INFORMATION SECURITY

PRINCIPLES AND GOVERNANCE

PAULA QUEIROZ | JANUARY 2024

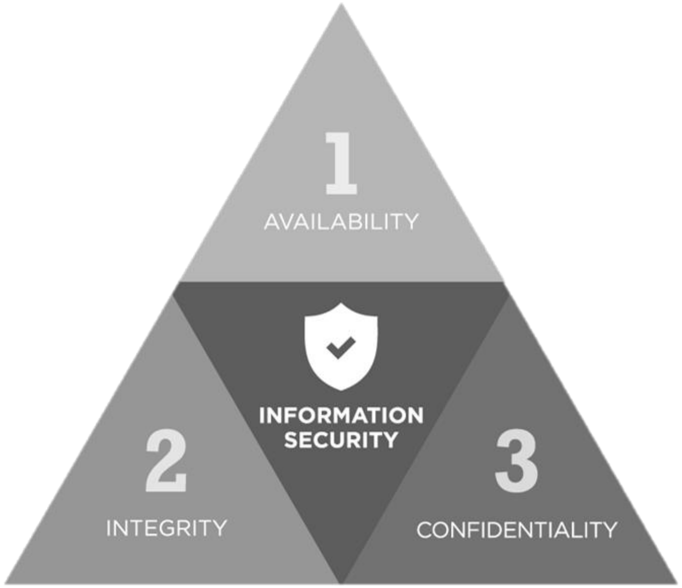
AGENDA

- The CIA Triad
- Identification, Authentication, Authorisation and Accountability
- Access Control Categories, Types and Models
- Corporate Governance and Information Security Governance
- InfoSec Governance and People
- Legal Concepts
- Governance Standards and Control Frameworks

PART 1

THE CIA TRIAD

THE CIA TRIAD



At the very core, the base pillars of information security, from which every other security concept derives, are confidentiality, integrity and availability of information. This definition is commonly known and the CIA Triad or Information Security Triad where each of these three most fundamental aspects of information security carries the same importance and weight as the other two.

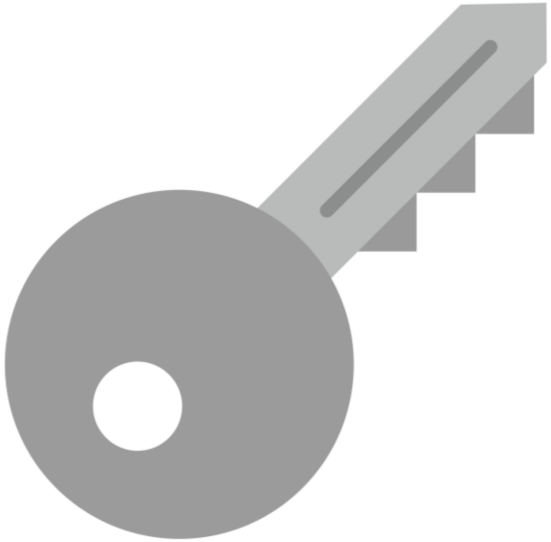
These 3 fundamental concepts are, therefore, deeply intertwined and indivisible and the 3 of them together form the very core of information security. Regardless of the circumstances, whatever data/system/service we refer to as being secure must be so when it comes to all 3. Where either of these isn't taken into consideration, the object we are referring to cannot, by definition, be considered secure as, as stated, the indivisible presence of all 3 is the base of information security.

Opposite to the CIA triad, we have what's generally abbreviated as DAD: disclosure (non-authorised access to information), alteration (data changes that render it non-accurate and/or incomplete) and destruction (data, systems and/or services are destroyed or inaccessible).

In practical terms, however, it's worth noting that, depending on the context (ie nature of a business), a component of the infosec triad may be perceived as weighing more or less than the other two. In any case, regardless of the context, information security will always aim at finding the right balance between these three, which fits the specific business needs, as very aggressive focus over one may affect the others.

Non-repudiation (which will be discussed later) is often also put at the same level of meaningfulness as confidentiality, integrity and availability over the information but, at this stage, it cannot be stressed enough how fundamental it is to understand the CIA triad as the base to understand everything else in terms of information security.

CONFIDENTIALITY



Confidentiality refers to the need for assurance that only those authorised to access information, whatever that information may be, can do so. Not all information is the same and needs to be protected as aggressively or accessed by the same set of people (data classification, principle of least privilege, etc will be discussed later on), so confidentiality should, at this stage, be simply understood as the need to ensure that information must be protected from being accessed by those who aren't authorised to access it.

Threats to confidentiality can include social engineering, attacks on encryption, steganography, key loggers and the IoT in general, where an ever-increasing number of connected devices constitute an ever expanding attack surface with backdoors to other systems.

Data can be mainly found in 3 "shapes": data at rest, data in use, and data in motion, where each is vulnerable in different manners and is likely to be subject to different types of attacks.

Whilst data at rest will normally rely on encryption (ie AES256) to be secured, and data in motion, in the use of security transport protocols (ie IPSec, TLS, SSL…), the security of data in use (for instance, a file that is open whilst a user is reading through its contents) will have to rely on controls which are less "technical" and of a more behavioural/physical nature, such as installing privacy screens, educating users to lock their computers when leaving their workstations, implementing clear desk policies, etc.

Other controls that will be used to protect confidentiality (amongst others) will be strong passwords, MFA, access control, the principle of least privilege, etc, which will be discussed in further detail later.

INTEGRITY

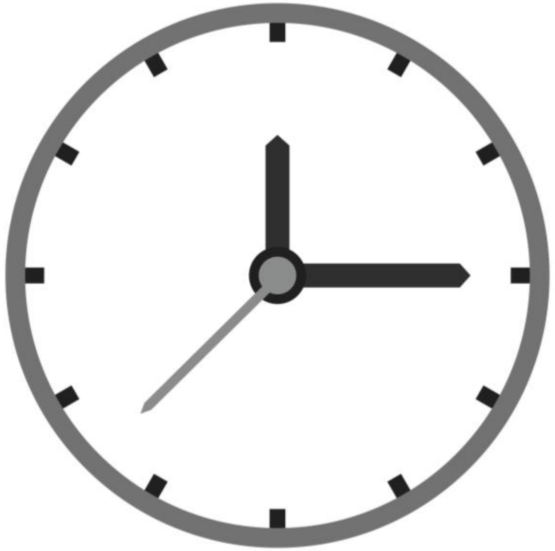
Integrity in information security is defined by the accuracy and completeness of the data, and has to do with the trustworthiness and correctness of the information as well as its source. For integrity to be assured, the assurance that data is not altered in transit, or altered by unauthorised people.

Common threats to integrity may include any changes to the data which render it inaccurate and incomplete, or changes made by unauthorised people. Code injections and cryptanalysis are also common threats to keep in mind.

There are two main types of protection for data integrity: preventative and detective. Preventative protection has to do with making sure that no one that is not supposed to change the data gets to do so and detective protection has to do with identifying situations in which the preventative measures have failed and unauthorised changes were made.

To protect integrity, we are likely to be looking at cryptography, hashing (message digests), checksums and digital signatures (which assure non-repudiation), as well as access control.

AVAILABILITY



Availability refers to making sure that the information (and systems or services) is promptly available for all users authorised to access it.

Attacks against availability are generally known as DoS (Denial of Service). These can be intentional (malicious, for instance, DDoS) or non intentional (natural disasters, broken equipment, application failure, human errors, etc) where, statistically speaking, most events resulting in DoS derive not from malicious attacks but by preventable human error.

To make an environment less prone to malicious exploitability, we will normally perform regular patching and put in place IDS/IPS systems. Additionally, to be able to withstand failure when it does happen, we will rely on redundancy (hardware, networking, etc), high availability, fault tolerance, and also on 3rd parties and suppliers, where SLA definitions become very relevant.

In a scenario where availability is seriously compromised, good Business Continuity and Disaster Recovery plans (to be also discussed in greater detail later on) can be of a major help to keep the business running, minimising the damages and financial losses.

PART 2

ACCESS CONTROL

IDENTIFICATION, AUTHENTICATION, AUTHORISATION AND ACCOUNTABILITY

Information Security is protected by four main control mechanisms: Identification, Authentication, Authorisation and Accountability, where:

A) Identification is the first step in the sequence and it has some intrinsic properties such as its scope, locality and uniqueness. In terms of scope, identification name spaces can be local or global – whatever the situation is, two user accounts should never have the same ID in the same system as this would compromise the ability to enforce ID-based access control and it would become impossible to establish accountability for user actions.

B) Authentication happens as a means to verify the authenticity of the identity declared during Identification. It is at this stage that the person or system needs to prove that they are indeed who they claim to be. We can think of three main ways to authenticate something or someone, which should always be used in combinations of at least two (MFA, multi-factor authentication):

What we know (type 1): covers authentication methods such as passwords, PINs, passcodes, etc. When performing this type of authentication, it is assumed that only the person/system X knows the password Y or passcode Z. This method is widely used as it is relatively cheap when compared to other more secure authentication strategies.

What we have (type 2): covers keys, tokens, smartcards, etc. When performing this type of authentication, the individual is presumed to be in possession of an identifying object that only that individual should have. This method is also not perfectly secure given the obvious reasons (keys get lost, tokens get stolen, etc) besides that it involves a cost superior to that in “what we know” authentication due to the need to purchase per-user hardware.

What we are (type 3): covers authentication through biometric data, including fingerprints, iris, retina and voice recognition, etc. This method is far more complex than the previous two. It also involves much superior costs both in terms of deployment and maintenance but, specially if well managed and used in conjunction with the previous two methods, it can be extremely secure.

IDENTIFICATION, AUTHENTICATION, AUTHORISATION AND ACCOUNTABILITY

C) Authorisation defines what we are able to access and is normally used in conjunction with a number of different access control models depending on the specific circumstances.

D) Accountability is sometimes referred to as auditing and as mentioned previously, it is closely related to the concept of non-repudiation, as it refers to the possibility of tracking actions and events back in time to their origin, establishing responsibilities for actions and/or omissions. Accountability is one of the main principles of Information Security so, general terms, systems that provide no Accountability are not to be considered secure.

Logs and Audit Trails are the main means for providing Accountability in the context of Information Security. Per definition, Logs are ordered lists of actions and events and, although similar to Audit Trails, they are considered to be more “high level”, whilst Audit Trails are more “low level” and “detailed”. Both Logs and Audit Trails are only considered Trusworthy if their Integrity is assure and if they are correctly timestamped.

ACCESS CONTROL

Authorisation (and, therefore, very importantly but not exclusively, confidentiality) is done through the implementation of access controls.

Subject and object:

Because we often refer to them as such, it's important to understand the difference between a subject and an object, where:

- A subject will always be something or someone (active) which manipulated an object (passive). Subjects will most often be people, but they can also be software.

- An object is something (passive) which is manipulated by a subject (active). Objects will normally refer to data (in either soft or hard format), but they can also be pieces of software.

Access control categories

There are three main access control categories:

Administrative controls

Also referred to as directive controls consist of everything that relates to corporate policies and procedures, laws and regulations, staff training and awareness, and other non-technical and non-physical controls in place to assure security.

Technical controls

These are, as the name indicates, all of a technical nature that will enforce information security. These can range from firewalls to encryption, to software - literally anything technical from an IT perspective.

Physical controls

These are everything that is in place to prevent physical access to facilities. Locks, gates, fences, etc are all physical controls.

ACCESS CONTROL

Access Control Types

In additional to categories, controls are also divided by types, where the same asset should always be secured by more than one of these, as we'll discuss further on when exploring defense in depth.

Like the different control categories, the different control types also have names which are quite self-explanatory:

1. Deterrent controls

They are similar to preventative controls (which will be seen next), although we tend to them as of a "less technical" nature than preventative controls. They basically try to discourage individuals from trying to cause a security breach.

A "beware of the dog" sign, for instance, is a deterrent control: it won't stop an intruder from breaking in, but it tries to discourage them from trying to do so.

2. Preventative controls

Are used to attempt to stop the breach from happening. Unlike deterrent controls which attempt to dissuade an individual from committing a breach, these controls are aimed to prevent a breach that is about to take place with no concern for the individual's possible change of hearts.

From good hiring practices (to be discussed later) to the commissioning of security appliances and implementation of encryption (amongst many others), these are controls put in place to prevent security breaches.

3. Detective controls

These are controls that assure that, if a security breach happens, it is identified. They neither prevent a breach from happening nor take any sort of action other than identifying and normally raising the alarm when it does.

From IDS appliances to all sorts of alarms that may be raised by whatever system whenever a condition that is identified as posing a security threat is met, these are all detective controls.

ACCESS CONTROL

Access Control Types (continued)

In additional to categories, controls are also divided by types, where the same asset should always be secured by more than one of these, as we'll discuss further on when exploring defense in depth.

Like the different control categories, the different control types also have names which are quite self-explanatory:

4. Corrective Controls

These are controls which allow for an effective response to a security breach with proper halting of the breach progress and damage correction.

IPS appliances (notice the "P" for protection vs the "D" for detection in IDS, although appliances that do one also tend to do the other if so configured), anti malware software, etc, they are corrective controls as their purpose is the correction of breach which is already taking place.

5. Recovery controls

They are, as the name indicates, controls which are implemented in order to allow us to effectively and efficiently recover from a breach which has already taken place.

These are always used "after the fact". Data recovery software and backup tapes or, in the event of a major disaster, a full-blown DR plan using a different datacenter, these are recovery controls. DR and BCP will be discussed in much greater detail later on.

6. Compensating controls

These can be seen as "second best" controls. They are basically those which are put in place when other controls which are the first choice are impossible to implement (because they are too costly, too complex, etc).

They can literally be anything and overlap any of the above, so long as they are there to compensate for the lack of another more suitable control.

ACCESS CONTROL

Access Control Models

Access Control is one of the most important concepts to have in mind when it comes to information security as they enforce access to systems and information. Access Control Models are the abstract foundations the access control mechanisms are built upon. Access Control Models can be centralized or distributed, where:

- **Centralised Access Control** Models involve a single, central entity that is responsible for making the decisions when it comes to information access and sets of permissions.
- **Distributed (Decentralised) Access Control** Models are present when each region, branch of the business, etc is responsible for creating their own sets of access control rules.

Mandatory Access Control (MAC)

This model is far more restrictive than DAC as users are left with little or nothing to say with regards to what permissions are set for the information they own. Instead, system-wide security sets of rules and policies are put in place and often enforced by Operating Systems. These permissions are set by the systems' administrators in agreement with corporate policies.

MAC-based systems classify data (public, confidential, secret, top-secret, etc) and security clearance labels corresponding to the security classification of the data to decide which control restrictions to apply.

Discretionary Access Control (DAC)

In this model, the owner of the information can decide the set of permissions to grant or deny and who should be granted or denied those permissions.

Although this model allows for extreme flexibility, it is also not the safest model as too much can be allowed too easily and this can lead to malicious or accidental security breaches.

Role-Based Access Control (RBAC)

In this model, the sets of rights and permissions are assigned per role and not per user, making it more flexible in terms of administration, easier to manage than MAC and more secure than DAC.

PART 3

SECURITY GOVERNANCE PRINCIPLES

SECURITY GOVERNANCE PRINCIPLES

Corporate Governance - an overview

In this section, we will briefly explore some security governance principles which we're hopefully familiar with in the sense that these should be in place/had into account in our work environments.

Here, it is important to notice the difference between governance and management, where:

- **Governance** is an expression of the business needs as defined by its stakeholders and/or owners. It sits at a very strategic level close to the very top of the business organigramme and, driven by risk appetite, it defines the business objectives, defines priorities and sets directions, and monitors for performance and compliance against the direction and objectives defined.

- **Governance** in the shape of strategic planning will have long-ish lifecycles that will normally has the duration of several years, the most common being 3 to 5.

- **Management** defines how we get from where we are to the objectives set in terms of governance, and in alignment with the direction defined. Management is, in this sense, more 'practical' than governance; it sets out to plan, build run and monitor systems/services/activities aligned with business objectives, and defines what, in practical terms, is the level of risk acceptable to meet the business' risk appetite (risk tolerance).

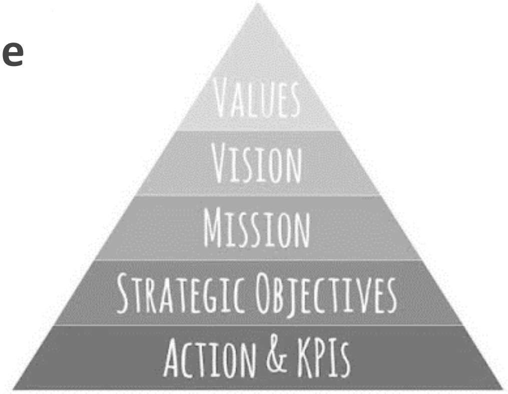
- **Management** takes, therefore, a shape of tactical planning aligned with the strategic plan (governance), with shorter lifecycles that that be from meeting annual targets to completing a certain project in whatever time it takes to complete it, to the process of hiring certain staff, etc.

In sum, these are tactical blocks of action that, put together, aim to meet the business strategy and, at a functional hierarchical level, sit right under governance and right above staff/operations, at which level the management tactics will be implemented, executed and updated at a very granular, operational level.

SECURITY GOVERNANCE PRINCIPLES

Corporate Governance

Normally, in an enterprise context, governance in general (not restricted to information security) can be visualised as:



Where:

Values describe the enterprise's ethics, core principle and beliefs.

Vision defines what the enterprise wants to become, its ambition.

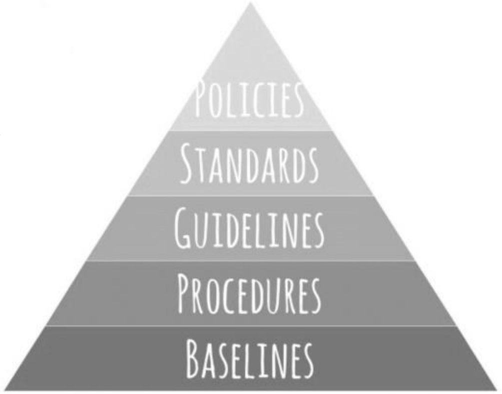
Mission describes why the enterprise does what it does and aspires to be what it aspires to be, so it's all about purpose and motivation.

Strategic objectives give guidelines on how to progress in alignment with the corporate values, vision and mission, setting plans, goals, etc.

Action and KPIs reflect the strategic objectives at a more granular and 'practical' level, describing not only how to act in order to meet the strategic objectives, but also how to know that targets have been met. It will include from actions and resources to owners, timeframes and the actual outcomes.

InfoSec Governance

A corporate information security governance model will normally be composed of policies, standards, guidelines (non-mandatory, albeit recommendable), procedures and baselines, which will have the following hierarchy:



Where:

Policies will be very high-level and non-specific - for instance, they can contain "patching must be done" and "strong encryption" but they'll never say what exactly needs patching or what encryption will be used.

Standards will describe the technology at a more granular level, but what they will do is will be defining what the technology will look like from a more specific but not procedural perspective. Standards may say things like "all laptops should use this OS and should have full disk encryption", for instance.

Guidelines, which are not mandatory, will provide suggestions and/or recommendations on how to apply the standards defined.

Procedures will provide the step-by-step, how-to, very granular low level description of how the standards are implemented, ie "all laptops should be this make/model, purchased from this vendor, have Windows 10 installed have full disk encryption with BitLocker".

Baselines will define the minimum requirements - anything below the baseline will be considered non-acceptable. They will often be used for hardening purposes in the context of information security (ie CIS baselines for server hardening).

SECURITY GOVERNANCE PRINCIPLES

People

It is widely said that, in information security, people are always out weakest link. As a matter of fact, most security breaches don’t derive from outside attacks, but rather from insiders’ activity instead. This activity isn’t necessarily malicious and is often the result of lack of knowledge or lack of care.

Users can be internal employees, but they can also be external, contractors, outsourced staff, 3rd party (vendors, suppliers), etc, all of whom may pose an intentional or unintentional security threat. To mitigate the threat inherently posed by staff, a number of measures can be taken, as described below.

Personnel security, like much in terms of information security, is an iterative process which accompanies staff through their entire employment lifecycle.

1. Hiring practices

Hiring staff should be done in close proximity between HR and the information security teams. Although the hiring is likely to be done between HR and the new staff’s line management, hiring practices should always take place in alignement with the information security policies, standards and guidelines in place.

When hiring staff (or on-boarding external people), background checks should always be performed - how aggressive these checks are will depend on the nature of the business and the level of threat the staff being hired may pose.

Signing NDAs (non-disclosure agreements) is also common practice as they legally bind the user to not share information concerning the enterprise and, possibly, its partners and clients, during and (ideally) after their employment.

2. Sensibilisation, awareness and training

Users should always be made aware of the threats posed by some of their behaviours, and educated/encouraged to change them. Bad user behaviours can often derive from lack of knowledge of that behaviour’s possible consequences so, if a user is able to understand why the behaviour is unacceptable, they will be more likely to change it.

Information security training should be regularly provided and knowledge acquisition verified. Ideally, this should be done prior to allowing the user into the corporate network, and information security sensibilisation campaigns in a simplified, user-friendly shape should take place. Useful information can be made available in an informal manner in office cafeterias and other common areas where staff hang out.

SECURITY GOVERNANCE PRINCIPLES

People (Continued)

3. Termination practices

Like hiring, terminating staff employment should be done with information security in mind.

Good termination practices should include termination of employment interviews where staff are reminded of what is expected from them (how they are contractually obliged to behave) in terms of the company assets (including data), as well as giving them the opportunity to have a say so the enterprise has some insight concerning their state of mind.

In terms of user accounts and access, permissions should be removed at the right time, which is when the employee leaves - not before the termination of their employment (except for specific situations where, for instance, an employee is put into ‘garden leave’ post gross negligence, etc), and not days or weeks after the termination of their employment either.

4. External resources

Many businesses will regularly rely on external human resources such as vendors and contractors who will be granted access to their premises and their systems. These resources should be provided with information security training too, and their systems need to be compatible with our security standards and policies - that is, contractually, any third party dealing with our data and accessing our premises must be secure enough as to not pose a direct or indirect security threat to us.

The same is valid for outsourcing and offshore staff which, albeit often reducing costs, can bring on the additional challenge of having staff and data which, depending on where they are geographically located, are likely to subject to different laws and different data protection standards and regulations.

PART 4
LEGAL CONCEPTS

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Introduction

The way we handle information is, in every case, subject to laws and regulations. This is not a choice and, although the laws and regulations may change depending on geo-political and contractual contexts, there will always be something well above us that will dictate what we can, cannot, must and must not do when it comes to information security.

Given that this subject is far too vast to shrunk into a few slides on a presentation, we will approach it at a high level similar to how it would be approached during CISSP training. Although this section is obviously not exhaustive (it would be rather hard to write down all laws and regulations everyone will be subjected to, all over the world), it provide an overview of the minimum knowledge IT professionals touching information security should have.

A deeper dive into information security governance standards and control frameworks (of which there are very many) will be done separately, outside the scope of this document.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Concepts

1. Criminal Law

Criminal law is that which applies to crimes in which society itself is the victim and, for a conviction to be issued, proof must be beyond reasonable doubt. Without wanting to sound overly dramatic, depending on where we are (and, therefore, the law applicable to us), penalties in this context can go from fines all the way to the death penalty, depending, obviously, on how much damaged is deemed as having been caused to the society.

2. Civil Law

Civil law applies to crimes where individuals or groups/organisations (so, not the whole society, just a limited subset of individuals/entities) are the victims. Here, a guilty verdict does not require proof beyond reasonable doubt and the concept of the “majority of proof” applies. In this case, penalties will normally be fines.

3. Administrative Law (regulatory law)

Administrative laws (aka regulatory laws) are those issued by specific government agencies. Again, for the CISSP, a bit of knowledge concerning administrative law in the USA is required, so here we must think about HIPAA, FDA and FAA laws, etc.

4. Private Regulations

Private regulations (such as PCI-DSS, ISO, etc.) are not law, but as there may be a contractual obligation to comply with them, failure to do so may result in lawsuits too.

5. Customary and Religious Law

Depending on where we are, we may also be subjected to customary law (related to behaviour patterns which may or may not match the customs and traditions of the region), as well as religious law, which is self-explanatory.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Concepts (continued)

Liability, Due Diligence and Due Care

Liability, in practical terms, is the definition of who is responsible and/or accountable, and "takes the blame" for something which has happened and, when the question of who is ultimately liable for something is posed within a corporate context, the answer will be senior leadership.

Albeit senior leadership being ultimately liable, this does not mean others down the corporate hierarchy won't be liable too. The liability of others will be directly linked to their performance in the way of "due care". As a hint: follow the corporate policies, as described next.

Due diligence is related to research, that is, in information security terms, everything that must be done prior to implementing a system/service. This will include from the knowledge of the tech in conceptual terms, to the knowledge of the real context at a specific enterprise level, and the interaction between the two.

Due care has to do with how people act after research is completed, so it covers from the design and implementation of the system/service, all the way to running it on a daily basis, including keeping it alive and healthy, taking remediating action when something goes wrong, and communication with users/consumers and stakeholders.

When due care is the subject, corporate security policies will be of extreme importance as following them, even if the outcome is not good, will define the liability of the individual who followed them (or not, in which case their liability is likely) - in plain terms, follow the corporate rules by the book, if you do as written and something goes wrong, you're far less likely to take the blame.

Negligence

Negligence is the opposite of due care, that is, when an incident happens affecting a system/service under our control, where due care hasn't been performed, that classifies as negligence (or gross negligence, more serious even), and makes us liable for it.

On the other hand, should an accident happen affecting the same system where it is shown that our due care has been performed (we have followed the corporate rules by the book), despite the incident taking place, it won't classify as negligence and, therefore, we won't be liable.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Concepts (continued)

Evidence

At the end of the day, whether or not an information-security crime (or any other sort thereof) has been committed, will depend on the evidence available to prove it. Handling evidence is a huge subject in the domain of computer forensics but here we'll just have a quick look at some of what makes up the concept of "evidence".

Types of Evidence

1. Real evidence will always refer to tangible, physical objects, for instance, a USB stick or HDD are real evidence, but the data they may contain is not.

2. Direct evidence is first hand witness testimony and will always involve an individual describing something they experienced themselves (saw something, heard something, smelled something - something they experienced with their own senses).

3. Circumstantial evidence is evidence which is not direct but might lead a jury to believe a particular fact or set of facts. It basically relies on what circumstances lead us to believe happened rather than what we can directly prove with hard evidence.

The classical example of circumstantial evidence is all evidence that is presented in court in a no-body murder case: all evidence collected, when contextualised, will point in the direction that the person is dead, and has been killed in a certain manner, even though there is no body to match it against.

4. Corroborating evidence is any evidenced that supports other evidence, reinforcing it and proving its veracity/accuracy. Corroborative evidence does not attempt to prove the fact, but rather supports other evidence which, in turn, attempts to do so.

For instance: if we are trying to prove that John has stolen object X, and Mary is providing direct evidence by saying she saw him stealing it, CCTV footage showing both Mary and John at the alleged spot where the theft took place will be corroborative evidence, and it reinforces the likely veracity of Mary's testimony.

5. Hearsay is normally not admissible in court as it's not first-hand knowledge and it's just as the name indicates: hearsay. The fact that computer-generated records (ie log files) might or might not be considered hearsay depending on where we are and the legal framework applicable to us.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Concepts (continued)

Evidence Quality

Best Evidence Rule refers to how courts will always prefer the best evidence which can possibly be presented, which should always be “accurate, complete, relevant, authentic and convincing”.

Secondary evidence is normally how IT-related evidence will be referred to. Any computer-generated files, logs, etc will be considered secondary evidence.

Evidence integrity is mandatory and its name is self-explanatory. In computer forensics, evidence integrity will be assured, for instance, through hashing: all forensics are done using the copies of the original, unchanged evidence, and hash checks are performed before and after the forensic activity is concluded.

Chain of Custody must be carefully controlled as to assure the integrity of the data being provided as evidence. Loss of control over the chain of custody and make evidence non-admissible as it may result in data tampering which will put in question its authenticity. We ensure the chain of custody is maintained through full control, visibility and recording of:

- **Who** handled the data
- **Where** did they handle it
- **When** did they so
- **What** did they do with the data

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – LEGAL CONCEPTS

Reasonable Searches

We are likely to work under a legal framework in which there is a certain level of legally granted respect for individual privacy, so finding information will have to be done according to certain rules. However, increasingly, whilst some rules are there to protect individual privacy, others are there to protect national security, in which case individual privacy may end up being compromised. The point being that everything will depend on the specific circumstances and understanding the context will be key.

Just as a random example, for instance, in the USA, the Fourth Amendment of the Constitution protects citizens from unreasonable government searches and seizure of possessions. Simultaneously, the Patriot Act of 2001 largely expands law enforcement snooping capabilities and allows for search and seizure without immediate disclosure.

Entrapment and Enticement

Entrapment refers to when an individual is persuaded into committing a crime they had no intention to commit and end up being charged with. It is both illegal and unethical.

Enticement refers to when the commission of a crime, which someone has already decided to commit, is made more appealing/enticing. Here the individual is not persuaded to commit a crime, they made that decision already, all that's being done is making the commission of that crime more interesting - and example of enticement being honeypots - this is both legal and ethical.

PART 5
MUST KNOW’S

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – MUST KNOW'S

Depending on our industry and location, some of these may be more or less relevant, or even not relevant at all. It is, however, a good idea to know at least what they refer to:

GDPR: the EU's General Data Protection Regulation is part of the EU law and focus on data protection and privacy for all individuals within the EU and EEA. It protects the privacy of EU and EEA-based people, regardless of the location of the provider whose services they are using. We will go deeper into GDPR later on. To find out more about GDPR, please follow the link: https://gdpr-info.eu.

PCI-DSS: born in the USA, the Payment Card Industry Data Security Standard is widely used around the world and was created by the payment card industry. It applies to debit and credit cardholders' data and enforces the need for those handling such data to meet certain security requirements, with security policies, control techniques, monitoring, etc. More about PCI-DSS can be found in this quick reference guide: https://www.usf.edu/business-finance/controller/documents/pcisscquickguide.pdf.

HIPAA: the American Health Insurance Portability and Accountability Act, providing strict privacy and security rules for the handling of Protected Health Information. If you want to read more about it, a summary can be found here: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

ECPA: the American Electronic Communications Privacy Act, providing protection for data privacy, against warrantless wiretapping - this has, however, been significantly weakened by the Patriot Act. For more about the ECPA, here's some quick-reading: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

Patriot Act of 2001: provides authorities with extended electronic monitoring capabilities, allowing for search and seizure without immediate disclosure. For the USA Patriot Act, here's some quick reading too: https://www.justice.gov/archive/ll/highlights.htm.

CFAA: the Computer Fraud and Abuse Act Title 18 Section 1030 is the most commonly used law for the prosecution of computer crimes. Here is some quick information on the CFAA: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – MUST KNOW'S

GLBA: the Gramm-Leach-Bliley Act is applicable to financial institutions. To learn more, check https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

SOX: the Sarbanes-Oxley Act of 2002 is also finance-oriented and came as a response to the numerous accounting scandals in the USA during the late 90s. To read more about SOX, please follow the link: https://www.soxlaw.com.

OECD Privacy Guidelines: 30 member-nations agree on these guidelines for the "protection of privacy and transborder flow of personal data", with eight driving principles:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

A document with the OECD privacy framework can be found here: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Wassenaar Agreement (Arrangement): the Wassenaar Agreement, signed by 41 countries, sets import/export controls for "conventional arms and dual-use goods and technologies". The agreement is very relevant when it comes to encryption, as this is considered to be dual-use tech. For more own the Wassenaar Arrangement, please check: https://www.wassenaar.org.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – MUST KNOW'S

ISO 27000 Series

One of the most widely implemented set of information security standards is the ISO 27000 series. This post will not cover it in great detail (although, personally, I would recommend anyone working in the IT industry, in security or not, to be comfortable with it), but here's an overview. Of the ISO 27000 series, at this stage, in the context of the CISSP, we must highlight:

ISO (IEC) 27001

This is the standard everyone will certainly be most familiar with, as it is provides a very widely used framework for the management of information security, which has the purpose of helping enterprises making their information-related assets, including physical ones, more secure. It provides guidelines on to implement, manage and continually improve information security, in an iterative, PACD (plan, do, check, act) fashion.

For being ISO 27001-certified, and enterprise will be required (and audited on it) to treat all aspects of information security in a certain way:

Systematic risk analysis is required, with the implementation of a risk management methodology which will ensure that risks (threats, vulnerabilities…) and their impact are systematically analysed, and that controls are in place to handle risks appropriately. Risk management will, however, be looking into in more depth later on.

The information security management and controls in place must cover the entire organisation and demonstrably be applied to the entire corporate structure, all the way down to individual employees, as the certification is aimed to look at information security in all its aspects and is nowhere near restricted to IT.

Again, in an iterative manner, ISO 27001 will rely upon and result in consistent, comprehensive, business-wide ISMS. Other ISO standards will be discussed later on, in the context of DR-BCP and Risk Management but, for now, we should be well aware of the following.

GOVERNANCE STANDARDS AND CONTROL FRAMEWORKS – MUST KNOW’S

ISO 27002

The ISO 27002 will provide practical, best-practice information on how to implement security controls, targeting those responsible for the corporate ISMS directly by providing them guidelines concerning how their job can be done in a proper manner, covering from Human Resources, to physical and environmental security, to access control.

ISO 27001 is advisory and extremely flexible, allowing for fully bespoke implementations that follow specific organisation needs.

ISO 27004

The ISO 27004 (fully named Information Technology - Information Security Management - Measurement) provides, as the name indicates, organisations with metrics that will allow them to evaluate how successful their ISMS is.

Like most within the ISO 27000 series, ISO 27004 is perfectly aligned with ISO 27001, helping organisations measuring how compliant their are with the ISO 27001 requirements.

ISO 27005

ISO 27005 relates to risk management, providing a standards-based approach to it. It will help enterprises implement information security from risk management perspective.

Within the context of ISO 27005, organisations will be guided on how to establish risk management, including assessing, addressing, monitoring and reviewing risks (iteratively, as usual), including also risk-related communication with the relevant parties.

ISO 27799

If you work or are thinking of working in/with healthcare/healthcare-related information, ISO 27799 (fully named will be especially important, as it provides directives on how to ensure the security of PHI (protected health information).

In the “personal confidentiality scale”, health information is at the top of the scale, or at least very close to it, and ISO 27799 will help organisations handling this sort of data, and implementing controls which will assure confidentiality, integrity and availability, as well as full auditing and traceability over the entire data lifecycle.

PART 6

FOCUS ON GDPR

FOCUS ON GDPR

As mentioned, GDPR is the EU's General Data Protection Regulation is part of the EU law and provides regulation for data protection and privacy for all individuals within the EU and EEA, also addressing the transfer of personal data to outside the EU ans EEA, providing individual control over their personal data.

In sum, GDPR consolidates and unifies personal data regulation within the EU, simplifying the regulatory environment for international business, whilst protecting individuals within the EU and EEA, forcing any vendors or suppliers to be compliant with it, regardless of where they are located, so long as they store/handle EU/EEA citizens' data.

GDPR violations can result in fines up to EUR 20 million or up to 4% of the violating enterprise's annual worldwide turnover of the preceding financial year, depending on what's greater.

Some GDPR concepts/definitions which must be kept in mind:

Restrictions to it do exist, such as when it comes to national security, lawful interception, justice system, military and policy.

Right to access is granted, so data controllers must provide individuals with a free copy of their data when they request it.

Data portability means that individuals can request their data in electronic format.

Right to erasure is also provided, where individuals have the "right to be forgotten", that is, a provider cannot keep your personal data if you don't wish them to.

Data breach notification assures that both users and data controllers must be notified within 72 hours of a breach occurring.

The EU's General Data Protection Regulation is part of the EU law and focus on data protection and privacy for all individuals within the EU and EEA. means that all data-related processes but be carefully designed to ensure the security of personal data, where business are required the assurance that they'll only collect, access/handle and keep data which is "absolutely necessary for the completion of duties".

Data protection officers must be appointed in any businesses of which the activity involves data processing and monitoring.