



Less is More

Freddy Dezeure
Microsoft Deputy CISO for Europe

Flashback



Flashforward





EU Compliance

NIS2

Network
Information
Security

DORA

Digital
Operational
Resilience Act

CRA

Cyber
Resilience Act



NIS2

Network
Information
Security

DORA

Digital
Operational
Resilience Act

CRA

Cyber
Resilience Act

Guidance – best practice security & resilience

Transparency – reporting obligations

Supply chain dependencies

Accountability – board involvement

Risk-based

Risk

Insecure

Exposed

Targeted

ICT is a primary business process

ICT is top #3 corporate risk


Impact is beyond local

ICT experts work in silos

ICT perceived as “dark art”

ICT risk is delegated



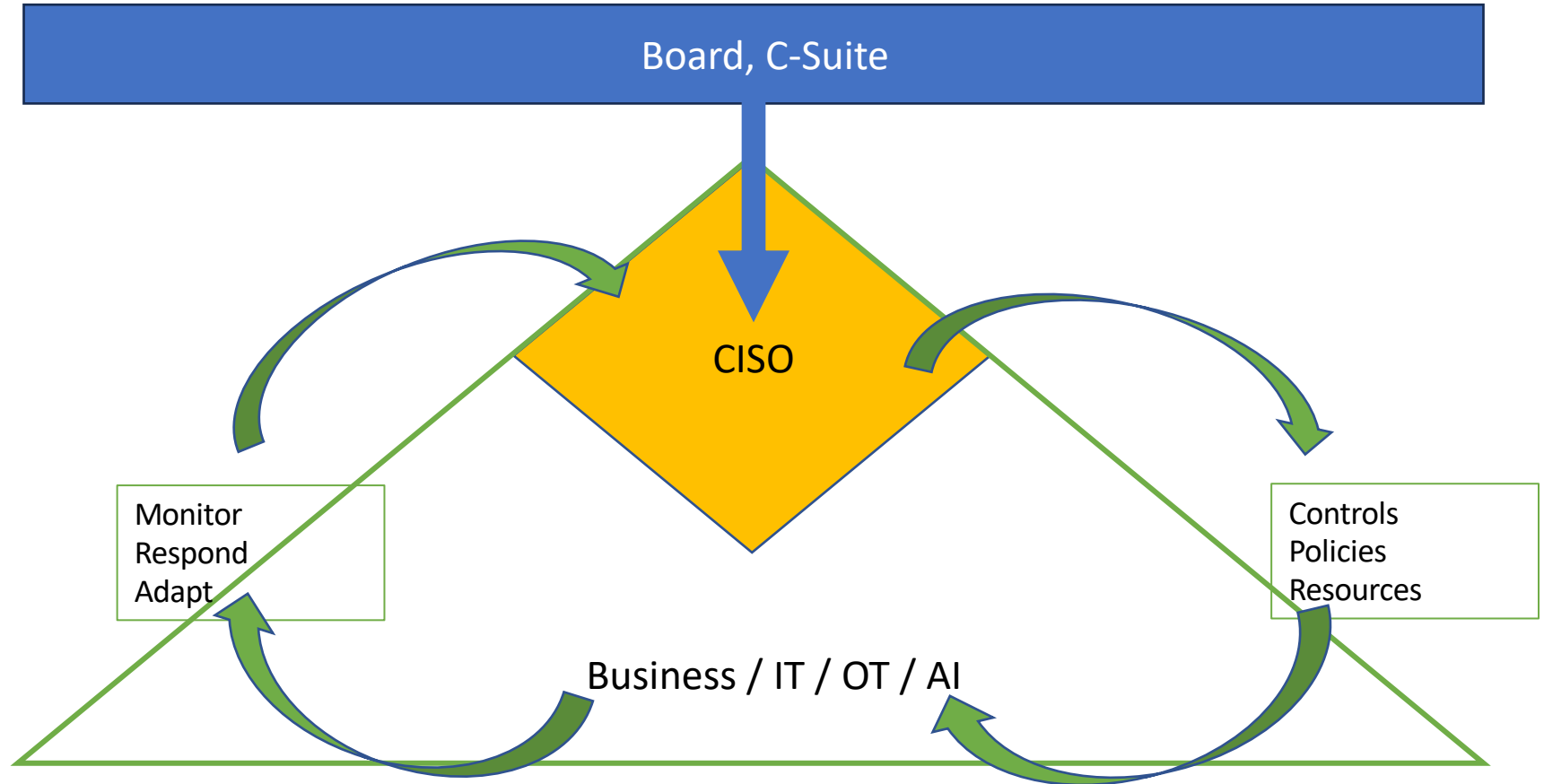


NO-ICT
is no ICT problem*

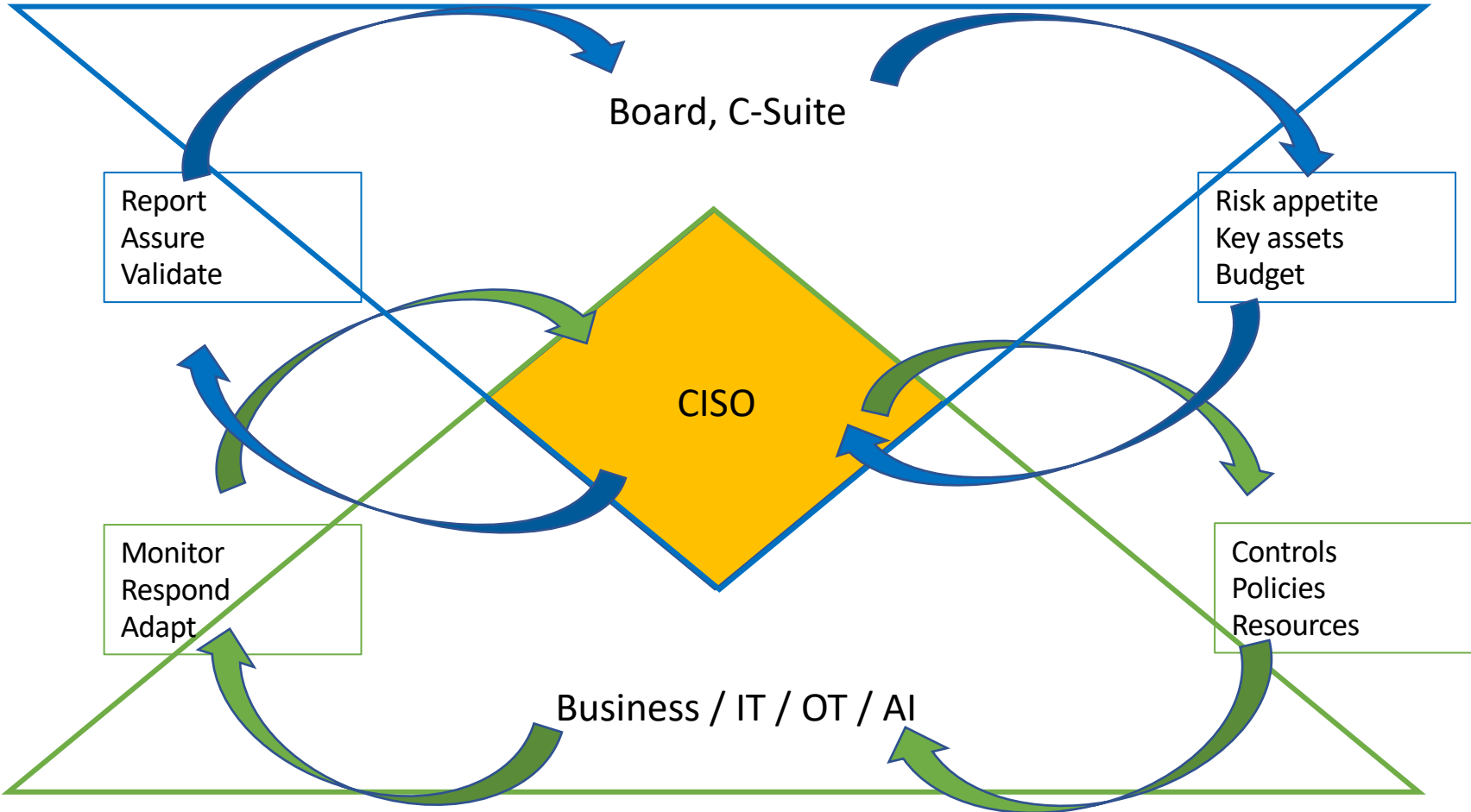
Accountability + Liability



Accountability



Accountability

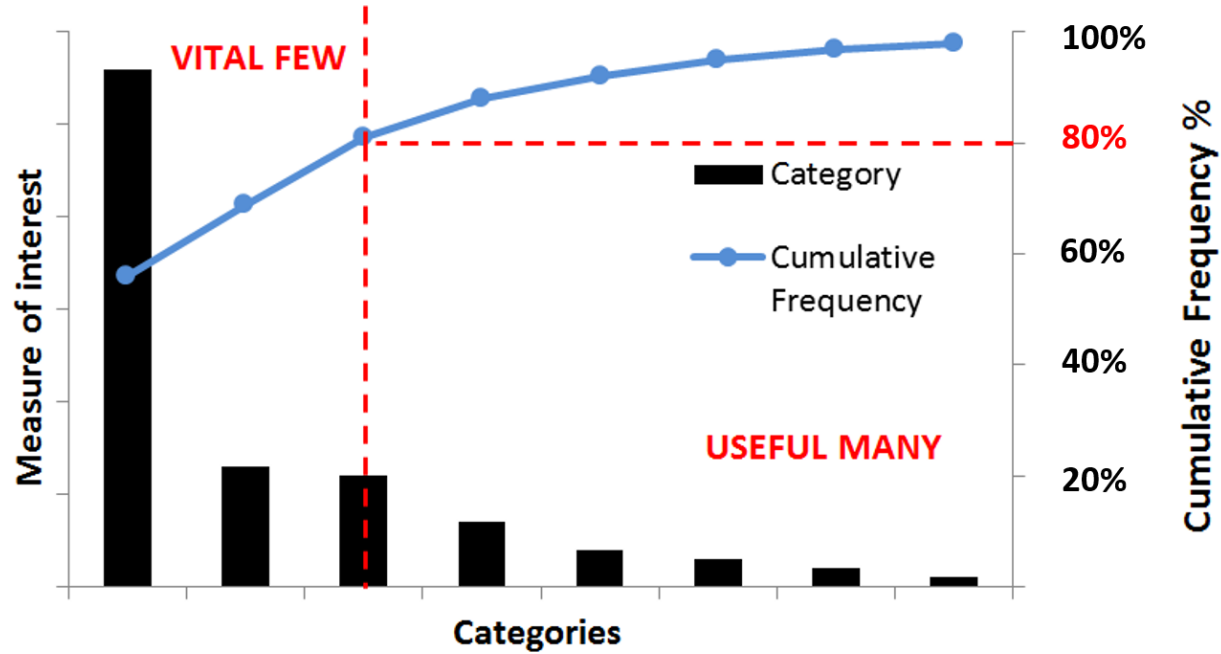


A modern conference room with a large wooden table, black leather chairs, and a panoramic view of a city skyline. The room is well-lit with natural light from the large windows. The text "Board Oversight of Risks" is overlaid in a red box at the top right, and "Lessons learnt" is overlaid in white text at the bottom center.

Board Oversight of Risks

Lessons learnt

Less is More



Oversight pitfall 1

Report everything, indifferently

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



Oversight pitfall 1

Report everything, indifferently

KCI 1	Asset Inventory	% assets in the inventory within policy
KCI 2	Privileged accounts	% privileged accounts managed within policy
KCI 3	Timely patching	% high risk patches within N hours # of known exploited vulnerabilities detected
KCI 4	Back-up	Maximum time to recover key assets (% of critical assets recoverable in N hours)
KCI 5	Endpoint protection	% endpoints configured in line with policy
KCI 6	Logs collection	% critical systems onboarded to log collection
KCI 7	Network security	% compliant key network security configurations
KCI 8	Third Party compliance	% compliant key third-party connections
KCI 9	Identity management	% coverage of systems using MFA
KCI 10	Major Incidents	% major cyber incidents with business impact
KCI 11	Risk Acceptance	# risk accepted policy deviations
KCI 12	Internet exposed assets security coverage	% of Internet exposed assets covered by security monitoring and regular security assessment
KCI 13	Crown jewel coverage	% of crown jewels covered by security monitoring, vulnerability scanning and regular security assessment
KCI 14	Origin of Security Incidents	% of security incidents related to failures from at least one Key Control Indicator

- Prioritise over completeness
- Align internally
- Define outcomes, measure, report

Oversight pitfall 2

Condense everything in averages





Oversight pitfall 2

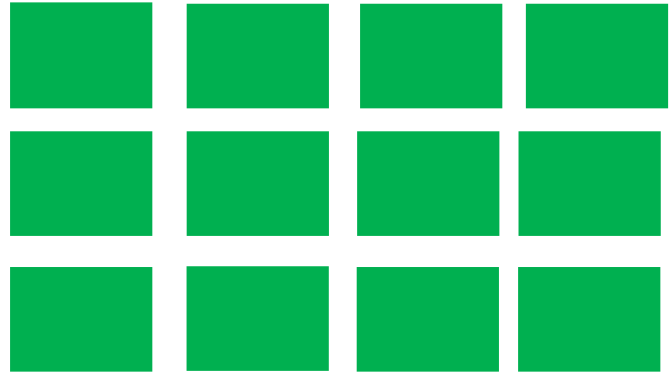
Condense everything in averages

- “God is in the details”
- Simplify – but not too much
- Identify critical risks - and their impact



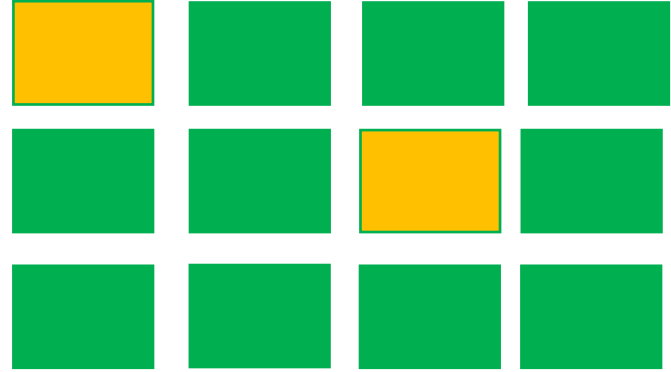
Oversight pitfall 3

Report all green



Oversight pitfall 3

Report all green



- Report key gaps and exceptions
- With the risk impact
- And the mitigation / remediation plan

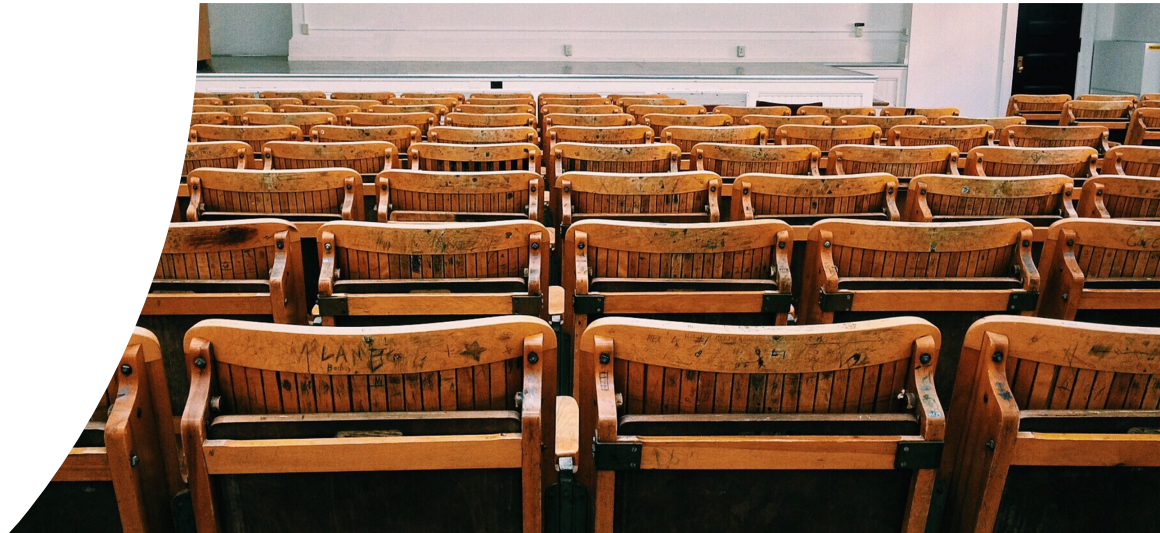
A person wearing a dark blue suit, a white shirt, and a red tie. Their right hand is raised, with the index and middle fingers extended upwards, forming a 'V' shape. The background is a solid light blue.

TRAINING

Lessons learnt

Board training pitfall 1

Send your Board members to class



Board training pitfall 1

Send your Board members to class



Training in all hands meeting

In person

During a regular Board meeting

Board training pitfall 2

Use off-the-rack training content



Board training pitfall 2

Use off-the-rack training content



- Content tailored to the organisation
- Using their language
- Referring to their existing governance
- Providing feedback on gaps

Board training pitfall 3

Train them as mini-CISOs

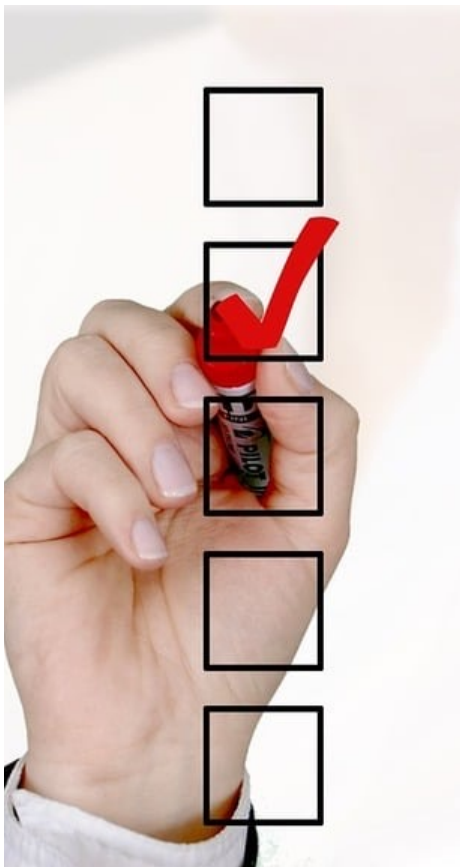


Board training pitfall 3

Train them as mini-CISOs



- Explain cyber risk as business risk
- Identify risk appetite
- Provide guidance to oversee
- Less is more

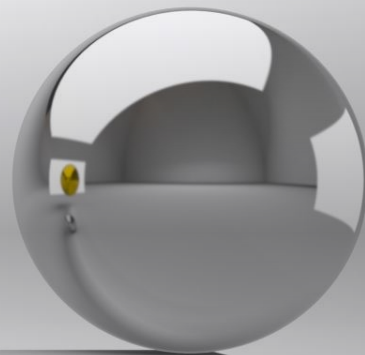
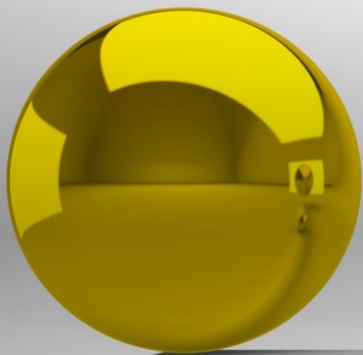


Compliance?

Security & Resilience?



Auditors - Regulators

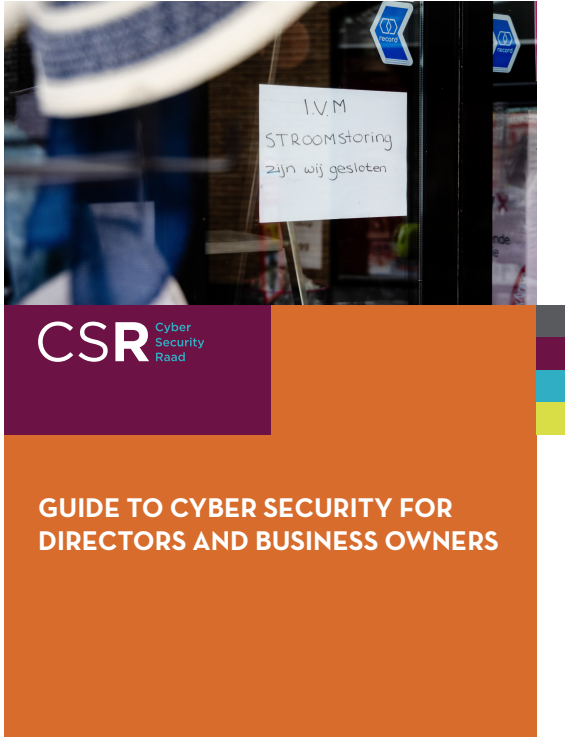


Risk-based means prioritization

- Risks - controls - oversight
- Governance - accountability
- First, second and third line of defense
- But also audit and regulatory oversight
- Compliance turning into security and resilience
- The goal is within reach



More



<https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/>

<https://www.cybersecuritycouncil.nl/documents/2025/08/14/guide-to-cyber-security-for-directors-and-business-owners>