



Train or Blame your Board?

Freddy Dezeure
Cybersec Europe

Insecure
Exposed
Targeted

ICT experts working in silos
ICT perceived as “dark art”
ICT risk is delegated

ICT is a primary business process
ICT is top #3 corporate risk
Impact is beyond local



The image shows two soldiers in camouflage uniforms and caps. The soldier on the left is holding a black handheld radio to his mouth. The soldier on the right is looking down at a piece of equipment on the ground. A green equipment case with 'CAME' written on it is visible. To the right, there is a large, complex antenna structure on a tripod. The background is a hazy, outdoor setting with some vegetation and a fence.

NO-IT
is no IT problem*

*Quote Schuberg Philis

New EU legislation

NIS2

Network
Information
Security

DORA

Digital
Operational
Resilience Act

CRA

Cyber
Resilience Act

New EU legislation

NIS2

Network
Information
Security

DORA

Digital
Operational
Resilience Act

CRA

Cyber
Resilience Act

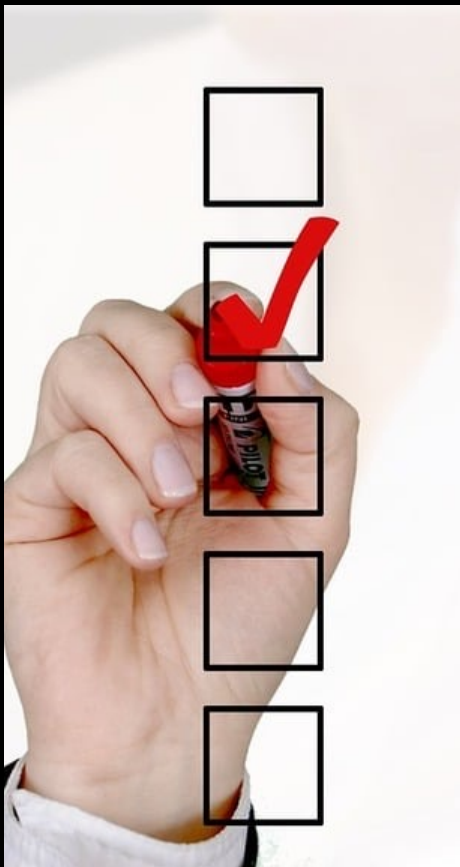
Guidance – best practice security

Transparency – reporting obligations

Accountability – board involvement

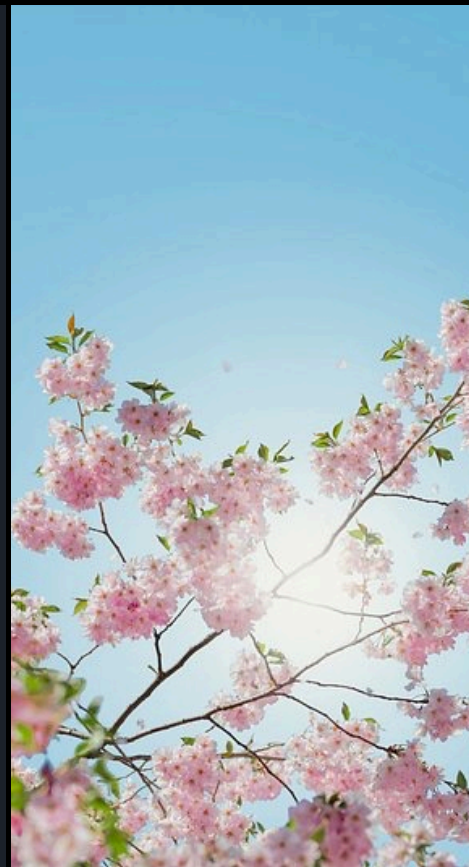
Liability – individual/collective

Competency – training obligations



Compliance?

Resilience?



Accountability + Liability



A person wearing a dark blue suit, a white shirt, and a red tie is shown from the chest up. Their right hand is raised, with the index and middle fingers extended upwards and slightly to the left, while the thumb, ring, and pinky fingers are curled. A semi-transparent blue rectangular box is overlaid across the middle of the image, containing the word 'TRAINING' in large white capital letters. Below this box, the words 'Lessons learnt' are written in a smaller white font. The background is a solid light blue.

TRAINING

Lessons learnt

Pitfall 1

Send your Board members to class



Pitfall 1

Send your Board members to class



Training in all hands meeting

In person

During a regular Board meeting

Pitfall 2

Use off-the-rack training content



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

Pitfall 3

Train them as mini-CISOs



Pitfall 3

Train them as mini-CISOs



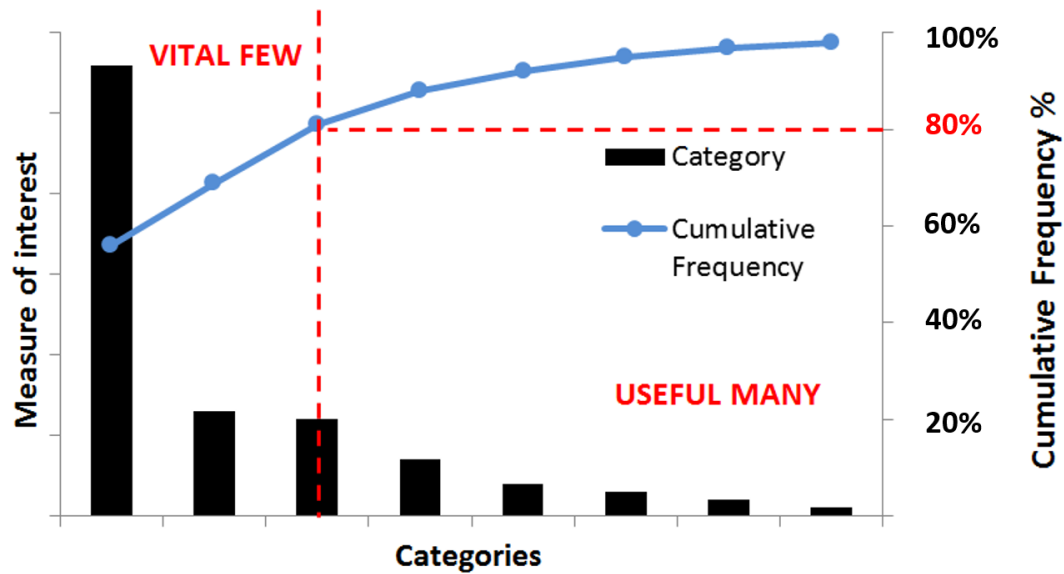
- Explain cyber risk as business risk
- Identify risk appetite
- Prompt the questions to ask
- Provide guidance to oversee

Framework + Certificate?



Not the panacea
Choose One

Less is More



Less is More



Prioritize



Align internally



Define outcomes



Measure



Report

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

Pitfall 4

Condense everything in averages





Pitfall 4

Condense everything in averages

- Simplify – but not too much
- Help to identify critical risks
- And their impact



Content part 1: Legal context

- Developments regulatory frameworks in EU-US
- Disclosure of risk oversight / incidents
- Personal responsibility/liability
- Management/supervisory Board scope
- Role / exposure of CISO

NIS2

Network
Information
Security

DORA

Digital
Operational
Resilience
Act

CRA

Cyber
Resilience
Act

Tailoring

- Specific Board structure (one/two tier, exec/non-exec, subsidiaries)
- Specific regulatory and liability aspects
- Current oversight modalities and governance
- Insurance of corporate and individual risk

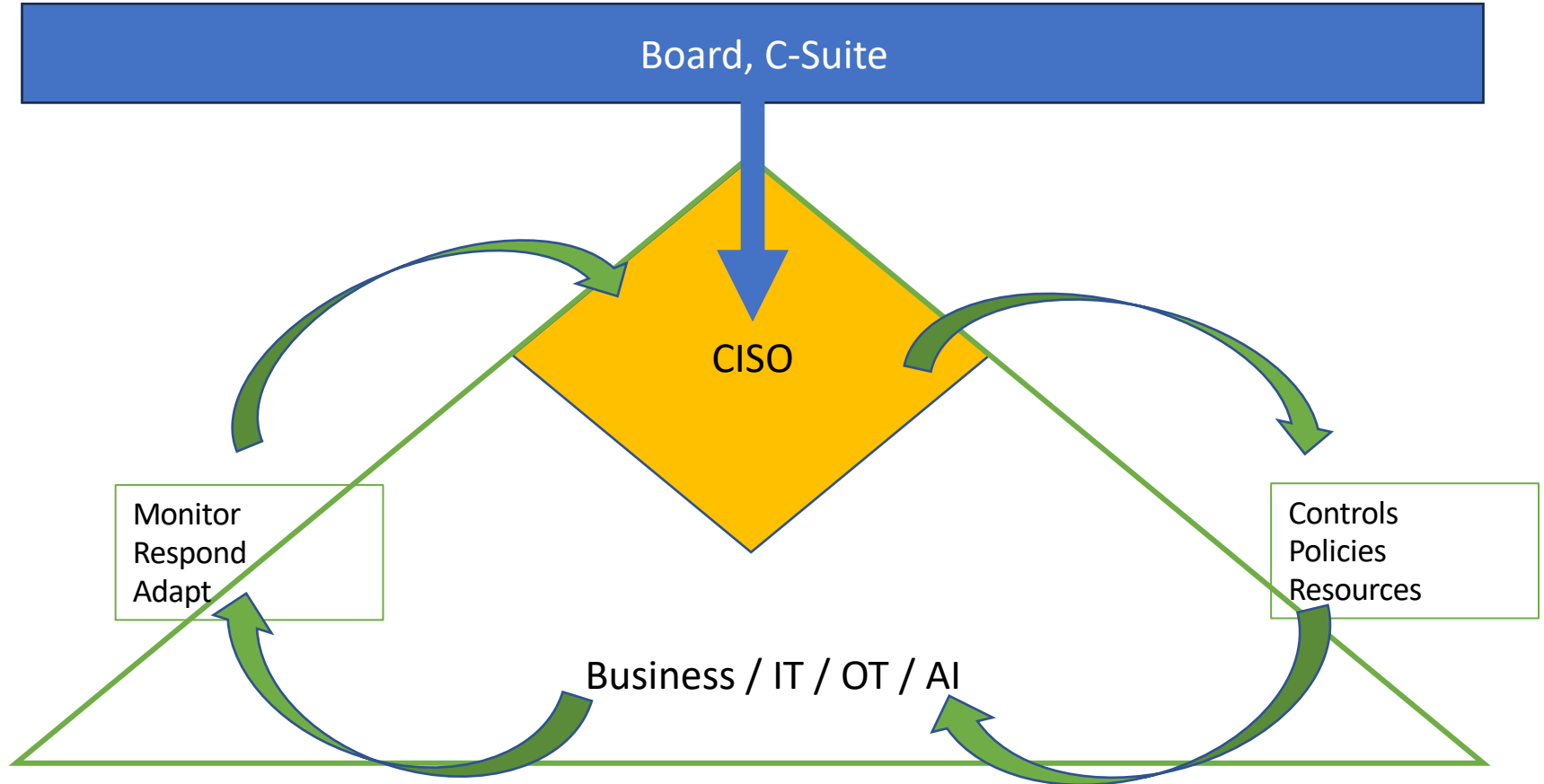
Content part 2: Risk management

- IT/Cyber risk <-> business risk
 - Risk appetite
 - Compliance <-> resilience
 - Frameworks / mapping
 - Key controls
-
- Specific threat environment and risk appetite
 - Prioritisation of controls and outcomes
 - Internal alignment
 - CISO reporting line and airtime

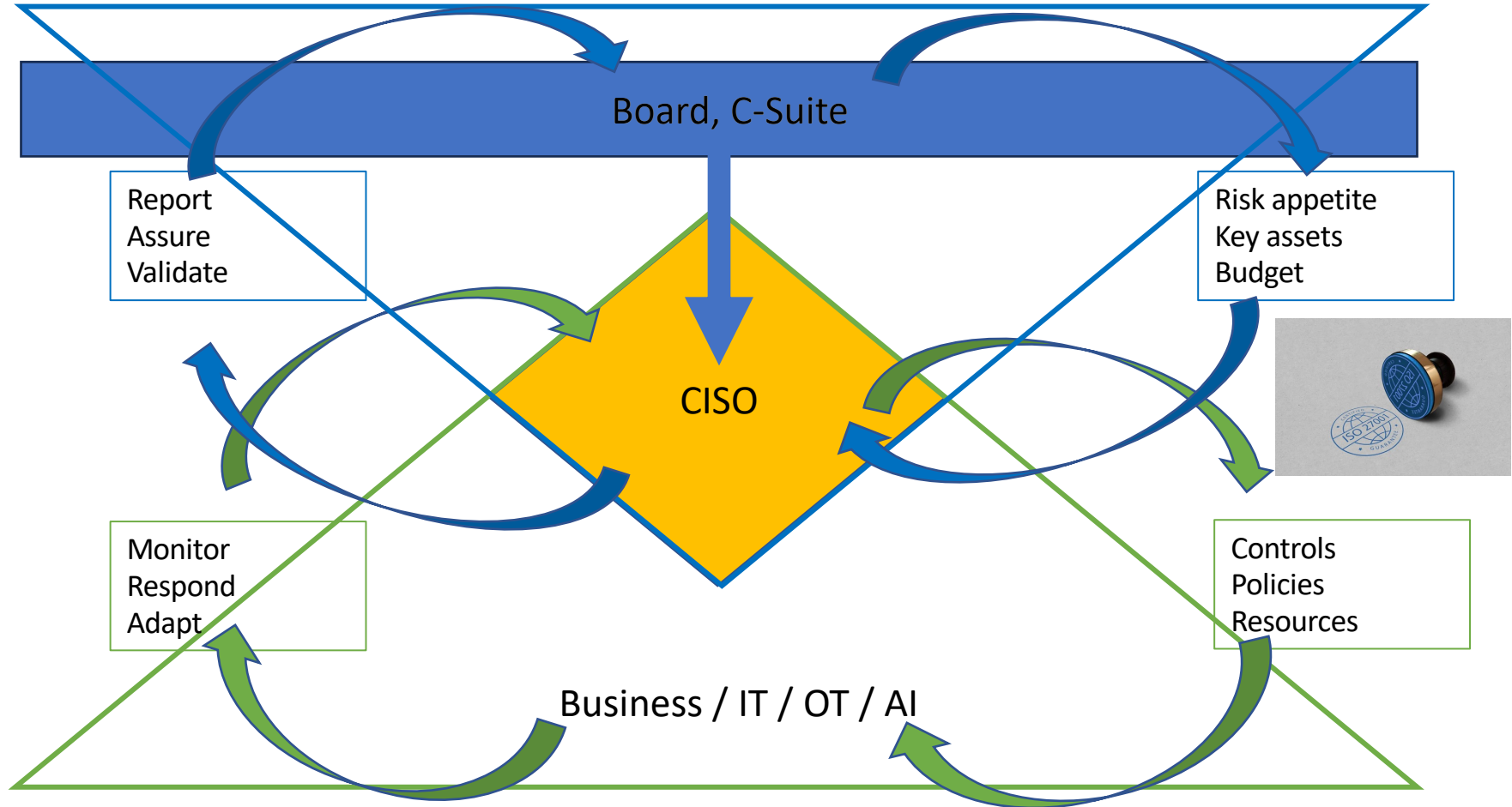
Tailoring



Accountability



Accountability



Preparation (with CISO, risk, audit, GC)

- Initial discussion to explain approach and request material
 - Analysis of current situation (governance, reports)
 - Tailoring of the slide deck, including feedback
 - Discussion with the stakeholders
 - Multiple versions of the deck
-
- Anxiety and resistance on slides and feedback
 - Laborious process, unavoidable and necessary



A photograph of pink cherry blossoms in full bloom, with some petals falling, set against a clear blue sky. The blossoms are in the lower-left foreground, and the sky fills the rest of the frame.

Training with impact

- The organisation changes in the process
- The Board asks to improve reporting and integrates cyber in their oversight
- The governance is changed and the CISO is put into 'position'
- Compliance turned into resilience
- The impossible comes within reach

Want to know more?

[Ten key insights for informed cyber oversight](#)

Available in EN, FR, DE, NL, IT, ES, PT, EL, PL, RO



Don't hide the risk, manage it

FreddyDezeure.eu