

Cybersecurity KPIs for companies and how to communicate them to executives

Today's lecturer – Governance & Tech in a boutique firm

Managing projects in this areas

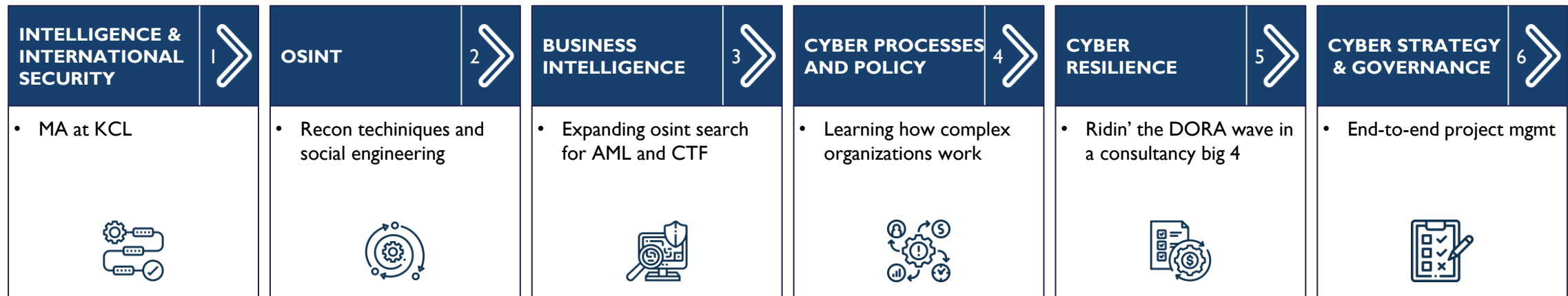
1. Cyber Strategy

- *Supporting clients in gaining an objective view of their cyber posture*
- **Assessing how cyber investments and initiatives are designed, planned and executed within clients**

2. Cyber Crisis Management

Building tailor made procedures on relevant cyber scenarios that are relevant for the clients' industry and defining actions at the operational, tactical and strategic level

My journey so far



How can you use today's lecture for further research?



- There is a growing body of literature revolving around resilience and NIST 800-160
- Monitoring of cyber is an enabler of governance and cyber planning cross industry
- Various organizations are trying the best way to merge their Cyber risk management and Enterprise Risk Management

ASSET PRIORITIZATION

MY FOCUS

- Identifying the right assets to be protected alloww to craft custom metrics
- Is there any metric related to the human factor?

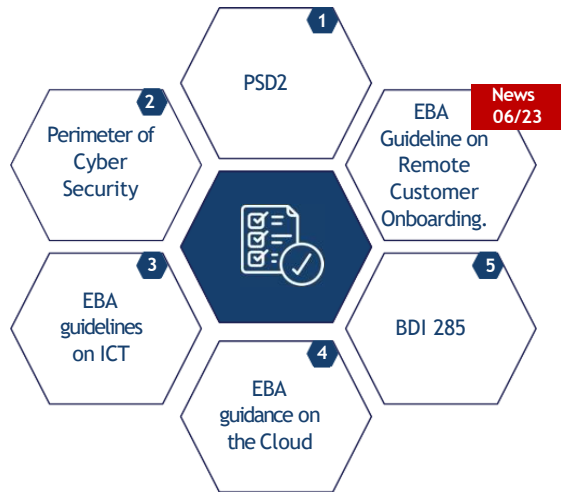
INTEGRATION AND NOISE REDUCTION

- Data feeds are embedded into security operations functions and not machine readable
- This is more frequent when some cyber functions are outsourced

Overview of the regulatory framework



CURRENT LEGISLATION



- 1 Legislation governing **payment services** and promoting openness and innovation in the financial sector
- 2 Technologies, policies and procedures to **protect computer network**
- 3 Practices for information technology management in **banking**
- 4 Measures and practices taken to protect data and resources hosted on **cloud platforms**
- 5 Harmonized framework of risk management measures **inherent in the use of ICT technologies** and security measures that Banks must have.



EMERGING REGULATIONS

DORA

JANUARY 2025

The Digital Operational Resilience Act aims to improve the digital operational resilience of the financial sector and creates a framework for collaboration between government and business to ensure operational resilience.

The regulation provides 5 areas of requirements (pillars) for financial sector organizations: cyber risk management; cyber incident management, classification and reporting; digital operational resilience testing; cyber risk management; and information sharing.

Examples of DORA requirement areas

ILLUSTRATIVE

- Methods and specific digital resilience goals
- Response and restoration
- Learning and skill development
- Mapping and interdependencies of processes and information assets
- Monitoring technological developments

NIS2

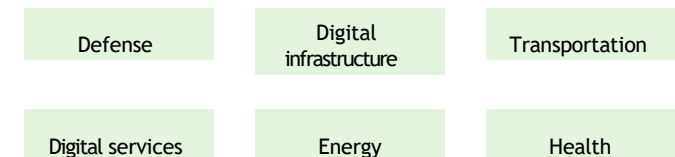
OCTOBER 2024

The obligations under NIS 2 cover several areas of cybersecurity, namely risk analysis, incident management and business continuity. In addition, security measures in the supply chain and evaluation of the effectiveness of security measures taken are required.

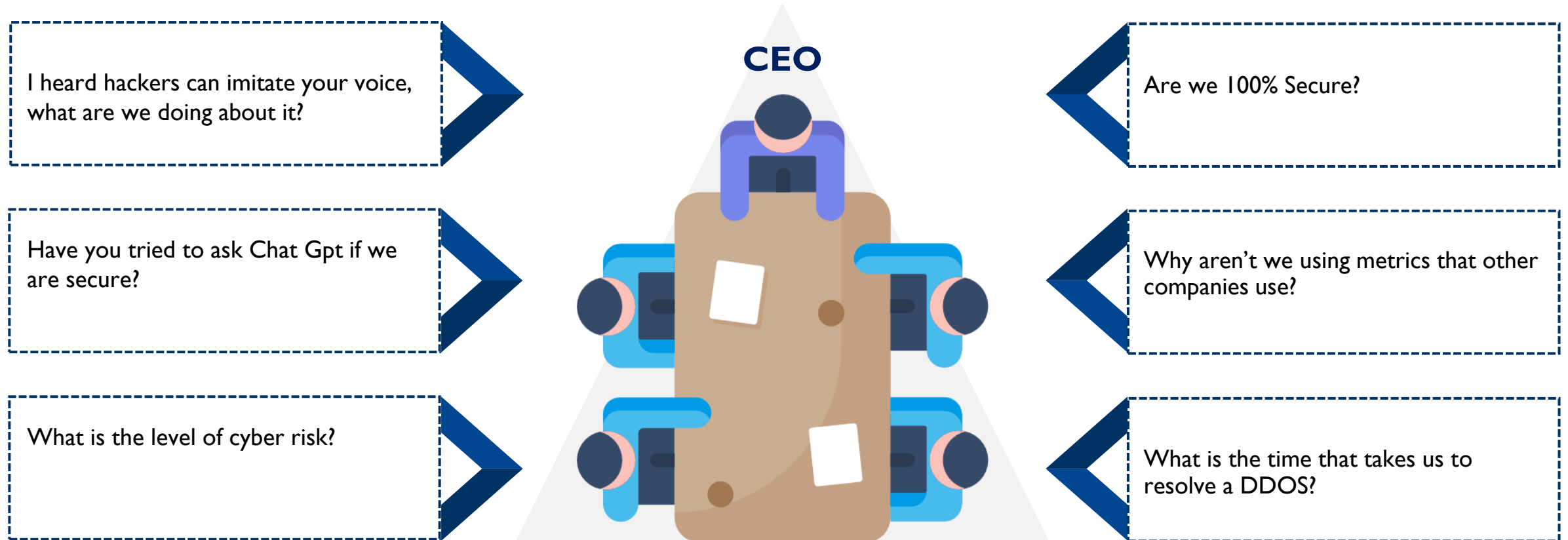
Finally, NIS 2 promotes information hygiene and training, human resource security and access control, and the adoption of multifactor authentication solutions.

Examples of NIS2 sectors.

ILLUSTRATIVE



Some of the questions you will have to answer as a CISO...



Looking at cyber from the outside, Dunning Kruger and strategic objectives

The Dunning–Kruger effect is a cognitive bias in which people with limited competence in a particular domain overestimate their abilities.

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources

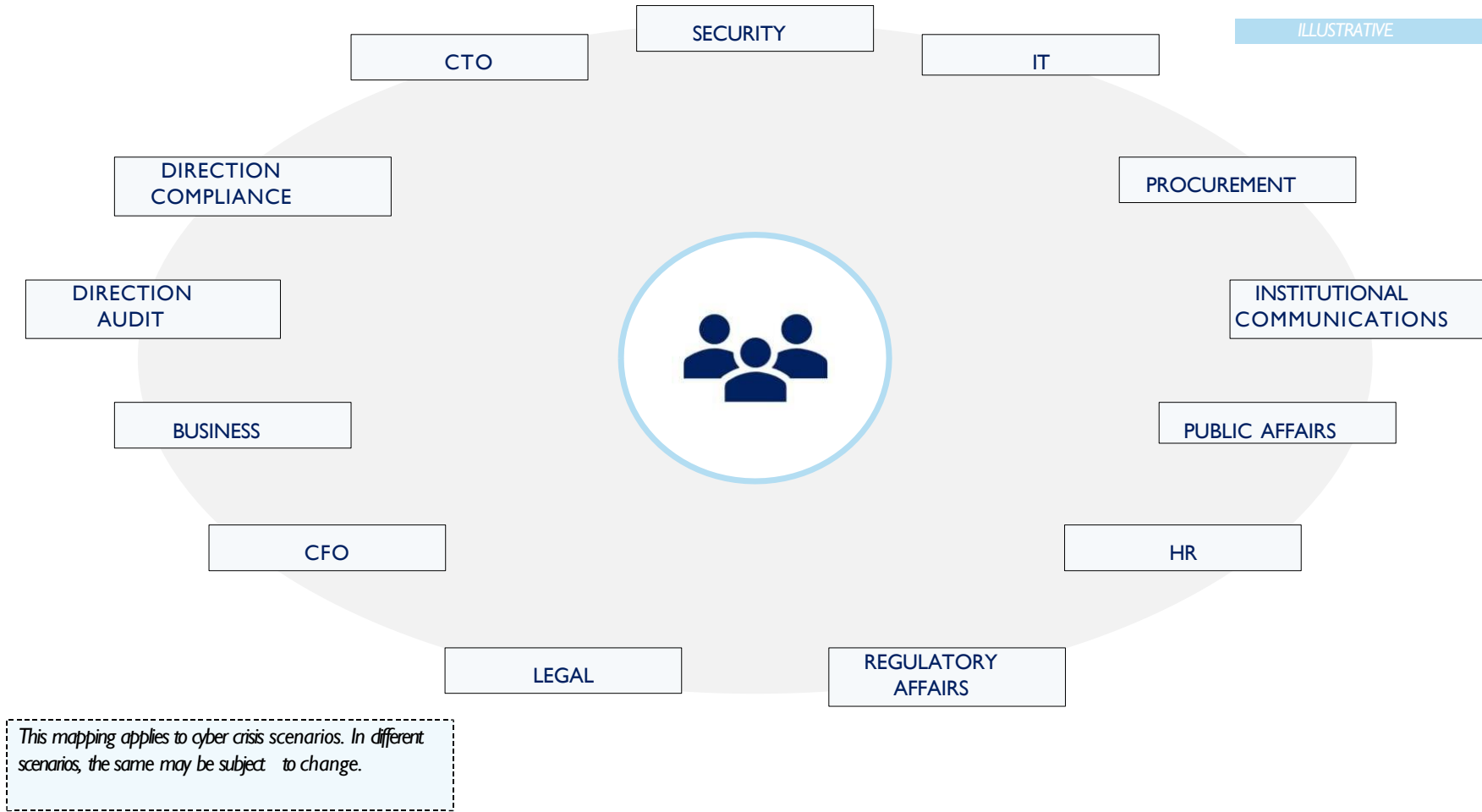
Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Event Triggered Execution (15)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Dynamic Resolution (3)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Remote Services (6)	Data from Information Repositories (2)	Encrypted Channel (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Replication Through Removable Media	Data from Local System	Fallback Channels
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Software Deployment Tools	Data from Network Shared Drive	Ingress Tool Transfer
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Group Policy Modification	Group Policy Modification	Network Sniffing	Network Share Discovery	Taint Shared Content	Data from Removable Media	Multi-Stage Channels
	Windows Management Instrumentation	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (6)	OS Credential Dumping (8)	Network Sniffing	Use Alternate Authentication Material (4)	Data from Removable Media	Non-Application Layer Protocol
		Hijack Execution Flow (11)	Impair Defenses (6)	Hijack Execution Flow (11)	Steal Application Access Token	OS Credential Dumping (8)		Data Staged (2)	Non-Standard Port
		Process Injection (11)	Indicator Removal on Host (6)	Impair Defenses (6)	Steal or Forge Kerberos Tickets (3)	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling
		Scheduled Task/Job (5)	Indirect Command Execution	Indicator Removal on Host (6)	Steal Web Session Cookie	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)
		Valid Accounts (4)	Masquerading (6)	Indirect Command Execution	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Remote Access Software
			Modify Authentication Process (3)	Masquerading (6)	Unsecured Credentials (1)	Query Registry		Man-in-the-Middle (1)	Traffic Signaling (1)
			Modify Authentication Process (3)	Modify Authentication Process (3)	Unsecured Credentials (1)	Remote System Discovery		Screen Capture	Web Service (3)
			Modify Authentication Process (3)	Modify Authentication Process (3)	Unsecured Credentials (1)	Software Discovery (1)		Video Capture	
			Modify Authentication Process (3)	Modify Authentication Process (3)	Unsecured Credentials (1)	System Information Discovery			

Cyber is inherently complex and often cannot be answered without technical explanations

In most cases cyber is not a business enabler, or at least top management does not see it this way

Top management has a different background and is required to keep the big the eyes on core business

The actors involved in managing cybersecurity in the enterprise



The strategic dimension of cybersecurity



The evolution of cybersecurity monitoring in the enterprise

Description

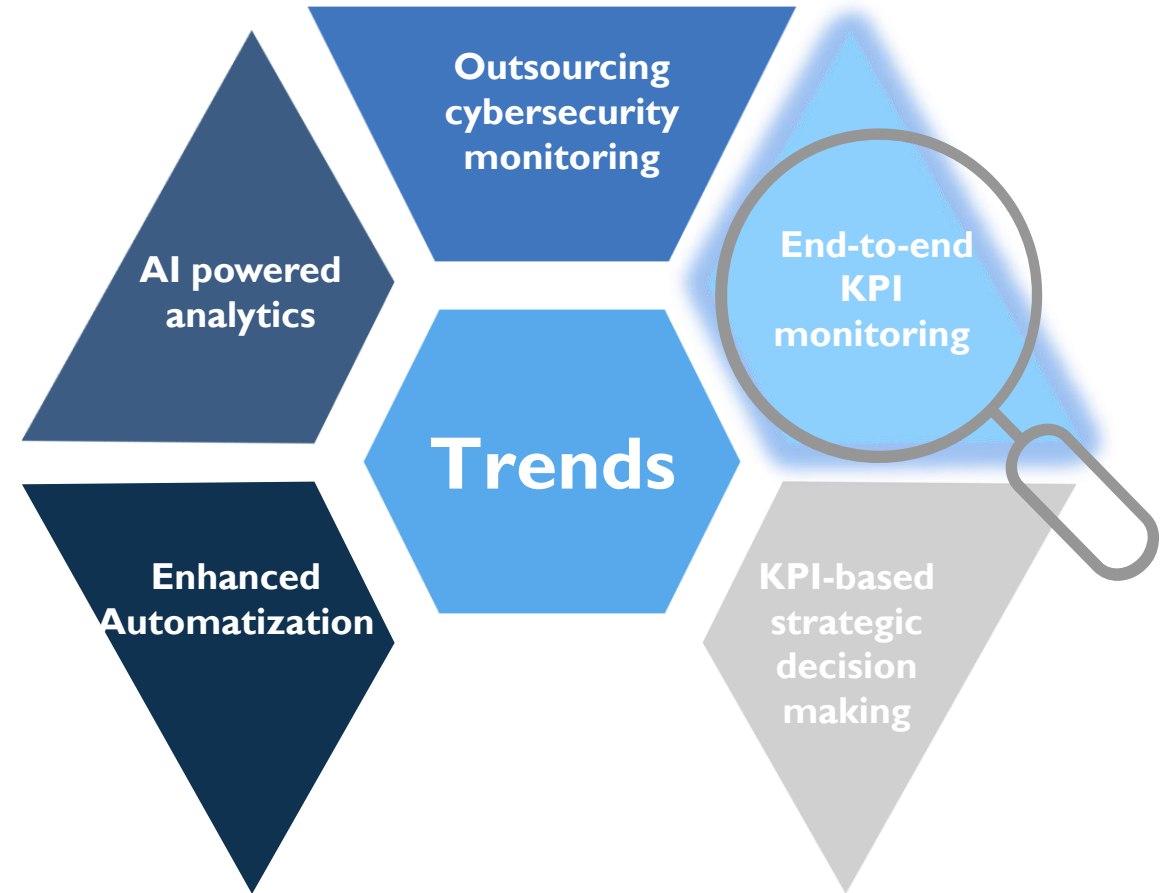
End-to-end KPI monitoring is a practice of involving all levels of the enterprise in the monitoring, surveillance and evaluation of cybersecurity-related KPIs.

Benefits

End-to-end KPI monitoring increases cyber awareness across all levels of the enterprise, helping to prevent threats and reduce risks, in a holistic sense. Executive participation can also facilitate the allocation of appropriate resources to cyber security enhance cybersecurity governance activities.

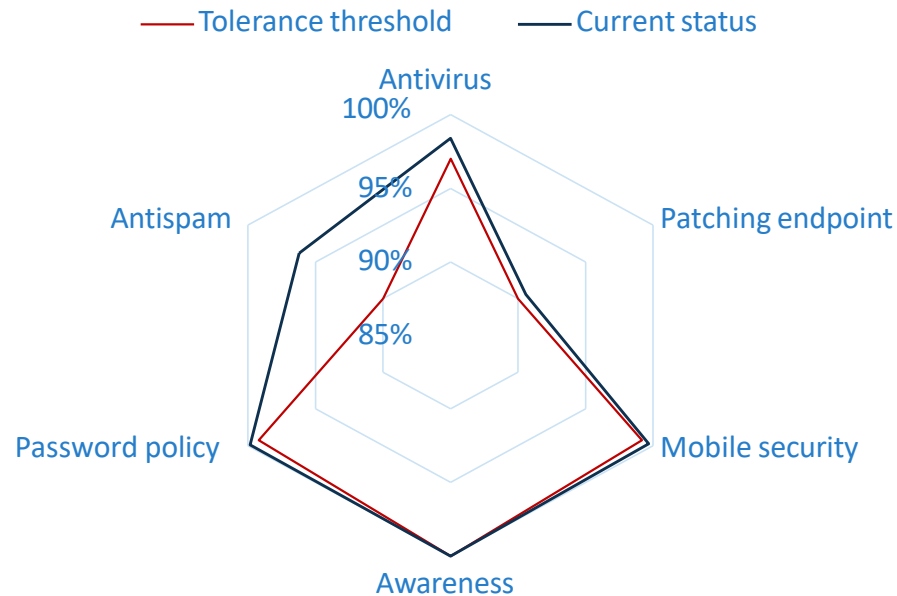
Applicability

The end-to-end KPI monitoring approach requires clearly defining the strategic, tactical and operational rationale and objectives to be observed in defining the appropriate narrative for the relevant stakeholders. In addition, fostering the correct interpretation of the insight provided by KPIs requires activating awareness projects with respect to cybersecurity issues at all levels of the company.



The current state of cybersecurity monitoring in the enterprise

The organization's cyber security posture is kept monitored through the constant measurement of a set of synthetic security indicators, identified according to international best practices (SANS CSC, Cyber Security Controls), which summarize the effects of the preventive and protective technological organizational measures taken.



All indicators are above target thresholds and in line with 2023 expectations. No incidents with real impacts on operational security of data and business processes were detected

TECH PROTECTION

Monitors the security of applications and devices. Ensures they are up-to-date, properly configured, and protected against the latest threats, reducing potential entry points for attackers

- **Antivirus:** 10,888 systems (7,842 Laptop/Desktop, 1,804 server age, 1,242 central servers)
- **Patching endpoints:** 12,145 systems (7,934 Laptop/Desktop, 2,168 server age, 2,043 central servers)
- **Mobile Security:** 12,051 systems (7,895 Laptop/Desktop, 2,128 server age, 2,028 central servers)

HUMAN PROTECTION

This indicator highlights the effectiveness of our employee account training and protection initiatives.

- **Antispam:** 11.8 Mln total input emails/month processed. 38,000 boxes (10k dir + 28k age)
- **Password Policy:** About 38,000 users (10k management + 28k agency)
- **Awareness:** : Preparation and activation of the new Course 2023 "Cyber Security Awareness.

CYBER HARDENING

This KPI focuses on reducing vulnerabilities within the infrastructure and applications. It indicates the effectiveness of initiatives to strengthen defenses and reduce attack surfaces.

- **Security Operations:** 10,987 systems (7,496 Laptop/Desktop, 3,491 server age)

KPIs with respect to business activity levels



Strategic



Macro-categories

Macrocategories are instrumental in aligning cybersecurity strategy with overall business objectives. These include indicators such as strategic positioning, employee awareness, and risk context.



Tactical



Categories

Categories are associated with macrocategories to articulate strategic objectives at the tactical level to provide cyber management guidelines to the functions involved.



Operational



KPI

Cybersecurity KPIs is represent with measurable indicators the corporate cyber posture and the applicable risk context.

The relationship between governance and monitoring in legislation and best practices



The **Digital Operational Resilience Act**, is a European Union regulation that aims to **improve the cybersecurity of financial institutions and the relevant cybersecurity ecosystem** by promoting shared digital operational resilience



IT governance framework that focuses on the **management and control of IT processes** to ensure **alignment of business objectives, control of risks, and maximization of benefits** from information technology



The **Cybersecurity Framework 2.0** is a **cybersecurity framework** developed to **guide organizations in protecting their systems and data** from cyber threats that provides a framework and guidelines for cyber risk management, breach prevention, etc.



MITRE ATT&CK provides several matrices regarding the **detailed picture of tactics, techniques, and procedures (TTPs)** used by threat actors. In addition, MITRE is a reference with respect to methodologies for evaluating metrics relevant to threat identification.




Set of **cybersecurity best practices** developed by the Center for Internet Security (CIS) to **help organizations protect ICT infrastructure and operations** including through reference controls



The **National Institute of Standards and Technology (NIST)** is a U.S. government agency that **develops and promotes guidelines and standards** to enhance both the technical and governance aspects of cybersecurity.

Some synthesis approaches between the business and the cyber domain regarding KPIs (COBIT)

Domain: Deliver, Service and Support		Focus Area: COBIT Core Model	
Management Objective: DSS05 - Managed Security Services			
Description			
Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.			
Purpose			
Minimize the business impact of operational information security vulnerabilities and incidents.			
The management objective supports the achievement of a set of primary enterprise and alignment goals:			
Enterprise Goals			Alignment Goals
<ul style="list-style-type: none"> • EG02 Managed business risk • EG06 Business service continuity and availability 			<ul style="list-style-type: none"> • AG02 Managed I&T-related risk • AG07 Security of information, processing infrastructure and applications, and privacy
Example Metrics for Enterprise Goals			Example Metrics for Alignment Goals
EG02 <ol style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of updating risk profile 			AG02 <ol style="list-style-type: none"> Frequency of updating risk profile Percent of enterprise risk assessments including I&T-related risk Number of significant I&T-related incidents that were not identified in a risk assessment

Some synthesis approaches between the business and the cyber domain regarding KPIs (MITRE – prevent/avoid)

Sub-Objective: Apply basic hygiene and risk-tailored controls	
Representative Activity and Corresponding Approaches	Possible Representative Metrics and Measures
PA-S1-A6: General (assumes standard practices for vulnerability scanning and patching)	<p>Average length of time to patch systems [MT-38]</p> <p>Average length of time to patch network components [MT-41]</p> <p>Percentage of systems in compliance with organizationally mandated configuration guidance [MT-39]</p> <p>Percentage of managed systems checked for vulnerabilities in accordance with the organization's policy [MT-55]</p> <p>Percentage of systems without “high” severity vulnerabilities based on Common Vulnerability Scoring System (CVSS) scoring [MT-56]</p> <p>Average length of time for the organization to mitigate identified vulnerabilities [MT-57]</p> <p>Percentage of managed systems for which an automated patch management process is used [MT-58]</p> <p>Average length of time from patch release to patch installation [MT-60]</p> <p>Percentage of cyber resources that are properly configured [MT-1]</p> <p>Frequency of audit record analysis for inappropriate activity [MT-42]</p> <p>Percentage of systems for which a defined security configuration is required [MT-62]</p>

The construction of relevant metrics and KPIs

Complexity in Research



Identification of Relevant Data



Alignment with Corporate Goals



Standards and Best Practice



Construction of the Metrics



Clear and Measurable Definition



Perimeter and Standardization



Validation and Replication



Creating an Understandable Taxonomy



Language and Terminology



Categorization and Organization



Training and Engagement

Data acquisition flows

GOVERNANCE CONTINUITY AND SECURITY				
DATA MANAGER	PROCESS	DATA ACQUIRED.	RECEIVING MODE	TOOL
MONITORING FUNCTION	Monitoring Incidents and Safety Events	Security events, logs, incidents	Pdf Report	SOC
GOVERNANCE CONTINUITY AND SECURITY	Report production	Organization and Supplier Ratings	Application	Security Scorecard, Bitsight
RISK MANAGEMENT	Assessment of impacts	Analysis of impacts	Report pdf	N/A
GOVERNANCE CONTINUITY AND SECURITY	Testing DR plan	DR results	Report pdf	N/A
GOVERNANCE CONTINUITY AND SECURITY	Vulnerability monitoring and pentesting	Vulnerability information	Application	Qualys

The validation of KPIs

KPI description

KPI	Metrics	Description (to complete the organization)
Scanning application	No. critical applications not traced to critical services	...

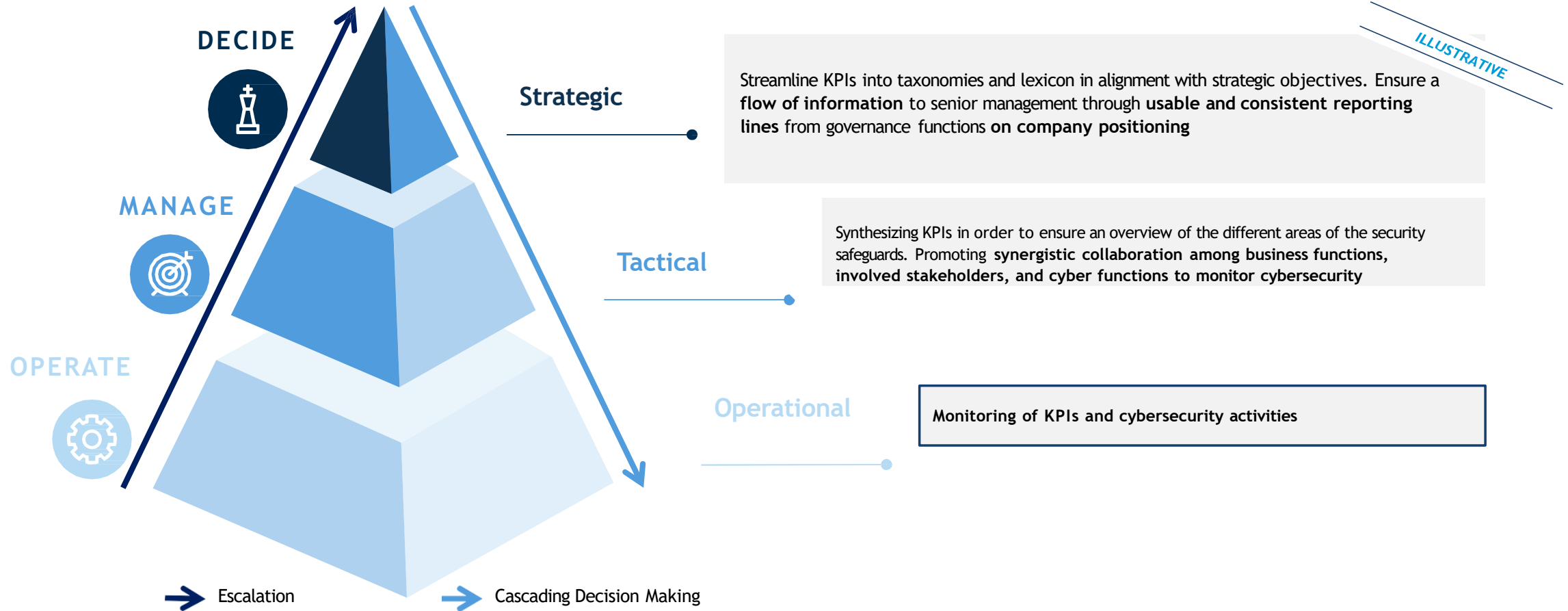
Market Benchmarks

KPI	Metrics	Operator 1	Operator 2	Operator 3	Operator 4	% of use
Scanning application	No. critical applications not traced to critical services	✓		✓	✓	75%

Regulatory references and best practices

KPI	Description and associated cyber risks	References to resilience goals
Scanning application	The objective of the KPI is to assess the proportion of externally visible critical applications in relation to total applications, providing an indication of potential exposure to security risks. A higher percentage indicates a potentially larger attack surface and a need to strengthen protection measures.	UN-S2-A1: Perform an impact analysis to identify critical assets or capabilities. RA-S1-A1: Restructure systems or subsystems to minimize the number of critical assets RA-S1-A4: Restructure systems or subsystems to improve defensibility in the face of anticipated changes in adversary capacity, intent, and targeting (including long-term)

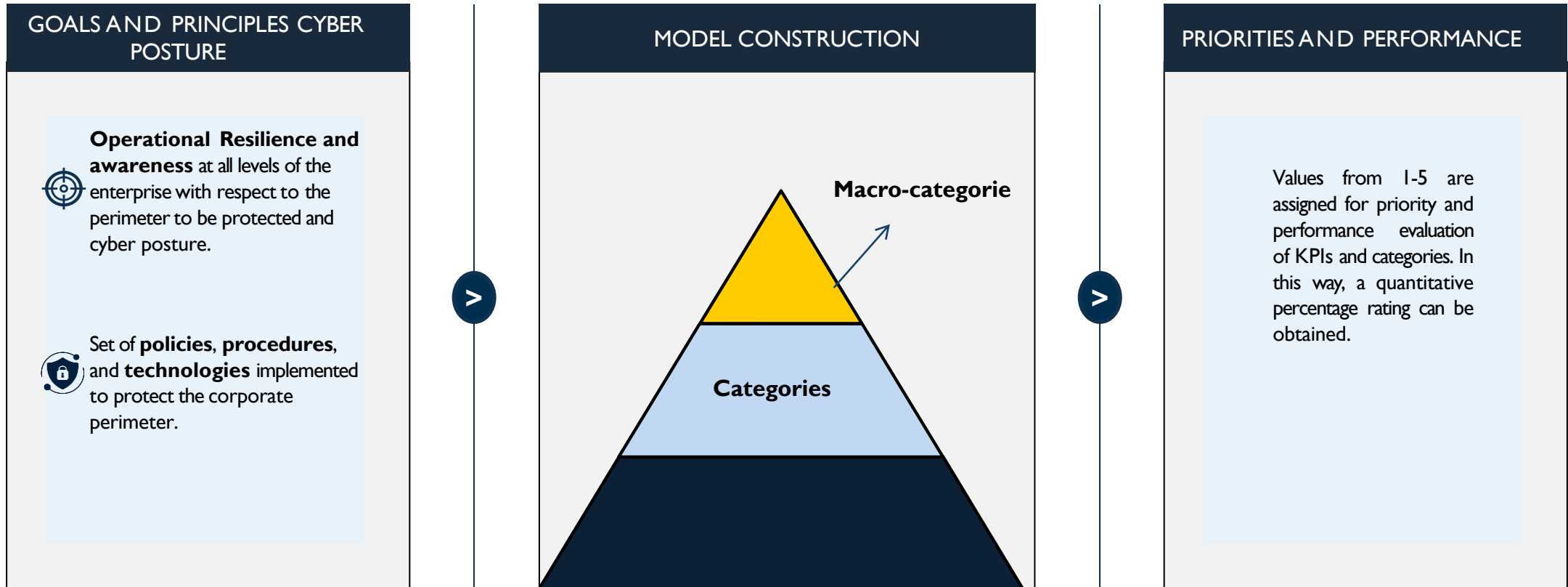
The positioning of KPIs against requirements



Methodology for building a strategic model

Based on the goals and principles of cyberposture, the categories and macro-categories of the proposed model were defined.

A methodology for ranking and aggregating KPIs was then applied:



Goal and principles of cyber posture

Goal

Perimeter protection by ensuring the integrity, availability, and confidentiality of applications and data within an organization through accurate identification and protection of the attack surface.



Principles of cyber posture

- **Monitor and protect the attack surface:** protection is about implementing strategies and measures to defend against attacks and preserve the integrity of data and applications. To succeed in this mission, it is essential to focus on the attack surface, which includes every digital and physical entity that could be exploited to conduct cyber attacks.
- **Update and verification:** In the constant evolution of threats and vulnerabilities, updating and verification are critical aspects of ensuring that the environment is continuously protected and safe from potential threats. This category includes practices and processes that involve the timely application of security patches and implementation of updates, as well as verification of the integrity and authenticity of those changes.



Goal

Protection of physical devices used by the organization (e.g., computers, mobile devices, servers, and other hardware) to ensure that these devices are configured and managed securely, minimizing the risk of threats and security breaches.



Principles of cyber posture

- **Monitor and protect the attack surface:** involves identifying and analyzing possible vulnerabilities and access points in physical devices used by the organization, including computers, mobile devices, servers, and other hardware.
- **Update and verification:** a key pillar in ensuring the security of physical devices within the organization. This category focuses on keeping devices constantly updated and verifying the integrity and security of these devices.



Goal and principles of cyber posture

Goal

Consolidate and improve the organization's cyber reputation through analysis, monitoring, and targeted actions, taking into account rating agency assessment, and ensuring adequate resources and projects to maintain a strong cyber reputation.



Principles of cyber posture

- **Positioning with Rating Agencies:** Assessing the organization's positioning with rating agencies reveals the company's cyber image in the marketplace, offering insights into its security posture and threat management. Periodic analysis helps identify strengths and weaknesses in security posture
- **Monitoring and Improving Cyber Operations:** To manage and improve cyber reputation, it is critical to adopt a proactive strategy. Constant monitoring, early threat identification, and responsiveness are supported by tracking tools and initiatives such as training, incident response, and transparent communication
- **Resource and Budget Allocation:** It is essential to allocate specific resources and budget for cyber reputation protection. These funds should cover monitoring tools, external consulting, and outreach activities. A dedicated team with expertise in crisis management and communication is also crucial to ensure a strong reputation over time



Goal

Mitigating the risks associated with the activities and behaviors of individuals in a business context by preventing incidents and vulnerabilities that could be exploited by malicious actors



Principles of cyber posture

- **1st line of defense- Authentication:** Multi-factor authentication (MFA) emerges as a **crucial pillar in the fight against human-based threats**. MFA successfully thwarts credential-based attacks, such as phishing, by requiring users to provide multiple levels of verification to gain access by combining elements they know, have, and are.
- **2nd line of defense-Filters and Safe Browsing Tools:** Companies can adopt safe browsing tools and filters to **protect users from malicious content and fraudulent sites, reducing the risk** of inadvertent interactions with online threats.
- **3rd Line of Defense - Cyber Training and Awareness:** To address the threat of ignorance or negligence, it is critical to **invest in cyber training and awareness programs**. Through workshops, courses and simulations, employees become the first line of defense, aware of best practices and able to recognize and respond to threats



Goal and principles of cyber posture

Goal

Create and maintain a **secure cyber environment** in which business resources, data and operations are protected from external and internal threats, ensuring the integrity, confidentiality and availability of information.



Principles of cyber posture

- **Attack surface monitoring:** Each account represents a possible entry point for attacks, so **granting access only to authorized individuals** and according to their **operational needs** is essential. Monitoring user activity enables **early detection of suspicious behavior**, reducing the risk of breaches.
- **Account and access protection:** Accounts with high privileges, such as those of administrators, pose a **significant security threat**, as they have **broad access to corporate resources**. Closely monitoring, restricting and regularly reviewing these accounts is crucial. The "**principle of least privilege**" approach, which assigns only the permissions strictly necessary to perform specific functions, helps mitigate the risk.
- **Account and privilege verification:** Accounts with high privileges, such as those of administrators, need to be validated through recurring procedures. Account verification involves **validating the identity of users, applying multi-factor authentication mechanisms**, and **constantly monitoring** for suspicious activity or potential security breaches.



Goal

Ensure that **cybersecurity is not compromised by interaction with and dependence on third parties**, such as vendors, partners, and other external parties, who may represent potential attack vectors or vulnerabilities for the organization.



Principles of cyber posture

- **Mapping Suppliers and Attack Surface:** In an interconnected business ecosystem, suppliers and third-party partners become a critical component of the attack surface. It is essential to perform **detailed mapping of all business relationships with third parties**, including the various ways they access and interact with corporate resources. This process identifies and assesses potential attack vectors, ensuring that these interactions are properly monitored and protected.
- **Verification and updating:** A key element in third-party security is ensuring that **vendors comply with security requirements** to update the catalog and assess the security of information and interactions undertaken with them.
- **Supplier Security Assessment:** Supplier security should be assessed and monitored regularly through **audits, reviews, and security rating tools**. Tools such as third-party security rating services can provide valuable insights into suppliers' security posture and help identify any vulnerabilities or deficiencies..



Goal and principles of cyber posture

Goal

Ensure **prompt identification of, response to, and recovery from cyber security events**, ensuring the **operational resilience** of the organization. This is achieved through well-defined actionables, regular drills and simulations, and recovery procedures, with a specific focus on ensuring the business continuity of the enterprise.



Principles of cyber posture

- **Readiness:** cyber crisis preparedness is a key element in mitigating the impact of an incident.
- **Recovery and Continuity:** after a cyber incident, rapid recovery and ensuring continuity of operations are critical
- **Learning and Adaptation:** develop specialized training sessions to learn from each incident and adapt response strategies.



Goal

Strengthen the resilience and robustness of IT systems and infrastructure against potential threats and attacks through the process of "cyber hardening." This involves identifying, assessing and addressing vulnerabilities, ensuring that the organization's digital assets are well protected.



Principles of cyber posture

- **Application protection:** Vulnerability mitigation is the **first line of defense in the hardening process**. This involves identifying, assessing and implementing measures to address vulnerabilities in systems.
- **Attack surface mapping: Simulations of attacks** carried out by **security experts** in order to assess the resilience of a system. Through such tests, organizations gain an **empirical understanding of their vulnerabilities**, obtaining a concrete visualization of the attack surface and the possible ways in which an attacker could exploit existing weaknesses
- **Verification and update:** Carry out verifications regarding the **security level of policy principals and controls** through testing, and periodically update internal procedures..



Goal and principles of cyber posture

Goal



Ensure that an organization's executives and C-level are adequately prepared and resilient to cyber risks. Executive resilience translates into informed decisions, effective leadership, and a competitive advantage in an increasingly digitized marketplace

Principles of cyber posture



- **C-level and executive training:** Through targeted training sessions, workshops, and crisis simulations, executives and C-level leaders can gain a holistic view of the threat landscape and best practices for managing them. Not only does this help them make informed decisions but also provide clear guidance to their teams in crisis situations.
- **Executive Empowerment:** The cyber expertise of an organization's leaders can build stakeholder trust
- **Cyber Strategic Planning:** A solid understanding of cyber challenges allows leaders to allocate resources more effectively. Trained executives are able to adequately assess cybersecurity needs, balance risks and opportunities, and allocate budget optimally.

Goal



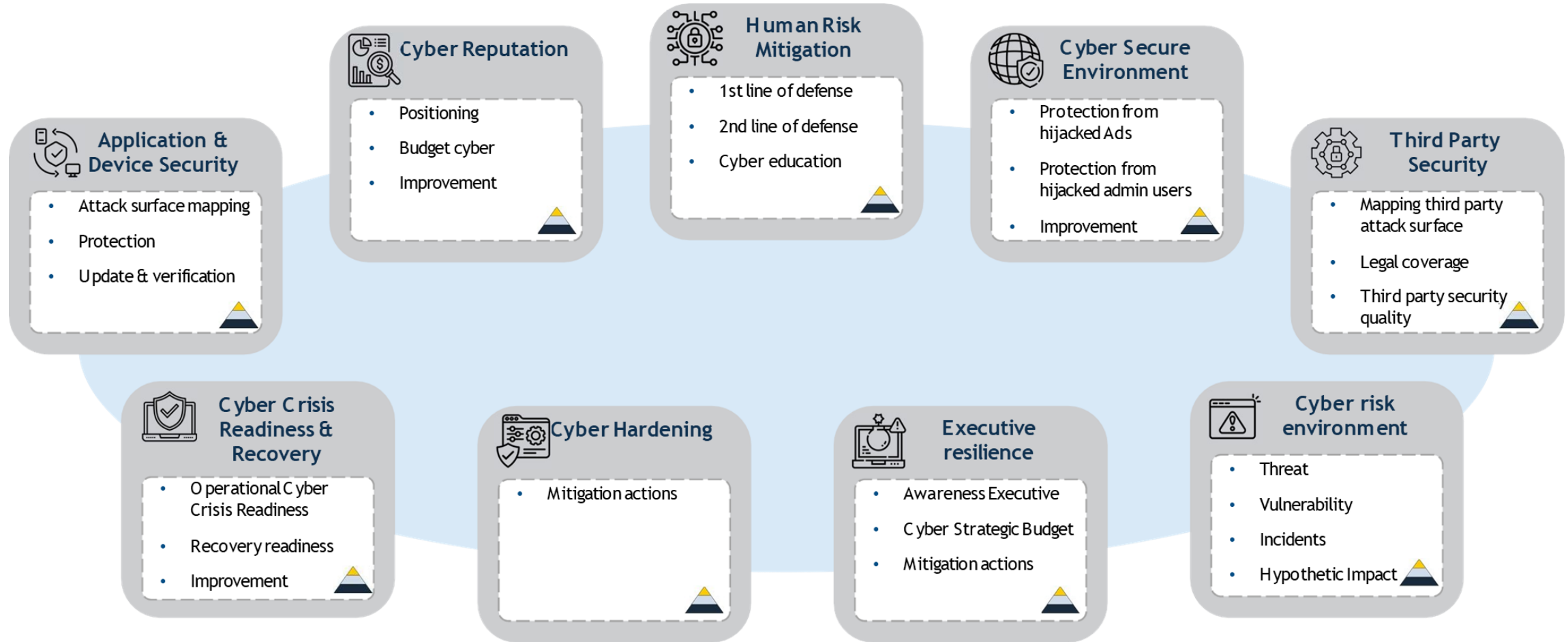
Understand the "cyber risk environment", i.e. the full spectrum of potential threats, incidents and impacts related to cybersecurity in order to proactively identify, assess and manage risks, protecting the organization and ensuring business continuity.

Principles of cyber posture



- **Prevention:** Prevention aims to identify, prevent, and mitigate cybersecurity threats before they can cause harm. This involves implementing security policies and procedures, protecting IT infrastructure, educating employees on security, and constantly monitoring for possible vulnerabilities and threats
- **Response:** This involves being prepared and able to respond quickly and effectively to cyber threats and security breaches. Response activities include threat assessment, damage mitigation, systems recovery, communication with stakeholders, and enforcement of emergency procedures

The construction of cybersecurity monitoring categories and macrocategories



From KPIs to categories and macrocategories - aggregation methodology

For the integration of KPIs into categories and macrocategories, a **MITRE-based** methodology for classification, metrics prioritization, and **cyber posture** assessment was adapted, represented below:

Assessment of priority	Performance evaluation
<p>Each metric is assigned a rating from 1 to 5 where the maximum indicates that keeping the indicator at a level below the defined risk tolerance target threshold is crucial for the organization. This allows KPIs to be prioritized within categories and in turn to prioritize categories within macrocategories to indicate which are most impactful in determining a score.</p>	<p>A rating from 1 to 5 is expressed where the maximum indicates that the activity monitored by the KPI is performed correctly in the operational and threat context. This weighting of the KPI within the categories is what allows a quantitative value to be expressed with respect to the organization's cyber posture, expressed succinctly through the macrocategories.</p>

Some KPIs

Cyber risk environment



KPI	Description and associated cyber risks	References to resilience goals
Monitoring of email attachments	Monitor exposure to the risk of malicious attachments (protection)	UN-S4-A1: Track effectiveness of defenses at different architectural locations [Analytic Monitoring: Monitoring and Damage Assessment].
Malware monitoring (email attachments) INBOUND and OUTBOUD	<p>The KPI aims to highlight the effectiveness of the antimalware mechanisms implemented by the company and the procedures for managing them.</p> <p>The lack of mechanisms to measure the effectiveness of these technologies could make their presence ineffective and highlight inadequate configuration.</p> <p>In addition, monitoring of attachments sent and received allows for the detection of attack patterns based on social engineering or the spread of malware.</p>	UN-S4-A1: Track effectiveness of defenses at different architectural locations [Analytic Monitoring: Monitoring and Damage Assessment].

Some KPIs

Cyber risk environment



KPI	Description and associated cyber risks	References to resilience goals
Major accidents	<p>The KPI is intended to highlight the presence of security incidents that appear not to have been addressed and resolved.</p> <p>Incidents that are not handled quickly expose the company to the risk of systems compromise.</p>	<p>UN-S4-A1: Track effectiveness of defenses at different architectural locations.</p> <p>[Analytic Monitoring: Monitoring and Damage Assessment]; Additional /diverted level of effort to maintain mission-essential functions for a given CCoA [MT-10].</p> <p>Percentage of data irrevocably lost due to an incident [MT-24]</p> <p>Average length of time to recover from incidents [MT-37].</p> <p>Percentage of incidents reported within required timeframe per applicable incident category [MT-46].</p> <p>Average length of time for the organization to recover from damage caused by a cyber incident [MT-53]</p>

Some KPIs

Third Party Security

Mapping third party attack surface

Legal coverage

Third party security quality

KPI	Description and associated cyber risks	References to resilience goals
Audit findings resolved	The objective of this KPI is to measure the proportion of audit findings that were effectively resolved relative to the total number of findings identified. A high percentage indicates an effective and timely response to issues identified during audits, demonstrating a commitment to address and mitigate issues that have arisen.	PA-S1-A6: General (assumes standard practices for vulnerability scanning and patching) Frequency of audit record analysis for inappropriate activity [MT-4]
Audit findings on suppliers resolved	The objective of this KPI is to measure the proportion of audit findings that were effectively resolved relative to the total number of findings identified. A high percentage indicates an effective and timely response to issues identified during audits, demonstrating a commitment to address and mitigate issues that have arisen.	CN-S2-A3: Coordinate response activities to ensure synergy rather than interference [Coordinated Protection: Orchestration] UN-S2-A5: Validate assumptions about dependencies and criticality by controlled disruption. 36 [Coordinated Protection: Self-Challenge]

Some KPIs

Third Party Security

Mapping third party attack surface

Legal coverage

Third party security quality

KPI	Description and associated cyber risks	References to resilience goals
Audit findings resolved	The objective of this KPI is to measure the proportion of audit findings that were effectively resolved relative to the total number of findings identified. A high percentage indicates an effective and timely response to issues identified during audits, demonstrating a commitment to address and mitigate issues that have arisen.	PA-S1-A6: General (assumes standard practices for vulnerability scanning and patching) Frequency of audit record analysis for inappropriate activity [MT-4]
Audit findings on suppliers resolved	The objective of this KPI is to measure the proportion of audit findings that were effectively resolved relative to the total number of findings identified. A high percentage indicates an effective and timely response to issues identified during audits, demonstrating a commitment to address and mitigate issues that have arisen.	CN-S2-A3: Coordinate response activities to ensure synergy rather than interference [Coordinated Protection: Orchestration] UN-S2-A5: Validate assumptions about dependencies and criticality by controlled disruption. 36 [Coordinated Protection: Self-Challenge]

Some KPIs

APPLICATION & Device Security

Attack Surface
Mapping

Protection

Update &
Verification

KPI	Description and associated cyber risks	References to resilience goals
Monitoring utilities without password expiration	<p>The KPI aims to highlight the presence of users with no associated password expiration.</p> <p>Lack of password expiration exposes the company to the risk of user compromise through attacks such as "brute-force" (by making numerous consecutive attempts to enter credentials) and sniffing (theft of login credentials or authentication tokens).</p>	<p>Password Policies Set and enforce secure password policies for accounts. ID: M0927 Security Controls: IEC 62443-3-3:2013 - SR 1.5, IEC 62443-4-2:2019 - CR 1.5, NIST SP 800-53 Rev. 4 - IA-5 Version</p>
Monitoring AdS users without password expiration	<p>The KPI aims to highlight the presence of AdS users with no associated password expiration.</p> <p>Lack of password expiration exposes the company to the risk of user compromise through attacks such as "brute-force" (by making numerous consecutive attempts to enter credentials) and sniffing (theft of login credentials or authentication tokens).</p>	<p>Password Policies Set and enforce secure password policies for accounts. ID: M0927 Security Controls: IEC 62443-3-3:2013 - SR 1.5, IEC 62443-4-2:2019 - CR 1.5, NIST SP 800-53 Rev. 4 - IA-5 Version</p>

Some metrics

Cyber risk environment - Prevention & response

Prevention

Response

KPI	Tech Integration	Frequency
MTTR Incident	//	Weekly
MTTR Third party incident	//	Settimanale
MTTRS – mean time to resolve escalation	//	Monthly
Escalated incident (critical) / total incidents	//	Yearly

Cyber Rating: Impacts and Relevance

What is Cyber Rating?

- Assessment of the organization's cybersecurity posture.
- Indicator for external actors with respect to the possible trustworthiness of the Organization.



What is it for?

- Assesses the quality of information security practices used by the Organization.
- Guide organizations in improving their security measures.
- Helps define the organization's positioning over time and relative to market peers.



V

IMPACTS ON AN ORGANIZATION

RISK MANAGEMENT
MANAGEMENT



STAKEHOLDER TRUST
TRUST



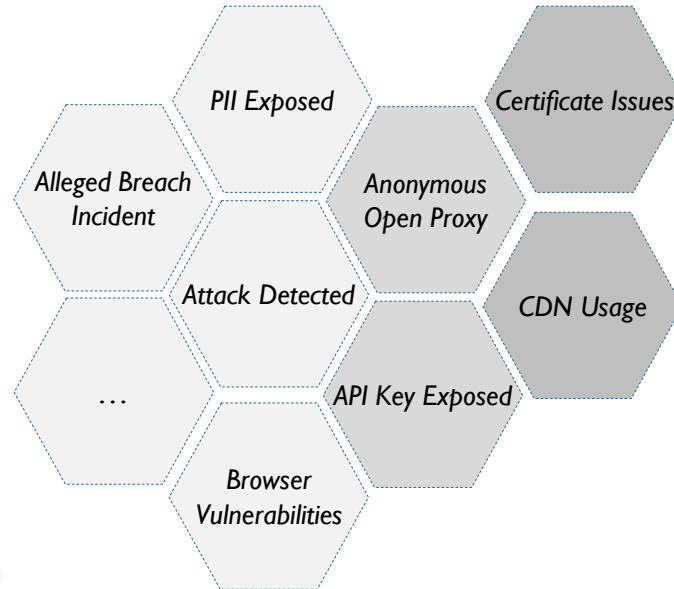
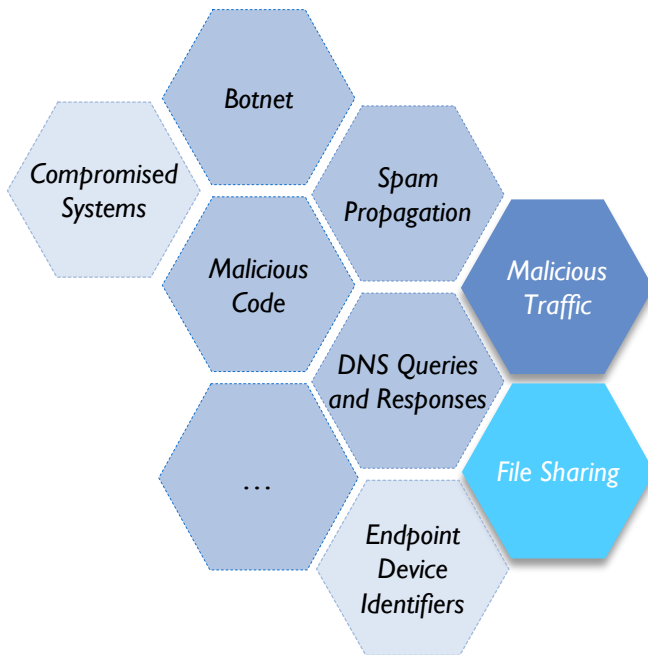
MERGER &
ACQUISITION



GREATER
TRANSPARENCY

Cyber Rating: how KPIs support maintaining optimal positioning

BITSIGHT



KEY SUCCESS FACTORS

✓ Analysis of metrics

Assessment about the garrisoning of KPIs adopted by cyber rating agencies to evaluate the organization

✓ Aggregation in the model

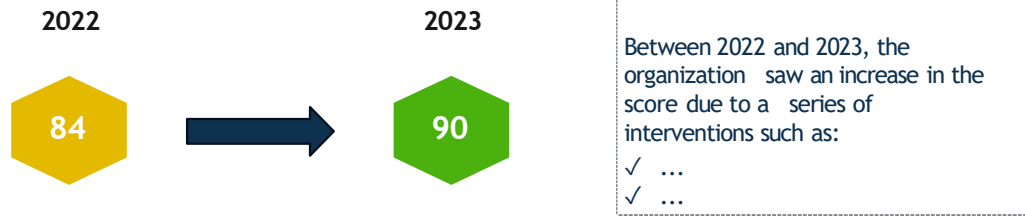
Strategic rationalization of cyber rating to monitor corporate reputation trends diachronically and relative to peers

Strategic cyber rating communication

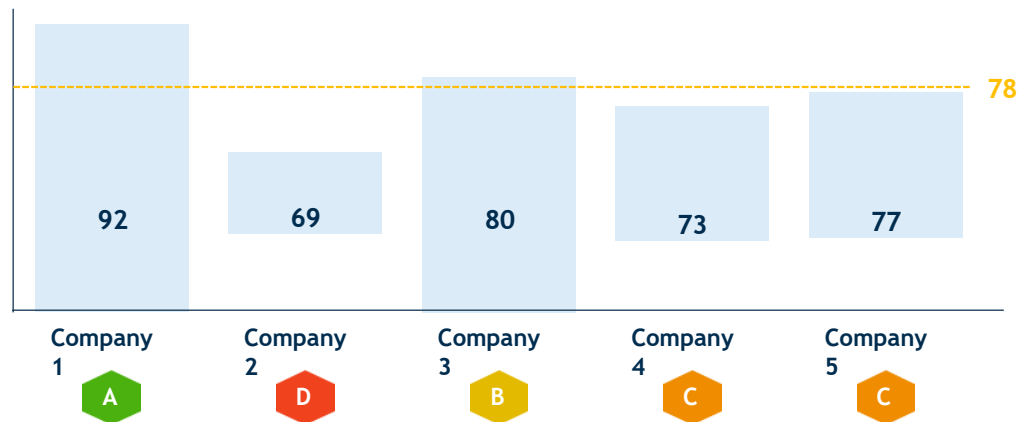
Cyber Reputation - Aggregate KPI



Cyber Reputation Trends



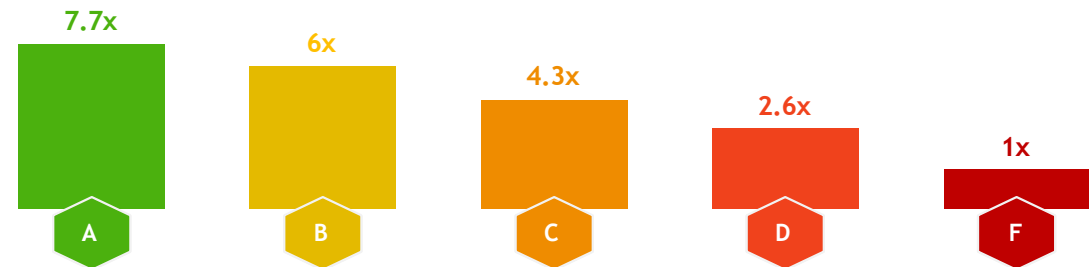
Market Positioning



INSIGHT

Illustrative not exhaustive

The scores given in the "Market Positioning" by *SecurityScorecard* (cyber rating company and partner of Fitch Ratings), show how the Organization ranks as a **Best Practice** compared to industry peers and in continuous improvement from previous surveys. Specifically, the Organization achieves a score of 90 by ranking within the security range of Grade A, which is 7.7 times less likely to experience a data breach than companies with an F rating.

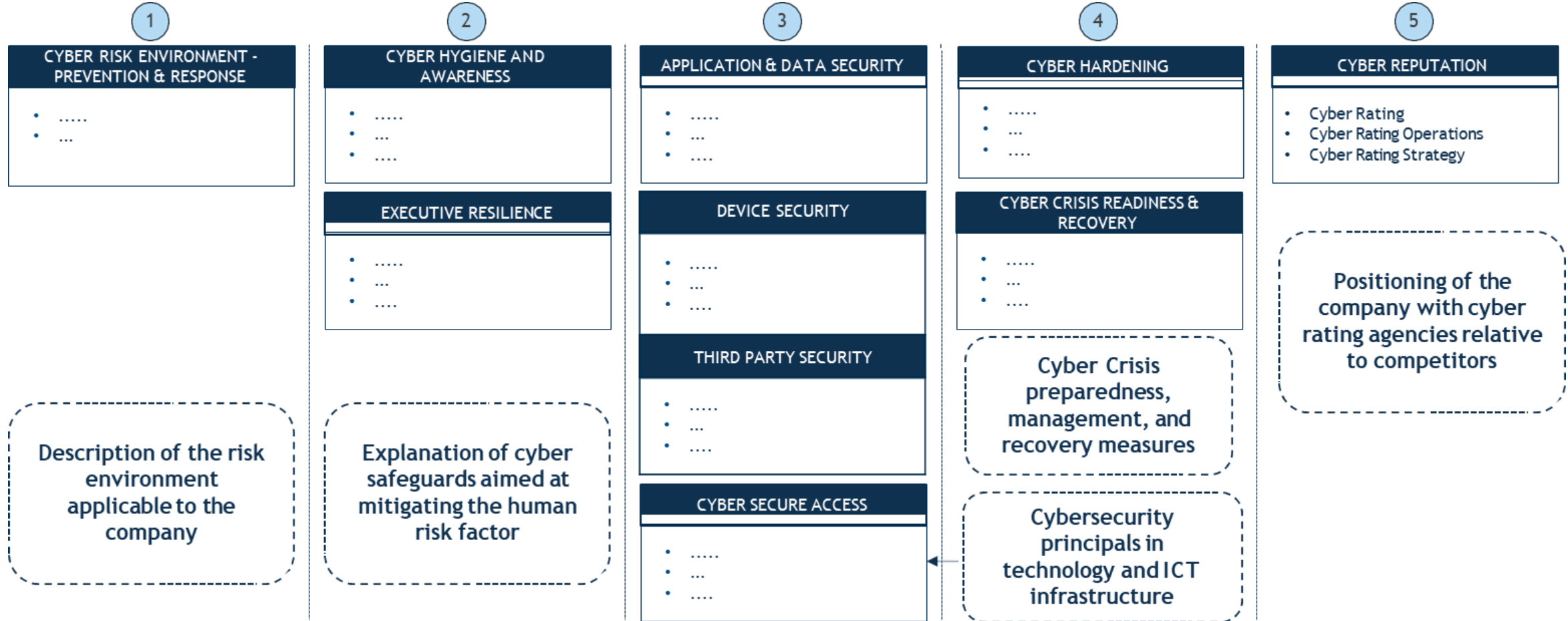


Methodology applied by SecurityScorecard

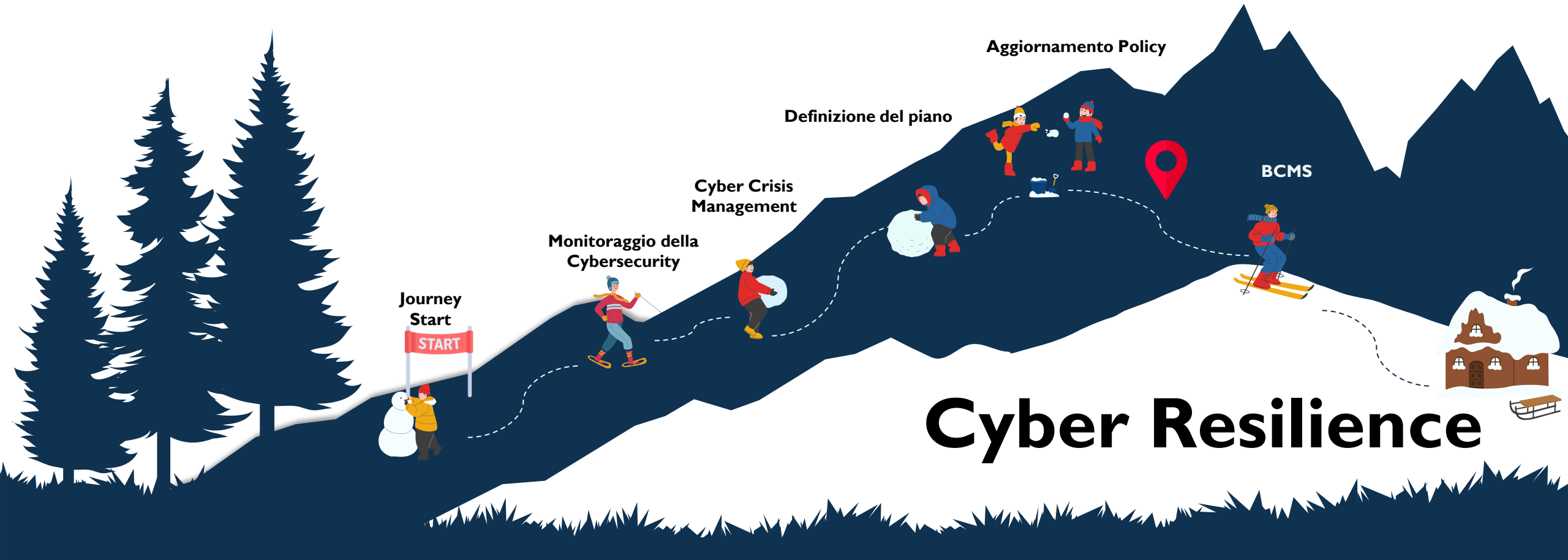
The total score, consists of an easy-to-understand letter scale which overall indicates an organization's level of security.

GRADE	A	B	C	D	F
SCORE	> 90	80 - 89	70 - 79	60 - 69	< 69

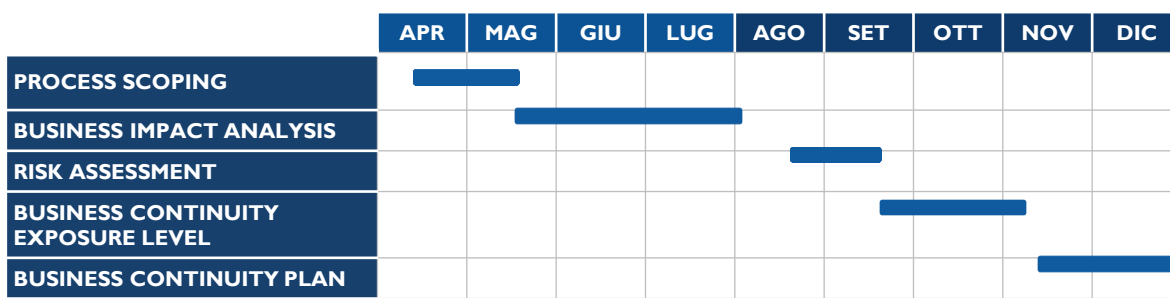
Strategic KPI communication: narrative for executives



Cyber monitoring as the first step of supporting resilience



Trying to merge KPIs with BC / DR functions




Deadline	Stato
XX/XX/XX	█
XX/XX/XX	█
XX/XX/XX	█
XX/XX/XX	█
XX/XX/XX	█

BC owner xxxxxx

BC Specialist xxxxxx

Inizio lavori BCM

Fine lavori BCM



RPO
Recovery Point Objective

L'RPO is the point in the time where you want your backup to be updated to

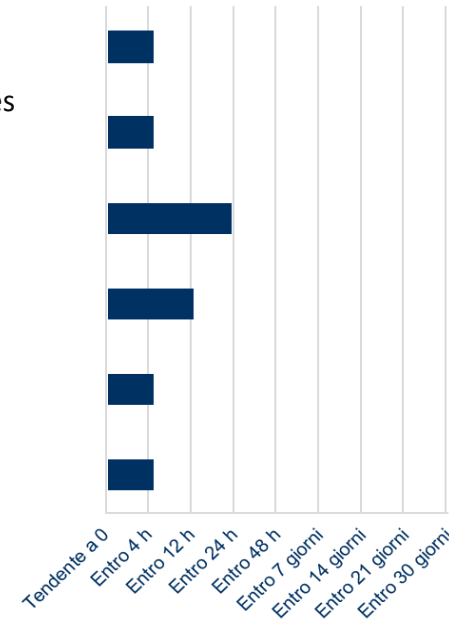
MTTR
Mean Time to Repair

How long it take the system to get repaired

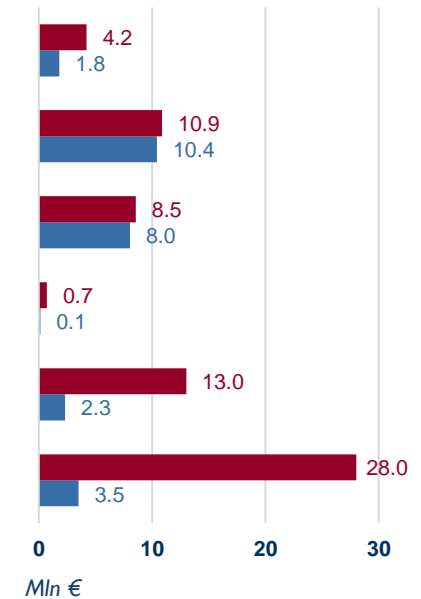
MTBF
Mean Time Between Failures

L'MTBF how frequently does a system experience malfunctions

Recovery Time Objective



Estimated Loss (financial)



What if the system is not yours?
How do you estimate reputational damage

Contacts

Thank you for your time

You can find some more info on the topics I am working on on [Cyber360](#)

Lorenzo Vacca

lorenzovacca.ita@gmail.com

<https://www.linkedin.com/in/lorenzo-vacca/>