ISMS Notes by Barzani Jawi

Corporate Governance

It's the organization as whole, it directs and controls the organization so that we can achieve our objective. Corporate Governance is the system of rules, practices and processes by which a company is directed and controlled, with the objective of achieving the company's goals, objectives and mission in a responsible, transparent and accountable manner. This is typically done by the board of directors, management and the shareholders, to set the strategy, direction and decision making of the company, through a combination of rules, procedures and mechanisms to protect the rights of shareholders and other stakeholders, while maintaining accountability, transparency and ethical conduct.

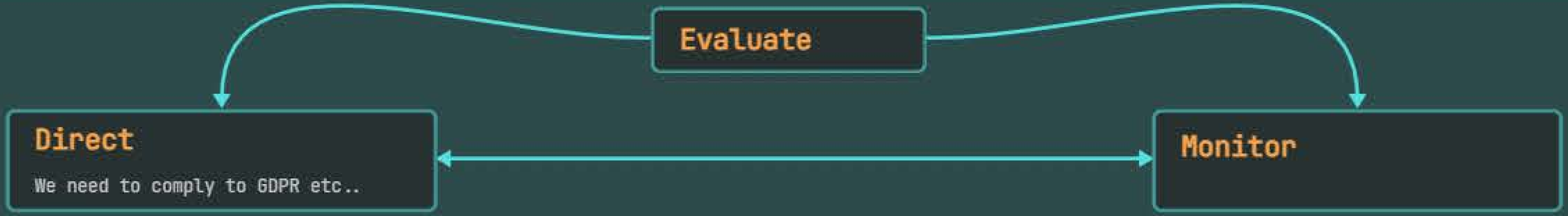
Corporate Governance of ICT

It is the why and what we need to do to achieve our goals. CFO Chief Information officer and chief Operations Officer. Example: We need to ensure that our stored credit card information is secure, because we need to comply to the GDPR, we say that's Why. What needs to happen? The credit card information needs to be secured (encrypted)

ICT Governance

It's how to achieve directives of Board. When we get to ICT governance, that's when we get to the how, how do we do that? Well, we implement encryption.

Corporate Governance and Corporate Governance of ICT



Management

Plan

Build

Run

Monitor

Information Security Governance

ICT Governance

States how to achieve goals. Implement policies, network. COBIT is the best practice guideline for ICTG. Depending on the viewpoint from which COBIT is introduced in a company, it may be used for different purposes:

1. ICT auditing viewpoint
2. Viewed as a broader

- ICT Governance tool used to determine the ‘completeness’ of a company’s ICTG approach.
- Used to determine if company is doing the ‘right things’ provides a Best Practice Framework against which a company can compare its own ICT management approach.
- Provides a Best Practice Framework against which a company can compare its own ICT management approach.

1. Viewed from a maturity angle

- Used to determine how well the company has advanced in its implementation, and how it is progressing maturity wise.

Information Security Governance

ISG consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensures that the confidentiality, integrity and availability (CIA). ISG is an integral part of Corporate Governance of ICT.
Objectives of ISG: ISO/IEC 27014

- Objective 1: Establish integrated comprehensive entity wide information security
- Objective 2: Make decisions using a risk based approach
- Objective 3: Set the direction of acquisition
- Objective 4: Ensure conformance with internal and external requirements
- Objective 5: Foster a security positive culture
- Objective 6: Ensure the security performance meets current and future requirements of the entity

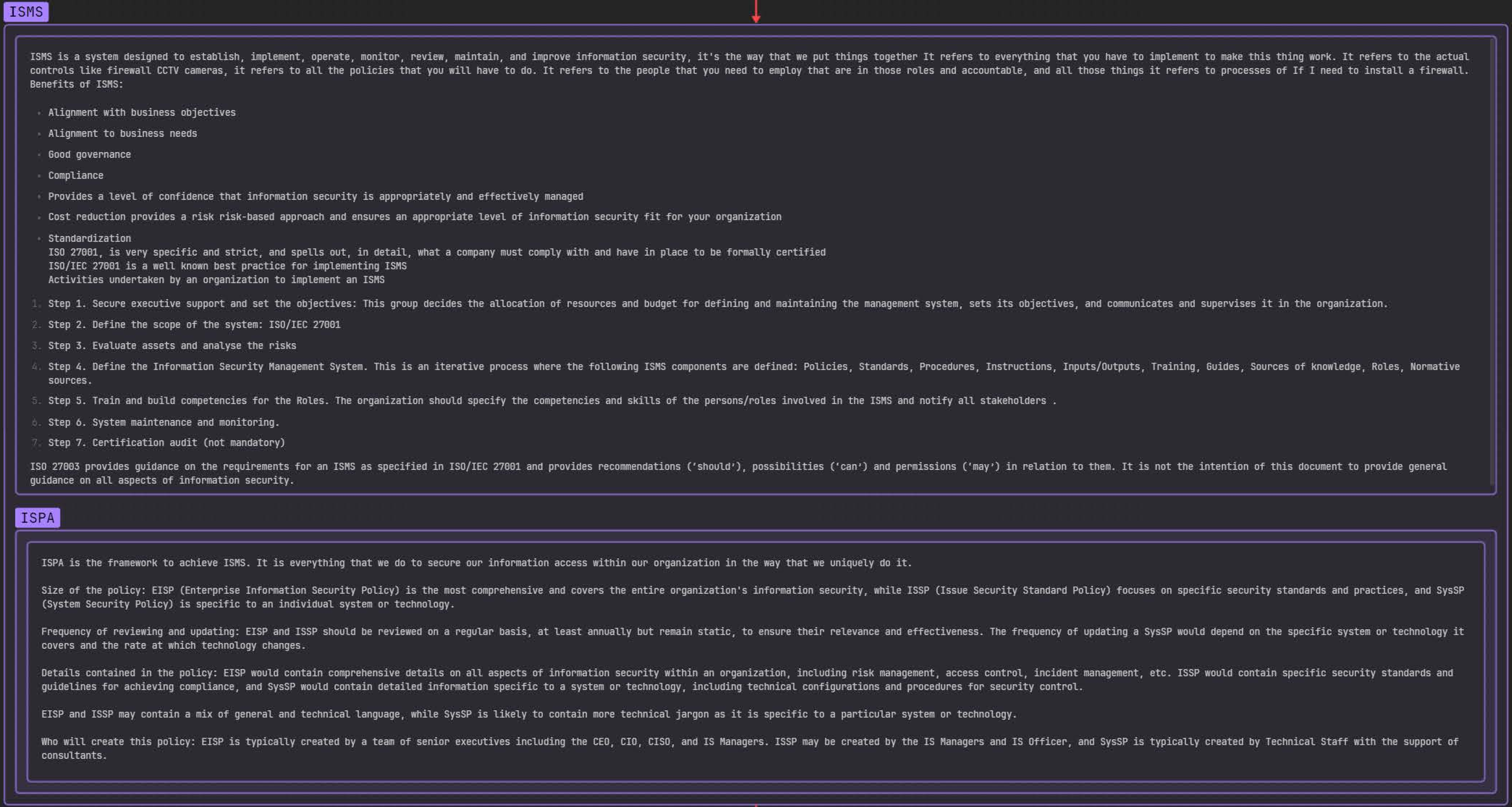
IS Managment System

Align, Plan and Organize (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)



ISMS

ISMS is a system designed to establish, implement, operate, monitor, review, maintain, and improve information security, it's the way that we put things together It refers to everything that you have to implement to make this thing work. It refers to the actual controls like firewall CCTV cameras, it refers to all the policies that you will have to do. It refers to the people that you need to employ that are in those roles and accountable, and all those things it refers to processes of If I need to install a firewall.
Benefits of ISMS:

- Alignment with business objectives
- Alignment to business needs
- Good governance
- Compliance
- Provides a level of confidence that information security is appropriately and effectively managed
- Cost reduction provides a risk risk-based approach and ensures an appropriate level of information security fit for your organization
- Standardization
  ISO 27001, is very specific and strict, and spells out, in detail, what a company must comply with and have in place to be formally certified
  ISO/IEC 27001 is a well known best practice for implementing ISMS
  Activities undertaken by an organization to implement an ISMS

1. Step 1. Secure executive support and set the objectives: This group decides the allocation of resources and budget for defining and maintaining the management system, sets its objectives, and communicates and supervises it in the organization.
2. Step 2. Define the scope of the system: ISO/IEC 27001
3. Step 3. Evaluate assets and analyse the risks
4. Step 4. Define the Information Security Management System. This is an iterative process where the following ISMS components are defined: Policies, Standards, Procedures, Instructions, Inputs/Outputs, Training, Guides, Sources of knowledge, Roles, Normative sources.
5. Step 5. Train and build competencies for the Roles. The organization should specify the competencies and skills of the persons/roles involved in the ISMS and notify all stakeholders .
6. Step 6. System maintenance and monitoring.
7. Step 7. Certification audit (not mandatory)

ISO 27003 provides guidance on the requirements for an ISMS as specified in ISO/IEC 27001 and provides recommendations (‘should’), possibilities (‘can’) and permissions (‘may’) in relation to them. It is not the intention of this document to provide general guidance on all aspects of information security.

ISPA

ISPA is the framework to achieve ISMS. It is everything that we do to secure our information access within our organization in the way that we uniquely do it.

Size of the policy: EISP (Enterprise Information Security Policy) is the most comprehensive and covers the entire organization's information security, while ISSP (Issue Security Standard Policy) focuses on specific security standards and practices, and SysSP (System Security Policy) is specific to an individual system or technology.

Frequency of reviewing and updating: EISP and ISSP should be reviewed on a regular basis, at least annually but remain static, to ensure their relevance and effectiveness. The frequency of updating a SysSP would depend on the specific system or technology it covers and the rate at which technology changes.

Details contained in the policy: EISP would contain comprehensive details on all aspects of information security within an organization, including risk management, access control, incident management, etc. ISSP would contain specific security standards and guidelines for achieving compliance, and SysSP would contain detailed information specific to a system or technology, including technical configurations and procedures for security control.

EISP and ISSP may contain a mix of general and technical language, while SysSP is likely to contain more technical jargon as it is specific to a particular system or technology.

Who will create this policy: EISP is typically created by a team of senior executives including the CEO, CIO, CISO, and IS Managers. ISSP may be created by the IS Managers and IS Officer, and SysSP is typically created by Technical Staff with the support of consultants.

Risk Management

The process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures , if any, to take in reducing the risk to an acceptable level , based on the value of the information resource to the organization. The purpose of risk management is to firstly identify risks and evaluate it.

International Standard: ISO/IEC 27005 Application of Risk

International Standard

Context Establishment

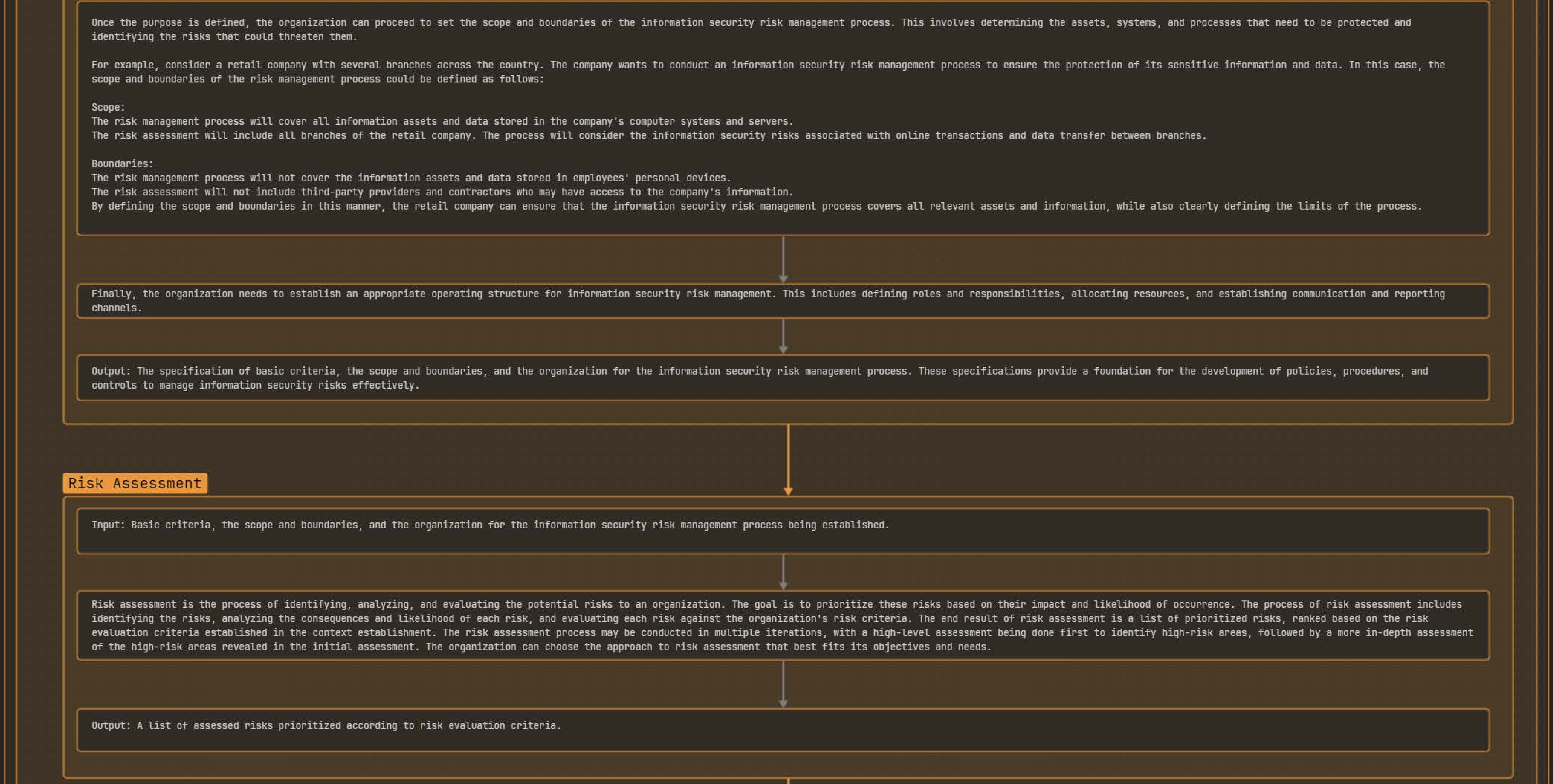
Context establishment in information security risk management refers to the process of defining and setting the basic criteria necessary for effective risk management. This involves identifying and understanding the external and internal factors that could affect the organization's information security, such as regulatory requirements, organizational goals, and stakeholder expectations.

To establish the context, the organization should determine the purpose of the information security risk management process. This purpose could be supporting an Information Security Management System (ISMS), ensuring legal compliance, preparing for business continuity, developing an incident response plan, or defining the security requirements for a product or service.

A small business is evaluating the risk associated with its customer data, which is stored in a database on a server in the company's office. The business considers the following:

Basic Criteria:
The strategic value of the business information process: Customer data is vital to the business's ability to generate revenue and maintain customer relationships.
The criticality of the information assets involved: Customer data is highly sensitive and personal, making it a critical asset for the business.
Legal and regulatory requirements: The business must comply with data privacy regulations, such as the General Data Protection Regulation (GDPR), which require the protection of personal data.
Operational and business importance of availability, confidentiality, and integrity: The business depends on the availability of the customer data to serve its customers and maintain its operations. Confidentiality and integrity of the data are also essential for maintaining customer trust and avoiding costly data breaches.
Stakeholders' expectations and perceptions: The business's customers expect their data to be protected and secure. A breach of customer data could harm the business's reputation and result in a loss of customers.

Impact Criteria:
Level of classification of the impacted information asset: Customer data is considered to be confidential and restricted.
Breaches of information security: A breach of customer data could result in the loss of confidentiality, integrity, and availability of the data.
Impairment of operations: A breach of customer data could result in the loss of customers and a reduction in revenue.
Loss of business and financial value: The business could suffer a financial loss as a result of a data breach, including the cost of investigating and remedying the breach and potential legal costs.
Disruption of plans and deadlines: A data breach could disrupt the business's operations and plans, potentially delaying important projects and initiatives.
Damage of reputation: A data breach could harm the business's reputation and result in a loss of customer trust and loyalty.
Breaches of legal, regulatory, or contractual requirements: A data breach could result in legal and regulatory penalties and a violation of the business's contractual obligations with its customers.
Based on these criteria, the business could determine that the risk associated with its customer data is high and that it needs to take steps to mitigate this risk, such as implementing stronger security measures, regularly backing up the data, and conducting regular security audits.



Once the purpose is defined, the organization can proceed to set the scope and boundaries of the information security risk management process. This involves determining the assets, systems, and processes that need to be protected and identifying the risks that could threaten them.

For example, consider a retail company with several branches across the country. The company wants to conduct an information security risk management process to ensure the protection of its sensitive information and data. In this case, the scope and boundaries of the risk management process could be defined as follows:

Scope:
The risk management process will cover all information assets and data stored in the company's computer systems and servers.
The risk assessment will include all branches of the retail company. The process will consider the information security risks associated with online transactions and data transfer between branches.

Boundaries:
The risk management process will not cover the information assets and data stored in employees' personal devices.
The risk assessment will not include third-party providers and contractors who may have access to the company's information.
By defining the scope and boundaries in this manner, the retail company can ensure that the information security risk management process covers all relevant assets and information, while also clearly defining the limits of the process.

Finally, the organization needs to establish an appropriate operating structure for information security risk management. This includes defining roles and responsibilities, allocating resources, and establishing communication and reporting channels.

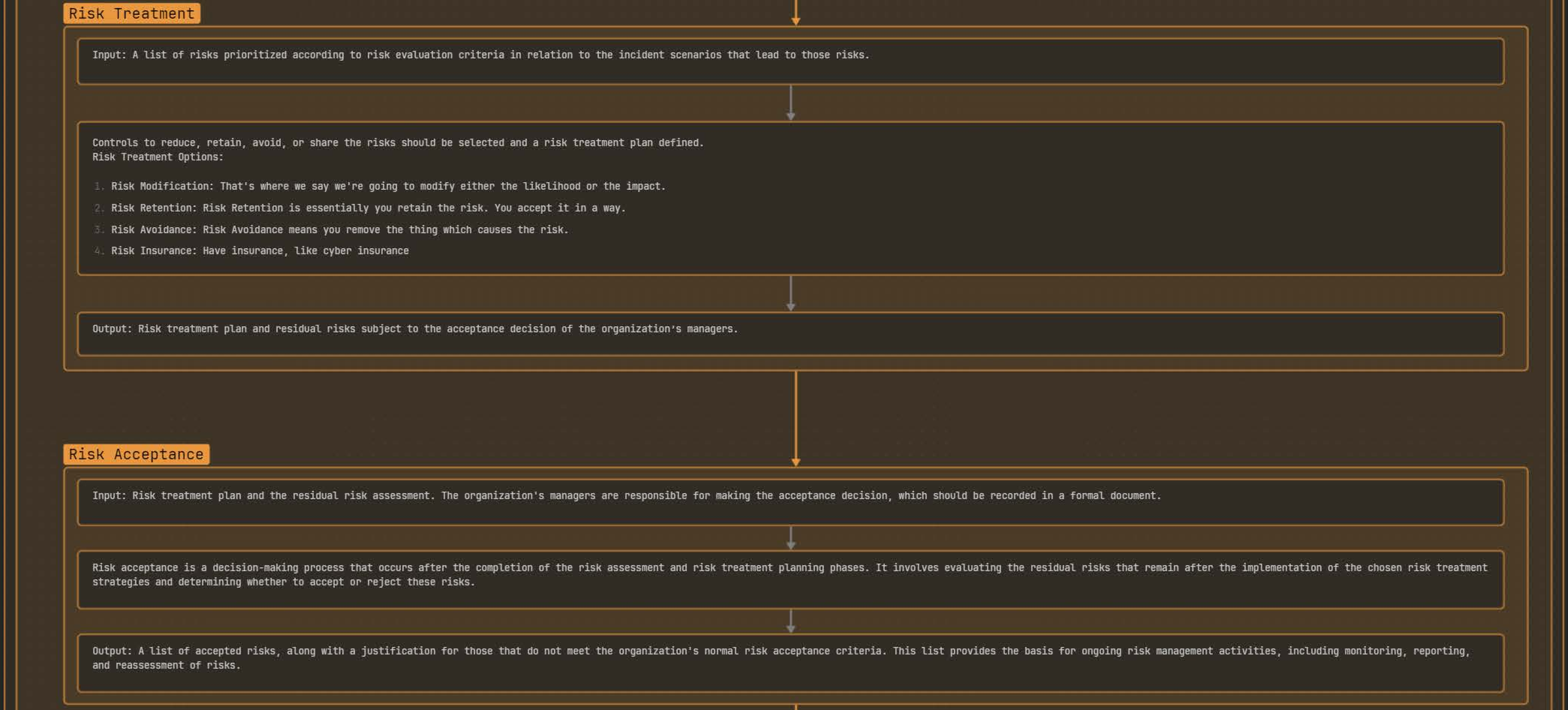
Output: The specification of basic criteria, the scope and boundaries, and the organization for the information security risk management process. These specifications provide a foundation for the development of policies, procedures, and controls to manage information security risks effectively.

Risk Assessment

Input: Basic criteria, the scope and boundaries, and the organization for the information security risk management process being established.

Risk assessment is the process of identifying, analyzing, and evaluating the potential risks to an organization. The goal is to prioritize these risks based on their impact and likelihood of occurrence. The process of risk assessment includes identifying the risks, analyzing the consequences and likelihood of each risk, and evaluating each risk against the organization's risk criteria. The end result of risk assessment is a list of prioritized risks, ranked based on the risk evaluation criteria established in the context establishment. The risk assessment process may be conducted in multiple iterations, with a high-level assessment being done first to identify high-risk areas, followed by a more in-depth assessment of the high-risk areas revealed in the initial assessment. The organization can choose the approach to risk assessment that best fits its objectives and needs.

Output: A list of assessed risks prioritized according to risk evaluation criteria.



Risk Treatment

Input: A list of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks.

Controls to reduce, retain, avoid, or share the risks should be selected and a risk treatment plan defined.
Risk Treatment Options:

1. Risk Modification: That's where we say we're going to modify either the likelihood or the impact.
2. Risk Retention: Risk Retention is essentially you retain the risk. You accept it in a way.
3. Risk Avoidance: Risk Avoidance means you remove the thing which causes the risk.
4. Risk Insurance: Have insurance, like cyber insurance

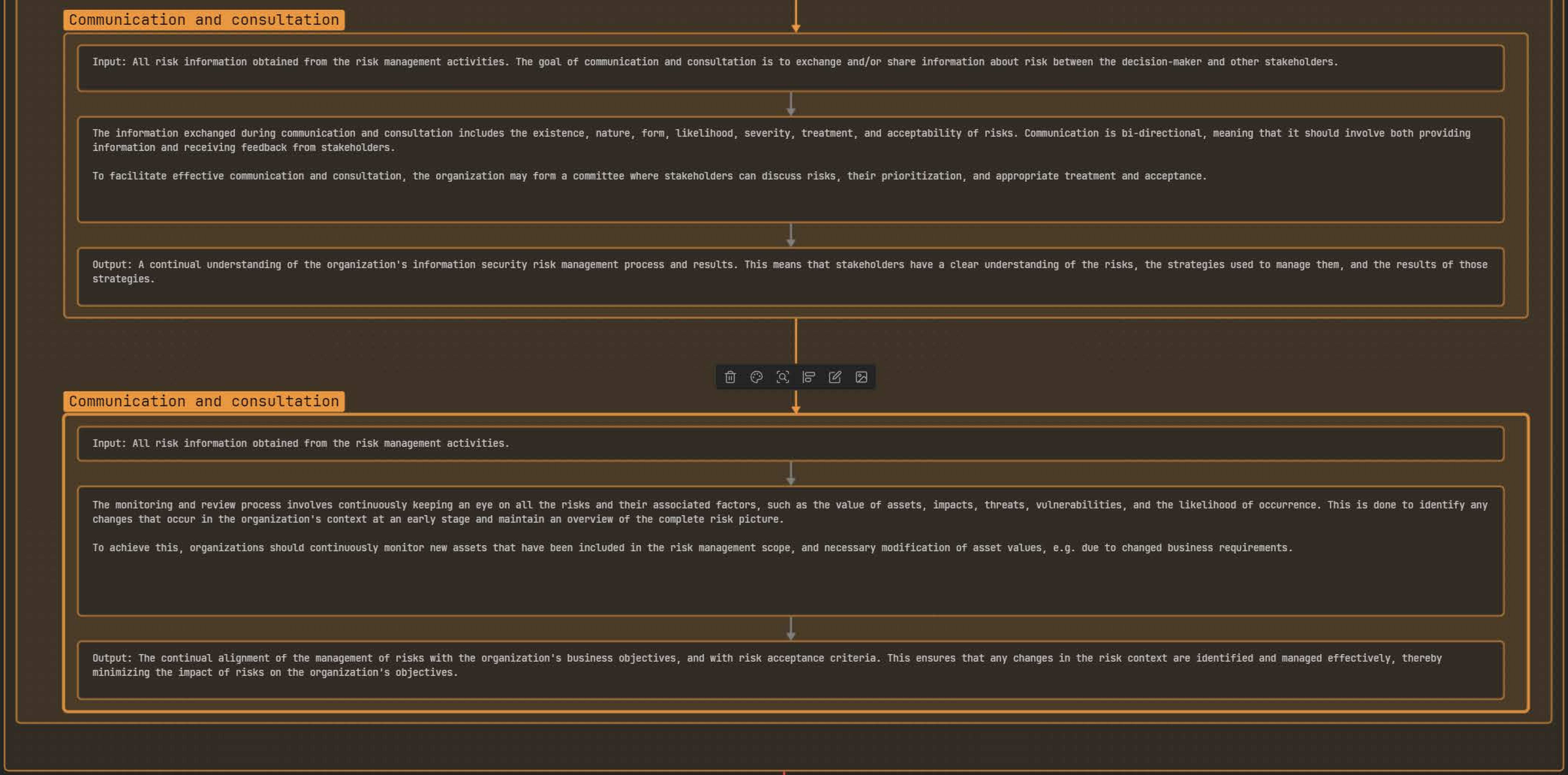
Output: Risk treatment plan and residual risks subject to the acceptance decision of the organization's managers.

Risk Acceptance

Input: Risk treatment plan and the residual risk assessment. The organization's managers are responsible for making the acceptance decision, which should be recorded in a formal document.

Risk acceptance is a decision-making process that occurs after the completion of the risk assessment and risk treatment planning phases. It involves evaluating the residual risks that remain after the implementation of the chosen risk treatment strategies and determining whether to accept or reject these risks.

Output: A list of accepted risks, along with a justification for those that do not meet the organization's normal risk acceptance criteria. This list provides the basis for ongoing risk management activities, including monitoring, reporting, and reassessment of risks.



Communication and consultation

Input: All risk information obtained from the risk management activities. The goal of communication and consultation is to exchange and/or share information about risk between the decision-maker and other stakeholders.

The information exchanged during communication and consultation includes the existence, nature, form, likelihood, severity, treatment, and acceptability of risks. Communication is bi-directional, meaning that it should involve both providing information and receiving feedback from stakeholders.

To facilitate effective communication and consultation, the organization may form a committee where stakeholders can discuss risks, their prioritization, and appropriate treatment and acceptance.

Output: A continual understanding of the organization's information security risk management process and results. This means that stakeholders have a clear understanding of the risks, the strategies used to manage them, and the results of those strategies.

Communication and consultation

Input: All risk information obtained from the risk management activities.

The monitoring and review process involves continuously keeping an eye on all the risks and their associated factors, such as the value of assets, impacts, threats, vulnerabilities, and the likelihood of occurrence. This is done to identify any changes that occur in the organization's context at an early stage and maintain an overview of the complete risk picture.

To achieve this, organizations should continuously monitor new assets that have been included in the risk management scope, and necessary modification of asset values, e.g. due to changed business requirements.

Output: The continual alignment of the management of risks with the organization's business objectives, and with risk acceptance criteria. This ensures that any changes in the risk context are identified and managed effectively, thereby minimizing the impact of risks on the organization's objectives.

Risk Assessment

Assessment approach talks about the idea that we have to go through certain steps, you have to identify your assets, risk identification, go down into the next block, which is risk and analysis going down, respond, etc.
It is important to consider the likelihood and impact to determine the risk level then we can respond. Identifying the risk. then analyzing it then evaluating that these are 3 core steps in risk assessment.

Risk Identification: Determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen.
The following should be identified:
Assets - Threats - Existing Controls - Vulnerabilities - Consequences

Risk Identification

Identification of Assets

An asset is anything that has value to the organization, and which therefore requires protection.

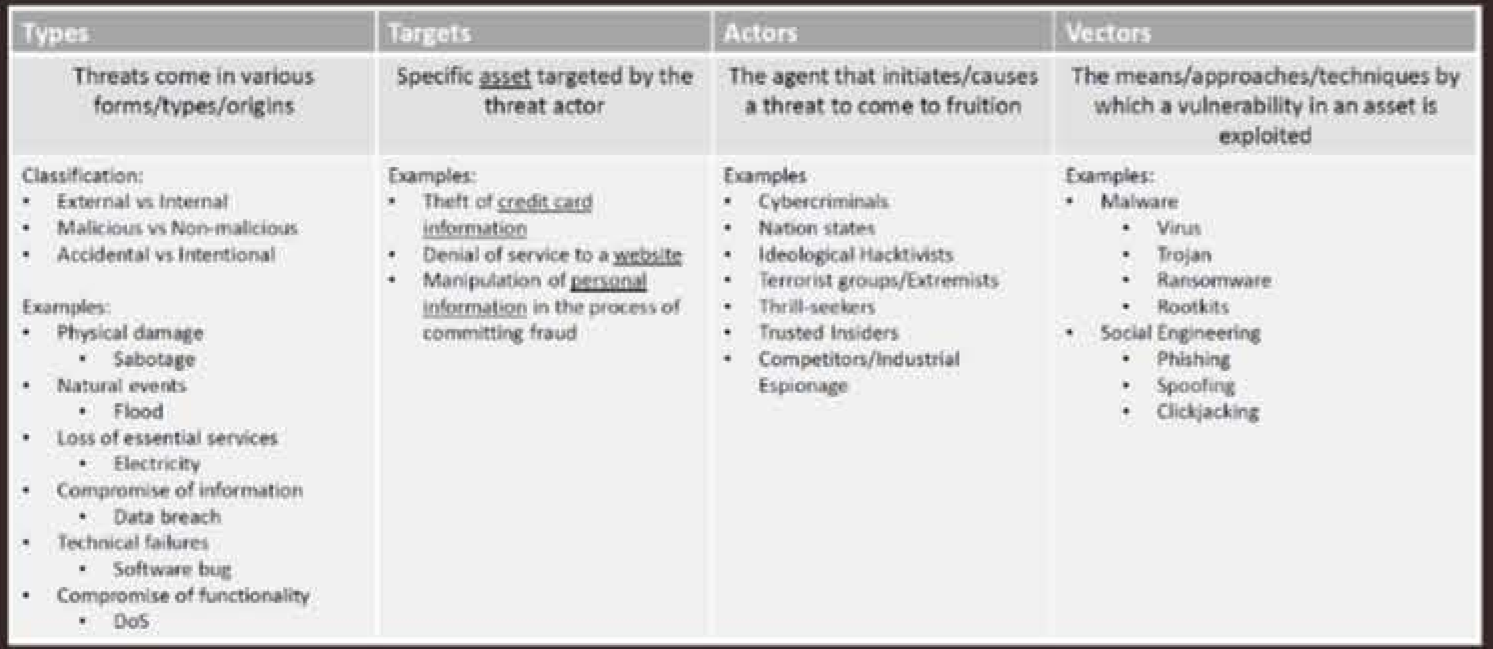
1. Asset identification is done at a suitable level of detail to provide enough information.
   - The level of detail chosen for asset identification influences the amount of information collected during risk assessment.
   - The level of detail can be refined in further iterations of risk assessment, meaning that as more information becomes available or risks are better understood, the level of detail can be adjusted accordingly.
2. An asset owner should be identified for each asset providing responsibility & accountability for the asset.
   - The asset owner may have responsibility for its production, development, maintenance, use and security
   - Asset owner often most suitable person to determine its value.

Identification of Threats

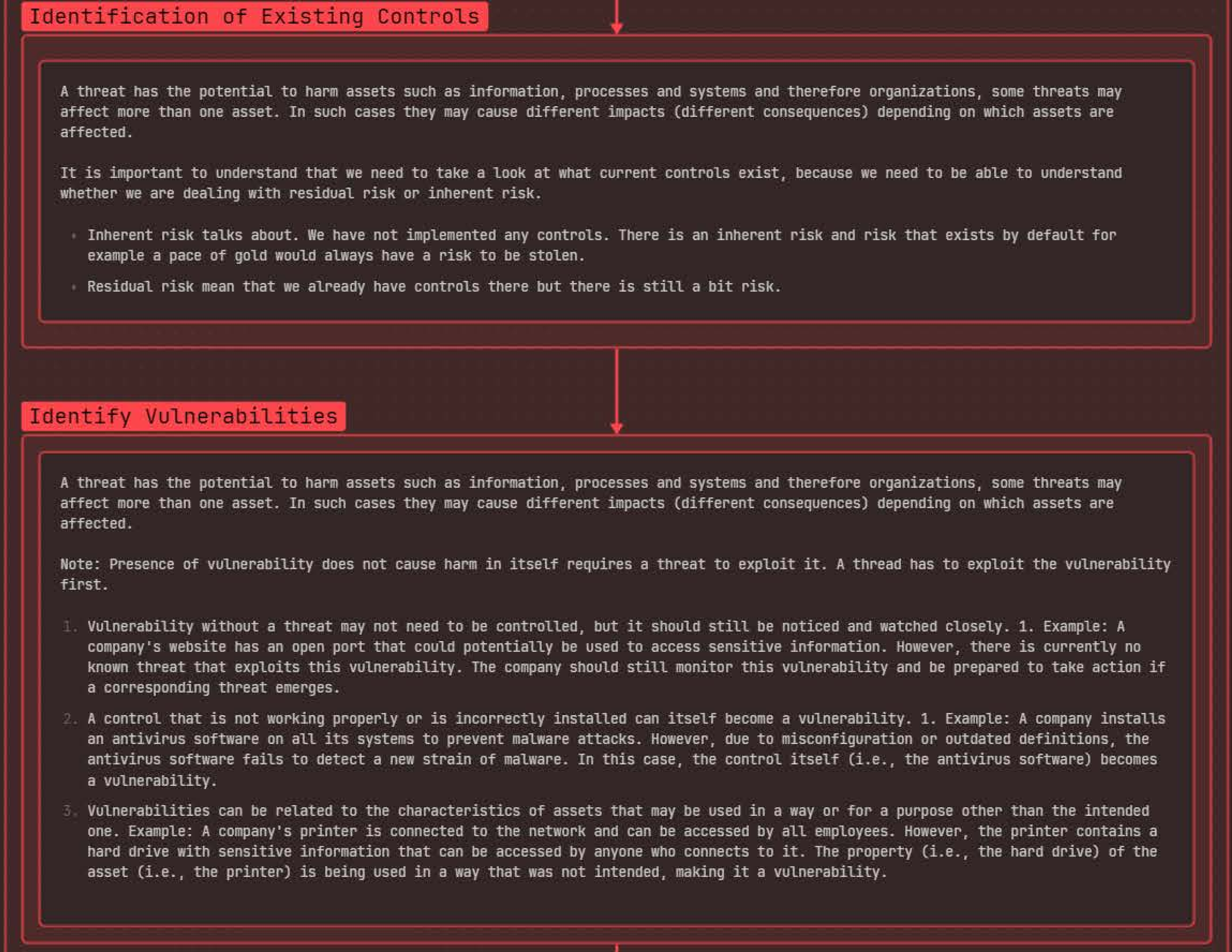
A threat has the potential to harm assets such as information, processes and systems and therefore organizations, some threats may affect more than one asset. In such cases they may cause different impacts (different consequences) depending on which assets are affected.

It is important to understand that we need to take a look at what current controls exist, because we need to be able to understand whether we are dealing with residual risk or inherent risk.

- Inherent risk talks about. We have not implemented any controls. There is an inherent risk and risk that exists by default for example a pace of gold would always have a risk to be stolen.
- Residual risk mean that we already have controls there but there is still a bit risk.



Types	Targets	Actors	Vectors
Threats come in various forms/types/origins	Specific asset targeted by the threat actor	The agent that initiates/causes a threat to come to fruition	The means/approaches/techniques by which a vulnerability in an asset is exploited
Classification: • External vs Internal • Malicious vs Non-malicious • Accidental vs Intentional Examples: • Physical damage • Sabotage • Natural events • Flood • Loss of essential services • Electricity • Compromise of information • Data breach • Technical failures • Software bug • Compromise of functionality • DoS	Examples: • Theft of credit card information • Denial of service to a website • Manipulation of personal information in the process of committing fraud	Examples • Cybercriminals • Nation states • Ideological Hacktivists • Terrorist groups/Extremists • Thrill-seekers • Trusted Insiders • Competitors/Industrial Espionage	Examples: • Malware • Virus • Trojan • Ransomware • Rootkits • Social Engineering • Phishing • Spoofing • Clickjacking



Identification of Existing Controls

A threat has the potential to harm assets such as information, processes and systems and therefore organizations, some threats may affect more than one asset. In such cases they may cause different impacts (different consequences) depending on which assets are affected.

It is important to understand that we need to take a look at what current controls exist, because we need to be able to understand whether we are dealing with residual risk or inherent risk.

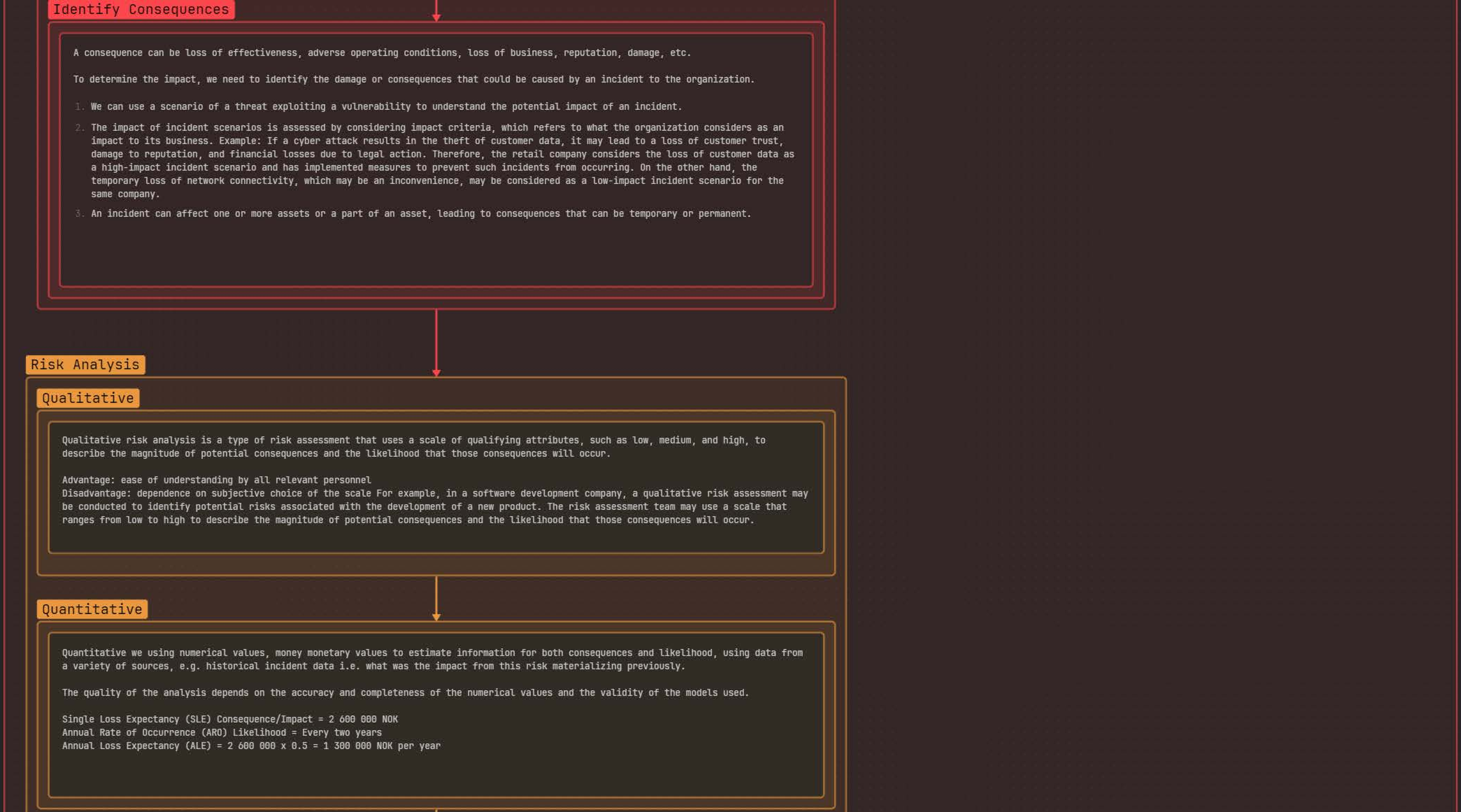
- Inherent risk talks about. We have not implemented any controls. There is an inherent risk and risk that exists by default for example a pace of gold would always have a risk to be stolen.
- Residual risk mean that we already have controls there but there is still a bit risk.

Identify Vulnerabilities

A threat has the potential to harm assets such as information, processes and systems and therefore organizations, some threats may affect more than one asset. In such cases they may cause different impacts (different consequences) depending on which assets are affected.

Note: Presence of vulnerability does not cause harm in itself requires a threat to exploit it. A thread has to exploit the vulnerability first.

1. Vulnerability without a threat may not need to be controlled, but it should still be noticed and watched closely. 1. Example: A company's website has an open port that could potentially be used to access sensitive information. However, there is currently no known threat that exploits this vulnerability. The company should still monitor this vulnerability and be prepared to take action if a corresponding threat emerges.
2. A control that is not working properly or is incorrectly installed can itself become a vulnerability. 1. Example: A company installs an antivirus software on all its systems to prevent malware attacks. However, due to misconfiguration or outdated definitions, the antivirus software fails to detect a new strain of malware. In this case, the control itself (i.e., the antivirus software) becomes a vulnerability.
3. Vulnerabilities can be related to the characteristics of assets that may be used in a way or for a purpose other than the intended one. Example: A company's printer is connected to the network and can be accessed by all employees. However, the printer contains a hard drive with sensitive information that can be accessed by anyone who connects to it. The property (i.e., the hard drive) of the asset (i.e., the printer) is being used in a way that was not intended, making it a vulnerability.



Identify Consequences

A consequence can be loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.

To determine the impact, we need to identify the damage or consequences that could be caused by an incident to the organization.

1. We can use a scenario of a threat exploiting a vulnerability to understand the potential impact of an incident.
2. The impact of incident scenarios is assessed by considering impact criteria, which refers to what the organization considers as an impact to its business. Example: If a cyber attack results in the theft of customer data, it may lead to a loss of customer trust, damage to reputation, and financial losses due to legal action. Therefore, the retail company considers the loss of customer data as a high-impact incident scenario and has implemented measures to prevent such incidents from occurring. On the other hand, the temporary loss of network connectivity, which may be an inconvenience, may be considered as a low-impact incident scenario for the same company.
3. An incident can affect one or more assets or a part of an asset, leading to consequences that can be temporary or permanent.

Risk Analysis

Qualitative

Qualitative risk analysis is a type of risk assessment that uses a scale of qualifying attributes, such as low, medium, and high, to describe the magnitude of potential consequences and the likelihood that those consequences will occur.

Advantage: ease of understanding by all relevant personnel
Disadvantage: dependence on subjective choice of the scale For example, in a software development company, a qualitative risk assessment may be conducted to identify potential risks associated with the development of a new product. The risk assessment team may use a scale that ranges from low to high to describe the magnitude of potential consequences and the likelihood that those consequences will occur.

Quantitative

Quantitative we using numerical values, money monetary values to estimate information for both consequences and likelihood, using data from a variety of sources, e.g. historical incident data i.e. what was the impact from this risk materializing previously.

The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used.

Single Loss Expectancy (SLE) Consequence/Impact = 2 600 000 NOK
Annual Rate of Occurrence (ARO) Likelihood = Every two years
Annual Loss Expectancy (ALE) = 2 600 000 x 0.5 = 1 300 000 NOK per year

Level of Risk

1. When assessing risk, consider the likelihood and ease of exploiting vulnerabilities.
2. Likelihood can be assessed using qualitative or quantitative analysis techniques.
3. Factors to consider when assessing likelihood include experience, statistics, motivation, capabilities, resources, attractiveness, vulnerability, geographical factors, human errors, and equipment malfunction.
4. Vulnerabilities should be assessed both individually and in aggregation.
5. Consider the effectiveness of existing controls in reducing vulnerabilities.
6. Assign values to likelihood and consequences to estimate the level of risk.
7. This estimated level of risk is called inherent risk.
8. Inherent risk is the level of risk before any treatment or mitigation measures are applied. An example of inherent risk could be a company that operates in a high-risk industry such as oil and gas exploration. Inherent risk in this case would refer to the risks that are inherent to the industry itself, such as the risk of oil spills, accidents on oil pips, or fluctuations in oil prices. These risks cannot be eliminated entirely and are always present due to the nature of the industry.

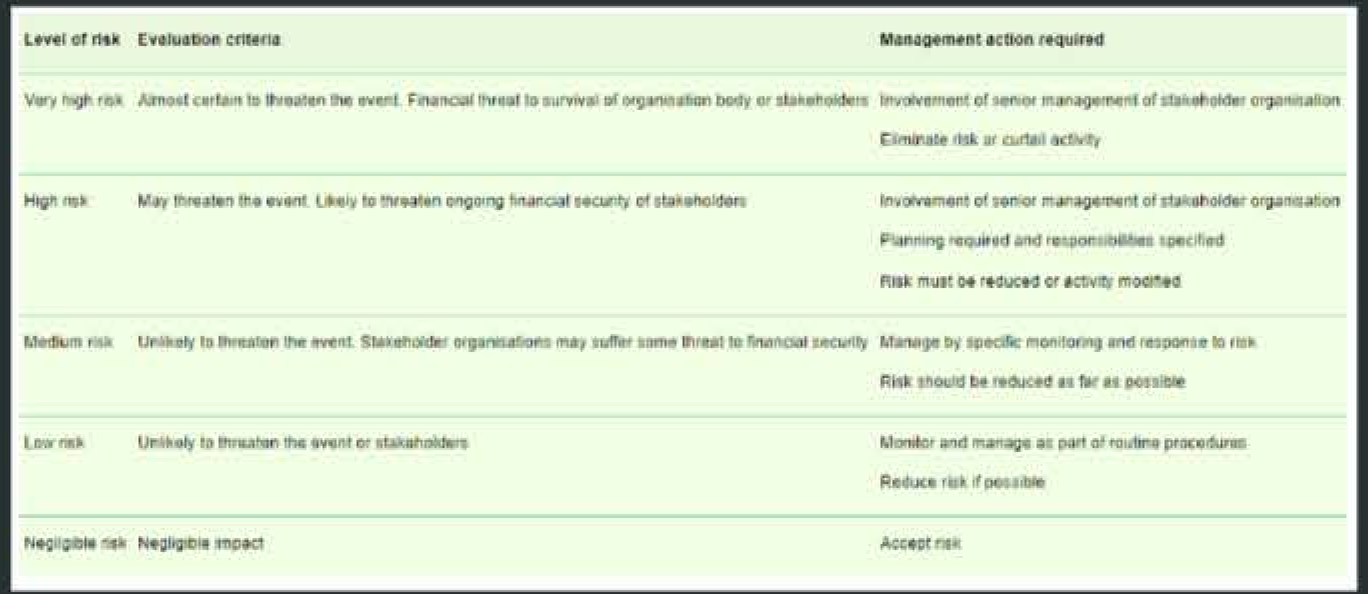
- Consequence/Impact + Likelihood = Inherent Risk
- Inherent Risk + Existing Controls = Residual Risk

Risk Evaluation

Risk evaluation uses the understanding of risk obtained by risk analysis to determine whether the risk and/or its magnitude is acceptable or tolerable and to make decisions about future actions actions.
During the risk evaluation stage, contractual, legal and regulatory requirements are factors that should be considered in addition to the estimated risks.

NOTE: Level of risks should be compared against the risk evaluation criteria and risk acceptance criteria defined during context establishment phase.

- Risk Acceptance Criteria: Specifies the criteria a risk needs to adhere to for the organization to be able to accept the level of risk that exists or decide to treat the risk. Aa organization may say if a risk looks like this we can accept it.
- Risk Evaluation Criteria: Considers various factors, to evaluate and prioritize risks for management action. Aa organization may say if a risk looks like this, it's a high risk for us.
  Prioritized Actions for Risk Treatment = Level of Risk + Evaluation Criteria



Level of risk	Evaluation criteria	Management action required
Very high risk	Almost certain to threaten the event. Financial threat to survival of organisation body or stakeholders	Involvement of senior management of stakeholder organisation Eliminate risk or curtail activity
High risk	May threaten the event. Likely to threaten ongoing financial security of stakeholders	Involvement of senior management of stakeholder organisation Planning required and responsibilities specified Risk must be reduced or activity modified
Medium risk	Unlikely to threaten the event. Stakeholder organisations may suffer some threat to financial security	Manage by specific monitoring and response to risk Risk should be reduced as far as possible
Low risk	Unlikely to threaten the event or stakeholders	Monitor and manage as part of routine procedures Reduce risk if possible
Negligible risk	Negligible impact	Accept risk

Risk Treatment

Risk treatment can involve:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Taking or increasing risk in order to pursue an opportunity;
- Removing the risk source;
- Changing the likelihood;
- Changing the consequences;
- Sharing the risk with another party or parties (including contracts and risk financing); and
- Retaining the risk by informed choice.

Treating Risks

Risk treatment options are selected based on:

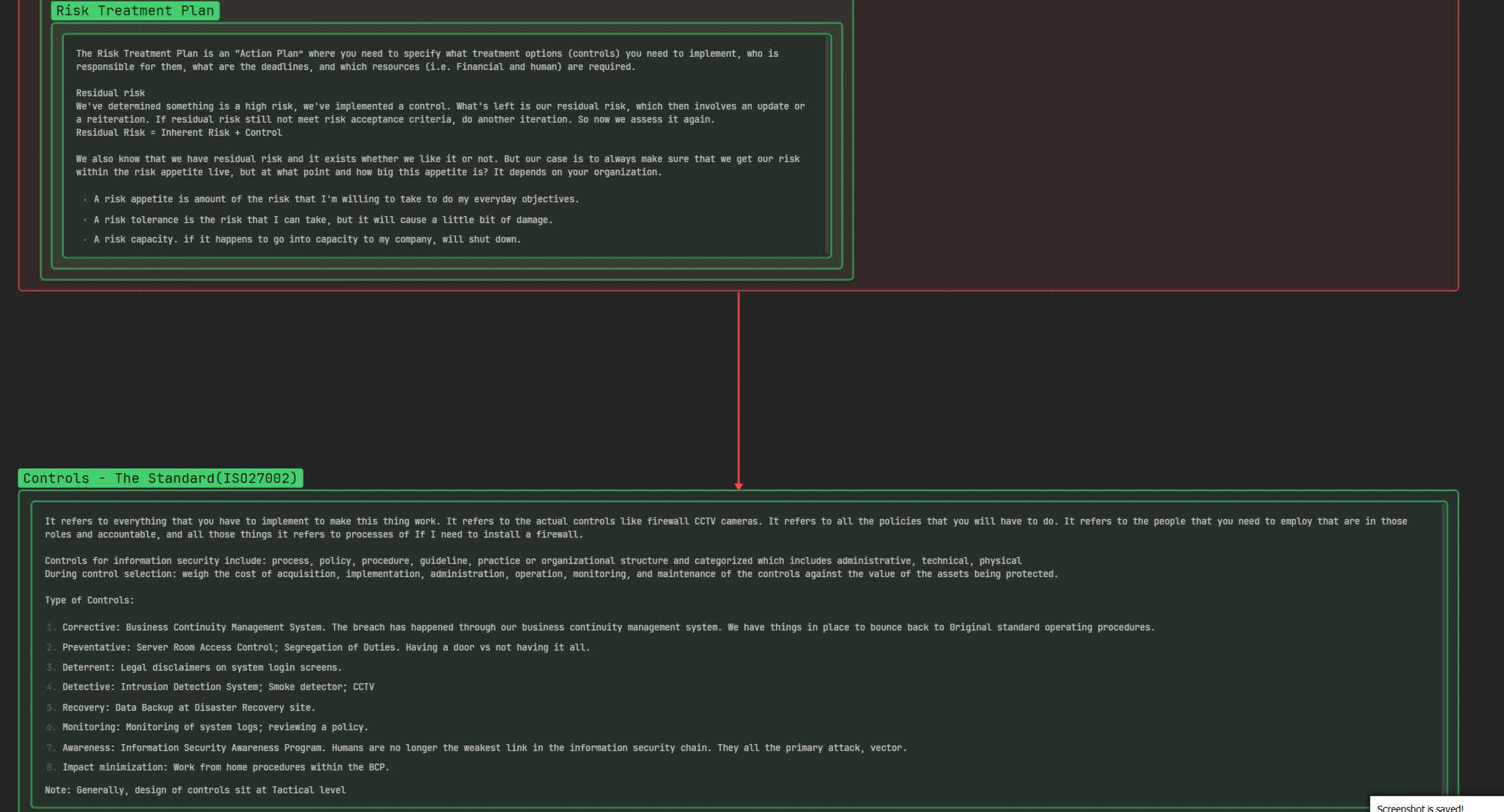
- The outcomes of the risk assessment
- The expected cost for implementing these options
- The expected benefits from these options
  And when we value these 3 things and put it on the scale only, can we then start making the actual call And what we want is, we want a big reduction in risk for low price.
  Risk treatments that deal with negative consequences are sometimes referred to as Risk mitigation, Risk elimination, Risk prevention and Risk reduction.

Treatment Options
Risk Modification: This is achieved through implementing or changing the controls which may protect assets through correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness. Note: It might be that you are currently paying a huge amount of subscription fees to lower risk, which is minimal impact so you may just cancel the subscription.
Types of Controls:
Corrective-Business Continuity Management System
Preventative-Server Room Access Control; Segregation of Duties
Deterrent-Legal disclaimers on system login screens
Detective-Intrusion Detection System; Smoke detector; CCTV
Recovery-Data Backup at Disaster Recovery site
Monitoring-Monitoring of system logs; reviewing a policy
Awareness-Information Security Awareness Program
Impact minimization -Work from home procedures within the BCP

Risk Retention (Acceptance): If according to risk evaluation and risk acceptance criteria the results show that the risk is acceptable, it can simply be retained with no need to implement or change any controls.

Risk Avoidance: This can be achieved through completely avoiding an activity or risk which gives a rise to the condition. This option is suitable when the costs of treating a risk are too high, or the risk itself is too high.

Risk Sharing (Transfer): This risk treatment option involves other parties such as insurance companies, or subcontractors who would monitor the information system against an attack. This does not mean that the liability is shared - the responsibility for the consequences still lies with the organization.



Risk Treatment Plan

The Risk Treatment Plan is an "Action Plan" where you need to specify what treatment options (controls) you need to implement, who is responsible for them, what are the deadlines, and which resources (i.e. Financial and human) are required.

Residual risk
We've determined something is a high risk, we've implemented a control. What's left is our residual risk, which then involves an update or a reiteration. If residual risk still not meet risk acceptance criteria, do another iteration. So now we assess it again.
Residual Risk = Inherent Risk + Control

We also know that we have residual risk and it exists whether we like it or not. But our case is to always make sure that we get our risk within the risk appetite live, but at what point and how big this appetite is? It depends on your organization.

- A risk appetite is amount of the risk that I'm willing to take to do my everyday objectives.
- A risk tolerance is the risk that I can take, but it will cause a little bit of damage.
- A risk capacity. if it happens to go into capacity to my company, will shut down.

Controls - The Standard(ISO27002)

It refers to everything that you have to implement to make this thing work. It refers to the actual controls like firewall CCTV cameras. It refers to all the policies that you will have to do. It refers to the people that you need to employ that are in those roles and accountable, and all those things it refers to processes of If I need to install a firewall.

Controls for information security include: process, policy, procedure, guideline, practice or organizational structure and categorized which includes administrative, technical, physical
During control selection: weigh the cost of acquisition, implementation, administration, operation, monitoring, and maintenance of the controls against the value of the assets being protected.

Type of Controls:

1. Corrective: Business Continuity Management System. The breach has happened through our business continuity management system. We have things in place to bounce back to Original standard operating procedures.
2. Preventative: Server Room Access Control; Segregation of Duties. Having a door vs not having it all.
3. Deterrent: Legal disclaimers on system login screens.
4. Detective: Intrusion Detection System; Smoke detector; CCTV
5. Recovery: Data Backup at Disaster Recovery site.
6. Monitoring: Monitoring of system logs; reviewing a policy.
7. Awareness: Information Security Awareness Program. Humans are no longer the weakest link in the information security chain. They all the primary attack, vector.
8. Impact minimization: Work from home procedures within the BCP.

Note: Generally, design of controls sit at Tactical level

Controls Category

1. Organizational controls includes measures that involve policies, procedures, and other administrative actions to manage risks. These controls are related to the organization's structure, management, and culture, rather than to specific technical solutions or physical barriers. Examples of organizational controls include documented policies, processes, and procedures for information security (ISPA), which define the rules and guidelines for employees to follow in order to maintain the confidentiality, integrity, and availability of information assets. Another example of an organizational control is the principle of segregation of duties, which involves dividing critical tasks and responsibilities among different people to reduce the risk of errors, fraud, or abuse. For example, a company may require that the person who authorizes a financial transaction is different from the person who processes the transaction, and that both are different from the person who reconciles the accounts. This helps to ensure that no single person has too much power or control over financial transactions and reduces the risk of financial losses due to errors or fraud.
2. Physical Controls focus on protecting the physical assets of an organization, such as buildings, equipment, and other tangible resources. For example, gates, lock stores, access control boxes, CCTV cameras, all physical control.
3. Technological Controls. The technical category of controls consists of measures that are primarily related to technology and its configuration. For example, Data Backups - IPS/IDS - ACL's - Logical Access /Authentication - Logging
4. People Controls: Talks about correct skills and individuals that you should have in the correct position and the security, education, training, and awareness of employees really fall into that one as well. It includes:

- Background Screening: This control is used to verify the background of individuals before they are given access to sensitive information or systems.
- Remote Working: This control is used to manage the risks associated with employees working from outside the organization's physical premises. Remote working typically involves the use of virtual private networks (VPNs) to provide secure access to the organization's network and systems.
- Training (SETA): This control is used to provide employees with the knowledge and skills they need to protect the organization's information assets. The training typically covers topics such as information security policies and procedures, data classification, password management, and social engineering. The aim is to ensure that employees are aware of their responsibilities regarding information security and understand how to prevent security breaches. SETA stands for Skills Education Training Authorities, which is a type of training program in South Africa.

ISO27002

Designed for organizations to use as a reference for selecting controls within the process of implementing an ISMS based on ISO/IEC 27001. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

Selecting Controls

- Controls can be selected from the 27002 standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.
- The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization and should also be subject to all relevant national and international legislation and regulations.
- Control selection also depends on the manner in which controls interact to provide defense in depth.
- Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations.

NIST Cyber Security Framework

The Framework is a voluntary guidance designed to help organizations manage and reduce cybersecurity risk. It is based on existing standards, guidelines, and practices and aims to foster risk and cybersecurity management communications among internal and external stakeholders. The Core includes five high level functions: Identify - Protect - Detect - Respond - Recover. It consists of 5 Functions 23 Categories 108 Subcategories 6 Informative References

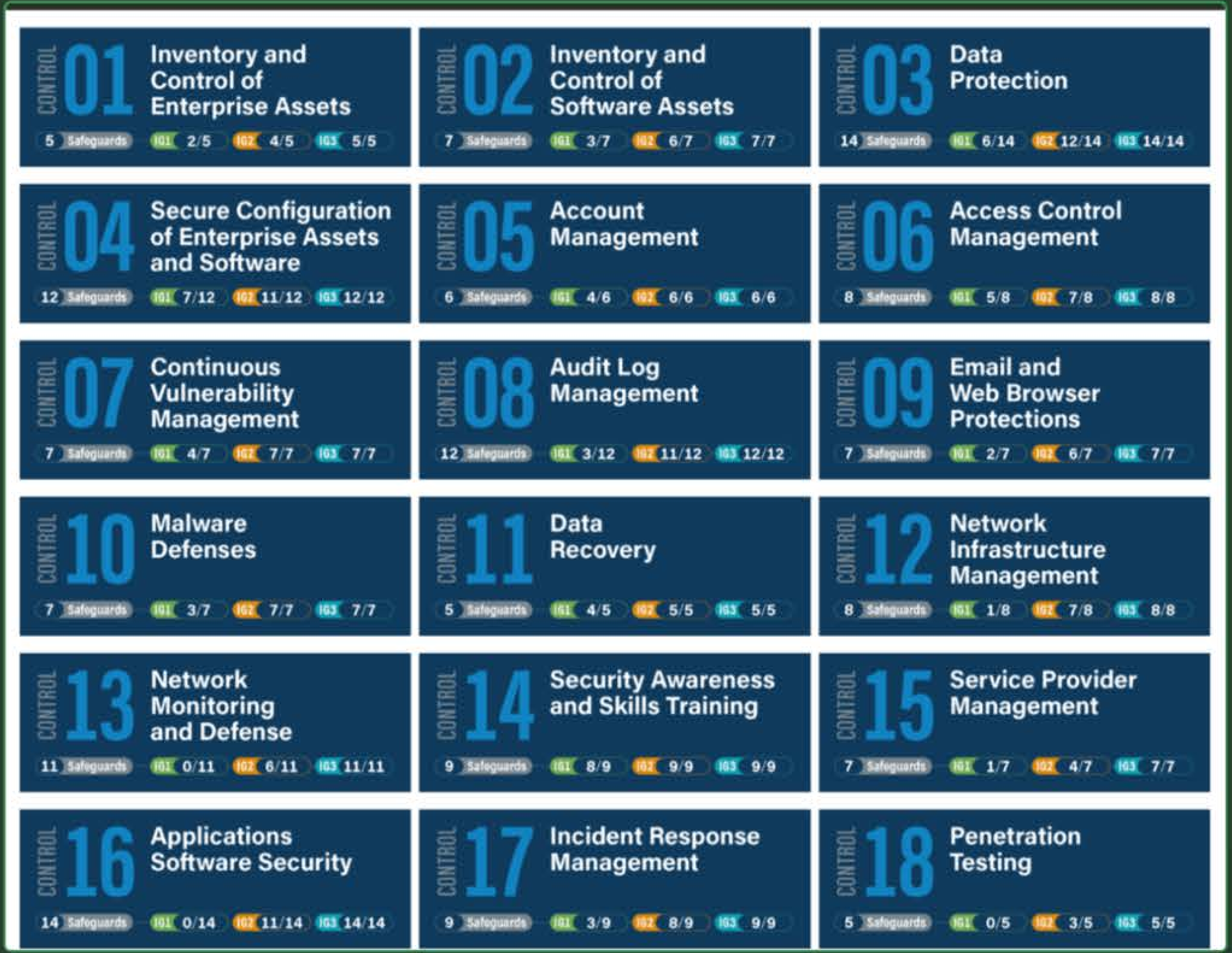
- These 5 functions are not only applicable to cybersecurity risk management, but also to risk management at large.
- The next level down is the 23 Categories that are split across the five Functions.
- There are 108 Subcategories, which are outcome driven statements that provide considerations for creating or improving a cybersecurity program.

CIS Critical Security Controls

The CIS (Center for Internet Security) Critical Security Controls, formerly known as the SANS Top 18 (V8), is a prioritized set of 18 cybersecurity measures that organizations can implement to improve their overall security posture. Implementation Groups are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls.

|G1 is the definition Of basic cyber hygiene and represents a minimum standard Of information security for all enterprises. IGI assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.
|G2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.
|G3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

Pasted image 20230424005545.png

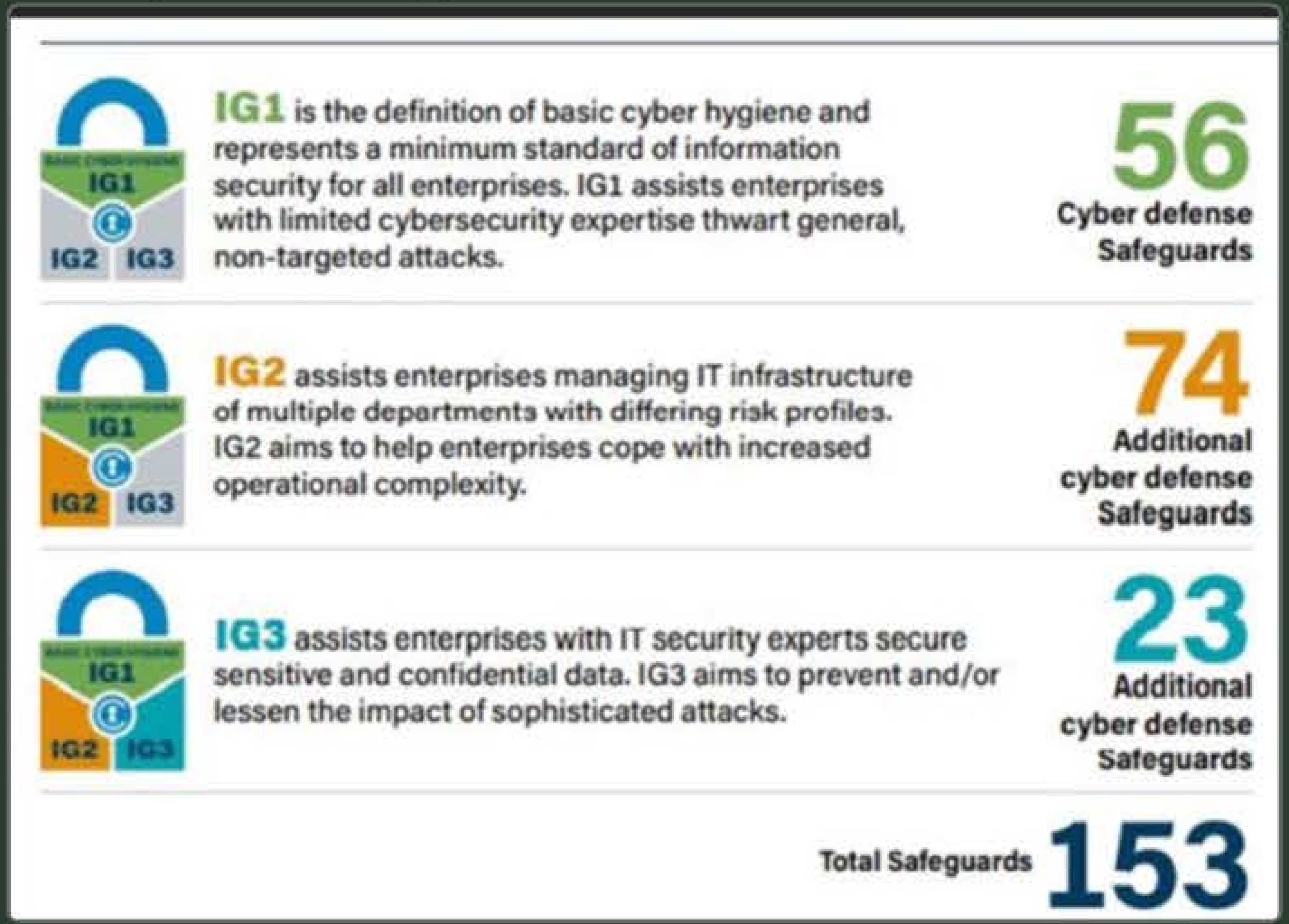


CONTROL 01	Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02	Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03	Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04	Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05	Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06	Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07	Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08	Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09	Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10	Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11	Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12	Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13	Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14	Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15	Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16	Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17	Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18	Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

Pasted image 20230424011301.png

- Self-assessed
- Based on risk profile
- Available resources

Pasted image 20230424011314.png



IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks. — **56** Cyber defense Safeguards

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity. — **74** Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks. — **23** Additional cyber defense Safeguards

Total Safeguards **153**

Monitoring and Review (Control Assurance for Risk Treatment)

Assurance is a critical part of corporate governance in which management provides accurate and current information to the stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with the statutory obligations. It focus usually on anything that could affect the enterprise desire to reach its
objectives otherwise known as risk
Internal audits vs External audits
Internal audits are performed by employees or contractors within the organization to evaluate the effectiveness of the ISMS and identify areas for improvement. The purpose of internal audits is to assess whether the organization's policies, procedures, and controls are being implemented effectively and whether they are meeting the objectives of the ISMS.
External audits are conducted by an independent third-party auditor who is not affiliated with the organization being audited. The external auditor evaluates the organization's ISMS to determine whether it meets a specific standard or set of standards, such as ISO 27001 or the CIS Critical Security Controls. The purpose of external audits is to provide an objective evaluation of the organization's information security posture and to ensure that it is complying with relevant standards and regulations.

From an ISO27005 Perspective; In an ISMS, according to ISO/IEC 27001, this is supported by the measurement of control effectiveness. A way to estimate the effect of the control is to see how it reduces the threat likelihood and ease of exploiting the vulnerability, or impact of the incident. Management reviews and audit reports also provide information about the effectiveness of existing controls

Business and ICT Residency it's talking about. If an incident occurs. how will I be able to continue? Do I have the proper things in place? Do I have a backup site. Do I have backups, and how resilient am I? In other words, if you talk about a a night in armor, and you talk about resiliency. Resiliency means how much blows to the armor

Relation between FSA and ICT: A financial statement audit is the examination of an entity's financial statements and accompanying disclosures by an independent auditor. As part of this audit, the effectiveness of the entity's suite of controls, including those related to authorization, safeguarding of assets, and segregation of duties, is assessed through internal controls testing. This includes ICT controls that directly affect financial systems, therefore: General IT Control audits are performed during FSA, to provide assurance over the systems that store, transmit and process financial operations.

Assurance over General IT Controls

1. Access to Programs & Data

- Physical Access – controls to physically restrict access to systems to authorised individuals; include environmental controls
- Configuration of Access Rules – System access roles and access
- Access Administration – Controls around granting, modifying and terminating user access
- Identification – Controls around users with access to multiple, duplicates and generics accounts
- Authentication – Controls for user authentication such as passwords, 2fa etc.
- Monitoring – Controls around logging and monitoring of user activity in high risk systems
- Super Users – Controls around restricting, logging, monitoring of super user access

2. Program Changes

- Authorization, Development, Test & Approval of changes: Auditing the entire change management process and that all program changes in a specific period followed the process.
- Controls around migration to production: Auditing if changes were tested within the test and development environments; and did all stakeholders (CAB) sign off that changes could be migrated

3. Program Development

- Design, Development, Test, Approve and Implementation: Auditing whether all newly developed programs followed the correct program development process within a specific period
- Data Migration: Auditing whether during the process of changing systems data was migrated to new system completely and accurately – checking the controls that were put in place to ensure this.

4. Computer Operations

- Batch job processing and interfaces – Testing: Authorisation of changes to batch jobs, Scheduling and access, Monitoring, Job failure resolution
- Backup and restoration controls: Disaster Recovery
- ICT Incident and Problem management controls

Control Audits - Examples of control audits:
A full review of the organizations ISMS against the "ISO27000; NIST CSF etc" standard
A penetration test of a newly acquired CRM system
A test and simulation of an organization's Disaster Recovery plan
Vulnerability assessment of an organizations external facing servers
Security review of an organization's AD domain service against CIS best practice
Physical controls implemented within an organization's data center

Performing Control Audits
The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards. Many audit companies have their own methodologies, mostly based on recognized standards and regulatory body requirements (IFRS, Sarbanes-Oxley, GAAP, ISAE, PCAOB, COBIT)

General Approach to Control Testing

Test Of Design

TOD tests whether the organization have designed and documented a control that is appropriate.

- Check policies, processes and procedures against best practice
- Document anomalies
- Determine design of control adequate to address the risk in context of organization If e.g. not documented, TOD fails and a finding is raised, e.g You have a good password policy but it's not documented.

For example
Is there a control? Yes the lock
Functionality: There is a lock and it's function is to look the door.

Test of Implementation

TOI tests whether the control has been implemented in the system as designed and documented.

- Check evidence from the system such as configurations
- Document any anomalies
- Determine if configuration match design If not, a finding will be raised that system has not been configured in line with policy: A case has happened where the password settings configured were stronger than what the policy required, in such case, finding raised will be the same, but the recommendation will be to update policy, not the config.

Test of Operating Effectiveness

TOE tests whether the implemented control is operating effectively throughout an entire specified period, e.g. an entire financial year.

- Obtain a sample of evidence that covers the entire period: Sampling methodologies exist where e.g. if the control is a monthly CAB meeting to approve system changes, one will request approval evidence from 5 of the 12 CAB meetings.
- Determine if control followed the design (policy) throughout the year. If not, a finding will be raised that the control did not operate effectively throughout the period under review.

Test Of Design
Is there a control? Yes the lock - Functionality: There is a lock and it's function is to look the door.
Test of Implementation
Is it installed? Yes - Is the lock installed correctly? Yes - No in case the lock installed in the middle of the door, it become useless
Test of Operating Effectiveness
If we have 1kg of gold, will this lock be enough to protect it?

Business and ICT Resilience

Business and ICT Residency it's talking about. If an incident occurs. how will I be able to continue? Do I have the proper things in place? Do I have a backup site. Do I have backups, and how resilient am I? In other words, if you talk about a a night in armor, and you talk about resiliency. Resiliency means how much blows to the armor. Resiliency says we don't just want to focus on continuing off to something happen. Resiliency says, let's try and not get it to happen in the first place, or absorb as much as possible, so that we can continue.

Business and ICT Residency it's talking about. If an incident occurs. how will I be able to continue? Do I have the proper things in place? Do I have a backup site. Do I have backups, and how resilient am I? In other words, if you talk about a a night in armor, and you talk about resiliency. Resiliency means how much blows to the armor. Security Culture is one of the risks that you will always have in the organization and if you did not included it in the assessment, then it's a mistake.

ICT Disaster Recovery (continuity): The ability of the ICT elements of an organization to support its critical business functions to an acceptable level within a predetermined period of time following a disruption.
Business Continuity: The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
Incident Response: The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively.

BCMS ISO 22301
Business Continuity Management System is part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. ISO22301 is the standard that we will generally use to guide us to implement business continuity management. Just like an ISMS, Risk management: Plan, Do, Check, Act

ICT Resilience ISO 27301

Monitoring Response and Recovery
If we assume monitor before an incident happens so that we can pick it up so that we can respond. If we do not monitor, we cannot respond. If we do not monitor, we can only react after the incident has happened, so respond is talking about preemptively respond we, seeing that there is an attack happening, isolated, lock it down, identify and you respond to the incident. If we assume that the controls in the response failed that we will have to recover from it.

1. ISO 27031 introduces a management systems approach to address ICT which SUPPORTSthe broader business continuity management system, as described in ISO 22301.
2. ISO 27031 describes a management system for ICT readiness for business continuity (IRBC). IRBC is a management system focused on IT disaster recovery (ICT Continuity).
3. ISO27031 ensures ALIGNMENTbetween ICT and Business Continuity and as such promotes business resilience.
   ISO 27031 states that strategies needs to incorporate six elements into monitoring for, responding to and recovering from disruptions to information and communication technology:

- Skill and Knowledge: Ensure no individual holds specialized skills or knowledge required to operate ICT systems in case of a disruption.
- Facilities: Mitigate risks associated with operating ICT systems based in a single facility by ensuring that the systems can be operated even if a primary facility is rendered inoperable.
- Technology: Ensure that hardware and applications are able to be recovered within the time and data recovery required by the organization by meeting the organization's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and including support systems such as power, cooling, staffing, vendor support, and WAN connectivity.
- Data: Protect the data required by the organization by considering security, validity, and availability of the data required by end-users.
- Processes: Sustain the processes necessary to monitor, operate, and recover ICT systems in order to meet business requirements by identifying the ICT processes necessary before, during, and after a disruption to ICT systems.
- Suppliers: Inform and engage suppliers who are needed to recover and operate ICT systems by identifying what suppliers are engaged in the operation and recovery of ICT systems before, during, and after a disruption has occurred.

ICT Readiness for BC (IRBC) - In Practice

IRBC aims to:

- improve incident detection capabilities;
- prevent a sudden or drastic failure;
- enable an acceptable degradation of operational status should the failure be unstoppable;
- further shorten recovery time; and
- minimize impact upon eventual occurrence of the incident.

Basically what we are trying to do is we trying to minimize the time and lower the consequence of the impact.

Principles of IRBC:

Incident Prevention -Protecting ICT services from threats, such as environmental and hardware failures, operational errors, malicious attack

Incident Detection -Detecting incidents at the earliest opportunity will minimize the impact to services, reduce the recovery effort, and preserve the quality of service

Response-Responding to an incident in the most appropriate manner will lead to a more efficient recovery and minimize any downtime. Reacting poorly can result in a minor incident escalating into something more serious

Recovery-Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data.

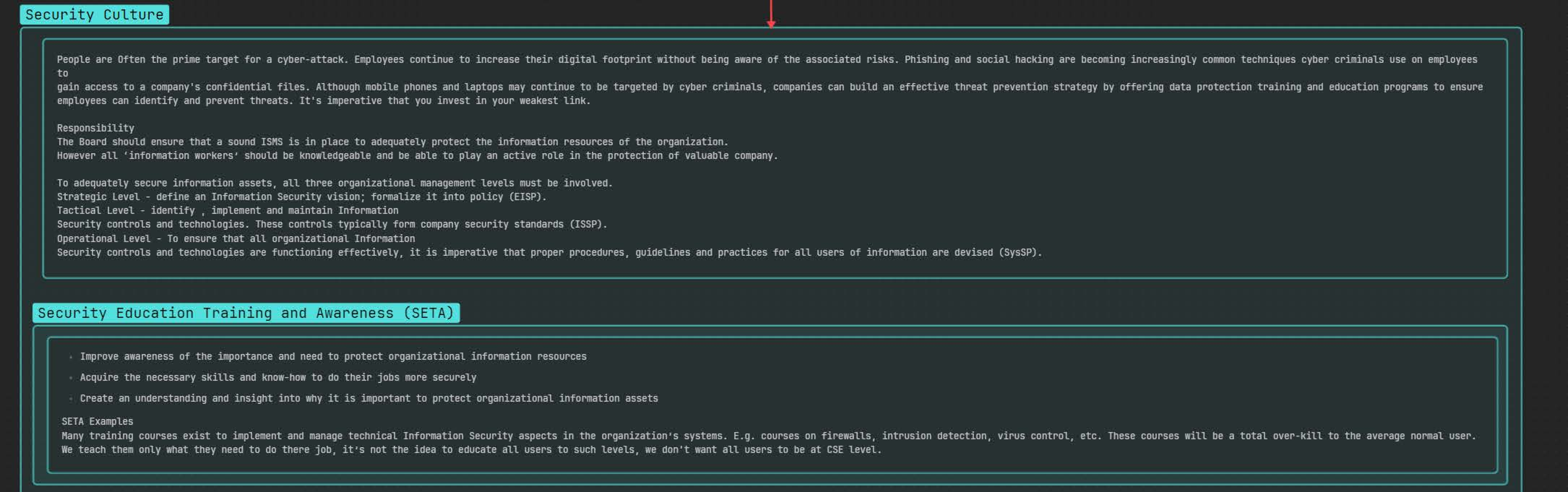
Improvement: Lessons learned from small and large incidents should be documented, analyzed and reviewed. Understanding these lessons will allow the organization to better prepare, control and avoid incidents and disruption.

Business Impact Analysis

BIA is a process used to identify and evaluate the potential effects of an interruption or failure of critical business functions and processes. The BIA identifies the urgency of each business activity undertaken by the organization assessing the impact over time of an interruption to this activity on the delivery of products and services.

BIA helps organizations to identify their critical assets, prioritize them, and develop strategies for protecting them in case of a cyber-attack, natural disaster, or other unexpected events. BIA includes analyzing the potential impact of downtime, lost data, and the cost of recovering from an incident. The process involves a thorough examination of the organization's operations, systems, applications, and data to identify vulnerabilities and evaluate their potential impact on business continuity.

General BIA Process: Data Gathering ⇒ Analyze ⇒ Report



Security Culture

People are Often the prime target for a cyber-attack. Employees continue to increase their digital footprint without being aware of the associated risks. Phishing and social hacking are becoming increasingly common techniques cyber criminals use on employees to
gain access to a company's confidential files. Although mobile phones and laptops may continue to be targeted by cyber criminals, companies can build an effective threat prevention strategy by offering data protection training and education programs to ensure employees can identify and prevent threats. It's imperative that you invest in your weakest link.

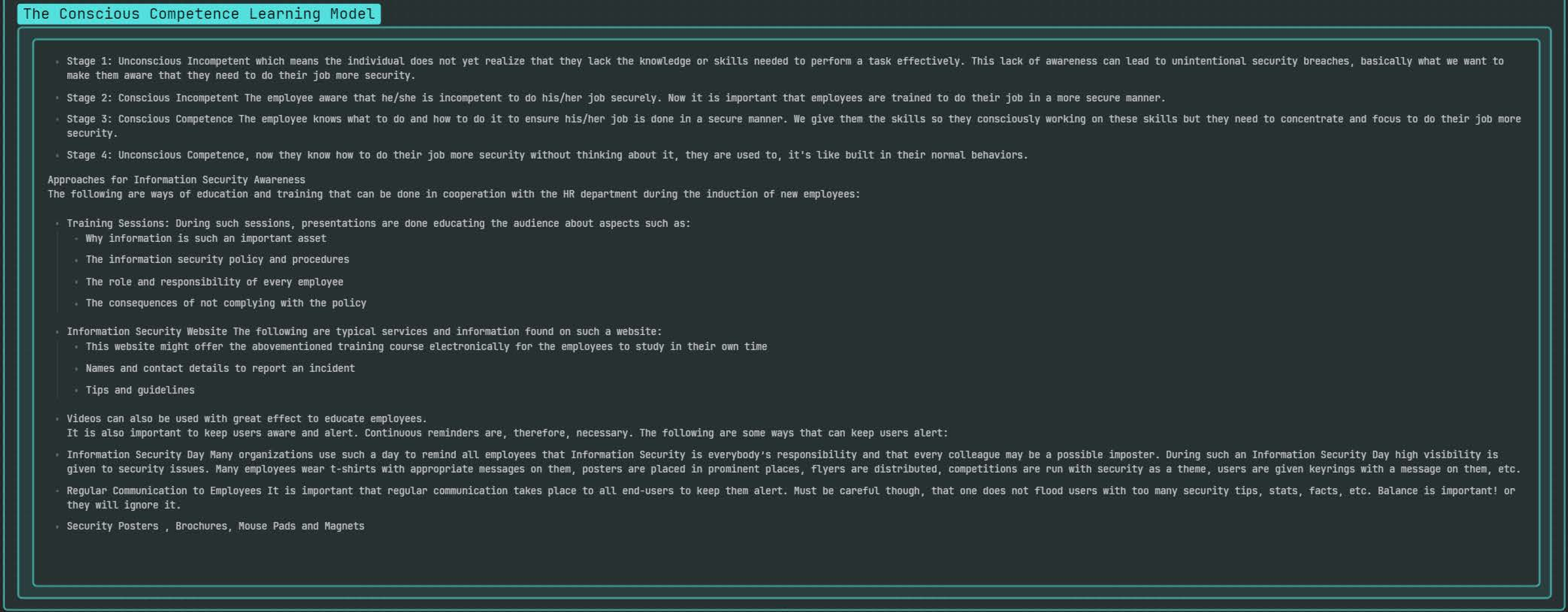
Responsibility
The Board should ensure that a sound ISMS is in place to adequately protect the information resources of the organization.
However all ‘information workers‘ should be knowledgeable and be able to play an active role in the protection of valuable company.

To adequately secure information assets, all three organizational management levels must be involved.
Strategic Level - define an Information Security vision; formalize it into policy (EISP).
Tactical Level - identify , implement and maintain Information
Security controls and technologies. These controls typically form company security standards (ISSP).
Operational Level - To ensure that all organizational Information
Security controls and technologies are functioning effectively, it is imperative that proper procedures, guidelines and practices for all users of information are devised (SysSP).

Security Education Training and Awareness (SETA)

- Improve awareness of the importance and need to protect organizational information resources
- Acquire the necessary skills and know-how to do their jobs more securely
- Create an understanding and insight into why it is important to protect organizational information assets

SETA Examples
Many training courses exist to implement and manage technical Information Security aspects in the organization‘s systems. E.g. courses on firewalls, intrusion detection, virus control, etc. These courses will be a total over-kill to the average normal user.
We teach them only what they need to do there job, it‘s not the idea to educate all users to such levels, we don‘t want all users to be at CSE level.



The Conscious Competence Learning Model

- Stage 1: Unconscious Incompetent which means the individual does not yet realize that they lack the knowledge or skills needed to perform a task effectively. This lack of awareness can lead to unintentional security breaches, basically what we want to make them aware that they need to do their job more security.
- Stage 2: Conscious Incompetent The employee aware that he/she is incompetent to do his/her job securely. Now it is important that employees are trained to do their job in a more secure manner.
- Stage 3: Conscious Competence The employee knows what to do and how to do it to ensure his/her job is done in a secure manner. We give them the skills so they consciously working on these skills but they need to concentrate and focus to do their job more security.
- Stage 4: Unconscious Competence, now they know how to do their job more security without thinking about it, they are used to, it's like built in their normal behaviors.

Approaches for Information Security Awareness
The following are ways of education and training that can be done in cooperation with the HR department during the induction of new employees:

- Training Sessions: During such sessions, presentations are done educating the audience about aspects such as:
  - Why information is such an important asset
  - The information security policy and procedures
  - The role and responsibility of every employee
  - The consequences of not complying with the policy
- Information Security Website The following are typical services and information found on such a website:
  - This website might offer the abovementioned training course electronically for the employees to study in their own time
  - Names and contact details to report an incident
  - Tips and guidelines
- Videos can also be used with great effect to educate employees.
  It is also important to keep users aware and alert. Continuous reminders are, therefore, necessary. The following are some ways that can keep users alert:
- Information Security Day Many organizations use such a day to remind all employees that Information Security is everybody's responsibility and that every colleague may be a possible imposter. During such an Information Security Day high visibility is given to security issues. Many employees wear t-shirts with appropriate messages on them, posters are placed in prominent places, flyers are distributed, competitions are run with security as a theme, users are given keyrings with a message on them, etc.
- Regular Communication to Employees It is important that regular communication takes place to all end-users to keep them alert. Must be careful though, that one does not flood users with too many security tips, stats, facts, etc. Balance is important! or they will ignore it.
- Security Posters , Brochures, Mouse Pads and Magnets

Laws and Regulations - Security and Privacy

So privacy is what we deem important, so that we can control the access and the use of our personal information. A right to privacy is a right to control access to and uses of—places, bodies, and personal information. Data security and privacy are interconnected, but they are not the same.

International Association of Privacy Professionals
The IAPP offers a full suite of educational and professional development services, including privacy training, certification programs, publications and annual conferences.

Privacy typically refers to the user’s ability to control, access, and regulate their personal information, and security refers to the system that protects that data from getting into the wrong hands, through a breach, leak, or cyber attack. The other core difference between privacy and security has to do with the type of protection involved and who is seeking access to the data in question.
Privacy regulations protect a user from having their information shared with a third-party without their consent or knowledge. Security measures protect a user’s data from being hacked or stolen -identity theft with malicious intent is not the same as a third-party marketer.
Can You Have Security Without Privacy? You can have security without privacy, but they go better together. For example, a company may write into their privacy policy that they can share or sell a user’s data. In that case, privacy is less protected, but the organization’s systems and the systems of those they sell the data to can be secure.
Most of the time, data security and privacy are equally important If you are adhering to HIPAA guidelines, privacy is the star of the show and security measures you must take to comply with HIPAA are all designed to protect patients’ privacy.

GDPR

Purpose

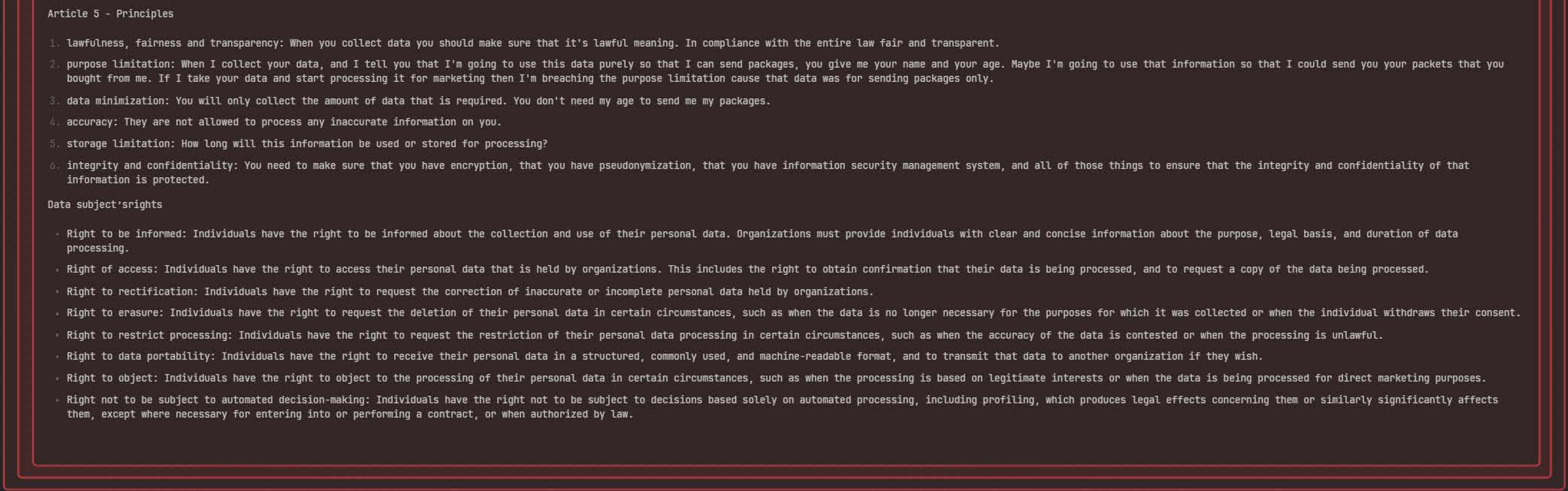
- Giving Data Subjects more control
- Making Data Controllers/Processors more accountable
- Making personal data processing more transparent: How long is it being processed? What purposes are it being processed for? Who has access to it? What is the reason?
- Reducing personal data security vulnerabilities

Article83
General conditions for imposing administrative fines

- Minor breach: Up to €10 million, or 2% of annual global turnover -whichever is greater
- Big data breaches: Up to €20 million, or 4% of annual global turnover -whichever is greater.

Article 4
What is Personal Data?

- personal data means any information relating to an identified or identifiable natural person(‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- Processing/behandling means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- Pseudonymization’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- Controller are all the people that will process the information for you.
- Processor, etc. The processor is the one that's doing the processing on your behalf.
- Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her



Article 5 - Principles

1. lawfulness, fairness and transparency: When you collect data you should make sure that it's lawful meaning. In compliance with the entire law fair and transparent.
2. purpose limitation: When I collect your data, and I tell you that I'm going to use this data purely so that I can send packages, you give me your name and your age. Maybe I'm going to use that information so that I could send you your packets that you bought from me. If I take your data and start processing it for marketing then I'm breaching the purpose limitation cause that data was for sending packages only.
3. data minimization: You will only collect the amount of data that is required. You don't need my age to send me my packages.
4. accuracy: They are not allowed to process any inaccurate information on you.
5. storage limitation: How long will this information be used or stored for processing?
6. integrity and confidentiality: You need to make sure that you have encryption, that you have pseudonymization, that you have information security management system, and all of those things to ensure that the integrity and confidentiality of that information is protected.

Data subject'srights

- Right to be informed: Individuals have the right to be informed about the collection and use of their personal data. Organizations must provide individuals with clear and concise information about the purpose, legal basis, and duration of data processing.
- Right of access: Individuals have the right to access their personal data that is held by organizations. This includes the right to obtain confirmation that their data is being processed, and to request a copy of the data being processed.
- Right to rectification: Individuals have the right to request the correction of inaccurate or incomplete personal data held by organizations.
- Right to erasure: Individuals have the right to request the deletion of their personal data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected or when the individual withdraws their consent.
- Right to restrict processing: Individuals have the right to request the restriction of their personal data processing in certain circumstances, such as when the accuracy of the data is contested or when the processing is unlawful.
- Right to data portability: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another organization if they wish.
- Right to object: Individuals have the right to object to the processing of their personal data in certain circumstances, such as when the processing is based on legitimate interests or when the data is being processed for direct marketing purposes.
- Right not to be subject to automated decision-making: Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, except where necessary for entering into or performing a contract, or when authorized by law.