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


NO-IT
is no IT problem*
*Quote Schuberg Philis

New EU legislation

New EU legislation

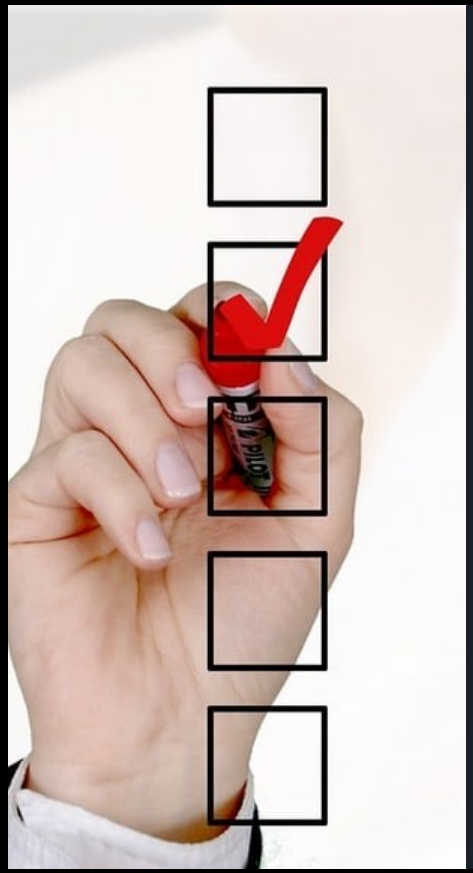
Guidance – best practice security

Transparency – reporting obligations

Accountability – board involvement

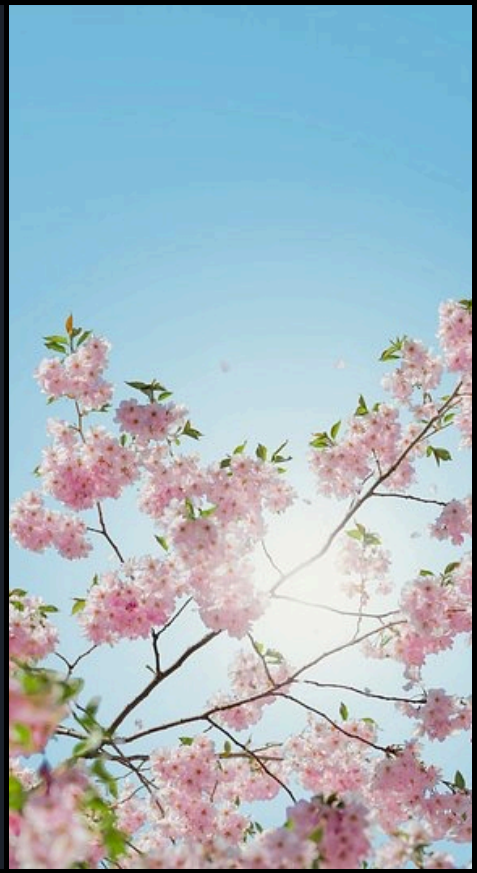
Liability – individual/collective

Competency – training obligations



Compliance?

Resilience?

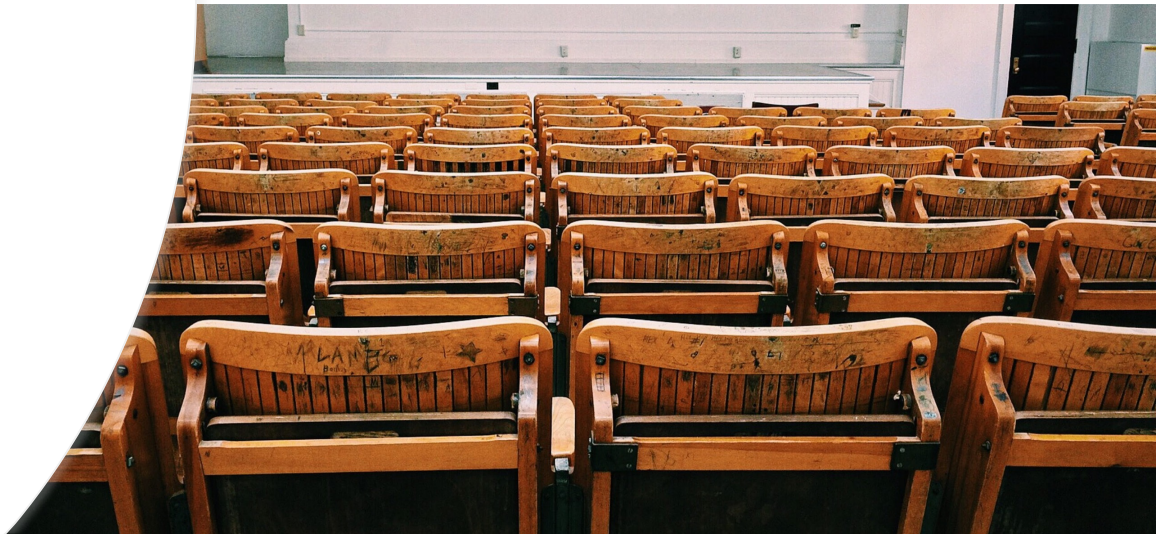



Accountability +
Liability


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

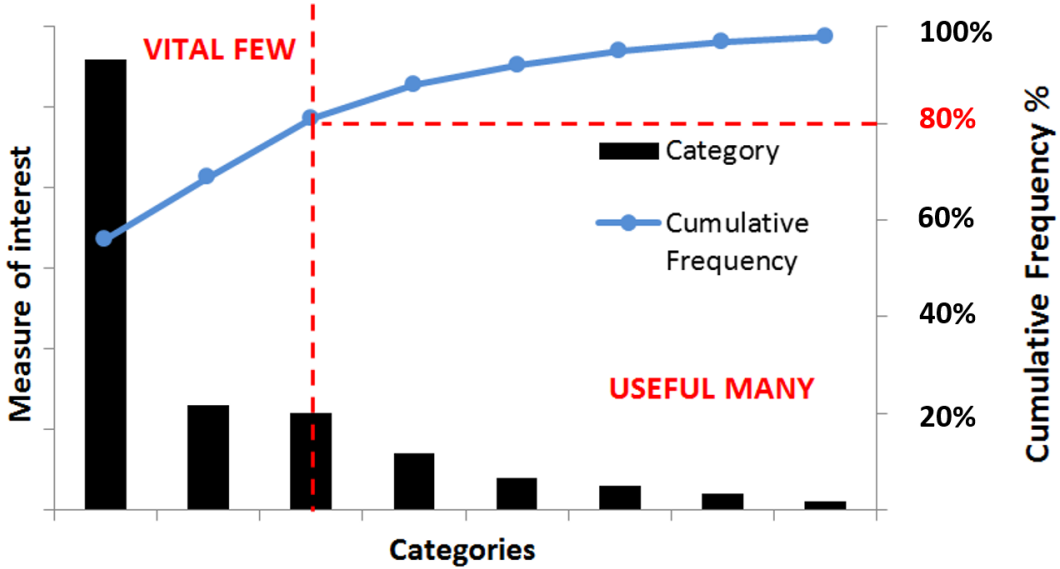
- Explain cyber risk as business risk
- Identify risk appetite
- Prompt the questions to ask
- Provide guidance to oversee

Framework + Certificate?

Not the panacea

Choose One

Less is More


VITAL FEW
USEFUL MANY
Category
Cumulative Frequency
Measure of interest
Categories
100%
80%
60%
40%
20%
Cumulative Frequency %

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

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

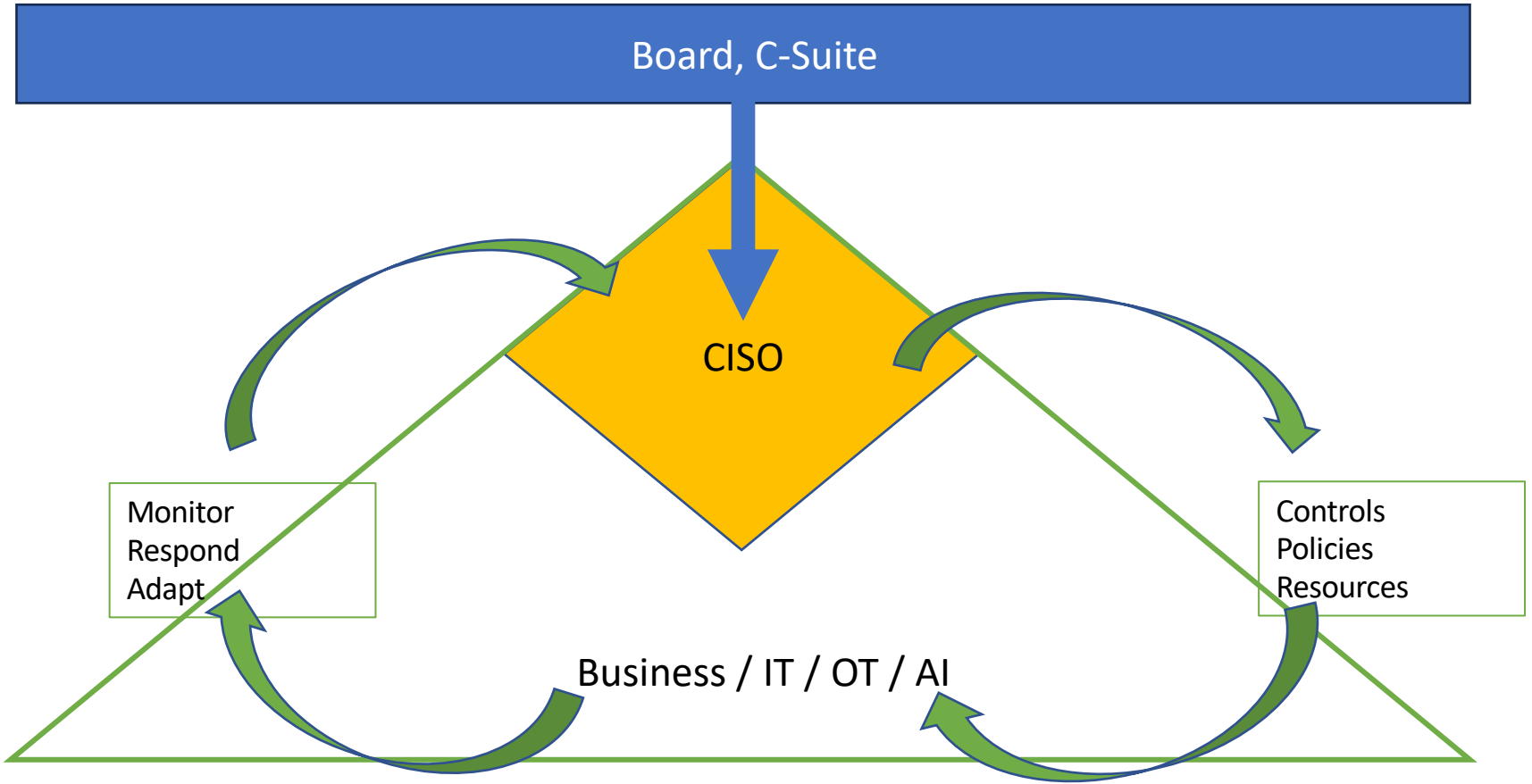
Content part 2: Risk management

- IT/Cyber risk <-> business risk
- Risk appetite
- Compliance <-> resilience
- Frameworks / mapping
- Key controls

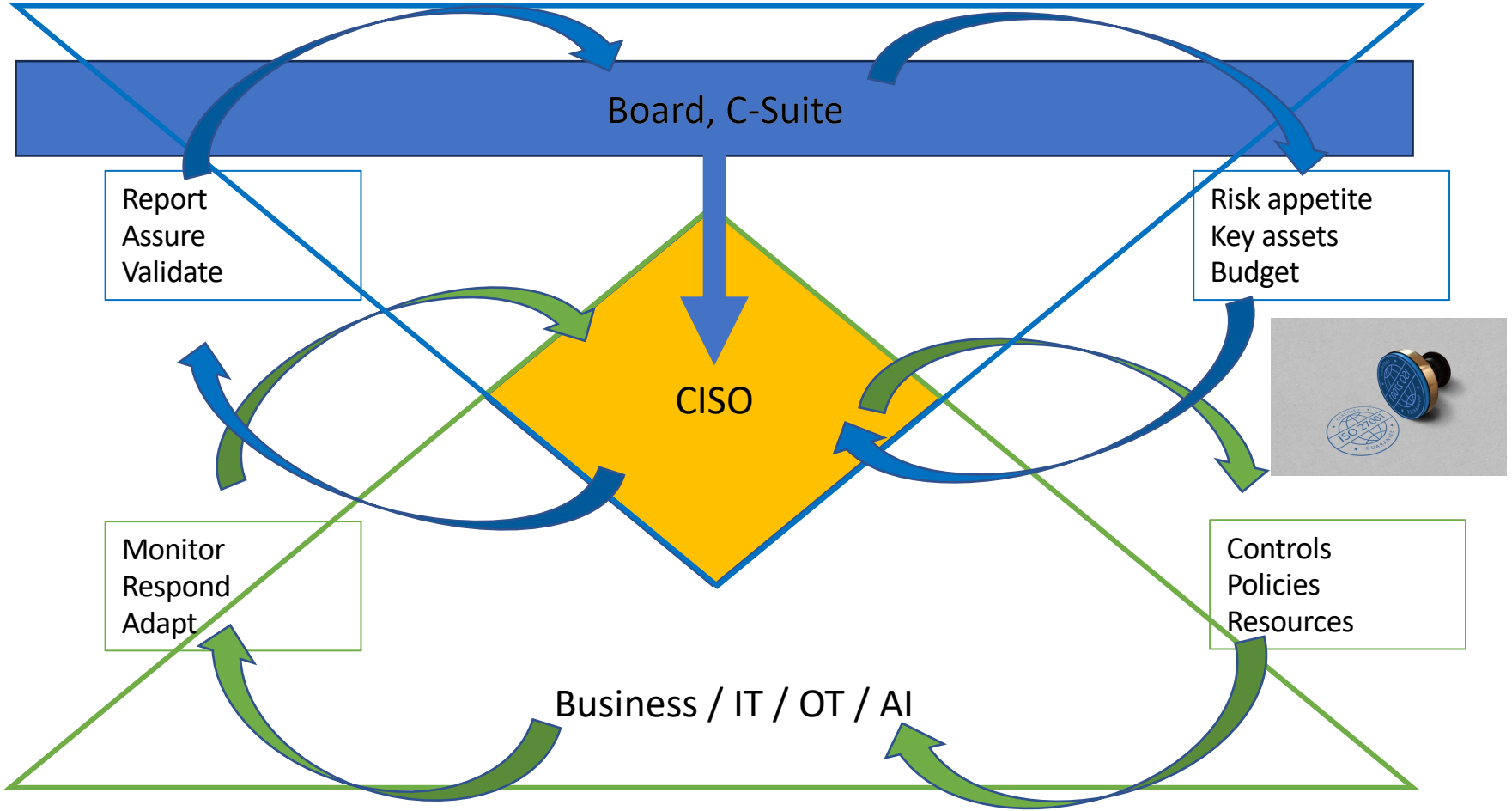
Tailoring

- Specific threat environment and risk appetite
- Prioritisation of controls and outcomes
- Internal alignment
- CISO reporting line and airtime

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

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