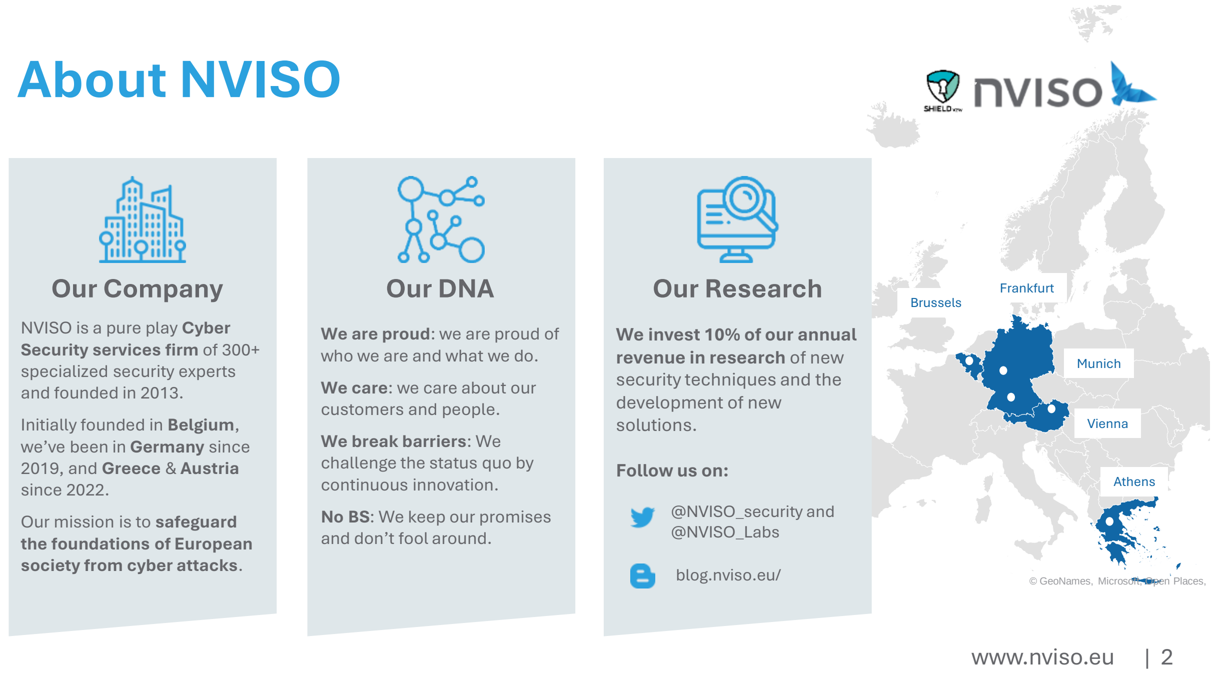
www.nviso.eu

Onboarding your Board on Cyber

Effective Cyber Risk Reporting to the Board: Insights and Strategies

Pieter Batsleer – pieter.batsleer@nviso.eu
11/03/2025

1



About NVISO

Our Company

NVISO is a pure play **Cyber Security services firm** of 300+ specialized security experts and founded in 2013.

Initially founded in **Belgium**, we've been in **Germany** since 2019, and **Greece** & **Austria** since 2022.

Our mission is to **safeguard the foundations of European society from cyber attacks**.

Our DNA

We are proud: we are proud of who we are and what we do.

We care: we care about our customers and people.

We break barriers: We challenge the status quo by continuous innovation.

No BS: We keep our promises and don't fool around.

Our Research

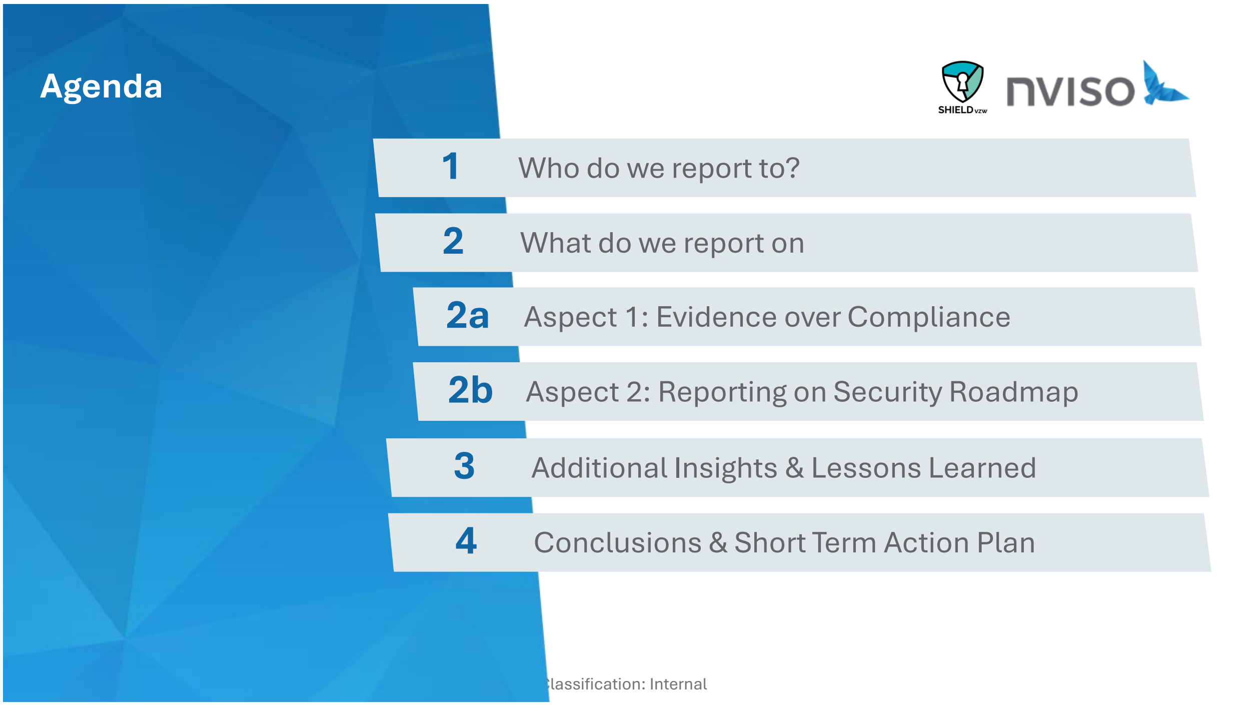
We invest 10% of our annual revenue in research of new security techniques and the development of new solutions.

Follow us on:

@NVISO_security and @NVISO_Labs

blog.nviso.eu/

2



Agenda

SHIELD vzw nviso

1	Who do we report to?
2	What do we report on
2a	Aspect 1: Evidence over Compliance
2b	Aspect 2: Reporting on Security Roadmap
3	Additional Insights & Lessons Learned
4	Conclusions & Short Term Action Plan

Classification: Internal

3

Who to report to?

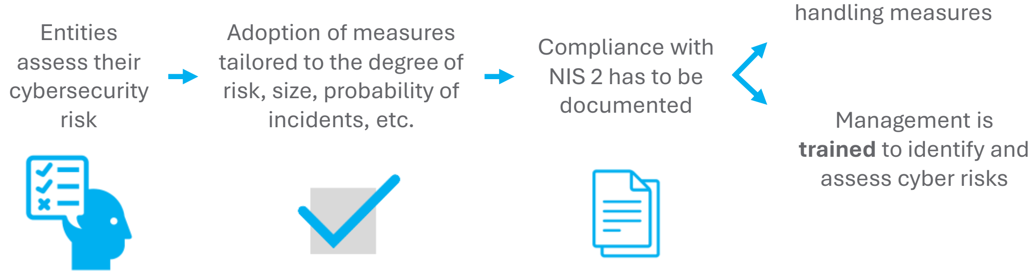
www.nviso.eu

SHIELD vzw nviso

4

What reporting is expected by NIS2?

Risk-based implementation of cyber security measures



Entities assess their cybersecurity risk → Adoption of measures tailored to the degree of risk, size, probability of incidents, etc. → Compliance with NIS 2 has to be documented

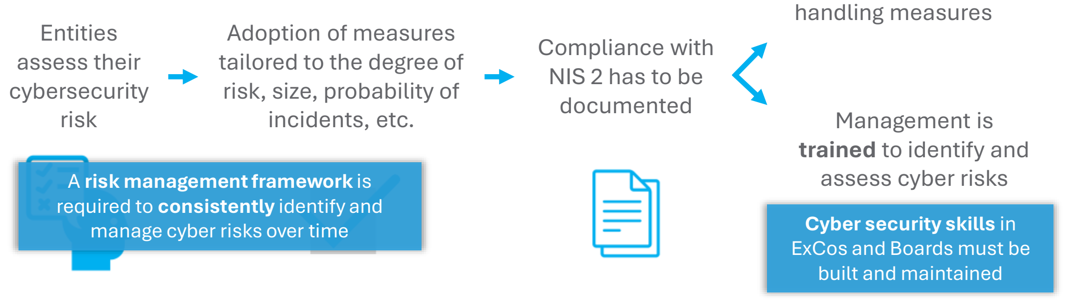
Management **approves** the cybersecurity risk handling measures

Management is **trained** to identify and assess cyber risks

What reporting is expected by NIS2?

Cyber risk management is **steered by ExCo & Board**

Risk-based implementation of cyber security measures



Entities assess their cybersecurity risk → Adoption of measures tailored to the degree of risk, size, probability of incidents, etc. → Compliance with NIS 2 has to be documented

Management **approves** the cybersecurity risk handling measures

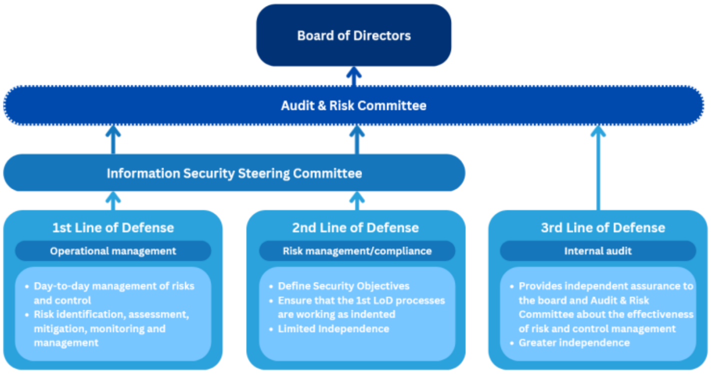
Management is **trained** to identify and assess cyber risks

A **risk management framework** is required to **consistently** identify and manage cyber risks over time

Cyber security skills in ExCos and Boards must be built and maintained

Reporting Structures

Thre Three Lines of Defense Model



Board of Directors

Audit & Risk Committee

Information Security Steering Committee

1st Line of Defense

Operational management

- Day-to-day management of risks and control
- Risk identification, assessment, mitigation, monitoring and management

2nd Line of Defense

Risk management/compliance

- Define Security Objectives
- Ensure that the 1st LoD processes are working as indented
- Limited Independence

3rd Line of Defense

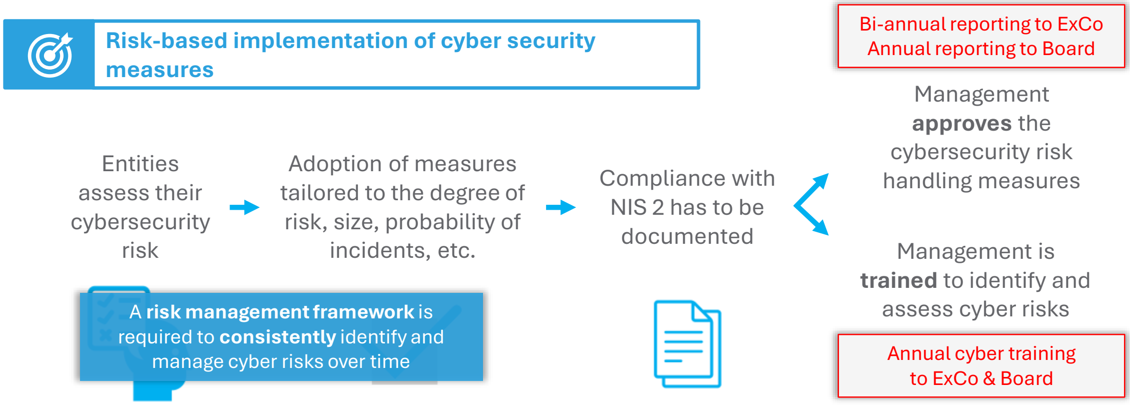
Internal audit

- Provides independent assurance to the board and Audit & Risk Committee about the effectiveness of risk and control management
- Greater independence

Key Considerations

- Setup of an Information Security Steering Committee is essential (but can be limited to 1st LoD & 2nd LoD)
- Compose your information security steerco carefully:
  - Ensure certain executive representation (mandate); &
  - Keep it mind it is better to meet less frequently with the right people than more frequently with the wrong people.
- Don’t forget, however, periodic updates to the board, too. Possibly by leveraging the “Audit & Risk Committee”, or ad-hoc.

What reporting is expected by NIS2?



Risk-based implementation of cyber security measures

Entities assess their cybersecurity risk → Adoption of measures tailored to the degree of risk, size, probability of incidents, etc. → Compliance with NIS 2 has to be documented

A **risk management framework** is required to **consistently** identify and manage cyber risks over time

Bi-annual reporting to ExCo
Annual reporting to Board

Management **approves** the cybersecurity risk handling measures

Management is **trained** to identify and assess cyber risks

Annual cyber training to ExCo & Board

What to report on?

www.nviso.eu

9

Aspect 1: Evidence Over Compliance

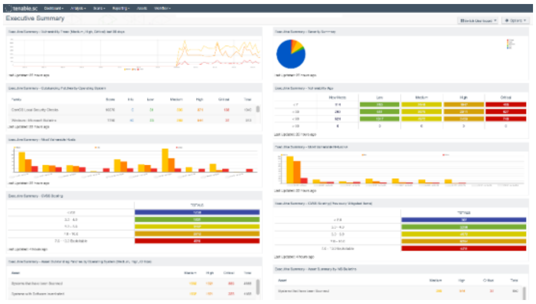
- Too often, there's too much focus on reporting purely based on a compliance framework.
- Compliance checklists, while useful for ensuring adherence to regulatory requirements (such as NIS2), often **fail to address** the dynamic and evolving nature of cyber threats.
- To enhance board reporting and decision-making, it is essential to shift the focus from mere compliance to **evidence-based risk assessments**.
- Continuous monitoring and data-driven insights provide a more **accurate** and **nuanced** picture of the organization's security posture, enabling the board to understand the actual risks and make informed decisions.

10

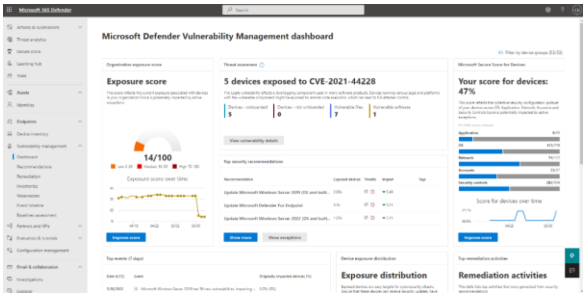
Aspect 1: Evidence Over Compliance

Examples

Vulnerability Management Solution: Helps organizations proactively detect weaknesses that could be exploited by attackers, thereby enhancing their security posture. Typically, however Vulnerability Scanners/Management Solutions provide by default Executive/CISO-view dashboards, from which interesting insights can be reported.



https://www.tenable.com/sc-dashboards/executive-summary-dashboard



https://learn.microsoft.com/en-us/defender-vulnerability-management/tvm-dashboard-insights

Aspect 1: Evidence Over Compliance

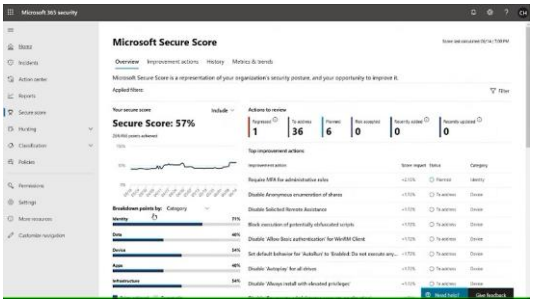
Examples

Microsoft 365 Secure Score

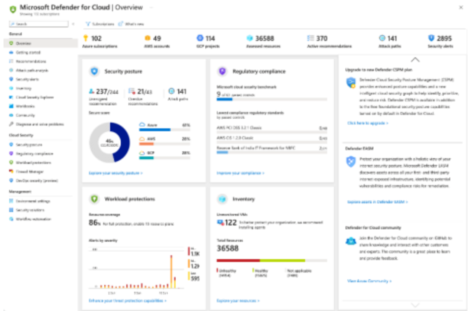
Provides a clear, numerical value that reflects how well your organization has implemented security controls. The score is determined by assessing the configurations, behaviors, and other security-related activities within your Azure Microsoft 365 tenant.

Defender for Cloud Secure Score

Microsoft Defender for Cloud's Secure Score measures an organization's cloud security posture, identifying misconfigurations, vulnerabilities, and compliance gaps



Source: https://www.microsoft.com/nl-be/security/business/microsoft-secure-score



https://learn.microsoft.com/en-us/azure/defender-for-cloud/overview-page

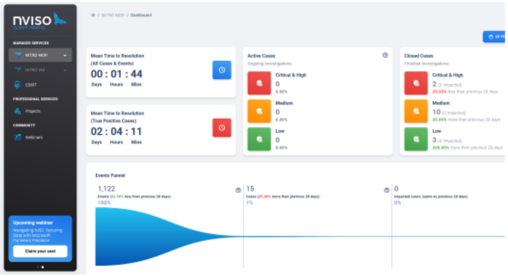
Aspect 1: Evidence Over Compliance

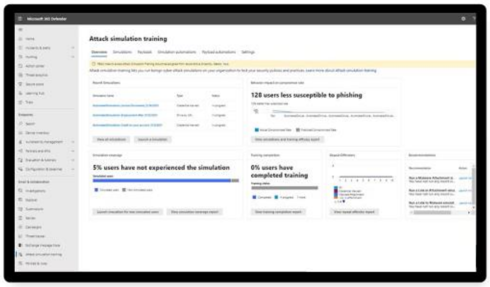
Examples

SHIELD vzw nviso

Statistics can have a significant business impact by providing insights into the effectiveness of an organization's security posture and the efficiency of its incident response processes

Statistics can have a significant business impact by providing insights into the effectiveness of an organization's security posture and the efficiency of its incident response processes




Microsoft 365 Defender
Attack simulation training
Overview
Simulations
Payloads
Simulation automations
Payload automations
Settings
128 users less susceptible to phishing
5% users have not experienced the simulation
0% users have completed training

https://www.microsoft.com/en-us/security/business/threat-protection/attack-simulation-training#tabx0116a224db0245ed8d83fd510b6d86c5

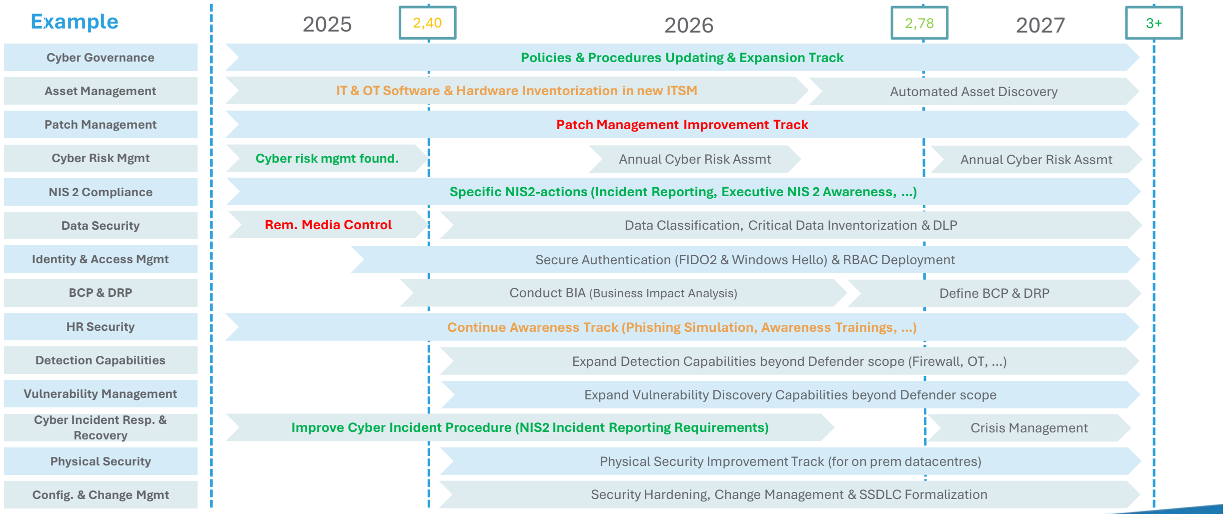
Aspect 2: Reporting on Security Roadmap

SHIELD vzw nviso

Priorization of Key/Critical Controls

- In any organization, resources are **limited**, and it is not feasible to protect all assets equally. **Prioritizing key/critical controls** that mitigate the most significant risks is essential.
- In the healthcare sector, examples of critical controls include **data encryption, access controls,** and regular **security assessments** of internet-facing assets.
- Identifying the "**crown jewels**" of your organization—those assets that are most critical to patient care and business operations—is a key step in prioritizing controls.
- By prioritizing critical controls, organizations can **focus resources** where they are most needed and provide the board with assurance that key risks are being addressed.

Aspect 2: Reporting on Security Roadmap



Cyber Governance	Policies & Procedures Updating & Expansion Track
Asset Management	IT & OT Software & Hardware Inventorization in new ITSM Automated Asset Discovery
Patch Management	Patch Management Improvement Track
Cyber Risk Mgmt	Cyber risk mgmt found. Annual Cyber Risk Assmt Annual Cyber Risk Assmt
NIS 2 Compliance	Specific NIS2-actions (Incident Reporting, Executive NIS 2 Awareness, …)
Data Security	Rem. Media Control Data Classification, Critical Data Inventorization & DLP
Identity & Access Mgmt	Secure Authentication (FIDO2 & Windows Hello) & RBAC Deployment
BCP & DRP	Conduct BIA (Business Impact Analysis) Define BCP & DRP
HR Security	Continue Awareness Track (Phishing Simulation, Awareness Trainings, …)
Detection Capabilities	Expand Detection Capabilities beyond Defender scope (Firewall, OT, …)
Vulnerability Management	Expand Vulnerability Discovery Capabilities beyond Defender scope
Cyber Incident Resp. & Recovery	Improve Cyber Incident Procedure (NIS2 Incident Reporting Requirements) Crisis Management
Physical Security	Physical Security Improvement Track (for on prem datacentres)
Config. & Change Mgmt	Security Hardening, Change Management & SSDLC Formalization

Aspect 2: Reporting on Security Roadmap

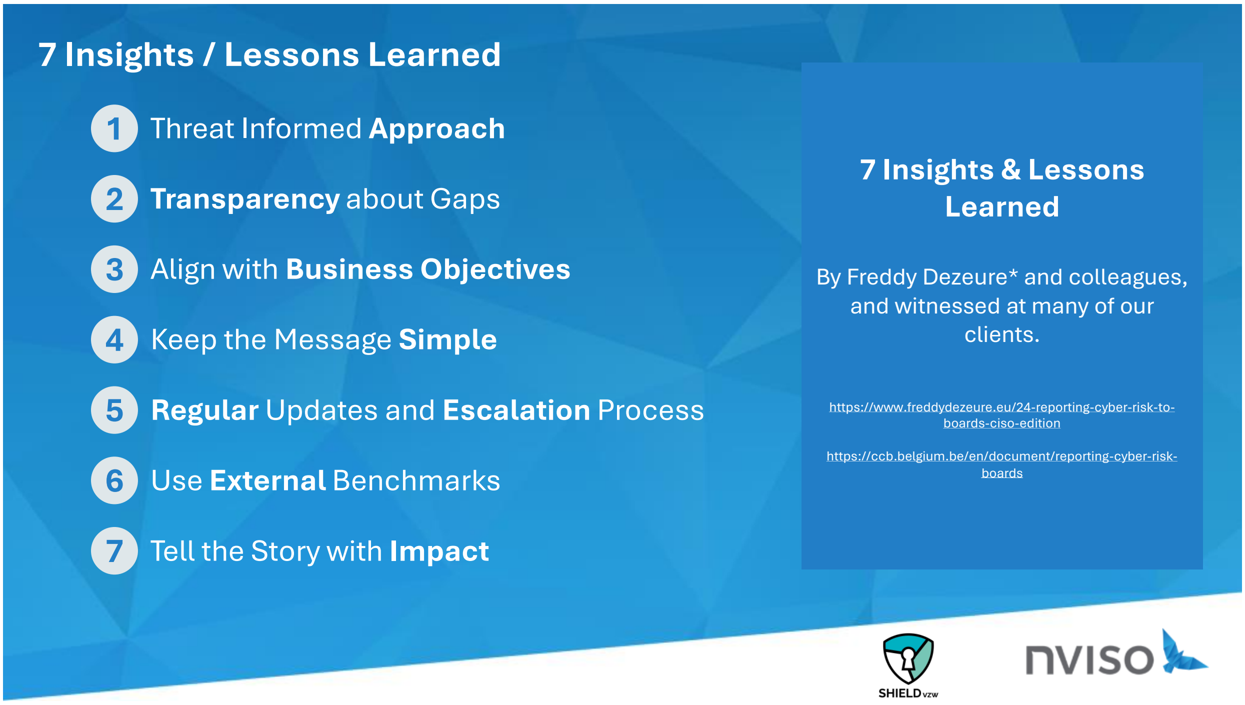
Key Control Indicators

- As an extension to key controls, you can utilize key control indicators (KCIs).
- Key Control Indicators are metrics that provide insights into the effectiveness of critical security controls. For healthcare organizations, relevant KCIs may include:
  - Percentage of systems with Multi-Factor Authentication (MFA) implemented.
  - Percentage of critical assets with regular vulnerability assessments.
  - Time to recover key assets following a cybersecurity incident.
  - Percentage of endpoints with up-to-date antivirus software.
- By focusing on KCIs, IT and security professionals can provide the board with a clear and concise view of the organization's cybersecurity posture.
- In addition to identifying relevant KCIs, it is important to establish benchmarks and targets for each indicator. Regularly reviewing and updating KCIs ensures that they remain aligned with the organization's evolving risk landscape and strategic priorities.
- Not only relevant for the board. This is essential in CyFun & ISO27001 for your NIS2 compliance too.

Insights & Lessons Learned

www.nviso.eu

17



7 Insights / Lessons Learned

1. Threat Informed **Approach**
2. **Transparency** about Gaps
3. Align with **Business Objectives**
4. Keep the Message **Simple**
5. **Regular** Updates and **Escalation** Process
6. Use **External** Benchmarks
7. Tell the Story with **Impact**

7 Insights & Lessons Learned

By Freddy Dezeure* and colleagues, and witnessed at many of our clients.

https://www.freddydezeure.eu/24-reporting-cyber-risk-to-boards-ciso-edition

https://ccb.belgium.be/en/document/reporting-cyber-risk-boards

18

Wrap Up

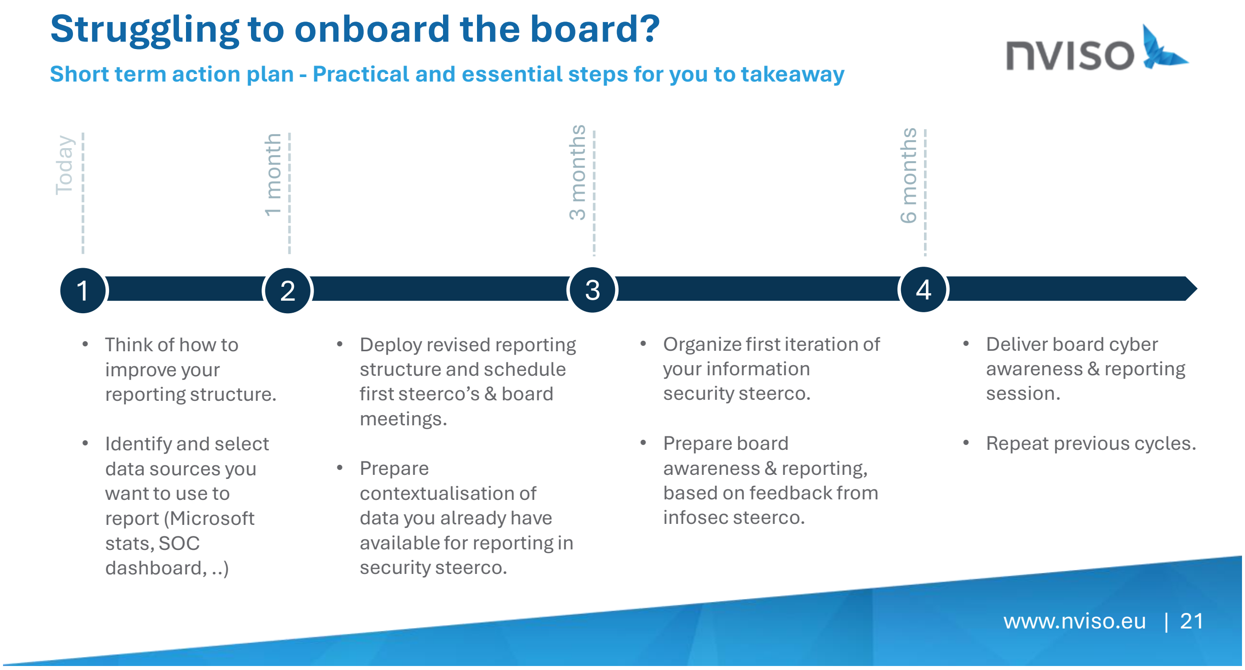
Conclusion & advised next steps

www.nviso.eu

SHIELD vzw

Struggling to onboard the board?

- Define a reporting structure, which involves executives and the board, fit for your organisation: *"It's better to report less frequent to the right people, than more frequently to the wrong people".*
- Identify what you want to report on, in the limited time you have with them.
  - Evidence over compliance; and
  - Reporting progress of your roadmap (with the goal to achieve risk-reduction and compliance).
- Keep messages simple and linked to the business objectives, so that it is relatable for people who are not cyber security experts.



Struggling to onboard the board?

Short term action plan - Practical and essential steps for you to takeaway

nviso
Today
1 month
3 months
6 months
1
2
3
4

1 (Today)

- Think of how to improve your reporting structure.
- Identify and select data sources you want to use to report (Microsoft stats, SOC dashboard, ..)

2 (1 month)

- Deploy revised reporting structure and schedule first steerco's & board meetings.
- Prepare contextualisation of data you already have available for reporting in security steerco.

3 (3 months)

- Organize first iteration of your information security steerco.
- Prepare board awareness & reporting, based on feedback from infosec steerco.

4 (6 months)

- Deliver board cyber awareness & reporting session.
- Repeat previous cycles.

Questions & Answers

www.nviso.eu

SHIELD vzw
nviso