Cyber Indicators Framework:

THE CISO AND SENIOR MANAGEMENT

Cisco, through its Country Digital Acceleration (CDA) investment programme (known as DIGITALIZA in Spain) is committed to accelerating digitalisation across the various sectors of the Spanish economy and society. A key focus is promoting awareness and understanding of cybersecurity practices within Spanish organisations. This document analyses how cybersecurity metrics can be used to help management committees and/or Boards of Directors understand the impact of these aspects on organisations' operations and corporate risk, thus aiding them in their decision-making.

AUTHORS

Coordinators:

Sergio Padilla
Toni García
Nuria Jordi

Participants:

Alberto Bernáldez
Amelia Maria Torres
Angel Ortiz
Carlos Martinez
José Manuel Rivera
Iago Crespo
Javier Pinillos
Josep Bardallo
Manuel Sánchez
Mariano J. Benito
Mario Encinas
Martín de Riquer
Oscar Sánchez

Editors:

Sergio Padilla
Oscar Sánchez

Project management:

Beatriz García

Layout and typesetting:

Susana Marín
Beatriz García

CONTENT

INTRODUCTION AND CONTEXT

1.

1.1.

PURPOSE OF THE DOCUMENT

There are many organisations that define governance models to guide their operations, based on their size, objective, mission and vision. In these models, a person or committee is typically responsible for making final decisions within each domain. One such domain is undoubtedly information security. This document will refer to all of these organisations, whatever their characteristics, as “organisations” and to these people or committees as “senior management”.

Moreover, organisations often have a role dedicated to managing information security, which can vary significantly across organisations. It may be a dedicated role or one whose functions comprise other responsibilities, and in the organisational structure it may fall within the technological, risk or compliance areas, among others. In any event, this role must exist and must report directly to senior management. This document shall refer to this role as “Chief Information Security Officer” or “CISO”.

It should be clarified that the responsibilities of senior management and those of the CISO are complementary but different: senior management has ultimate authority over the organisation’s cybersecurity decisions. It must ensure that the cybersecurity strategy is properly integrated into the corporate strategy. Other responsibilities include supervising and overseeing the implementation of cybersecurity risk management measures, making decisions and ensuring that the necessary resources are available. The CISO defines and implements the cybersecurity strategy, defines policies, manages information security risks on a daily basis and provides senior management with the necessary information for making decisions, among other activities. This separation of responsibilities is key to ensuring effective governance of information security.

The purpose of this guide is to give the CISO guidelines so that they can report to senior management data on the maturity of information security, in the form of a dashboard of key risk indicators (KRIs) and key performance indicators (KPIs).

However, it should be remembered that this is not just a technical aspect or the mere relaying of indicators, but a means for the CISO to effectively report so that senior management can fulfil its responsibilities. What are commonly known as “soft skills” therefore play an essential role.

Notwithstanding the above, this document also provides the CISO with a series of good practices and examples of types of indicators and explains how to choose the best indicators for each organisation and how to structure, measure and, not least, communicate them correctly to senior management. Having good metrics doesn’t necessarily imply knowing how to communicate them correctly. Defining good indicators enables us to transform the technical information obtained from the metrics into valuable data that will allow senior management to make informed decisions.

In this document the CISO will also find very valuable information on the different reporting models, how to adapt them to the various types of organisations regardless of their size or composition, how to tailor this reporting to each specific senior management and the skills needed for effective communication. The document also explains more management-oriented activities, how to retrieve the information from the different tools and sources, and how to transform it into metrics that allow us to properly reflect the indicators in the dashboards.

1.2.

IMPORTANCE OF REPORTING TO SENIOR MANAGEMENT AND THE ROLE OF THE CISO. REGULATORY CONTEXT.

The main information security goals for senior management involve understanding, guiding and supporting the organisation's general information risk strategy and current security stance. Senior management also has ultimate responsibility for ensuring that the organisation takes an appropriate stance against risk, which includes approving the cybersecurity strategy, allocating the necessary resources for its implementation and ensuring compliance with applicable rules and regulations. This accountability cannot be delegated, although it can be supported and complemented by the technical work of the CISO and their team.

Senior management also makes sure that appropriate controls, capabilities and measures are in place to provide reasonable protection and maintains accountability while encouraging continued progress. It is not expected to participate in the organisation's day-to-day information security and risk activity or have a thorough understanding of them, as this is the responsibility of the CISO and the teams that manage information security and risk. It generally forms its opinion and prepares its analyses and guidance based on the information provided to it by the CISO and other relevant actors in the organisation whenever they report to it. At that time, senior management will use the information received and the knowledge and understanding of those indicators to make informed decisions.

It is important for senior management to understand how cybersecurity risk can affect the organisation's business objectives and activities, and how vital it is to devote resources to reducing that risk and enhancing the organisation's cyber maturity.

Senior management should be aware that poor cybersecurity management can lead to serious legal, operational and reputational consequences, and that many regulatory frameworks, such as the NIS2 Directive, explicitly state that governing bodies have a direct responsibility over cybersecurity risks and should be actively involved in their oversight. Delegating is not enough: they must be informed and show diligence when making security-related decisions.

Article 20 of the NIS2 Directive reinforces this idea by providing that the management bodies of essential and important entities are to approve cybersecurity risk-management measures, oversee their implementation and be accountable for their compliance. It also requires members of management bodies to follow cybersecurity training on a regular basis to ensure that they have sufficient knowledge to understand risks and make informed decisions. These legal obligations highlight that cyber security is not just a technical issue, but a strategic responsibility that directly affects corporate governance.

Presentations to senior management can be stressful for many CISOs. The CISO, especially at the beginning, may be unsure of whether the information they provide will be useful and understandable for senior management and fear that, if not, senior management will lose interest in subsequent meetings. Good reporting to senior management is therefore essential for both the CISO and the organisation.

The CISO's soft skills undoubtedly play an important role. The CISO should be as comfortable with these skills as with hard skills, which relate to technical cybersecurity aspects.

The CISO's reporting should focus on providing clear, useful and relevant information for senior management decision-making. This implies understanding strategic leaders' priorities and structuring communication to respond directly to those needs.

Reports should be concise, comprehensive and informative, enabling decisions that align with business goals and support adequate risk management. However, the CISO report must necessarily refer to certain aspects (which are often also among most organisations' priorities). One of the most important is regulatory compliance. The CISO is responsible for understanding the regulatory framework that applies to its organisation and reporting to senior management the status of that compliance. There are rules and regulations that apply to almost all organisations and others that apply to certain sectors. The CISO must report the organisation's degree of compliance and explain the progress made in this area in successive reports.

“Reports should be concise, comprehensive and informative, enabling decisions that align with business goals and support adequate risk management.

1.3.

IMPORTANCE OF CYBERSECURITY INDICATORS AND A STANDARD FRAMEWORK

As we just explained, the reporting of indicators to senior management is an essential part of the CISO's functions that adds value to organisations' goals. But for that to happen effectively, and for senior management not to lose interest in these reports, the indicators of the dashboard must be relevant for senior management. Therefore, the success of reporting to senior management hinges on having good indicators based on objective data rather than the CISO's opinions. These indicators should be measurable, comparable with previous periods and actionable, enabling senior management to make informed decisions. Above all, their purpose should be clearly understandable. Mentioning that 70% of employees have completed cybersecurity training and awareness programmes is a relevant metric, but it is insufficient on its own. Senior management should also understand the level of risk and exposure entailed by that percentage and the potential benefits of investing resources to raise it to 80% or 90%.

This information makes it possible to evaluate the return in terms of reducing incidents, improving organisational resilience and regulatory compliance. This kind of information that goes beyond the specific metric is what the CISO's proposed indicators should provide.

To manage the information included in the report to senior management, the CISO should use a standard framework. This a tool that allows the CISO of any organisation to build a dashboard, identify the most appropriate indicators to this end, establish the best practices in managing these indicators and decide how to present them to senior management in the most appropriate way.

As mentioned above, each organisation is different. However, this standard framework is a guideline that can be adopted by any organisation, adapting it to its specificities and goals. It is undoubtedly a good starting point to help the CISO fulfil their important function of reporting to senior management.

These indicators are not an end in itself, but a tool for CISO and senior management to better understand cyber security and make informed decisions.

STANDARD FRAMEWORK
OF CYBERSECURITY INDICATORS

2.

2.1.

WHAT IS AN INDICATOR?

An indicator is any measure designed to track progress, facilitate decision-making or monitor performance against a set goal.

Information security indicators provide objective information on the security status and enable decisions to be made at the tactical, operational or strategic level. The aim is to measure and monitor security-related issues: how the security programme is being implemented, the level of maturity of the cybersecurity function and the degree of alignment with the organisation's strategy.

They can arise at various levels within the organisation:

At system level

Number of vulnerabilities per system, number of open ports.

At programme level

Number of security incidents, cost per incident.

At organisation level

Compliance with the strategic goals, Risk Level.

This allows CISOs to demonstrate the value of their area, as using the proper indicators enables them to explain how risks are reduced and show how security plans align with the organisation. Good communication can also increase collaboration between areas and the security budget.

An indicator should have the following characteristics:

Exact

It should collect the appropriate data within the established scope.

Precise

It should be numeric wherever possible. If qualitative, it should be based on objective criteria to establish a relative score.

Correct

It should be aligned with known standards and methodologies.

Consistent

It should allow the same result to be obtained regardless of who and how it is measured.

Time-based

It should be based on a fixed point of reference and allow its performance over time to be monitored.

Replicable

Under the same conditions and from different measuring points.

2.2.

CRITERIA FOR THE SELECTION OF INDICATORS

There are many indicators with different objectives. Indicators make it possible to understand the properties and behaviour of processes through defined, repeatable and easy-to-obtain measurements.

They can be classified according to different criteria:

1.

THE PURPOSE THEY PURSUE

Metric

A parameter than can be measured directly and monitored over time to determine trends.

KPI

A specialised parameter, generally obtained from several metrics, whose aim is to make decisions about the performance of a process or business.

Quantifiable metric

Measures progress towards a previously established goal or variations over time with respect to that goal.

KRI

A metric that makes it possible to identify, monitor and anticipate a risk.

Objectives and Key Results (OKRs)

Based on a defined objective, metrics are established that track progress towards achieving it.

2.

THE ASPECTS THEY MEASURE

Performance

Resources used.

Usability

Assesses whether the service is easy to learn and operate.

Degree of implementation

Shows the progress made in specific controls.is easy to learn and operate.

Impact

Assesses the impact of the security programme on the organisation's strategy and goals by tracking aspects such as costs saved and incurred, compliance levels, risk levels, etc.

Reliability

Ability to execute specific functions under certain conditions over a certain time window.

Functional adequacy

Assesses whether the functions meet the explicit and implicit needs required.

Effectiveness

Indicates how the processes and controls implemented achieve the established result.

Maintainability

Ability to efficiently and effectively maintain a process while it is being upgraded or repaired.

Efficiency

Ability to protect information assets.

- Confidentiality
- Integrity
- Authenticity
- Privacy
- Accountability

3.

THE LEVEL TO WHICH THEY REPORT

Strategic

At cost level

At goal level

Related to incidents and the risk level

Related to operational efficiency and maturity

Related to Compliance and Audit non-conformities

At the programme and project level

4.

THE TIME WINDOW THEY RELATE TO

Leading indicators

They are proactive and predictive. The information they provide allows a process or activity to be monitored, allowing the future expected performance of a system to be predicted or anticipated. This makes it possible to make decisions before the measured events materialise. They are difficult to define and monitor.

Lagging indicators

They show the current functioning of the systems based on already known data. They are easier to identify and monitor.

2.2.1. Strategic relevance

It is essential for cybersecurity programmes to be aligned with the organisation's global strategy and business goals. Through this strategic alignment, the cybersecurity function can be perceived as an enabler of sustainable growth, resilience and compliance, rather than a purely technical role. In this context, indicators are key tools for building an effective cybersecurity programme.

Measuring operational efficiency, costs and benefits helps confirm whether we are aligned with the organisation's goals. This requires focusing on the following questions:

- ***What are the main risk areas for the organisation and what is the plan to mitigate them?***
- ***What are the main risks to information assets?***
- ***Is the organisation sufficiently secure?***
- ***How does the organisation compare to others?***
- ***How secure is it today compared with before?***
- ***Does it have a security strategy?***
- ***What are the main security initiatives and how do they support the organisation's global mission?***
- ***How effective is the organisation's response to incidents and how is it tested?***
- ***Is the cybersecurity programme financially sustainable?***

It is important to know who this information is targeted at and to bear in mind:

What are the needs of the target?

- Identifying risks.
- Assessing costs.
- What is their general view of the security function.

What key messages do I want to share?

What is the purpose of the information?

- Informing.
- Persuading.
- Starting a discussion forum or debate.
- Showcasing the programme.

2.2.2. Measurement and comparability

Indicators should be addressed from two complementary perspectives:

TOP DOWN

Metrics are identified based on the established security goals to help determine whether they are achieved.

BOTTOM UP

Implemented security operations processes are analysed to identify which useful metrics can be obtained.

These metrics should help determine whether the organisation is doing the right thing and whether it is doing it the right way.

Magnitude means any characteristic that can be measured, whether directly or relatively.

The main magnitudes include:

NUMBER OF EVENTS

Vulnerabilities, incidents, alerts, open ports, attacks, affected components, critical risks, etc.

FREQUENCY

Of patch updates, control checks

TIME

Incident and vulnerability resolution, effort and analysis, resolution of non-conformities, etc.

PERCENTAGE

Of patched, vulnerable or supplier systems

Comparability refers to how datasets can be compared and is key to accurately interpreting data from different sources. Datasets can be internal or external. In internal datasets, the aim is to ensure consistent measurements throughout the organisation, using different tools and from different standpoints.

In external datasets, comparability involves being able to compare different datasets so that meaningful information and conclusions can be produced.

The key factors affecting comparability are measurement methods, variable definitions and data-collection techniques.

2.2.3. Scalability and adaptability

Scalability refers to a system's ability to handle an increasing number of components efficiently without the increase in demand compromising its performance and functionality.

Managing it requires:

- **Standardising the measurement process.**
- **Identifying possible bottlenecks.**
- **Automating as much as possible.**
- **Having flexible processes in the face of growth.**
- **Periodically revising the measurement process to confirm that it meets the desired goal.**

Adaptability is a system's ability to adjust and respond to changes while maintaining or improving its functionality, effectiveness or efficiency.

This concept can be considered from two points of view:

1. How indicators adapt to changes in the elements they measure. They must be able to handle changes in context without distorting or perverting the aim of the measurement.

2. Systems' ability to adapt to changes in terms of their functionality, efficiency, effectiveness, robustness, reliability and flexibility.

2.3.

TYPES OF INDICATORS

Indicators can be classified into two main categories:

KPIs

KEY PERFORMANCE INDICATOR

KRIs

KEY RISK INDICATOR

KPIs

KPIs are quantifiable metrics that reflect the performance of an organisation, area, process, etc. in relation to the established targets.

KPIs are essential tools for measuring the success and efficiency of the actions taken, allowing organisations to make informed decisions and adjust their strategies as needed.

Correctly defining and monitoring them allows organisations to make informed decisions and continuously improve their processes and results.

Key features of KPIs:

Specific: a KPI should be clearly defined and aligned with a specific goal, based on objective and verifiable data.

Achievable: KPIs should be realistic and be based on the organisation's operational capacity, to ensure that the goals are achievable with reasonable effort.

Measurable: KPIs need to be quantifiable. They should be expressed in figures or percentages to allow performance comparisons over time.

Time-based: It is important to set a certain time frame for evaluating performance.

Integrated: KPIs should be aligned with the organisation's strategic goals.

Comparable: KPIs should allow comparisons over time to identify trends and assess progress.

The main aim of KPIs is to provide information that allows decisions to be made and concrete actions to be taken.

KRIs

KRIs allow organisations to identify and measure potential risks that could affect the achievement of the organisation’s goals.

These types of indicators focus on predicting future risks:

- Early detection of risks, by identifying vulnerabilities ahead of the materialisation of such risks.
- Decision-making, by proactively adapting internal controls, improving efficiency and responsiveness.
- Continuous monitoring of trends to identify the accumulation of risks not detected by other means, and evaluation of the effectiveness of the mitigation measures taken.

Key features of KRIs:

Measurable: KRIs are quantifiable, expressed as percentages, numbers, etc., and it must be possible to measure them objectively.

Predictive: KRIs can be used as an early warning system, allowing organisations to anticipate problems before they materialise.

Integrated: KRIs are used to shape decision-making and must be integrated into the organisation’s internal controls and aligned with its internal goals.

Comparable: KRIs should be able to be compared internally and to industry standards.

2.4.

STRUCTURE OF AN INDICATOR

When defining KPIs and KRIs' structure, a series of steps must be followed to make sure certain key elements are considered.

↳ **Definition of the goal:** Indicators' purpose should be clearly established and it should be aligned with the organisation's strategic goals.

↳ **Identification of risks (for KRIs) / Identification of performance areas (for KPIs):** The specific risks/areas to be monitored should be determined.

↳ **Aspects to be measured:** The magnitude that will be measured should be defined, including the unit of measurement, frequency and relevant internal and external factors.

↳ **Quantification:** Indicators should be measurable and expressed in figures or percentages to facilitate comparison and analysis.

↳ **Relevance:** Indicators should be aligned with the organisation's critical goals to ensure they provide useful and actionable information.

↳ **Predictivity:** Indicators should be able to anticipate potential problems before they occur, allowing preventive measures to be taken.

↳ **Comparability:** Indicators should allow comparisons over time to identify trends and assess progress.

↳ **Actionability:** Indicators should provide information that allows informed decisions to be made and corrective action to be taken.

↳ **Time-based:** Indicators should be assessed over an established timeframe.

↳ **Data-driven:** Objective and verifiable data should be used for constructing indicators.

↳ **Clear communication:** Indicators should be defined and communicated in a clear and easy-to-understand manner to all members of the organisation.

↳ **Continuous monitoring:** A continuous monitoring system should be implemented to assess indicator performance and adjust strategies as needed.

↳ **Documentation:** Detailed documentation on indicators should be kept, including their definition, calculation methodology and historical results.

↳ **Review and update**: Indicators should be reviewed and updated regularly to ensure they remain relevant and effective.

2.5.

INDICATOR CATEGORIES

There are different approaches to defining the categories that should be included in a comprehensive dashboard which reflects the health and maturity of the organisation's information security.

A simple way of doing so is to divide indicators based on the main pillars of information security: confidentiality, integrity and availability. However, a more advanced classification could divide the indicators based on Information Security Management System (ISMS) domains, the international standards of the International Organisation for Standardisation (ISO), the ISO 27001 certification or the standard of the National Institute of Standards and Technology (NIST).

As mentioned above, the indicators should be adapted to the organisation's maturity level, adjustable within the dashboard and scalable. It is not about having many indicators, but about having indicators that deliver real value when reporting to senior management and consistently reflect changes in the organisation's maturity.

For guidance, the recommendation is to organise the indicators into six different subcategories:

1. **INCIDENT MANAGEMENT**
2. **REGULATORY COMPLIANCE**
3. **RESILIENCE AND CONTINUITY**
4. **AWARENESS AND TRAINING**
5. **RISK STATUS OF THE ORGANISATION**
6. **SECURITY STATUS OF THE ORGANISATION**

2.5.1. Incident management

ISMS and incident management best practices always strive for continuous improvement, following the Deming cycle1[1]

Within the incident management category there are indicators that measure the number of incidents over a certain period (the last quarter, year, five years, etc.) and the time to detection of the incident, mean time to acknowledge, time to respond, time to resolve, time to implement the lessons learnt during the incident, economic effort, time and resources devoted to incident resolution, reclassified incidents, recurrence rate, etc.

2.5.2. Regulatory compliance

In an increasingly regulated environment, compliance indicators are increasingly important for organisations.

Regardless of whether an organisation has obtained an ISO 27001 (or any other ISO information security standard) or NIST certification for its ISMS, different regulations could apply depending on the organisation's sector and size, including the Network and Information Systems Directive (NIS2), the Digital Operational Resilience Regulation (DORA), the European Union Cyber Resilience Act (EU Cyber Resilience Act), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Regulation (PCI).

In Spain, these international or European regulations and standards are complemented by regulations such as the National Security Scheme (NSS) or the Critical Infrastructure Law.

Moreover, the information security function may deem it necessary or relevant to implement indicators related to the General Data Protection Regulation (GDPR). While these indicators typically fall under the responsibility of the personal data protection officer, they may require technical controls for their implementation.

This guide does not aim to detail the indicators corresponding to each of these regulations, given their diversity and scope, but to provide an overview of the indicators that should be implemented in each organisation, depending on the sectoral or general regulations that affect it.

[1] The PHVA cycle, the Shewhart cycle and the Deming cycle are iterative designs and management methods for launching continuous improvement processes in firms producing goods and services.

2.5.3. Resilience and continuity

The resilience and continuity indicators provide information to senior management on the organisation's ability to recover and reduce downtime in the event of an attack. They also include information about the tests and drills carried out to prepare the organisation for a possible incident.

In terms of regulatory compliance, it is also possible to include controls related to ISO 22301 Business Continuity Management Systems, to manage the general risks to an organisation's business continuity.

The indicators should be aligned with the recovery time objective (RTO) and recovery point objective (RPO) defined by senior management, and show not only organisational redundancy (percentage of devices with backups, both in terms of user devices and information and storage servers, restoration times, etc.), but also these systems' efficiency based on cost or sustainability criteria (e.g. in line with ISMS Forum's Cyber Green Proof[2] Sustainable cybersecurity pact).

2.5.4. Awareness and training

This category covers all employee training, to demonstrate to senior management that employees have received ongoing education.

The indicators should show the courses followed by employees, the success rates, the percentage of employees who did not complete the training and the average of the scores obtained. Many awareness-raising and training tools also provide indicators by department, by country or even by sector.

Any tests performed by the organisation to measure employees' propensity to fall for scams that could allow an attacker to use them as entry points (such as phishing emails, QR codes, callbacks, etc.) should also be included in this category.

Awareness and training indicators should always guarantee anonymity and respect for employees by using aggregate data.

2.5.5. Risk status of the organisation

Key risk indicators (KRIs) show the level of risk posed by a specific threat or event and are often associated with a key performance indicator (KPI). KRIs should be based on a risk analysis and the organisation's risk map, and be aligned with its defined risk appetite. The ultimate purpose of KRIs is to proactively and consistently monitor risks to reduce the likelihood of the risk materialising.

Examples of KRIs include the risk of data breaches due to supplier leaks, compliance failures, human errors and database backup failures.

[2] https://master.ismsforum.es/pacto/

2.5.6. Security status of the organisation

One of the most common questions that senior management asks the CISO is: “Are we sure?”. Or when they see a news story about a large organisation that has been attacked: “Can this happen to us?”.

Beyond the fact that these questions are difficult to answer, the indicators of the organisation’s security status include the high-level indicators that measure the organisation’s general health and maturity.

Those indicators should also show how the organisation’s maturity level improves over time.

[2] https://master.ismsforum.es/pacto/

2.6.

EXAMPLES OF INDICATORS

In cyber security, indicators can be grouped into two main categories. Here are some relevant and representative examples:

1.

TECHNICAL INDICATORS:

External threats:

- Number of infections per device.
- Number of unresolved known vulnerabilities.
- Number of certificates not configured correctly.

Awareness:

- % of employees that have completed cybersecurity training.
- % of phishing simulation campaigns.

Operation:

- Number of components available and time they are available.
- Alert management.
- Mean time to resolve a vulnerability.
- % of systems patched.
- Etc.

Internal threats:

- Number of users with privileged access.
- Number of days between notification of a user's departure and the removal of access.

Incident management:

- Mean time to resolve an incident.
- Number of analyses performed.
- Number of incidents reported.
- Etc.

Audit and Compliance:

- Mean time to resolve a non-conformity.
- Number of compliances per project.

Supply chain:

- % of third-party software scanned before roll-out.
- Frequency with which third party controls are verified.
- Etc.

2.

SECURITY GOVERNANCE INDICATORS

Level of adoption of the cybersecurity programme:

- % of planned vs implemented security projects.
- % of covered services and assets.

Operational efficiency:

- % of incidents reported.
- Mean time to resolve.

Alignment with business value:

- Number of customers and suppliers affected by incidents.
- % of services affected.
- % of suppliers included in the security programme.

Level of governance:

- % of IT functions covered.
- % of exceptions vs risk management.
- Security-related KRIs.
- Progress in complying with security targets (%).

Risk mitigation:

- % of compliance with security policies.
- % deviation from security baseline.
- Severity of exceptions.

Costs:

- % of IT allocated to security.
- % of allocated vs consumed budget.
- Etc.

REPORTING MODELS AND DASHBOARDS

3.

In increasingly complex, uncertain and data-driven corporate environments, senior management reporting models have become a strategic tool for informed decision-making. An effective report not only presents information but also translates data into actionable knowledge. This is particularly relevant in the case of critical functions such as cyber security, where the CISO plays a key technical and also strategic role.

The fundamental principles of effective reporting, such as strategic relevance, clarity, focus on KPIs and effective presentation, are essential to ensure that senior management can swiftly interpret the business position and anticipate risks. In this setting, dashboards become vital instruments that must be designed with precision, visual narrative and a focus on value rather than data volume.

The CISO – traditionally perceived as a technical role – has evolved towards one that can become fully integrated into senior management. The role should be considered as just one more part of the business, whose purpose is not only to protect but also to facilitate business through cyber risk management aligned with the organisation’s strategic goals. This means that the CISO must be able to clearly communicate, through executive reports and dashboards, the cybersecurity position, emerging threats, the level of exposure and, above all, the potential impact on operational continuity, reputation and profitability.

In many organisations, the CISO no longer reports only to the CIO (if that was the case, it was quite common), but participates directly on management committees, reporting to other C-Level executives, to the CEO or even to the Board. This proximity to senior management requires that communication be clear, direct and business-oriented. The CISO must facilitate informed decision-making on technological and cybersecurity risks, allowing the organisation to take risks in a conscious and controlled manner, rather than avoiding them out of ignorance.

In short, clear and concise reporting to senior management is not only a matter of form but also of substance. It is the basis for a strategic conversation in which cyber security is no longer an isolated topic but rather a key enabler of business growth, innovation and resilience.

3.1.

PRINCIPLES FOR EFFECTIVE SENIOR MANAGEMENT REPORTING

The effectiveness of a senior management reporting model is not measured only by the amount of information it presents but also by its ability to facilitate strategic decision-making in an agile and informed manner. The essential principles that should guide the design and presentation of these reports are explained below.

1. Strategic relevance

Senior management needs information aligned with the organisation's strategic priorities. This means that the reports must answer key business questions: Are we moving towards our goals? Where are the main bottlenecks or risks? Which areas require immediate intervention?

Operational metrics or details that do not add value to the strategic vision should be avoided. Instead, priority should be given to information that enables assessment of compliance with strategic pillars such as growth, efficiency, innovation, sustainability, client experience or digital transformation.

2. Clarity and brevity

Senior management time is limited, and there might also be agenda issues, so time for presenting and reporting cybersecurity and risk status is also limited. In consequence, good executive reporting must eliminate the superfluous and prioritise clear and succinct communication. This means:

- using executive language, avoiding unnecessary technical jargon;
- including titles or insights for each block or chart;
- keeping reports short (e.g. a maximum of 10-15 pages or screen views);
- including executive summaries to present the general picture in just a few minutes.

Less is more: concision does not imply a lack of depth, but an intelligent selection of what is relevant for senior management.

3. Focus on key performance indicators (KPIs)

KPIs are the backbone of executive reporting. KPIs that are truly critical for the organisation must be selected.

Each KPI must include:

- its current value and a comparison with the relevant goal or benchmark;
- its trend over time;
- predefined thresholds that denote control, alert or critical status;
- a contextual analysis that explains possible deviations and corrective measures.

KPIs should be capable of transforming data into information and should enable your audience to transform information into relevant and informed decisions.

5. Data integrity and traceability

Trust in the information presented is essential. To ensure this trust, reporting must be based on accurate, complete data from reliable sources. In addition, it must be possible to:

- identify the source of each item of data or metric, through accessible legends or metadata;
- trace the data transformation to the final indicator.

It is also essential to ensure that the data have been validated and verified prior to publication.

A single inconsistency can cast doubt on the entire report and compromise strategic decisions. In this respect, data that are nuanced or not entirely clear could generate a debate, at which point the reporting focus would be lost.

4. Visibility of risks and opportunities

Effective reporting should not only present the current position, but should also include a vision, projecting future scenarios. This entails:

- identifying emerging risks (operational, financial, regulatory, reputational, etc.) and their potential impact;
- visualising strategic opportunities: new business lines, efficiency gains, synergies, alliances, etc.;
- offering a cross-cutting view, showing how a risk in one area can affect other business dimensions.

Including this proactive dimension allows senior management to anticipate situations rather than just react to them. This will provide important leverage to defend cybersecurity strategies and plans, enabling resources to be allocated to such a critical area.

6. Frequency and consistency

A good reporting model requires a defined frequency that responds to control and decision-making needs: for example, weekly for monitoring of critical operations, monthly for overall performance and quarterly for strategic review.

In addition, a consistent report format, structure and presentation facilitate quick reading, comparison with past reports and pattern identification. By contrast, frequent changes in design or indicators hamper reading and undermine a report's effectiveness.

7. Adapting to your reader

Not all executives require the same depth or visualisation of information. A CFO may be more focused on financial aspects, while a CEO seeks a global, cross-cutting view of the business.

3.2.

KEY DASHBOARD COMPONENTS

Dashboards are an essential tool for strategic, operational and financial monitoring of an organisation. Their value lies in their ability to condense and clearly present huge volumes of information, enabling assessment of the general business position and informed decision-making. To fulfil this purpose, they must be built on a solid architecture comprising the following key components:

1. Linked strategic goals

All dashboards must be clearly linked to the organisation's strategic goals. Each metric or graphic presented must answer a specific strategic question: How is our strategy execution going? Which indicators alert us to possible deviations?

This alignment ensures that dashboards become an effective management tool rather than just an accumulation of data.

2. Key performance indicators (KPIs)

KPIs are the core component. They must be selected based on their relevance, representativeness and capacity for action. Some essential aspects include:

- clear definition: what they measure, how it is calculated and why it is important;
- update frequency: daily, weekly, monthly, etc.;
- unit of measure and associated targets: establishing acceptable ranges, goals and alerts;
- appropriate presentation: using charts, tables, traffic lights or speedometers to facilitate quick reading.

Only the most significant KPIs should be selected, to avoid "infoxication".

3. Analysis dimensions

An effective dashboard allows you to view indicators from different perspectives or dimensions: by business unit, region, channel, client segment, product, etc.

These dimensions allow you to detect patterns, root causes and opportunities for improvement that would not be visible in an overall picture. They are also conducive to more granular and focused management.

5. Performance alerts and traffic lights

Although there has been some debate about the risk of oversimplifying reports to senior management, visual alert systems are still a recommended option. Traffic lights in their different forms, alert icons or priority tags help to quickly identify critical situations or areas under control, although how they are used will depend on the CISO and audience preferences.

These alerts can be configured according to previously defined thresholds, in all cases aligned with risk tolerance and business goals, and can be adapted to the level of detail and formality demanded by senior management.

4. Baseline and time profile

To correctly interpret any indicator, it is important to know how it has evolved over time. The dashboard should include:

- comparisons with the previous period (month, quarter, year);
- comparisons with the goal or budget;
- industry benchmarking (where applicable).

This approach allows trends, seasonal patterns or structural deviations that require attention to be identified.

6. Narrative and context

Each indicator should include a brief explanation that contextualises how it has evolved: What is affecting it? What actions have been taken? What are the future prospects?

Dashboards should include brief notes, insights or integrated analyses (for example, through tooltips or text fields) that enrich their informative value and prevent misinterpretations.

3.3.

VISUAL DESIGN AND PRESENTATION OF INFORMATION

Visual design is not a secondary aesthetic consideration, but rather an essential component of effective senior management reporting. Presenting information in a well-designed format enables better understanding, reduces the time required for analysis and focuses attention on the most important points. By contrast, poor design can lead to misinterpretations or visual fatigue or even to the report being ignored.

The following are the fundamental criteria for effective visual design.

1.

CLARITY ABOVE ALL ELSE:

The main function of visual design is to facilitate understanding. This entails:

- avoiding the excessive use of colours, shapes or unnecessary visual effects;
- using legible and appropriately sized fonts;
- presenting the information in descending order, highlighting the most important points;
- using blank spaces strategically to avoid visual saturation.

There must be a reason for every graphic element used and they must contribute to the information goal.

2.

APPROPRIATE CHICE OF CHARTS

Each type of data requires a specific type of chart that will facilitate its interpretation:

- bar charts: ideal for comparing values between categories;
- line charts: useful for showing trends over time;
- pie charts: advisable only for simple proportions (and a small number of elements);
- speedometer or thermometer type indicators: good for displaying KPIs with thresholds;
- heat maps or matrices: useful for showing levels of intensity or correlations.

Unnecessarily complex or decorative 3D graphics that hinder reading or distort data perception should be avoided.

3.

CONSISTENT VISUAL CODING

The use of colours, icons and shapes should be consistent throughout. Some key recommendations:

- use colours associated with clear meanings (green = positive, red = negative, amber = alert);
- don’t go overboard: three to five main colours are usually sufficient;
- use easily recognisable standard icons or labels (e.g. alert triangles, compliance tick-boxes);
- avoid using similar colours for indicators with different meanings, especially for visually impaired (including colour blindness) audiences (consider accessibility).

Visual coherence helps create cognitive patterns that facilitate interpretation.

4.

FOCUS ON THE VISUAL NARRATIVE

A good design not only presents data but it also tells a story. The order of the elements and how they are grouped and emphasised should guide the reader to the main conclusions. For instance:

- include clear titles with the main message ("Sales up 15% on the previous quarter") rather than generic ones ("Sales performance");
- arrange items from left to right and from top to bottom, in the natural reading order;
- group related indicators together, to facilitate reading by thematic blocks (finance, clients, operations).

This visual narrative transforms a dashboard into a strategic communication tool.

5.

MINIMISE COGNITIVE LOAD

The design should facilitate decision-making. Excessive mental effort should not be needed to interpret the data. Some recommended practices:

- avoid overloading dashboards with too many KPIs or charts in a single view;
- use logical groupings and visual separators to organise the information;
- prioritise the key data and leave the details for a second layer or expanded view.

A clean, intuitive and executive-focused design maximises the impact of the report.

3.4.

PERSONALISATION ACCORDING TO THE TARGET AUDIENCE

(CEO, CFO, CIO, MANAGEMENT COMMITTEE, BOARD OF DIRECTORS, ETC.)

It is important to identify the target audience for cybersecurity indicators: what are their interests, needs, concerns and knowledge in this area?

The CEO and the management team need to consider the progress and maturity of the organisation's cybersecurity programme, as well as its effectiveness and alignment with the overall strategy, including risk appetite and an appropriate risk management methodology. This will instil confidence, for example, enabling the CEO to report to the Board of Directors an accurate picture of the present situation and of the necessary actions to be taken in the event of a crisis or unfavourable indicators.

As the senior body that steers the organisation's strategy and oversees management actions to meet the strategic goals, the Board of Directors plays a key role in cybersecurity risk management.

For this reason, the Board of Directors must consider it a strategic risk and must:

- **be aware of the main regulations and related regulatory compliance measures;**
- **know the cybersecurity culture of the organisation;**
- **ensure that appropriate resources are available;**
- **know and evaluate the risks and be aware of the response plans and the main incidents.**

Each corporate area will be most interested in cyber security as it affects their specific function, from two standpoints:

1 Business processes for which they are responsible and how the information assets concerned are covered by the cybersecurity programme.

2 Accountability by the cybersecurity area to each business area. Mainly:

- The CIO, who will need a more operational picture of the programme, including the technological components used and the direct or complementary cybersecurity functions that must be carried out from the technology area.
- The CFO, who will need a financial picture of the programme, including budget progress, deviations and potential savings.
- Human Resources, which will be concerned about workforce training and awareness plans.
- Legal and Compliance, which will focus on how the necessary regulations and standards are implemented.

To tailor the reporting to the target audience, the CISO will need to be aware of the organisation’s strategic goals, key processes, technologies used, and the main risk scenarios and risk exposure.

3.5.

INTEGRATION WITH MANAGEMENT AND MONITORING TOOLS

DASHBOARD. A cybersecurity dashboard presents information that allows the CISO to draw data-driven conclusions for use in data-driven decision-making. Depending on its purpose, a dashboard can consolidate and centralise data on threats, compliance, performance and other cybersecurity data, using charts, tables and other visual resources to make the data easier to understand. Dashboards can be:

1. **strategic,** presenting key indicators on organisational health and helping management identify opportunities and threats;
2. **analytical,** offering detailed trend analysis, measuring data that change over time;
3. **operational,** focused on KPIs;
4. **tactical,** used at middle management levels, delving into key areas of the organisation.

As they rely on how the data are presented, dashboards should maximise visual representation and optimise content. The following recommendations could be added to those set out above:

- use visual hierarchies;
- use spaces well;
- choose colours well;
- apply the five-second rule: users should be able to identify the relevant information in that space of time;
- be minimalist: less is more, so, for instance, include no more than ten visual elements.

Information can be gathered in real time, or previously from various data sources. For a manual dashboard, data from various sources will have to be consolidated and then displayed on an integrated data platform. Valid options range from using a consolidated spreadsheet, designing a set of graphics and other visual elements, to using tools such as PowerBI or Tableau in cases of high data volume. These tools feed from separate spreadsheets and allow the data to be subsequently collated in a dashboard tailored to the specific needs of each case.

The most sophisticated alternative would be to directly integrate the different source platforms, achieving a real-time picture. Here the challenge is to include the different log management, vulnerability, endpoint, risk management, identity management and breach management monitoring tools on a single platform, enabling personalisation, so that a range of views may be obtained, according to the audience.

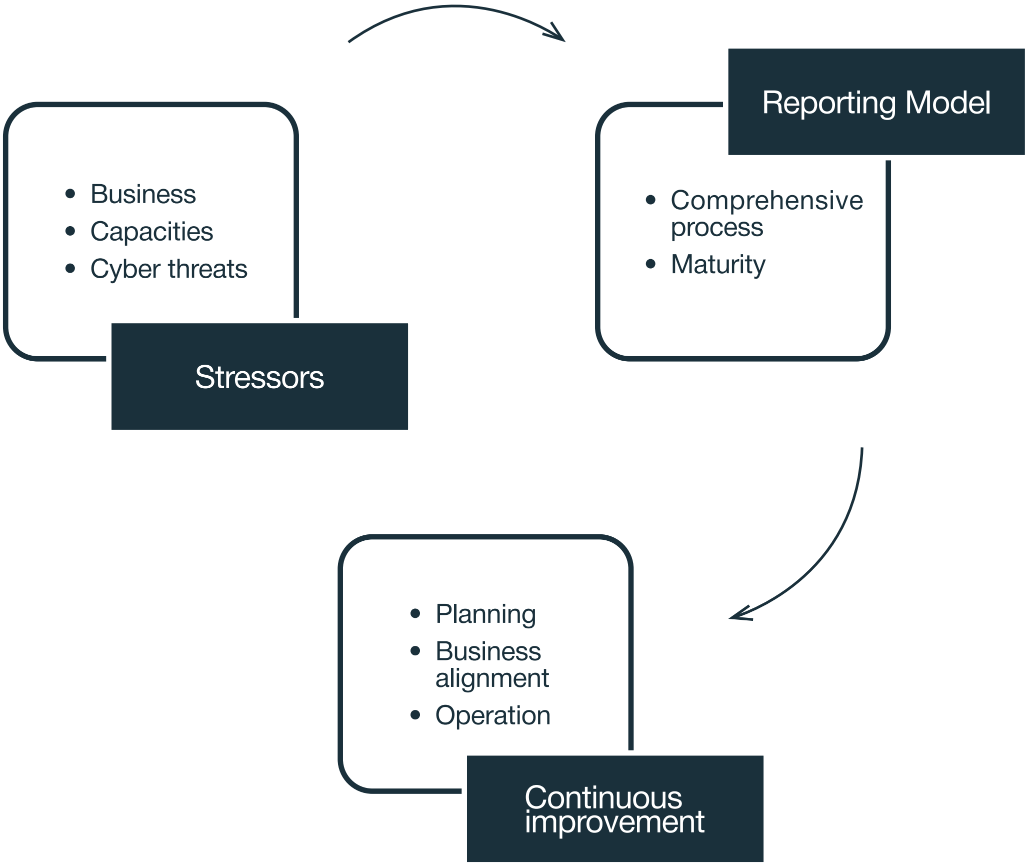
There are solutions available that provide direct connections through APIs to different cybersecurity monitoring tools, making it possible to consolidate real-time information on different types of dashboards, as required.

4. IMPLEMENTATION AND BEST PRACTICE

Implementing a system of cybersecurity risk indicators is a continuous process of tailoring the cybersecurity function to the needs of the organisation for which it works, in line with developing business activities, shareholder/stakeholder needs and the internal and external capacities and resources available to it, as well as the constant evolution of the cybersecurity landscape and the threats and actors that the organisation must face.

Therefore, the reporting process should not follow a static model – designed and implemented at an initial stage and then maintained over time. Instead, it should be understood and implemented as a comprehensive organisational process that requires continuous improvement in strategic planning, alignment with the organisation's needs and operational implementation of the model itself.

This chapter outlines the best practices for adopting the proposed model, including the fundamental steps for its launch, the role of automation and artificial intelligence and common challenges to arise during its implementation, along with the most effective solutions.



4.1.

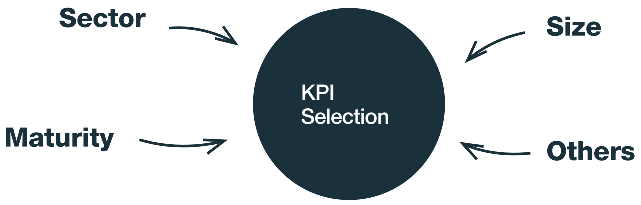
HOW TO ADOPT THE MODEL IN DIFFERENT TYPES OF ORGANISATION

Chapter 3 discussed the requirements that the selected indicators must meet for reporting to management. This includes both the organisation's KPIs and others that can provide the foundation for and complement these KPIs, as well as indicators that can provide relevant data under specific circumstances or at particular times.

The differences in implementing a model across various organisations can essentially be split into four groups:

- The organisation's and its executives' maturity in cyber security, as well as the organisational placement of the CISO.
- Business and regulatory requirements specific to the organisation's sector (and similar to those of its competitors), along with its international presence and structure and complexity.
- The size and/or resources available for the cybersecurity process and its reporting.
- Specific reporting needs, including information on new threats or lessons learned from previous incidents, as well as any circumstances that may influence these reports.

Combining these factors should enable the CISO and the organisation's management to identify the KPIs that ought to be included in the reporting model implemented. It should also guide them to develop the model over time.



Among all the aforementioned elements, **the organisation's maturity is the key factor in the model's adoption.** Not all firms start from the same point in their cybersecurity management, nor are they prepared to understand the value and data contained in some of the more advanced indicators. Therefore, the security officer must begin with a realistic assessment of the organisation's degree of maturity. This includes the existence and maturity of the ISMS, the assignment of cybersecurity roles and the training of the individuals who perform them, the existence of policies, applied controls, resources allocated to cybersecurity, and the level of automation. The security officer must also assess the organisation's culture regarding reporting to management in other areas and the management's receptiveness to such information.

In this regard, a firm with a low level of maturity in cybersecurity or reporting to management should initially choose a limited set of basic indicators focused on intuitive and fundamental cybersecurity activities, e.g. incident management and regulatory compliance. In contrast, a more mature and established firm can take a more sophisticated approach, incorporating predictive KPIs, efficiency indicators, sectoral benchmarking and comprehensive integration with technological tools. The security officer must be able to identify the true level of maturity and guide the firm towards more advanced and mature stages in cybersecurity reporting while simultaneously optimising the resources dedicated to this task.

The second most significant factor is the economic sector in which the organisation operates. Certain sectors are under intense regulatory pressure (e.g. the finance, healthcare and energy sectors and the public sector), where indicators must meet specific standards and comply with regulatory frameworks. For instance, financial institutions need to incorporate indicators related to DORA, NIS2, European Banking Authority (EBA) Guidelines and the NIST Cybersecurity Framework (CSF). Meanwhile, a healthcare institution must pay special attention to the protection of sensitive personal data in accordance with the GDPR and specific healthcare regulations.

Furthermore, there may be organisations within the sector that are further ahead in cybersecurity terms than others and have already progressed in identifying relevant and appropriate KPIs for sector-specific business needs. Access to this information allows the cybersecurity officer to expedite the selection of pertinent KPIs. It can also facilitate the exchange of comparable information among organisations in the sector for benchmarking purposes, both by the organisations themselves and by external entities such as regulators, industry associations and market research firms. Sectoral implementation should involve specialised areas, such as the compliance, legal and regulatory departments, to ensure that the indicators meet the requirements and expectations of supervisory and audit bodies.

The third factor to consider is the size and availability of resources within the organisation, which in this case acts as a limiting factor. It is essential to have sufficient resources to make all the relevant KPIs achievable. If resources are lacking, certain KPIs must be discarded and management should be informed of the same on the grounds of insufficient resources. The security officer must not conceal this information from management, as it will spark important discussions about key aspects for the organisation's CISO: the importance attached to the KPIs by management, their preferences the various KPIs, the growing maturity of cybersecurity leadership, the allocation of additional budget, etc.

On the opposite end, the CISO must strictly limit the use of resources for KPIs that have been dismissed by management, in order to optimise the budget. This does not mean that these KPIs should not be calculated at all, as they may still be useful for other areas. However, the effort spent on their calculation should be in line with the value they provide. Therefore, only those KPIs that offer sufficient value to the organisation should be considered and this value should be identified and quantified. A KPI that is currently deemed unnecessary may potentially become useful in future scenarios, once the organisation has matured or grown sufficiently.

Finally, the CISO must be mindful of the cost associated with calculating KPIs. The automation techniques outlined in Section 4.4 are particularly useful in this regard. Consequently, the CISO should sometimes prioritise KPIs that can be achieved at a lower cost, based on data availability and quality and how easy some are to calculate. In many cases, finding a rapid indicator that provides sufficient information may be preferable to an excellent indicator that is costly to compute.

The fourth and final factor relates to the organisation's occasional needs and specific circumstances. Here, the CISO must identify other reporting requirements that management may have, for whatever reason. Common examples include the organisation's security readiness in the face of known or emerging threats, progress made on improvements or towards goals and the status of remedial actions following incidents or audits. However, these may arise owing to particular people's spurious or short-lived interests. If this should occur, the CISO must know how to understand their needs and respond to them.

Taking all of this background into account, the CISO designs achievable KPIs with the resources available and structures the relationships between them, aiming to meet the sector-specific needs as efficiently as possible, in line with the organisation's maturity, business and established reporting methods.

The goal must always be to provide management with an accurate picture of the cybersecurity and risk status after each report, satisfying the need for insight and enabling the leadership to fulfil its responsibilities.

Lastly, and taking these initial KPIs as a starting point, the CISO guides the improvement of reporting by including or excluding new and old KPIs to meet information needs more efficiently and comprehensively.

4.2.

STEPS FOR IMPLEMENTING INDICATORS

Although the implementation of KPIs may appear to be a linear process, in reality, multiple feedback points must be in place to ensure their correct deployment and allow for later improvement.

The first step is to identify a minimum viable set of KPIs. This should be a small number of high-level indicators (at least six, ideally ten to fifteen, though more may be chosen if needed) that provide plenty of value and are easy to calculate, albeit with limited precision. These allow for measurable results in the short term, facilitating organisational learning and establishing a solid foundation for future generations of KPIs.

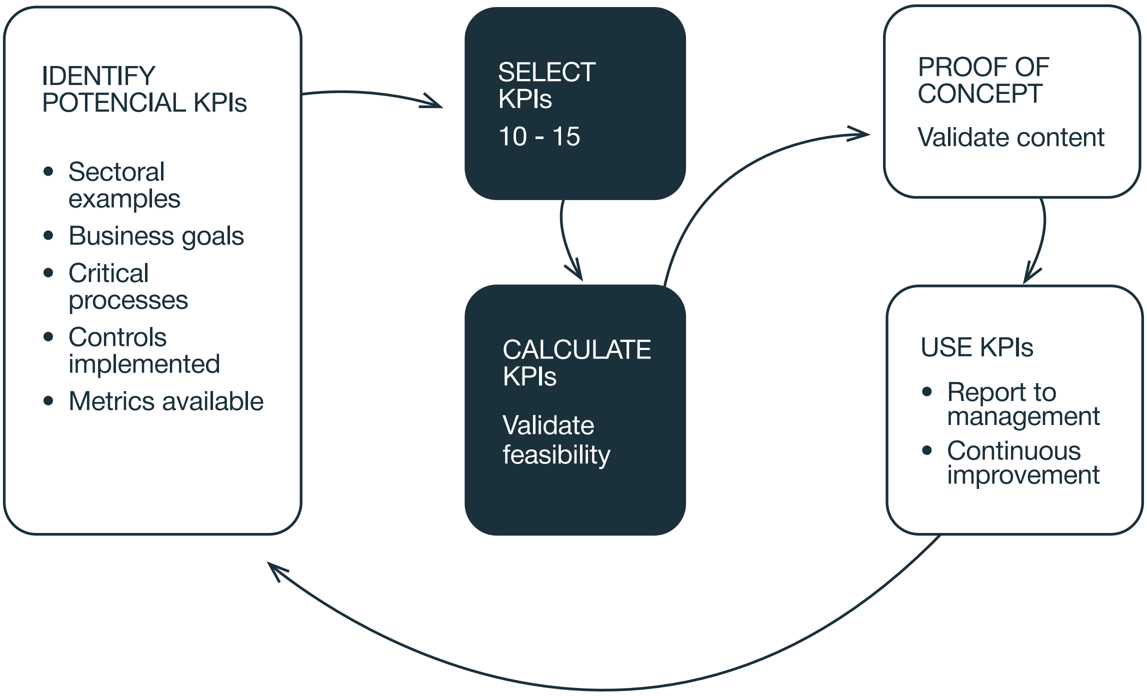
These initial KPIs may be sourced in various ways. If available, they may replicate KPIs used by other organisations in the sector or draw on them. They may also be identified by analysing the organisation's strategic goals, critical business processes and general cybersecurity controls (such as training, incidents, continuity, vulnerabilities, patching, etc.). Lastly, metrics that are already naturally collected by existing cybersecurity controls (such as security information and event management (SIEM) solutions; security orchestration, automation and response (SOAR) systems; ticketing solutions; governance, risk and compliance (GRC) platforms; dashboards; training and reporting portals) may be used. It is perfectly feasible to structure KPIs in levels, provided that, as noted in the discussion of dashboards, the number of indicators at the highest level is limited and indicators at different levels are interrelated.

The second step is the calculation and effective collection of KPIs. Sometimes, KPIs as designed turn out to be inadequate. Sometimes, they prove unsuitable, either because their calculation is too complex, slow or simply not feasible or because their results are not representative or do not provide information of interest to management. Whether a KPI is being added or retired, the CISO should double check its viability and, where appropriate, select alternative KPIs that do meet the desired goals. In practice, this process of testing and discarding potential KPIs will always be a work in progress.

The third step is the proof of concept for KPIs that have passed the previous phase. This involves subjecting the selected KPIs to scrutiny by a representative section of management to check that they provide the expected relevant information in terms of form and substance and that they are useful for cybersecurity decision-making. Ideally, this sample should include the organisation's most senior management. If a KPI is deemed to provide too little insight, the CISO should modify or replace it with one that management deems relevant. This step also makes it possible to verify that the earlier work carried out by security staff to discover the organisation's needs. If done correctly, all or almost all of the proposed KPIs will pass this phase.

The fourth, though not final, step is to use the selected KPIs for reporting to management. Again, these KPIs should be considered useful, but it is possible that some may require improvement or replacement.

The final step is the continuous improvement of the reporting indicator model, including new KPIs, retiring obsolete ones, and optimising their calculation. Some authors suggest that this optimisation may be carried out in earlier phases – this may be the best option for some organisations/KPIs.



4.3.

USING AUTOMATION AND ARTIFICIAL INTELLIGENCE

IN INDICATOR MANAGEMENT

Automating KPI computation processes enables the organisation to reduce and monitor the effort involved in reporting to management, making it sustainable over time. Manual data collection carries risks of error, inconsistency, delays in updates and high operational costs, whereas automation ensures efficiency, accuracy and regularity in KPI calculation for reporting.

As previously noted, the ability to automate and the calculation cost are both factors that the CISO must consider when selecting minimum or desirable KPIs. Automation should cover everything from data collection (accessing data via APIs or repositories, automated dashboards, push notifications, consumption of indicators generated by other areas) to calculation and presentation (dashboards, periodic reports, automated report delivery) and generation of historical records. Scheduled workflows, centralised databases, business intelligence platforms and artificial intelligence (AI) algorithms are all acceptable approaches. Once configured, these systems keep information up to date in real time or at defined intervals (daily, weekly, monthly), improving monitoring and decision-making.

Automation should also include the management of alerts and indicator traffic lights, enabling those responsible to act quickly in critical situations without waiting for a full reporting cycle.

Beyond basic automation, AI enables predictive and proactive cybersecurity management. AI can detect hidden patterns, less obvious correlations and anticipate deviations before they result in incidents. AI may be used for:

- ↳ Trend analysis: Assessing the evolution of certain indicators to identify cycles (short or long term), seasonality and unexpected changes in trends.
- ↳ Anomaly detection: Identifying unusual movements in selected KPIs, especially short-term changes.
- ↳ Automatic risk classification, action proposals and/or automatic response: Using historical variables and operational context, algorithms can establish automatic responses to anomalies, propose improvements in response to KPI changes and produce analytical information on organisational risks.

All these capabilities must be based on algorithms that are explainable, traceable, unbiased and supported by reliable, high-quality data, especially when reporting to senior management or in regulated environments. The organisation retains responsibility for its decisions, so human oversight of AI, or human decision-making assisted by AI, are the most advisable scenarios. The aim should be to bolster the CISO’s analytical capacity and support fact-based decision-making that can look further ahead.

4.4.

CHALLENGES AND SOLUTIONS IN IMPLEMENTATION

Implementing a KPI model presents numerous challenges. Seven aspects have been identified as particularly relevant, though you may identify or be obliged to address others in practice.

- KPIs downplayed
- Inconsistent data
- Data Quality
- Lack of engagement
- Unaligned interests
- Too many KPIs
- Out-of-date KPIs

A significant difficulty is that calculating KPIs is often seen as an unglamorous activity (among the CISO's various responsibilities) – one whose effort is not fully appreciated by management. It may also be affected by incidents and urgent short-term needs that demand resources for indicator calculation, especially when the process is not fully automated. KPIs can change rapidly, raising doubts about whether their automation is worthwhile if the indicator is not expected to be used for long enough. The end result may be that the process of calculating and analysing the KPIs is delayed and not given sufficient resources, and the security officer poorly motivated, resulting in the delivery of results being stifled by bureaucracy and not shared in a way that helps to bolster cyber security.

Data quality for reporting is another source of problems. Concerns range from the basic quality of collected data and its suitability for calculating the desired KPIs owing to the absence of better sources to inconsistencies between data recorded in different systems, whether in format, values or data types. Defining and applying a common data taxonomy across all systems and controls allows data to be normalised at source, improving reliability and accuracy. Continually identifying available data sources with relevant and applicable information helps improve and validate incoming data, filtering out low-quality or unsuitable sources.

Furthermore, when cyber security does not share goals or a common language with other areas (IT, legal, operations, business, etc.), cybersecurity KPIs may lack practical utility. The CISO must establish cross-cutting governance, validating KPIs with representatives from each area and ensuring that everyone understands their impact and utility. This requires using a common language that is comprehensible to all, otherwise each area must be addressed using its own jargon.

Such a model also helps reduce potential problems arising from a lack of collaboration between the areas that work with the business processes, services and controls in generating and communicating indicators. It also mitigates issues caused by insufficient definition of KPIs, their collection processes and applicable data sources, which may incorporate the know-how of individuals in these areas. Low enthusiasm or engagement has a particularly greater impact on KPIs that are not yet fully automated. Without the engagement, which allows the baseline information for indicator calculation to be established, or questions about data quality to be asked, the credibility and usefulness of the indicator model are called into question.

Some organisations apply a principle of overabundance to their KPIs: "Better too many than too few." The result is a dashboard overloaded with an excess of irrelevant indicators, complex graphics and actually relevant information being buried. Such a dashboard confuses and obscures information rather than revealing it and is of questionable utility for management. In such a case, it is necessary to return to the original KPI design and select indicators that offer management the most insight.

Finally, the CISO must avoid allowing KPIs to persist in the reporting model without periodically reviewing their necessity. Changing an indicator or modifying calculation formulas or sources is a costly and delicate process as it may result in the loss of historical data or traceability. Nevertheless, after several years, many KPIs grow irrelevant, but continue to be calculated out of inertia, providing value to nobody. The CISO must ensure that such KPIs are retired or relegated to lower levels of importance.

5.

CONTINUOUS EVALUATION AND IMPROVEMENT

Implementing a system of indicators and reporting in cyber security is the first step in a journey. The risk environment, business priorities, and technology are constantly changing, as are regulations. An active process for evaluation and improvement is therefore key to ensuring that metrics and their communication remain relevant and provide strategic value to the organisation.

This section details the approach for systematic evaluation and improvement.

5.1.

VALIDATION AND ADJUSTMENT

OF INDICATORS OVER TIME

KPIs defined early on require regular review to confirm their relevance and alignment with the organisation's strategic goals and current risks.

↳ **Periodic review process:** A defined routine (for example, each quarter or semester) is established to review the set of indicators. These sessions involve cybersecurity staff and representatives from other key areas (such as Risk, Legal, Technology and Operations), providing a comprehensive perspective.

↳ **Validation criteria:** During the review, each indicator is assessed according to criteria such as:

- Does it remain aligned with business goals and principal risks?
- Is the information it provides accurate and reliable? Does it adequately reflect operations?
- Does it facilitate decision-making and help to identify areas for improvement?
- Is the effort required to obtain it proportionate to the value it generates?

↳ **Adjustment process:** Based on the evaluation, it is decided whether an indicator:

- Is left unchanged.
- Requires modification (in its definition, calculation, thresholds or data source) to increase precision or usefulness.
- Is retired owing to loss of relevance, redundancy or disproportionate maintenance cost.
- If new indicators are needed to cover emerging aspects (new technologies, regulatory changes, etc.).

↳ **Documentation:** All changes to the set of indicators are duly recorded and communicated to stakeholders, updating the reference documentation for the system.

5.2.

INDICATORS OF SUCCESS AND MEASURING IMPACT

In addition to measuring specific aspects of cyber security, it is essential to assess the effectiveness of the system of KPIs and reporting itself. It is necessary to determine whether this system achieves its aim of improving decision-making and optimising resource allocation to strengthen the cybersecurity posture.

↳ **Defining indicators of the system's success:** Specific metrics may be used to evaluate the system itself, such as:

- The degree of senior management satisfaction with the clarity and usefulness of reports.
- Observable improvement in response times to critical incidents owing to increased visibility.
- Demonstrable reduction in recurrence of certain incident types following actions based on key indicators.
- Optimisation of cybersecurity investment, for example, by calculating the return on investment (ROI) of initiatives prioritised using key risk indicators (KRIs, which are defined in in Section 2, the glossary).
- Improved audit scores related to governance and reporting.

↳ **Measuring business impact:** The ultimate goal is to connect cybersecurity management with business outcomes. The aim is to quantify, as far as possible, how improvements in the indicators translate into tangible benefits:

- Reduction in financial losses resulting from incidents.
- Enhanced client trust and reputation.
- Efficient regulatory compliance.
- Secure enabling of new business initiatives.

↳ **Communicating value:** Communicating these impact results to senior management is essential to demonstrate the value of investment and effort in cyber security.

5.3.

FEEDBACK AND UPDATING THE INDICATOR FRAMEWORK

A key component of continuous improvement is considering the views of those who use and receive the generated information.

↳ **Feedback channels:** Formal and informal channels are established to gather this information:

- Specific review sessions with senior management and other relevant committees.
- Periodic surveys directed at different report audiences.
- Direct input from the cybersecurity team regarding the operational viability and usefulness of indicators.

↳ **Feedback analysis:** The information collected is systematically analysed to identify patterns, areas for improvement, and applicable suggestions.

↳ **Update cycle:** This feedback, together with the results of KPI validation (5.1) and impact measurement (5.2), feeds into a formal process for updating the overall indicator and reporting framework (described in Sections 2 and 3).

↳ **Framework governance:** Controls are applied to ensure that updates are implemented in an orderly, documented and communicated manner, maintaining system coherence.

In summary, this process of evaluation and improvement ensures that the cybersecurity indicator and reporting system remains a useful strategic tool and one that is suited to the organisation's development and environment.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1.

KEY BENEFITS OF USING CYBERSECURITY INDICATORS

The guiding principle behind these guidelines is as follows: “It’s not just about measurement; it’s about strategic and effective communication”. Given the diversity of circumstances across public and private organisations, bringing together the “what” and the “how” when it comes to using cybersecurity indicators and reporting to senior management is a significant challenge.

However, the ability to leverage cybersecurity indicators – and effectively communicate while doing so – will broaden CISOs’ influence within their organisations, ultimately leading to a more robust cybersecurity posture.

As outlined in this guide, the key benefits of using cybersecurity indicators can be summarised as follows:

- **They offer key information on the cybersecurity situation and anticipating trends to stay ahead of potential issues;**
- **They provide senior management with visual and easily understandable information;**
- **They equip the CISO with a powerful tool for both operational and strategic purposes, one that can easily be shared with both technical and non-technical staff;**
- **They promote awareness and recognition of the need for cyber security across the entire workforce, including senior management;**
- **They provide the right tool to break down any barrier with senior management, combined with effective communication.**

6.2.

IMPACT ON GOVERNANCE AND REGULATORY COMPLIANCE

Cybersecurity governance has progressively gained prominence in recent years. In the past governance typically received less attention, with organisations focusing their cybersecurity strategy and/or action plans around technological solutions, talent acquisition and management, and ultimately developing cybersecurity processes. However, in the latest update, NIST's own CSF was expanded from the traditional five functions to six, with the addition of Govern.

This guide seeks to place governance at a similar level of priority, ensuring that the principles outlined here position the CISO as a key element within the organisation.

The CISO's standing can vary across organisations, often depending on sector, size and maturity. At some, the CISO is a key role and can even be members of senior management, although most are positioned more or less adjacent to senior management. Such positioning is important for ensuring continuous improvement in cyber security, which must consistently evolve in line with the threat landscape and other factors. This governance and positioning allow organisations to effectively manage risks and their cyber security.

Such sound governance and positioning entail significant responsibilities for the CISO, who should view themselves not merely as a technical role, but as a business enabler and, ideally, as a participant in the organisation's strategy. Indeed, they should strive to advance this strategy, providing services and working to ensure that it is achieved securely, while also anticipating issues and proposing solutions and capabilities that add value to the organisation.

It is also worth noting that new regulations – whether sector-specific or more general – on information security/cyber security place emphasise, more clearly than ever, on the key role that the CISO and senior management both have to play. Senior management must not remain detached from these responsibilities, nor should the CISO stop emphasising this, offering support and guidance.

In addition, new regulations are becoming increasingly demanding, no longer covering "some organisations" deemed more or less critical and/or essential, but now extending to a growing number of public and private organisations. These new demands include not only being duly protected and having adequate identification and prevention capabilities, but also sound governance, as well as far-reaching cyber incident response and recovery capabilities.

This guide will undoubtedly assist CISOs in ensuring regulatory compliance, since effective monitoring and management of indicators – in addition to effective communication with senior management – not only provides continuous, real-time insight into the state of corporate cyber security, it also enables the anticipation of adverse trends and future issues. Moreover, it provides reliable data for risk management, allowing the CISO and senior management to make well-informed decisions.

6.3.

NEXT STEPS FOR DEVELOPMENT OF THE MODEL

The model presented in this guide is the first comprehensive approach developed by a broad community of CISOs and C-level executives, comprising key principles that should be updated regularly.

The indicators and metrics must be compiled, processed and managed as efficiently as possible, otherwise they lose their meaning and become a tedious, resource-intensive task that fails to bring the intended benefits.

As reiterated throughout this guide, there is no single model or universal approach; the sheer number of variables makes this impractical. Each organisation should adopt its “best version” of the model, adapting it to its needs. For instance, data that hold no value for a given organisation should no longer be collected, while indicators that fail to show meaningful trends or that barely move – becoming mere numbers of little value – should be discarded. And this should not worry the CISO, since it happens at all organisations.

Given the above, along with technological advances and a changing environment, many organisations are undergoing more or less significant transformation, driven by current trends and in preparation for the emergence of potentially disruptive “new paradigms” (e.g. the widespread adoption of artificial intelligence).

As a result, the model should be regularly updated at each organisation, as should this guide. Cyber security must be ready to respond rapidly to business needs, which will mean measuring more factors in different ways and in areas previously not measured or deemed less relevant.

6.4.

A CALL TO ACTION FOR CISOS AND SENIOR MANAGEMENT

The cybersecurity professionals involved in preparing this guide – either directly or as consultants – stress the importance of the practices presented here. They also emphasise that simply setting out key guidelines for CISO reporting to senior management is not enough: there must also be concrete actions that both the CISO and senior management can take where necessary.

It is worth further reinforcing the idea that CISOs must, if they haven't already, take the necessary step towards becoming an enabler, and viewing themselves as such. Not only should they stand as the organisation's main technical authority on cyber security, they must also develop their C-level capabilities on an ongoing basis. As such, they should be a senior leader who helps the organisation evolve towards the cyber security it needs, with vision, critical thinking and the ability to engage senior management, ensuring that the latter understands its responsibilities and is able to manage cybersecurity risks effectively, based on reliable data for informed decision-making. Many CISOs took this step long ago, some are currently in the process and others have yet to start. In any event, the continuous improvement, development and evolution of an organisation's CISO are essential at both the technical and governance levels.

As for senior management, it is essential that they understand their responsibilities when it comes to cyber security. They must acknowledge that the CISO is the best placed person to efficiently manage the organisation's cybersecurity risks, and to do so in a way that they can understand. They should demand from the CISO clear and effective communication of these indicators and any relevant cybersecurity issues, as well as the associated risks. Senior management must also maintain an active interest in cyber security that goes beyond the CISO's budget. They should allow the CISO to become a true business enabler, involved in and close to the organisation's strategy, rather than sidelined or in a position that prevents from working effectively.

Thise guide calls for joint reflection between the CISO and senior management to build bridges that foster a deeper understanding of the often-complex aspects of cyber security and its risks, supporting sound, well-informed decision-making.

REFERENCES

7.

Aufait UX. (n.d.). Cybersecurity dashboard UI/UX design: 5 things to consider for an engaging dashboard. Aufait UX. https://www.aufaitux.com/blog/cybersecurity-dashboard-ui-ux-design/

ColorBrewer 2.0. https://colorbrewer2.org/

CyberSaint. (2023, 5 October). The best cybersecurity dashboards: 5 key features for success. https://www.cybersaint.io/blog/the-best-cyber-security-dashboards

Datawrapper. (n.d.). Datawrapper Blog. https://blog.datawrapper.de/

Regulation (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

Fer, S. (2004). Show me the numbers: Designing tables and graphs to enlighten. Analytics Press.

Few, S. (2006). Information dashboard design: The effective visual communication of data. O'Reilly Media.

Few, S. (2009). Now you see it: Simple visualization techniques for quantitative analysis. Analytics Press.

Few, S. (2013). Information dashboard design: Displaying data for at-a-glance monitoring. Analytics Press.

Google. (n.d.). Looker Studio Help Center. https://support.google.com/looker-studio

Jit.io. (n.d.). Continuous security monitoring (CSM) tools. https://www.jit.io/resources/appsec-tools/continuous-security-monitoring-csm-tools

Knaflic, C. N. (2015). Storytelling with data: A data visualization guide for business professionals. Wiley.

Material Design. (n.d.). Data visualization guidelines. Google. https://m3.material.io/foundations/data-visualization

Microsoft. (n.d.). Power BI Documentation. https://learn.microsoft.com/power-bi/

National Institute of Standards and Technology (NIST). (n.d.). Cybersecurity Framework.

https://www.nist.gov/cyberframework

Secureframe. (2023, 30 June). Cybersecurity dashboards: What they are and how to use them.

https://secureframe.com/blog/cybersecurity-dashboards

Smartosh. (2022, 10 May). Indicadores preventivos (leading) o lagging: ¿Cuál es la diferencia? https://www.smartosh.com/indicadores-preventivos-leading-o-lagging/

Splunk. (2025). The CISO Report 2025. Splunk Inc.

Sprinto. (2023, 8 March). Cybersecurity dashboards: Why they matter and what to track.

https://sprinto.com/blog/cybersecurity-dashboards/

Tableau. (n.d.). Visual best practices guide. https://www.tableau.com/learn/whitepapers/visual-best-practices

TechTarget. (2023, 2 August). Top ERM software vendors to consider. https://www.techtarget.com/searchcio/feature/Top-ERM-software-vendors-to-consider

The Noun Project. (n.d.). Icon library. https://thenounproject.com/

TuDashboard. (n.d.). ¿Qué es un indicador lagging y leading? https://tudashboard.com/que-es-un-indicador-lagging-y-leading/

Tufte, E. R. (2001). The visual display of quantitative information. Graphics Press.

How CISOs Can Take Advantage of the Balanced Scorecard Method. https://www.isaca.org/resources/news-and-trends/industry-news/2024/how-cisos-can-take-advantage-of-the-balanced-scorecard-method

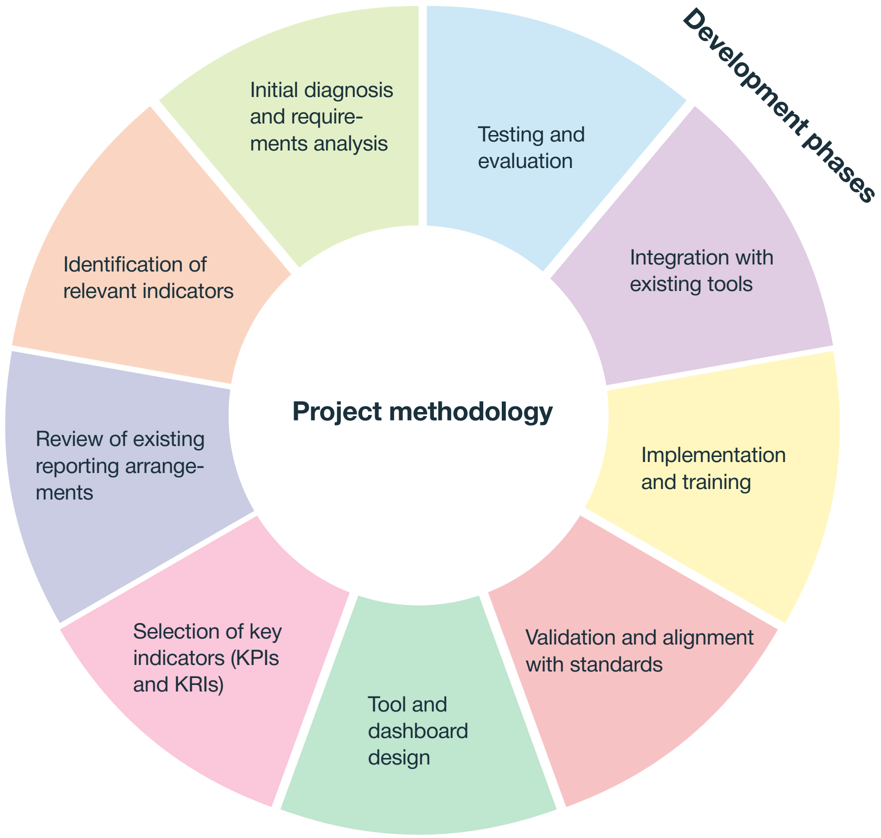
MIT Sloan – Balanced Scorecard Dashboard for Cybersecurity. https://cams.mit.edu/wp-content/uploads/Balanced-Scorecard-Dashboard-for-Cybersecurity.pdf

NIST – Developing a Cybersecurity Scorecard. https://csrc.nist.gov/CSRC/media/Presentations/Creating-a-Cybersecurity-Scorecard/images-media/Developing%20a%20Cybersecurity%20Scorecard.pdf

Wikipedia. (n.d.). Deming cycle. https://en.wikipedia.org/wiki/PDCA

ANNEX 1:
PROJECT METHODOLOGY

The guide has been prepared using the methodology outlined below:


Development phases
Project methodology
Initial diagnosis and requirements analysis
Testing and evaluation
Integration with existing tools
Implementation and training
Validation and alignment with standards
Tool and dashboard design
Selection of key indicators (KPIs and KRIs)
Review of existing reporting arrangements
Identification of relevant indicators

Design and development of the indicators and reporting system

The methodology aims to provide the CISO and senior management with key indicators (KPIs and KRIs) that provide a clear, objective and actionable understanding of the organisation's cybersecurity situation. A structured process is used to review needs, select the appropriate indicators and design effective tools to visualise and monitor them.

a) Development phases

The aim in this stage is to review the current situation in order to identify the organisation's cybersecurity needs. Understanding how cybersecurity risks affect the business is key here, to thus determine the appropriate indicators and evaluate the existing reporting arrangements (frequency, consistency, adaptability to different interlocutors, etc.).

Bear in mind that senior management does not deal with technical details; therefore, the selected indicators should be suitable for an executive-level view.

The development phases are as follows:

b) Initial diagnosis and requirements analysis

The aim is to identify requirements in relation to information security and protection.

Broadly speaking, senior management should understand how cybersecurity risks could affect their organisation's normal functioning, what resources should be dedicated to mitigating those risks and how to monitor them on an ongoing basis. Similarly, it is essential that they understand the applicable regulatory framework and have the right tools for compliance monitoring.

However, senior management is not expected to participate in day-to-day cybersecurity and information protection activities or to have specific technical knowledge.

All of which should be considered when selecting the appropriate indicators in the next phase.

c) Identification of relevant indicators

The indicators used for reporting to senior management should be:

- Measurable, with clear definitions and formulas;
- Comparable with past data (to establish a time scale) and with external references (for accurate data interpretation);
- Relevant, aligned with the business (they should contribute, not merely inform);
- Comprehensible in what they aim to measure and easy for interlocutors to understand;
- Scalable and adaptable, ready to support a growing number of components and to respond to a changing threat landscape;
- Actionable, to support decision-making.

The selected indicators will provide objective insights into security conditions and support decision-making at tactical, operational and strategic levels.

Similarly, when identifying the key indicators for an organisation, their strategic relevance – which may differ from one organisation to the next – must not be overlooked. This is key to ensuring that security objectives are aligned with the organisation's strategic goals, identifying the main risk areas for the business strategy and defining an action plan to mitigate those risks.

d) Review of existing reporting arrangements

The final development phase is a review of the organisation's existing reporting arrangements.

Our guiding principle is that merely presenting information is not enough; the information must be actionable and inform strategic decision-making on cyber security and information protection. Accordingly, when assessing the current state of reporting, we should ask questions such as:

- Is the information relevant to the business?
- Is it clear and understandable for all interlocutors, including those without a technical background?
- Does it focus on the indicators identified?
- Is it effective in measuring progress towards the goals?

All of this will help determine whether the current reporting arrangements are appropriate and identify areas for improvement to work towards the desired efficiency. Reporting must be effective, clear and focused on adding value to the business.

To the extent the CISO is viewed increasingly as part of senior management, their mission will not only be to protect the company but also to enable the business by managing cyber risk in full alignment with the strategic goals. Therefore, communication must be clear, effective and business-aligned, presenting the organisation's cybersecurity situation through executive reports and dashboards that are direct, relevant and understandable to business interlocutors.

e) Design and development of the indicators and reporting system

Once the existing situation regarding indicators and reporting has been evaluated, it is a matter of developing the desired indicators and reporting system by selecting the relevant indicators and designing effective tools. The following phases are distinguished:

f) Selection of key indicators (KPIs and KRIs)

The indicators are divided into two main types:

- KPIs - key performance indicators
- KRIs - key risk indicators

KPIs measure the progress made by the company, area, process, etc. towards the established goals. Their main aim, therefore, is to provide information for decision-making and concrete actions.

KRIs, on the other hand, aim to identify and measure potential risks that could affect the attainment of the company's goals.

Both must therefore be time-based metrics, measurable, aligned with the organisation's specific objectives and comparable.

In addition, the KPIs must also be achievable, realistic and based on the organisation's true capacity. There would be littles point in setting objectives that cannot be achieved with reasonable effort.

KRIs are intended to anticipate potential future risks and must therefore be predictive, serving as an early warning system to identify risks before they materialise.

Regulation and the regulatory framework are also important when it comes to selecting the appropriate KPIs and KRIs. Depending on the organisation's sector, size and geographical scope, a range of general or sector-specific regulations may apply and should be considered when selecting the appropriate indicators.

g) Tool and dashboard design

As noted above, communication between the CISO and senior management must be direct, clear, concise and aligned with the business. The reporting tools and dashboards must be designed accordingly.

The following design principles can be identified:

- ↳ Strategic relevance, presenting information aligned with the company's strategic priorities and not falling into the error of designing technical metrics.
- ↳ Clarity and concision, with executive language, no technical jargon and addressing key objectives.
- ↳ Focus on KPIs/KRIs, with these being the foundation of all reporting. Selecting, as indicated above, those that are relevant to the business objectives and transforming the data they present into actionable information.
- ↳ Visibility of risks and opportunities, projecting possible future scenarios and identifying not only potential risks but also opportunities (cyber security as a business enabler).

The dashboards should allow information to be synthesised into clear, concise visualisations to reflect the overall state of cyber security and information protection in relation to the business. This will allow senior management to make well-informed decisions in this domain.

The visual design is therefore an essential element of effective reporting. A well-designed visualisation enhances comprehension, shortens analysis time and directs attention to the most critical business elements. Accordingly, the visual design must comply with the following principles:

- ↳ Clarity, facilitating comprehension and avoiding information and visual saturation
- ↳ Appropriate choice of charts and graphs for each instance, supporting interpretation
- ↳ Consistent visual coding, ensuring the chosen visual code is applied consistently across all reporting to prevent audience fatigue or disengagement
- ↳ Guided narrative; the order in which the elements are presented, how they are grouped and emphasised should guide the audience towards key conclusions
- ↳ Avoid information overload, presenting key data and preventing the audience from having to work too hard to interpret the data.

h) Validation and alignment with standards

Today, CISOs face significant regulatory and compliance pressures. Accordingly, every indicator and dashboard must be properly validated and aligned with the regulatory framework adopted by the company and any applicable regulations.

i) Implementation and training

Once the indicators have been selected, validated and designed, they must be implemented.

j) Integration with existing tools

Part of the life cycle of senior management indicators – once they have been defined, validated and implemented – is the calculation process. Modern technology allows near real-time calculation and the direct display of indicators and dashboards from a digital platform.

k) Testing and evaluation

Risk management professionals should refrain from using any indicators and/or dashboards that have not undergone testing and validation. Each indicator should be verified to ensure alignment with its definition, the question it is intended to answer and the calculation formula. It is good practice to review these internally and then share them with trusted colleagues in other areas to perform an independent validation and act as “devil’s advocate”.

ANNEX 2:
REPORTING TEMPLATES AND DASHBOARDS

This annex provides practical examples and templates to help the CISO structure and present cybersecurity data to senior management. It includes suggested formats for regular reports, visual dashboards and special reports for critical and exceptional situations. In addition, it provides specific recommendations on areas that are particularly relevant for various executive profiles, such as the CEO, CIO and CFO.

1.Template for Monthly Executive Report

- **Cover page**

  Title: Monthly Cybersecurity Executive Report

  Date: [Month - year]

  Person responsible: [Name and position of the person responsible]

  Area: [e.g. Information Security]

- **Executive summary**

  Brief description (maximum 300 words) with key conclusions for the month:

  General state of security.

  Main incidents or events.

  Strategic recommendations.

  Significant trends or changes.

- **Changes in KPIs**[4]

KPI	Indicator	Current	Previous month	Trend	Notes
KPI 1	No. of incidents by severity (High/Medium/Low)	[###/###/###]	[###/###/###]	⇧/⇩	[Brief notes]
KPI 2	Average response and resolution times	[hh:mm:ss]	[hh:mm:ss]	⇧/⇩	[Notes]
KPI 3	% of patched critical systems	[%]	[%]	⇧/⇩	[Notes]
KPI 4	Regulatory compliance level (ISO 27001, GDPR, etc.)	[% or traffic light]	[%]	⇧/⇩	[Notes]
KPI 5	Staff awareness (% success in phishing simulation)	[% that clicked]	[%]	⇧/⇩	[Notes]

[4] Include charts where possible to show changes in each KPI.

- **Risks and opportunities identified**

Type	Description	Impact	Probability	Mitigation/ proposed action
Risk	[Risk description]	High/Medium/Low	High/Medium/Low	[Actions]
Opportunity		High/Medium/Low	High/Medium/Low	[Actions]

- **Next steps and actions needed**

AC1: Revision of access policies before [date]
AC2: Update critical asset inventory
AC3: Awareness campaign: phase 2 – [date]
AC4: Evaluation of solution X for [need]
AC5: Meeting with critical suppliers – [date]

2. Template for comprehensive dashboard

- **Visual design on a single page (Executive dashboard)**
- **Indicators organised by category**

Category	Indicator	Current value	Goal	Traffic light	Comment/context
Incident management	• Number of incidents • Type of incidents (malware, access, etc.) • Average severity				• For example: High number of incidents at mobile endpoints • Classification by most common category • Scale of 1-5 or critical/high/medium/low
Regulatory compliance	% regulatory compliance		100%		According to audit or self-assessment
Resilience and continuity	• Recovery time objective (RTO) • Recovery point objective (RPO) • Critical systems availability				• In hours • Backup frequency • Example of key productive systems
Awareness and training	• Training participation rate (%) • Success rate in simulations (phishing etc.)				• Based on attendance at sessions • % that did not “take the bait”
Risk status	Most relevant KRIs				Highest impact risks identified
General security status	% deviation from benchmark				Changes noted relative to initial setup

- **Visual alerts using traffic lights (green, amber , red)**

Green ✅: within the acceptable threshold or exceeding the target.
Amber ⚠️: close to the threshold or with minor deviations.
Red ❌: outside acceptable limits.

- **Brief annotations and explanatory context.**

Category	Indicator
1. Introduction and context	Brief summary of the quarter: Relevant events, threat environment, organisational changes
2. Comparative analysis	Comparison of current KPIs against previous quarters. Include charts if possible. Example: development regarding incidents, compliance, response times
3. Developments in strategic risks	Updated risks map: High, medium, low. Indicate changes relative to previous quarters
4. Strategic initiatives	Status of key projects: Name, goal, progress (%), challenges, next steps
5. Business impact	May include a risks table or bubble chart
6. Projections and future scenarios	Analysis of future trends: Emerging threats, budget needs, road map.

3. Template for a Strategic quarterly report

- **Incorporates tables of comparisons and line or bar charts for trend analysis.**
- **Uses colour codes and icons to highlight risks and achievements.**

4. Template for a Critical incidents report

Entry	Date and time	Systems affected	Financial impact	Operational impact	Reputational impact	Root cause	Response	Lessons learned	Recommendations	Preventive steps
Incident 1	01/05/2025 14:00	Payment system	50,000	Three-hour service downtime	Loss of potential clients	Authentication system vulnerability	Access revoked, forensic analysis	Improve multifactor authentication	Review security processes on critical platforms	Improve multifactor authentication, perform regular audits
Incident 2	12/06/2025 10:30	Database	30,000	Query interruption	Negative impact on customer trust	SQL injection in database	Restored from backups, patches applied	Enhance entry validation, firewall review	Review database security configuration	

5. Examples of recommended graphics for dashboards

Type of graphic	Main use	Visual example
Line chart	Show long-term trends	Developments in monthly incidents
Bar chart	Compare different categories	Compare incidents by type (phishing, malware)
Speedometer/traffic light	Show current status of a KPI or process	Regulatory compliance level (red, amber, green)
Heat map	Risk analysis in various areas or systems	Risk by department (more intense colour for greater risk)
Pie chart	Show proportions in a whole	Percentage of incidents by severity (high, medium, low)

6. Key elements for specific profiles

↳ CEO:

Goal: To provide a strategic overview of the impact of cyber security on the organisation in terms of continuity, reputation and compliance.

Key elements:

- Impact of critical incidents on business continuity:
  - Description: Summary of critical incidents and their impact on the organisation's key operations.
  - Presentation:
    1. Graphic: Line chart showing the frequency of incidents over time and their impact on service continuity
- Strategic risks affecting the global vision:
  - Description: The major strategic risks that could compromise the organisation's long-term vision (e.g. attacks on critical systems).
  - Presentation: Risk map classifying the most critical risks (high, medium, low).
- Regulatory compliance and reputational risks:
  - Description: How security incidents are affecting regulatory compliance and corporate image.
  - Presentation: Pie chart or bar chart showing the percentage of regulatory compliance or incidents with reputational impact.
- Progress and effectiveness of the strategic cybersecurity programme:
  - Description: Status of the cybersecurity programme, including strategic initiatives and their results.
  - Presentation: Progress indicators or bar charts showing the progress of each project.

Key elements	Description	Recommended presentation
Impact of critical incidents on business continuity	Effects of critical incidents on key operations	Line chart with the impact of incidents over time
Strategic risks that affect the global outlook	Main risks that could affect the long-term outlook	Map of risks showing severity (high, medium, low)
Regulatory compliance and reputational risks	Compliance with regulations and their impact on reputation	Pie chart or bar chart showing compliance and risks
Progress and effectiveness of the strategic cybersecurity programme	Status and progress of strategic cybersecurity initiatives	Progress indicators, bar charts and Gantt diagrams

↳ CIO:

Goal: Provide a technical and operational overview of the state of technological systems, incidents and the effectiveness of the cybersecurity measures in place.

- **Operational status of technological systems:**
  - » Description: Summary of the availability, functioning and general status of key technological systems Includes information on the performance of critical infrastructure such as servers, networks and databases.
  - » Recommended presentation: Bar chart or traffic light icons indicating the operational status of each key system (green = operational, amber = under maintenance, red = inactive or issues present).
    1. Bar chart or traffic light icons indicating the operational status of each key system (green = operational, amber = under maintenance, red = inactive or issues present).
- **Incident response and resolution times:**
  - » Description: Measurement of incident response effectiveness. Includes average response and resolution times for different types of incidents (for example, critical cybersecurity incidents).
  - » Recommended presentation
    1. Line chart showing response and resolution times over time.
    2. Speed indicators or gauges showing average time against established targets (ideally green when within target times, yellow and red when outside).
- **Percentage of critical systems updated and patched**
  - » Description: Indication of the percentage of the organisation's critical systems that have received updates and security patches to mitigate vulnerabilities.Presentation: Pie chart or bar chart showing the percentage of regulatory compliance or incidents with reputational impact.
  - » Recommended presentation:
    1. Pie chart showing the proportion of updated versus pending critical systems.
    2. Progress bar reflecting the percentage of systems updated against the update target.
- **Technical and operational impact of recent incidents**
  - » Description: Illustration of how recent incidents have affected the performance and operability of technological systems. This may include downtime or impacts on productivity.
  - » Recommended presentation: Bar chart showing the number of incidents and downtime per incident.

Scatter chart linking the duration of the impact and the affected systems.

Key elements	Description	Recommended presentation
Operational status of technological systems	Availability and operation of key systems	Bar chart or traffic lights (green = operational, amber = under maintenance, red = issues present)
Incident response and resolution times	Average critical incident response and resolution times	Line chart with response times and metrics compared with targets
Percentage of critical systems updated	Percentage of key systems with security patches and updates	Pie chart or progress bar showing updated versus pending systems
Technical and operational impact of recent incidents	Impact of recent incidents on operations and systems performance	Bar chart with the impact of each incident, downtime and services affected

↳ CFO:

The aim of the key elements for the CFO is to provide a clear financial insight into cybersecurity costs, investment and returns, and into how these impact the business. The CFO needs to make informed decisions based on accurate financial data, and the reports should help understand how cyber security affects the organisation's finances. The specific goals are: Operational status of technological systems:

- **Assessing Incident and Risk Management Costs:**

The CFO needs to understand how much cybersecurity incident management is costing the organisation, both in terms of direct expenses (e.g. recovery, fines) and indirect costs (loss of productivity, reputational damage).

The aim is to identify areas where incident management efficiency can be improved to reduce costs.

- **Measuring Return on Investment (ROI) in Cybersecurity Measures:**

The CFO needs to see if the cybersecurity investments made are providing tangible value to the organisation. This indicator helps determine whether investments are avoiding higher costs, such as data loss, operational failures or reputational damage.

The aim is to demonstrate that cyber security is not only an expense but also an investment that boosts efficiency and reduces financial risks.

- **Ensuring Financial Regulatory Compliance:**

The CFO must ensure that the firm complies with financial regulations relating to information security and privacy (e.g. GDPR, SOX). Failure to comply with these regulations may result in financial penalties or damages.

The aim is to avoid fines and ensure that the organisation is aligned with regulatory requirements, minimising legal risks.

- **Monitoring the Assigned Budget versus Actual Cybersecurity Expenditure:**

The CFO needs to monitor how the cybersecurity budget is being used and ensure that the allocated resources are used efficiently.

The aim is to ensure that the cybersecurity budget is being spent effectively and that budget deviations are identified and corrected.

Key elements	Description	Recommended presentation
Cyber incident and cyber risk management costs	Direct and indirect costs of cybersecurity incidents	A bar chart comparing costs of different types of cyber incidents
Return on investment in cybersecurity measures	Measures the ROI of cybersecurity investment	A bar chart presenting the cost-benefit analysis
Financial regulatory compliance	Status of compliance with financial regulations	A pie or bar chart depicting the compliance level as a percentage
Budget assigned versus actual cybersecurity expenditure	Comparison between the budget assigned and actual cybersecurity expenditure	A bar chart comparing the budget versus the actual cost

↳ Management Committee:

Goal: Provide a comprehensive view of the overall cybersecurity status in the organisation, allowing Management Committee members to make informed strategic decisions about asset protection and business continuity.

- **Executive summary of the general cybersecurity status**
  - » Description: The Management Committee needs an overall view of how cyber security is being managed within the organisation. This includes a clear summary of the overall status of cybersecurity measures, current threats and how they are managed.
  - » Recommended presentation:
    1. A summary in text format with supporting graphics: A brief and concise report with the main points, supported by bar, line or traffic light charts depicting the overall cybersecurity status in a clear and easily digestible format.
    2. A visual example: A traffic light or bar chart depicting the cybersecurity system status: green (safe), amber (attention required), red (high risk).

- **KPIs and developments:**
  - » Description: The Management Committee needs to understand how the organisation is evolving in terms of cybersecurity. This is achieved through KPIs, which must be monitored over time.
  - » Recommended presentation:
    1. A bar or line chart showing how the main KPIs – such as incident numbers, average resolution time, percentage of patched systems, etc. – have developed.
    2. Speedometer or traffic light indicators showing the level of compliance or KPI status in real time.

- **Emerging risks and mitigation plans:**
  - » Description: Management Committee members should be aware of new cyber risks that could threaten the organisation and of the action plans that are being implemented to mitigate them.
  - » Recommended presentation:
    1. A risk map (heat map) that depicts risks by colours according to their level of severity (red = high, amber = medium, green = low).
    2. A bubble diagram or radar chart to visualise emerging risks and their impact and to show how mitigation plans are being implemented.

- **Progress in staff training and awareness-raising:**
  - » Description: The Man   agement Committee should understand how cybersecurity awareness and training initiatives are being conducted. These are essential to reduce human risk
  - » Recommended presentation:
    1. A bar chart showing the participation rate in training programmes, with a breakdown of completed modules and results (success rate).
    2. A pie chart showing the percentage of employees who have completed training compared with those who have not.

These templates should be tailored to the specific characteristics of each organisation and regularly updated to maintain their strategic and operational relevance.

Key elements	Description	Recommended presentation
Executive summary of general cybersecurity status	A global view of the organisation's cybersecurity status	A bar or traffic light chart or executive summary with visual indicators
Main KPIs and developments	Development of KPIs over time (incident numbers, etc.)	A bar or line chart showing how the KPIs have developed
Emerging risks and mitigation plans	Identification of new risks and mitigating action plans	A heatmap, or bubble diagram or radar chart
Progress in staff training and awareness-raising	Progress in cybersecurity training and awareness-raising for staff	A bar or pie chart depicting participation rates

ANNEX 3: RELATED REGULATIONS

This annex presents the main current regulatory frameworks, standards and guidelines that warrant the need to implement cybersecurity indicators in the organisation. These enable the CISO to select, justify and communicate key performance indicators (KPIs) and key risk indicators (KRIs), aligned with regulatory and best practice requirements.

Below they are grouped according to whether they are legislation or regulations, technical standards, or methodological guidelines, with a table that sums up their practical application.

1. European and Spanish legislation and regulations

These define security and continuous assessment obligations applicable to organisations belonging to the public, private or regulated sectors.

- NIS 2 Directive (Directive (EU) 2022/2555): It establishes cybersecurity obligations for major and essential entities. It reinforces the role of senior management as the ultimate body responsible for risks.
- DORA (Regulation (EU) 2022/2554): It obliges financial institutions to implement digital resilience measures and monitor their effectiveness.
- Cyber Resilience Act (CRA): It requires that cyber security be ensured in the design and throughout the life cycle of products that contain a digital component.
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679): It sets out technical and organisational measures whose effectiveness can be assessed by indicators.
- Esquema Nacional de Seguridad (ENS) (Royal Decree 311/2022): Spanish national security framework. Mandatory compliance for the Spanish public sector. It establishes security levels and controls that must be monitored.
- Law 8/2011 on Critical Infrastructure Protection: It requires that risk-based security plans and measures be adopted and that their effectiveness be monitored.

2. International standards and technical frameworks

These standards provide widely recognised structures for establishing, measuring and improving information security and business continuity.

- **ISO/IEC 27001:2022**: International standard for establishing an information security management system (ISMS).
- **ISO/IEC 22301:2019:** It specifies requirements for business continuity management, including recovery times (RTO and RPO).
- **ISO 31000:2018:** It provides principles and guidelines for risk management in any type of organisation.
- NIST Cybersecurity Framework v2.0 (2024): A cybersecurity framework structured around six functions: govern, identify, protect, detect, respond and recover.
- CIS Controls v8: A prioritised set of critical security controls to improve the defence of information systems.
- COBIT: An IT governance framework that aligns business objectives with performance and risk measurement.

3. Specific sectoral regulations

Certain sectors are subject to specific regulations that require quantifiable monitoring and evidence.

- EBA Guidelines (EBA/GL/2019/04 – ICT and security risk management, EBA Supervisory reporting framework): These guidelines require banking sector entities to assess and monitor ICT and security risk.
- PCI DSS v4.0: A security standard to protect payment card data, with associated controls and metrics.
- HIPAA Security Rule (45 CFR Part 164): A US Federal Standard that regulates the protection of electronic personal health information.

4. Guidelines and good practice manuals

- Cyber Green Proof (ISMS Forum): A proposal to assess the environmental impact and efficiency of cybersecurity controls.
- CCN-CERT Guidelines on indicators: Recommendations for public bodies and strategic operators on measuring and monitoring controls.

5. Specific standards and frameworks

Standard / Framework	Approach	Indicator type	Main application
ISO/IEC 27004	Information security	KPIs, effectiveness of controls	Metrics guide to assess the effectiveness of the security controls as per ISO 27001
ISO/IEC 27014	Information security governance	Strategic KPIs	Provides guidance for senior management for supervision of the cybersecurity strategy
NIST SP 800-55	Performance measurement	Effectiveness, efficiency, impact	Establishes and manages cybersecurity performance metrics
NIST CSF v2.0	General cyber security	Functionals, maturity	A structured framework focused on measurement and continuous assessment
COBIT 2019	IT governance	KPIs and KRIs	Aligns IT metrics with strategic business goals
MITRE ATTACK / D3FEND	Tactical cyber defence	Tactical indicators	Design of technical indicators on threats and defences
ENISA Metrics Guidelines	European assessment	KPIs, maturity	ENISA Guidelines on security measures for the EU
Balanced Scorecard applied to cyber security	Strategic management	Organisational KPIs	Aligns security with strategy through a comprehensive performance view

ANNEX 4: RECOMMENDED TOOLS AND RESOURCES

1. Tools for the effective visualisation of information

In the reports for senior management, information should be visualised in a way that conveys the key messages clearly, quickly and effectively.

2. Data visualisation platforms

Below are some very practical general tools to visually organise and present the information following the above principles. These tools can be used to create visualisations that are impactful, clear and aligned with visual design best practices. Some examples are:

Tool	Description	Recommended use cases	Suitability for reporting to senior management
Tableau	Powerful BI tool. Interactive dashboards and visual narratives.	Visualisation of strategic and analytic KPIs.	High
Power BI	Native integration with Microsoft 365. Ideal for corporate environments.	Tactical and operational reports.	High (especially in Microsoft environments)
Canva/ Visme	They are both graphic design tools with visually clean templates.	Individual charts or visual material for reports.	High
Flourish	Specialises in narrative interactive charts.	Visual storytelling focused on non-technical audiences.	High
Looker Studio	(Google) Free, useful for quickly assembling simple dashboards	Dashboards for regular monitoring	Medium-high
Grafana	Specialises in real time monitoring	Oriented towards operational indicators	Average (optimal for operational KPIs)

*** Please note that the tools listed are those available on the market at the time of publication and that this list can change as the market evolves. In other words, these tools have their own life cycle: they are created, developed and may change or disappear, and other new tools may emerge.**

These solutions make it possible to integrate the principles of clarity, visual consistency and structured narrative into any report or executive presentation.

3. Specialised tools for cybersecurity reporting

There are also dedicated solutions designed to visualise and communicate security indicators. Examples include:

- **SecurityScorecard:** It provides easy-to-understand security ratings and comparative visualisations of an organisation's security status. Ideal for communicating the organisation's position relative to competitors or industry standards.
- **BitSight Security Ratings:** Similar to SecurityScorecard, it enables comparative visualisations of external security metrics and how they change over time, facilitating discussions about third-party risks with senior management. It is tailored for a very specific use case.
- **SIEM Dashboards (such as QRadar, Splunk, Microsoft Sentinel):**
  - » They can be configured to display high-level indicators.
  - » They allow drill-downs for detailed analysis when needed.
  - » They have predefined templates for executive reporting.
  - » They combine multiple sources of security data, which can be further integrated with ITSM platforms to enrich that data.
- **GRC Platforms (Governance, Risk & Compliance):** GRC platforms help incorporate risk and compliance data and are very useful for reporting to senior management.

4. Resources to ensure effective reporting design

5. Templates and reporting frameworks

They are useful for maintaining visual consistency and minimising the time it takes to prepare the report:

↳ **NIST Cybersecurity Framework Dashboard Templates:** Templates aligned with the five pillars of the NIST CSF (Identify, Protect, Detect, Respond, Recover), enabling communication of the organisation's maturity status and progress.

↳ **CIS Control Visualisation Templates:** Visual resources to report the implementation status of CIS Controls, with consistent colour coding and clearly defined levels of compliance.

↳ **ISO 27001 Compliance Dashboards:** They display the status of controls and non-conformities in a visually effective manner, grouped by domain to facilitate executive understanding.

6. Colour palette and visual coding recommendations

They are used to ensure visual consistency and improve intuitive interpretation. Below are some palette recommendations by information type:

Type of information	Recommended palette*	Justification
Risk levels	Green-yellow-orange-red gradient	Universally recognisable, allows critical areas to be rapidly identified
Regulatory compliance	Blues and greys, with accents in yellow/red for exceptions	Professional and serious, adequate for regulatory contexts
Progress indicators	Greens of varying intensity	Communicates positive developments and growth
Alerts and threats	Monochromatic with accents in red	Allows urgent matters to be highlighted without visually overwhelming the viewer

*** Accessibility note: Ensure that all palettes are understandable for people with colour blindness. Tools like Colour Oracle can help check if the visualisations are accessible.**

7. Additional visual design guides and libraries

The guides and libraries listed below can help improve the visual design of these presentations, so that it facilitates understanding rather than being a cognitive barrier. Examples include:

Resource	Main use
ColorBrewer 2.0	Selection of accessible palettes (colour-blindness, printing, etc.).
Material Design	Google design systems with UX/UI principles.
Noun Project / FontAwesome	Repositories of standardised and recognisable icons.
Storytelling with Data (Cole Nussbaumer)	Book and blog with corporate reporting examples.
Datawrapper Blog / Highcharts Examples	Repositories of use cases of well-designed charts.

8. Best practices for implementation

The selection of tools must be accompanied by a structured process to ensure the effectiveness of the reports:

9. Recommended implementation process

↳ **Mapping audiences and needs:**

- Identify the different stakeholders (CEO, CFO, Board, etc.)
- Document their specific concerns and level of detail required
- Set ideal reporting frequency per stakeholder

↳ **Inventory of data sources:**

- Catalogue the available sources (security tools, GRC systems, etc.)
- Assess their quality, completeness and update frequency
- Identify information gaps

↳ **Prototyping and validation:**

- Develop prototype dashboards for each audience
- Validate it with a small group of representative users
- Refine it based on feedback before full implementation

↳ **Continuous improvement cycle:**

- Gather regular feedback on usefulness and clarity
- Review KPIs quarterly to verify relevance
- Keep the dashboard updated with new threats and strategic priorities

10. Recommendations for optimising impact

- **Create information levels:** Starting from high-level indicators with the possibility of going into further detail (“drill-down”) depending on demand.
- **Incorporate benchmarks:** Where possible, include industry benchmarks or recognised standards to contextualise performance.
- **Balance technical and business metrics:** Link technical indicators with business impacts to improve their relevance for senior management.
- **Simplify intelligently:** Do not confuse simplicity with oversimplification. Choose visual representations that convey complexity in an accessible manner.

This structured approach, combined with the right tools, will ensure that reports to senior management not only inform, but allow them to make informed strategic decisions on cyber security.

11. Recommendations for use. Practical takeaways

Some key practices that can help the CISO are:

- Construct visualisations with a purpose: each chart must respond to a question or reinforce a key message.
- Adapt visualisations to the audience: reporting to a CFO is not the same as reporting to a management committee or to Human Resources.
- Apply the “five seconds” rule: if the main idea is not understood within five seconds, the chart should be redesigned.
- Less is more: avoid cluttered dashboards. Quality should be prioritised over quantity.
- Update visualisations: make sure the data are up to date and relevant for the decision cycle.

Cyber Indicators Framework:

THE CISO AND SENIOR MANAGEMENT

Contacta con nosotros

Si estás interesado en colaborar con nosotros o necesitas más información sobre nuestros proyectos, escríbenos a: **proyectos@ismsforum.es**