:** requirements identification, understanding the needs.
    - **Training:** execute the program.
    - **Post-training:** training assessment, support after training.

- **Hiring practices:** we do background checks where we check: references, degrees, employment criminal, credit history. New staff signs an NDA (Non-Disclosure Agreement).
- **Employee termination practices:** we want to coach and train employees before firing them. They get warnings. Coordinate with HR.
- **Vendors, consultants and contractor security:** outside people in our environments, we need to ensure they are trained on how to handle data. Their systems need to be secure enough for our policies and standards;
- **Outsourcing and offshoring:** having someone else do part of your work.
    - *This can lower cost, but a thorough and accurate Risk analysis must be performed. **Risk of outsourcing:** the **quality of the work** for a **lower price**. Offshoring can also pose problems with them not having to comply with the same data protection standards.*

Awareness / training: provide recognition, or security champions. Recognition can be in the form of a reward. Phishing training: department notifying the most phishing emails wins a prize! Security champions: you like this kind of title, right? Understand how to explain the concept to your end-user.

Access control categories and types

Categories:

- **Administrative (Directive) controls:** Organisation policies and procedures, regulation and training / awareness.
- **Technical controls:** hardware / software / firmware - firewalls, routers, encryption.
- **Physical controls:** locks, fences, guards, dogs, gates, bollards.

Types:

- **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, (XD)R, (ED)R.
- **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 dog signs, MOTD (Message Of The Day).
- **Compensating:** controls that compensate - when other controls are impossible or too costly to implement.

Risk Management - Identification

Risk = Threat * Vulnerability

The **risk management lifecycle is iterative**.

Exam: what do we do next after this step (not the theory - but the practical take). This is also iterative - step 4 will go back to step 1!

1. **IT risk identification:** know there is a risk.
2. **IT risk assessment:** how bad is this risk? Potential impact?
3. **Risk Response and Mitigation:** how do we want to react to this risk? Mitigation?
4. **Risk and Control monitoring and reporting.**

IT risk identification

- 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,...

Risk assessment

- Qualitative and quantitative risk analysis.
- Uncertainty analysis.
- Everything is done using cost-benefit analysis. *How much does it cost **and how much will it save us?***
- Risk mitigation / risk transference / risk acceptance / risk avoidance.
    - **Mitigation.**
    - **Transference:** transfer the risk to someone else (insurance, or share the risk).
    - **Acceptance:** accept the risk is there. We know it, Due Diligence and Due Care are in order - we know it will cost us something, but the countermeasure costs more. We live with the risk.
    - **Avoidance:** Due Diligence and Due Care are in order - financially not viable to mitigate, transfer or accept. We just **stop** and accept the losses (No laptop for the entire company, for example).
- Risk rejection is **NEVER** acceptable.
- We assess the current countermeasures:
    - Are they good enough?
    - Do we need to improve them?
    - Do we need to implement entirely new countermeasures?
- Assess the **current** countermeasures.

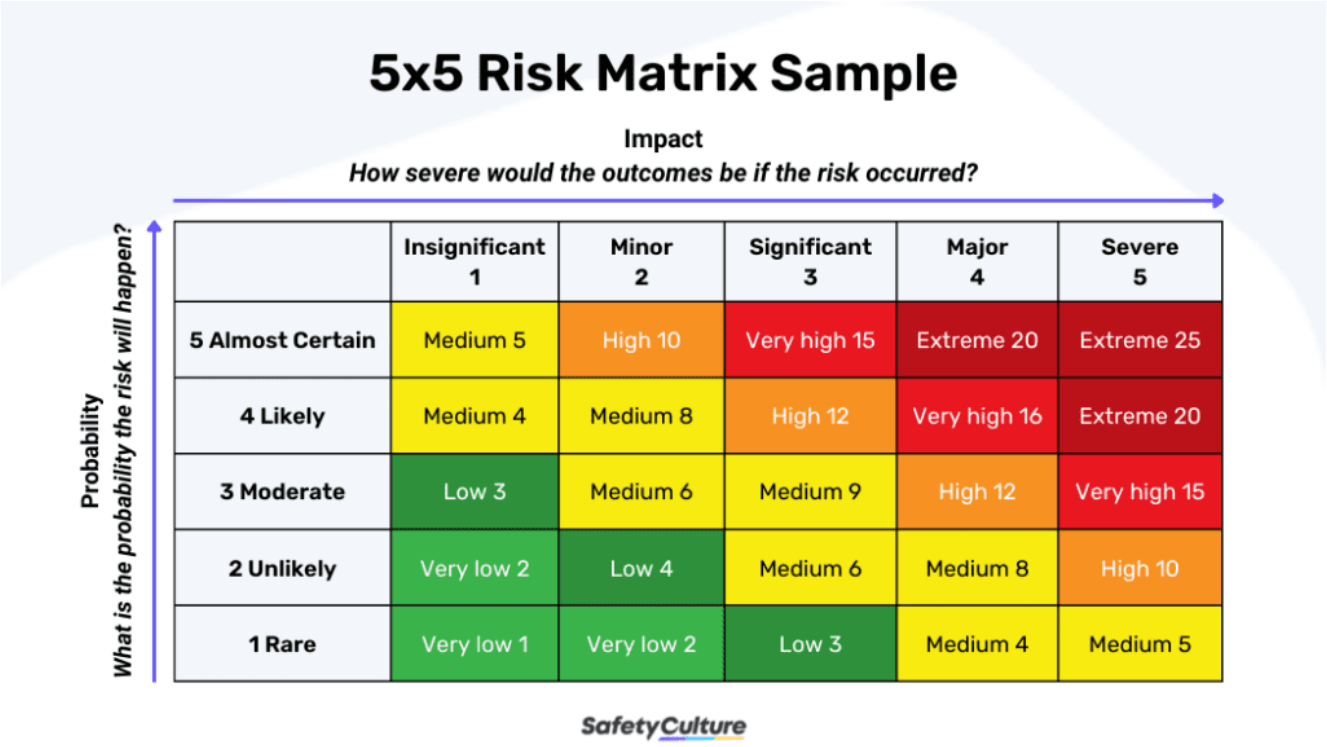
Qualitative and quantitative risk analysis

- **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 monetary value?
- **Threat:** a potentially harmful incident (Tsunami, Earthquake, Virus,...).
- **Vulnerability:** a weakness that can allow the threat to do harm. Having a datacenter in the tsunami flood area, not earthquake resistant, not applying patches, and anti-virus,...
- **Risk = Threat * Vulnerability.**
- **Impact:** can at times be added to give a more full picture.
- **Risk = Threat * Vulnerability * Impact.**
- **Total Risk = Threat * Vulnerability * Asset Value.**
- **Residual Risk = Total Risk - Countermeasures.**

Risk analysis matrix

Let's pick an asset - a laptop:

- How likely is one to get stolen or left elsewhere?
    - *I would think Moderate or likely.*
- How bad is it if it happens?
    - *Depends on a couple of things: encryption? PII? Likely and or minor issue.*



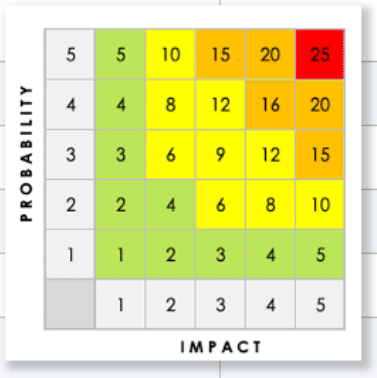
IMPACT ON PROJECT OBJECTIVES							PROBABILITY				
	Cost, $M	Schedule, Mos	Product Quality	Safety	Environm.	Reputation	< 0.1% Very Low (1)	0.1% - 10% Low (2)	10% - 50% Medium (3)	50% - 90% High (4)	>90% Very High (5)
Very High (5)	>50	>6	System requirements are not achieved	Single or multiple fatalities	Massive Effect	International media coverage. Irreparable stakeholder impact	5	10	15	20	25
High (4)	20 -- 50	3 -- 6	Substantial effect on performance objectives	Serious personal injury resulting in permanent disability	Major Effect	National media coverage. Substantial stakeholder impact	4	8	12	16	20
Medium (3)	5 -- 20	1 -- 3	All design and operating margins eliminated	Injury to personnel not resulting in permanent disability	Localized Effect	Regional media coverage. Moderate stakeholder impact	3	6	9	12	15
Low (2)	0.5 -- 5	0.5 - 1	Minor decrease in system performance	Medical treatment of personnel. Lost time incident	Minor Effect	Local media attention. Minor stakeholder impact	2	4	6	8	10
Very Low (1)	< 0.5	< 0.5	Slight degradation of element performance	Minor impact on personnel. First aid only. No lost time	Slight Effect	Slight media attention. Little stakeholder impact	1	2	3	4	5

Risk registers

- A risk category to group similar risks (a giant spreadsheet).
- 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 the event actually occurs rated on an integer scale.
- The probability or likelihood of its occurrence is rated on an integer scale.
- The Risk Score (Risk Rating) is the multiplication of Probability and Impact, and is often used to rank the risk.
- Common mitigation steps: identify, analyse, plan response, monitor and control.

SIMPLE SAFETY RISK REGISTER TEMPLATE

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated.	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Address highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Leaks from roof during rain make the floor slippery	Slips and falls	3	5	15	– Order "slippery when wet" signs – Have mops on hand – Fix roof	Allen
Shortage of eye protection	Increase in injuries Production delayed Increased insurance premiums	5	1	5	– Increase supply – Low inventory warnings – Find alternative suppliers	Linda
		4	5	20		
		5	5	25		
		2	1	2		
		3	4	12		
		1	1	1		
		2	4	8		
		4	4	16		



Quantitative Risk Analysis

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?
- **Annualised 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).

Laptop theft example as before: Laptop - Lost / Theft (unencrypted)

Risk acronym	Value
AV: Asset Value	10.000$
EF: Exposure Factor	100%
SLE (AV x EF): Single Loss Expectancy	10.000$
ARO: Annual Rate of Occurrence	25
ALE: Annualised Loss Expectancy	250.000$

- **AV:** Laptop (1.000$) + PII (9.000$) per loss (AV).
- **EF:** It is a 100% loss, it is gone.
- **SLE:** AV x EF.
- **ARO:** 25 laptops lost / year.
- **ALE:** Annualised loss is 250.000$.

Data Center - flooding

Risk acronym	Value
AV: Asset Value	10.000.000$
EF: Exposure Factor	15%
SLE (AV x EF): Single Loss Expectancy	1.500.000$
ARO: Annual Rate of Occurrence	0.25
ALE: Annualised Loss Expectancy	375.000$

- **AV:** Data center is valued at 10.000.000$
- **EF:** If flooding happens, 15% of Data Center is compromised
- **SLE:** AV x EF.
- **ARO:** flooding happens every 4 years (0.25 or 25%).
- **ALE:** Annualised loss is 375.000$.

Let's use a 4-year tech refresh cycle:
- Full disk encryption software and support: 75.000$ initial and 5.000$ / year.
- Remote wipe capabilities for the laptop: 20.000$ initial and 4.000$ / year.
- Staff for encryption and help desk: 25.000$ per year.

Doing nothing costs us 1.000.000$ per refresh cycle (250.000$ / year).
Implementing full disk encryption and remote wipe will cost 231.000$ per refresh cycle (57.750$ / year).

Laptop hardware is a 100% loss, regardless. What we are mitigating is the 25 x 9.000$ = 225.000$ by spending 57.250$.

This is our ROI (Return on Investment): TCO (57.250$) < ALE (250.000$). This makes fiscal sense, we should implement it.

Types of risk responses:
- **Risk acceptance:** we know the risk is there, but the mitigation is more costly than the cost of the risk (low risks).
- **Risk mitigation (reduction):** the laptop encryption / wipe is an example - acceptable level (leftover risk = Residual).
- **Risk transference:** 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.

This area is very testable, learn the formula, the risk responses to differentiate qualitative and quantitative risk:

- **Qualitative:** think “quality”: This concept is semi-vague: “pretty good quality”.
- **Quantitative:** think “quantity”: How many, a **specific number**.

NIST SP 800-30

United States National Institute of Standards and Technology Special Publication.
A 9-step process for Risk Management:

1. System characterisation (Risk management scope, boundaries, system and data sensitivity).
2. Threat identification (what are the threats to our systems?).
3. Vulnerability identification (what are the vulnerabilities of our systems?).
4. Control analysis (analysis of the current and planned safeguards, controls and mitigations).
5. Likelihood determination (qualitative - how likely is it to happen?).
6. Impact analysis (qualitative - how bad is it if it happens? Loss of CIA).
7. Risk determination (look at 5-5 and determine Risk and Associate Risk Levels).
8. Control remediations (what can we do to mitigate, transfer,... the risk).
9. Results documentation (documentation with all the facts and recommendations).

KGIs, KPIs, and KRIs

- **KGIs: Key Goal Indicator:** define measures that tell management, after the fact - whether an IT process has achieved its business requirements. *This is the WHOLE thing / goal.*
- **KPIs: Key Performance Indicators:** define measures that determine how well the IT process is performing in enabling the goal to be reached. *How are we doing on one specific task? Correlation between goal and performance. This is a DETAIL of the goal.*
- **KRIs: Key Risk Indicators:** metrics that demonstrate the risks that an organisation is facing or how risky an activity is. *How risky is a certain activity? How well do we adhere to the risk appetite of our organisation? Early warning system!*
    - They are the mainstay of measuring adherence to and establishing enterprise risk appetite.
    - Key indicators are metrics used by organisations to provide an early signal of increasing risk exposures in various areas of the enterprise.
    - KRI gives an early warning to identify potential event(s) that may harm continuity of the activity / project.

Risk Response and Mitigation & Risk and control monitoring and reporting

What happens after our risk management?

Risk response and mitigation

Risk mitigation, transference, acceptance and avoidance.

- We act on senior mgmt choices, which they made based on our recommendations for the assessment phase.
- Do we stop issuing laptops, or do we add full-disk encryption and remote wipe capabilities?
- We update the risk register, with the mitigations, the risk responses we chose and see if the new risk level is acceptable.

Risk and control monitoring and reporting

The process is ongoing, we have to keep monitoring both the risk and the controls we implement.

- This is where we would use the KRI (Key Risk Indicators).
- We would also use KPIs (Key Performance Indicators).
- You are the translating link, you have to be able to explain IT and IT security to the Senior mgmt in terms they can understand. *How does IT work… and especially how does IT security work! Translate into an understandable language.*
- It is normal to do the risk management lifecycle on an annual basis, and do out-of-cycle risk management on critical items. *Annual risk assessment + new servers we do a new risk assessment; and include those in the annual risk assessment. Every three months we do a full assessment.*

Risk management and maturity model

- **Level 1: initial:** limited, or no risk management. No predictability.
- **Level 2: repeatable:** basic risk mgmt processes. Inconsistent application. Some senior mgmt involvement.
- **Level 3: defined:** processes are documented. Some consistent applications. Limited predictability. More senior mgmt involvement.
- **Level 4: managed:** risk mgmt used in early stages. Risk mgmt is central in projects and investments. Senior mgmt is actively involved throughout projects.
- **Level 5: optimising:** risk mgmt is fully integrated into everything. Lessons learned are always used for future projects.

Lower: more risk and waste.
Higher: more productivity and quality.

Risk attackers and types of attacks

Types of attackers

Hackers:

- **Now:** anyone trying to get access to or disrupt any leg of the CIA triad.
- **Original use:** someone using something in a way not intended.
- **White hat hackers:** profession pen testers trying to find flaws so we can fix it (ethical hackers.
- **Black hat hackers:** malicious hackers, trying to find flaws to exploit them (Crackers - they crack the code).
- **Grey hat hackers:** they are somewhere between the white and black hats, they go looking for vulnerable code, systems or products.
- **Script kiddies:** they have little or no coding knowledge but many sophisticated hacking tools are available and easy to use.
- **Outsiders:**
    - Unauthorised individuals - trying to gain access. They launch the majority of attacks, but are often mitigated if the organisation has good Defence in Depth.
    - Interception, malicious code (virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage, or unauthorised system access.
    - 48 - 62% of risks are from outsiders.
- **Insiders:**
    - Authorised individuals - not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
    - This could be: assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified information, or corrupted data.
    - 38 - 52% are from insiders. *Authentication and authorisation controls are needed!*
- **Hacktivism / hacktivist:** hacking for political or socially motivated purposes.

    - Often aimed at ensuring free speech, human rights, freedom of information movement.
- **Governments:** state sponsored hacking is common; often you see the attacks happening between the hours of 9 and 5 in that time zone. It is a day job.
    - Approximately 120 countries have been developing ways to use the internet as a weapon to target financial markets, and government computer systems and utilities.
    - *Famous attacks: US elections (Russia), Sony website (N. Korea), Stuxnet (US/Israel), US Office of personnel management (China),...*
- **Bots and botnets (robots):** *also called a zombie.* Bots are systems with malware controlled by a botnet.
    - The system is compromised by an attack or the user installing a remote access trojan (game or application with a hidden payload).
    - They often use IRC, HTTP or HTTPs.
    - Some are dormant until activated.
    - Others are actively sending data from the system (credit card / bank information for instance).
    - Active bots can also be used to send spam emails.
    - **Botnets** are a **C&C (Command & Control) network,** controlled by people (bot-herders). They can often be 1.000s or more bots in a botnet.

Phishing

Fishing spelled in hacker slang with Ph not f.

- **Phishing:** social engineering mail attack.
    - Click to win, send information to get your inheritance,...
    - Sent out to hundreds of thousands of people. If just 0.02% follow the instructions they have 200 victims.
- **Spear phishing:** targeted phishing, not just random spam, but targeted at specific individuals.
    - Sent with knowledge about the target (person or company). Familiarity increases success.
- **Whale phishing (whaling):** spear phishing targeted at senior leadership of an organisation.
    - This could be “your company is being sued if you don’t fill out the attached documents (with trojan) and return them to use within 2 weeks”.
- **Vishing (voice phishing):** attacks over automated VOIP (Voice over IP) systems, bulk spam similar to phishing.
    - There are: “your taxes are due”, “your account is locked”, or “enter your PII to prevent this” type of calls.

Business Continuity Planning

Any organisation will encounter disasters every so often, how we try to avoid them, how we mitigate them and how we recover when they happen is very important.

- If we do a poor job, the organisation may be severely impacted or have to close.
- Companies that had a major loss of data, 43% never reopen and 29% close within two years.

BCP: Business Continuity Plan: process of creating the long-term strategic business plans, policies and procedures for continued operation after a disruptive event. *The excuse: it is often "too expensive". But never reopening or closing within 2 years is the real disaster!*

- It is for the **entire organisation**, everything that could be impacted, **not just IT.**
- Lists a range of disaster scenarios and the steps the organisation must take in any particular scenario to return to regular operations.
- BCPs often contain (sub plans):
    - **COOP (Continuity of Operations Plan):** How do we continue to operate our day-to-day functions? HR, Payroll,...
    - **Crisis Communications Plan:** specific people allowed to communicate internally and externally. Not part of the team? Don't talk to the press or internally even if you are asked questions.
    - **Critical Infrastructure Protection Plan:** protect specific critical assets.
    - **Cyber Incident Response Plan:** part of the DRP - IT infra.
    - **DRP (Disaster Recovery Plan).**
    - **ISCP (Information System Contingency Plan).**
    - **Occupant Emergency Plan.**
- We look at what we would do if a critical supplier closed, the facility was hit by an earthquake, what if we were snowed in and staff couldn't get to work,...
- They are written **ahead of time**, and continually improved open, it is an iterative process.
- We write the BCP with input from **key staff** and at times **outside BCP consultants**.

Developing our BCP

Older versions of the NIST 800-34 had these steps as a framework for building your BCP/DRP.

- **Projection initiation:** start project, identify stakeholders, get C-level approval, formalise project structure.
- **Scope of the project:** identify exactly what we are trying to do and what we are not (stakeholders!).
- **Business impact analysis:** identify and prioritise critical systems and components.
- **Identify preventive controls:** identify current and possible preventative controls we can deploy.
- **Recovery strategy:** how do we recover efficiently? What are our options? DR site, system restore, cloud,...

- **Plan design and development:** build a specific plan for recovery from a disaster, procedures, guidelines and tools.
- **Implementation, training and testing:** test the plan to find gaps and train staff to be able to act on the plan.
- **BCP / DRP maintenance:** iterative process! Organisation develops, adds systems, facilities, or technologies. Threat landscape also changes! Keep improving and tweaking our BCP and DRP.

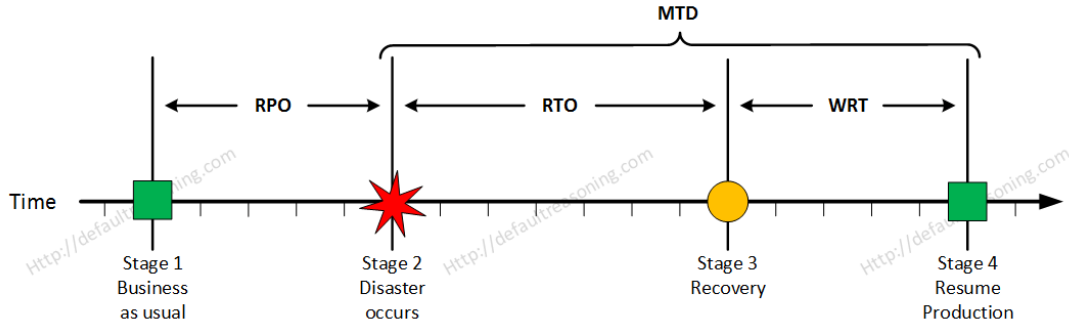
Senior mgmt needs to be involved and committed to the BCP / DRP process. *They need to be part of at least the initiation and the final approval of the plans.*

BIA (Business Impact Analysis)

- Identifies critical and non-critical organisation systems, functions and activities.
- Critical is where disruption is considered unacceptable, the acceptability is also based on the cost of recovery.
- A function may also be considered critical if dictated by law.

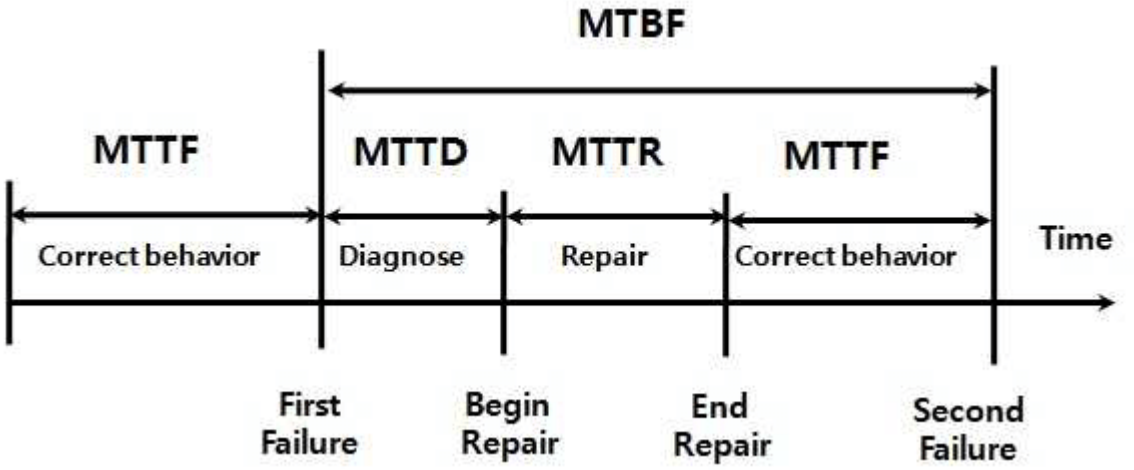
For each (in-scope) system, function or activity, two values are then assigned:

- **RPO: Recovery Point Objective:** acceptable amount of data that can not be recovered. **Tolerable amount of data loss.**
    - Maximum tolerable data loss for the system, function, or activity is not exceeded.
- **MTD: Maximum Tolerable Downtime:** MTD >= RTO + WRT:
    - System rebuild time, configuration and reinsertion into production must be less than or equal to our MTD.
    - The total time a system can be inoperable before our organisation is severely impacted.
- **RTO: Recovery Time Objective:** the amount of **time** to restore the system (hardware). **Down time**.
    - The recovery time objective must ensure that the MTD for each system, function or activity is not exceeded.
- **WRT: Work Recovery Time:** software.
    - How much time is required to configure a recovered system.

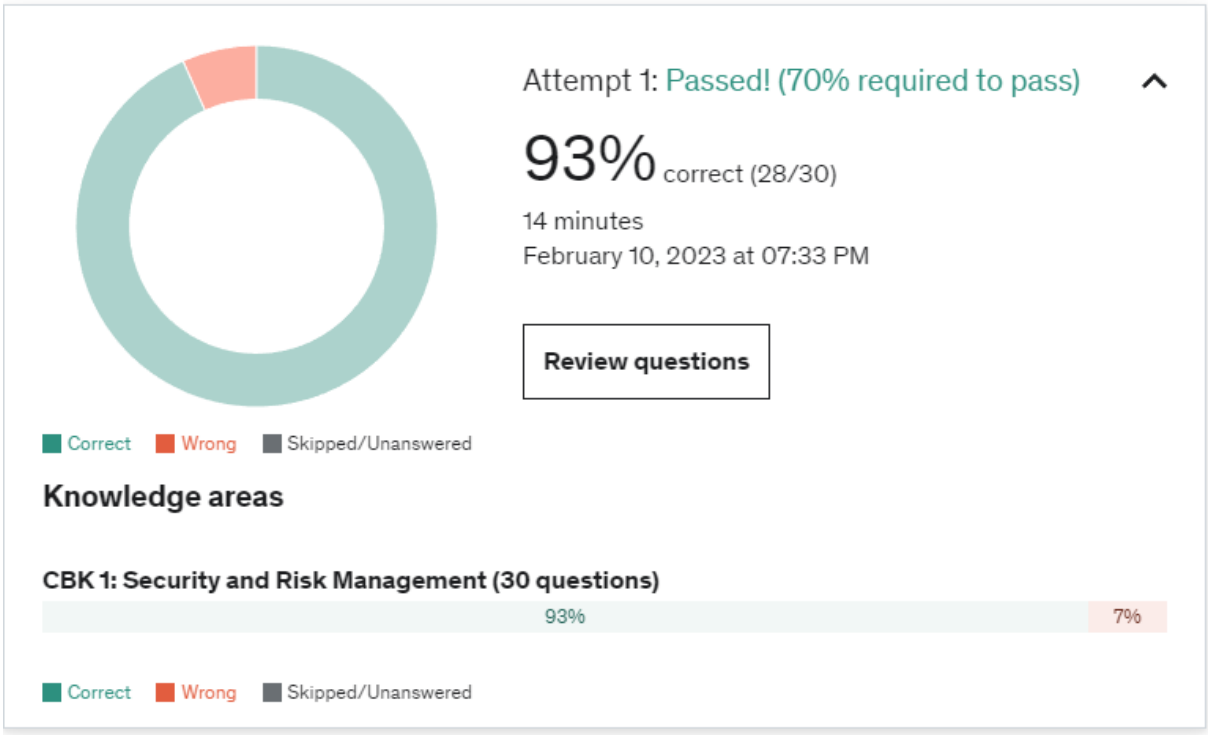


- **MTBF (Mean Time Between Failures):** how long a new or repaired system / component will function on average.
- **MTTF (Mean Time to Failure):** how long time before a device failure.

- **MTTR (Mean Time to Repair):** how long will it take to recover a failed system.
- **MOR (Minimum Operating Requirements):** the minimum requirements for our critical systems to function.
- **MTTD (Mean Time to Diagnose):** how long time to diagnose.



Test results first chapter



CISSP Domain 2: Asset Security

This domain is the smallest chapter - but percentage makes up for 10% of the exam.
Topics: information and asses classification, ownership, protect privacy, appropriate retention, data security controls and handling requirements.

Information life cycle

- **Data acquisition:** the information is either created or copied from another location. *Make it useful, index it, and store it: bank - someone needs a loan. We check PII (credit,...) and input it in a document. We want to encrypt it and store it securely. Procedures based on our policies. Who has access to it? Now it is **useful**.*
- **Data use:** how do we ensure the data is kept confidential, the integrity is intact, and it is available when needed (CIA!). *Do not mistake this for "DATA IN USE"! We are simply USING the data at this stage. We need to store it, as we are not going to use it right away - it needs to be available when we NEED it.*
- **Data archival:** retention required by law or the data will be used later. *Archival vs backup! Data retention - backup is to restore data, archival is data retention.*
- **Data disposal:** how do we dispose properly of the data once it is no longer useful and required.

Data classification

Military classification:

- **Top Secret (TS): exceptionally grave damage:** weapon blueprints, theatre or war plans, espionage data.
- **Secret (S): serious damage:** troop plans, deployment plans, plans not included in TS plans, reports on shortages or weaknesses.
- **Confidential (C): damage:** intelligence reports, operational or battle reports, mobilisation plans.
- **Unclassified (U):** available upon request, does not need a particular classification or has been declassified.

Private sector classification:

- **Confidential:** proprietary information, trade secrets, source code, anything that gives us competitive advantage.
- **Private:** PHI, PII, financial data, employee data, payroll.
- **Sensitive:** networking diagrams, IP assignments, system and software specific information.
- **Public:** websites, advertisements, any information we make publicly available.

Specific types of access for military classification:

- **Labels: <u>Objects</u> have labels** assigned to them. The label is used to allow Subjects with the right clearance to access them. *Label can be: "TOP SECRET".*
- **Clearance: <u>Subjects</u> have Clearance** assigned to them. A formal decision on a subject's current and future trustworthiness.

Specific types of access:

- **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.
    - Mostly used with RBAC.
- **Least privilege (mandatory access control):** users have the minimum necessary access to perform their job duties.

Sensitive information and media security

Sensitive information: any organisation has data that is considered sensitive for a variety of reasons. We want to project the data from Disclosure, Alteration and Destruction (DAD).

Data states

- **Data at rest: stored data:** data on disks, tapes, CDs/DVDs, USB sticks.
    - Data encryption (full / partial), USB encryption, tape encryption.
    - 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 cannot be encrypted:** use good practices: clean desk policy, print policy, allow no “shoulder surfing”, the use of view angle privacy screen for monitors, locking computer screen when leaving workstation.

Data storage and handling

- **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. *Need to know.*
- **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.
- **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 statutory requirements.

Data, system, mission ownership, custodians and user (roles)

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 infra manager.
- **Data controllers and data processors:**
    - **Controller:** create and manage sensitive data in the organisation (HR / Payroll).
    - **Processors:** manage the data for controllers (outsourced payroll).
- **Security administrators:** responsible for firewalls, IPs, IDS, security patches, create accounts and assign access to the data following the data owners directions.
- **Supervisors:** responsible for user behaviour 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 employee's 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, 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: 0s (off) and 1s (on) - switches representing bits.

- **ROM: Read Only Memory:** is nonvolatile. Retains memory after power loss. Most common use is the BIOS.
    - **PROM:** programmable read only memory. *Reprogrammable only once.*
    - **EPROM:** erasable (flash) programmable read only memory. *Can be reprogrammed many times using ultraviolet light. Not used anymore.*
    - **EEPROM:** electrically erasable programmable read only memory. *Reprogrammable using electric charges.*
- **PLD: programmable logic devices:** 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: 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, 5 SDRAM.
- **Firmware:** this is the BIOS on a computer, router or switch. Low-level operating system and configuration. Stored on an embedded device. PROM, EPROM or EEPROM are common firmware chips.
- **Flash memory:** small portable devices (USB sticks are an example) - they are a type of EEPROM.
- **SSD Drives: Solid State Drives:** combination of EEPROM and DRAM, cannot be degaussed.
    - To ensure no data is readable we must use ATA secure erase and or 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 cannot be retrieved. This pertains to both electronic media and paper copies of data.

Paper disposal: 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. Don't throw out sensitive data in your trash. Cross shredding: instead of 50 pieces, this will create 500 pieces - much more harder similar to password security.*

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 0s or random characters over the data.
    - **Sanitisation:** is a process of rendering target data on the media infeasible for a given level of recovery effort.
    - **Purge:** removing sensitive data from a system or data to a point where data recovery is no longer feasible even in laboratory env.
- **Degaussing:** destroys magnetic media by exposing it to a very strong magnetic field. Will most likely destroy the media integrity. *Put the SSD in a microwave!*

- **Full physical destruction is safer than soft destruction:**
    - **Disk crushers:** they crush disks.
    - **Shredders:** do the same as paper shredders do, but on metal.
    - **Incineration, pulverising, melting and acid:** ensure full data destruction.

It is common to do multiple types of data destruction: degaussing and disk crushing.

Data security controls and frameworks

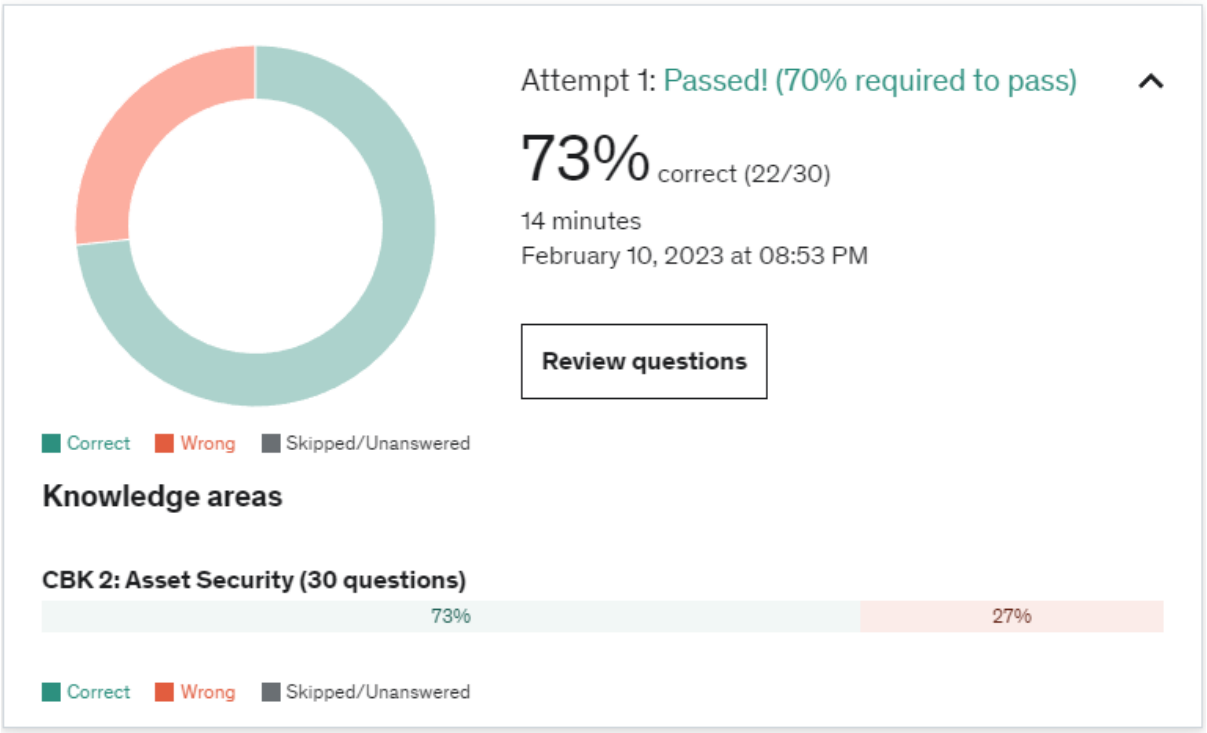
We use standards, baseline, scoping and tailoring to decide which controls we use, and how we deploy them. *ISO27000, OCTAVE, COBIT, ITIL or PCI-DSS.*

- **Scoping:** determining which portion of a standard we will deploy in our organisation.
    - 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**.
- **Tailoring:** customising a standard to your organisation.
    - Apply this standard, but use a stronger encryption.
- **Certification:** system and security measures to protect it meet the security requirements set by the data owner or by regulations / laws. *Server hardening, testing, validation,...*
- **Accreditation:** data owner accepts the certification and the residual risk. This is required before the system can be put into production.

Data protection

- **DRM: Digital Rights Management:** use technology and systems to protect copyrighted digital media.
    - Encryption.
    - Permissions management and limiting access:
        - Serial numbers, limiting installations, expiry dates, IP address, geolocation, VPN.
        - Copy restrictions: copy, edit, saving, screenshots, screen recording, printing.
    - Persistent authentication and audit trails.
    - Tracking: watermarks or metadata embedded in files.
- **CASB: Cloud Access Security Broker:** on-premise 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.
- **DLP: Data Loss Prevention:** loss vs leak. Data in use, motion and at rest. Network and endpoint DLP.

Test results second chapter



When assigning sensitivity to our data, which of these should NOT be a factor?
Who will access it, the value of the data and how impactful a disclosure would be should all factor into our sensitivity labels, how we use the data should not.

Which of these types of data destruction would we use to ensure there is no data remanence on our PROM, flash memory, and SSD drives?
We can't overwrite, format, or degauss PROM.
The only way to ensure proper destruction is shredding.

Which of these would be something we do during the e-discovery process?
e-Discovery or Discovery of electronically stored information (ESI) is the process of producing all relevant documentation and data to a court or external attorneys in a legal proceeding.

Which of these would be something we would consider for proper data disposal of SSD drives?
SSD drives can't be degaussed and formatting or deleting the files only removes the file structure, most if not all files are recoverable. We would need to shred the SSD drives.

We have many policies we need to adhere to in our organisation. Which of these would be part of our clean desk policy?
As part of a clean desk policy we should only use paper copies of sensitive data when strictly needed.

Bibliography

Log management:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
Security testing and assessment:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
Code of ethics:
https://www.isc2.org/Ethics