Agenda

1. Perspektiver på cyber-risici
2. Fokus på bestyrelsen
3. Cyber Risk Reporting

Felix Bozard
Manager
felix.bozard@pwc.com
T: +45 2366 3649

Peter Brock Madsen
Partner
peter.brock.madsen@pwc.com
T: +45 2056 8505

1

Perspektiver på cyber-risici

Perspektiver på cyber-risici

PwC's 27th Annual Global CEO Survey

Thriving in an age of continuous reinvention

As existential threats converge, many companies are taking steps to reinvent themselves. Is it enough? And what will it take to succeed?

pwc

www.ceosurvey.pwc

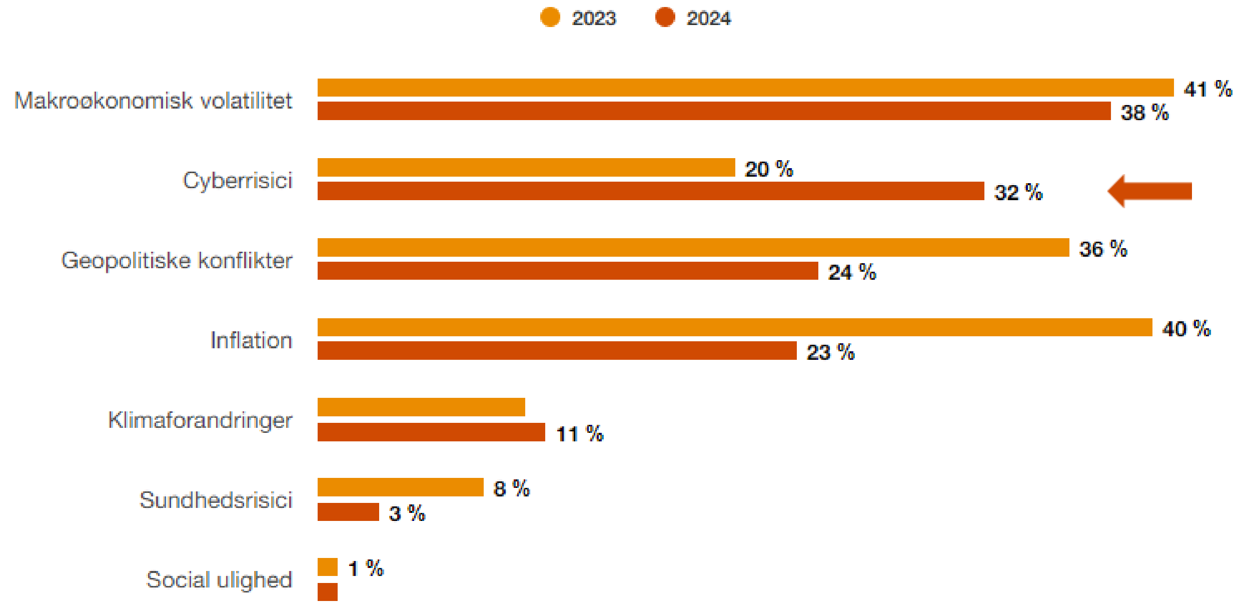
‹ › 1 / 2

Flere danske CEO'er vurderer, at deres virksomhed er påvirket af cybertruslen

Danmark

Hvor påvirket er din virksomhed af følgende trusler i de kommende 12 måneder?

(Viser dem, der har svaret "ekstremt/meget påvirket")



Kilde: PwC's 27th Annual Global CEO Survey (danske svar)

For 10. år i træk har PwC taget temperaturen på arbejdet med cybersikkerhed i Danmark. 463 topledere, sikkerhedschefer og fagspecialister fra den private og offentlige sektor har deltaget i undersøgelsen. Respondenterne har bidraget med deres indsigter i bl.a. investeringer, udfordringer og muligheder i arbejdet med cybersikkerhed. De har desuden vurderet det aktuelle trusselsbillede og rapporteret, hvordan og i hvilket omfang de arbejder med cyber- og informationssikkerhed.

61 %

anvender eller planlægger at anvende AI i arbejdet med cybersikkerhed

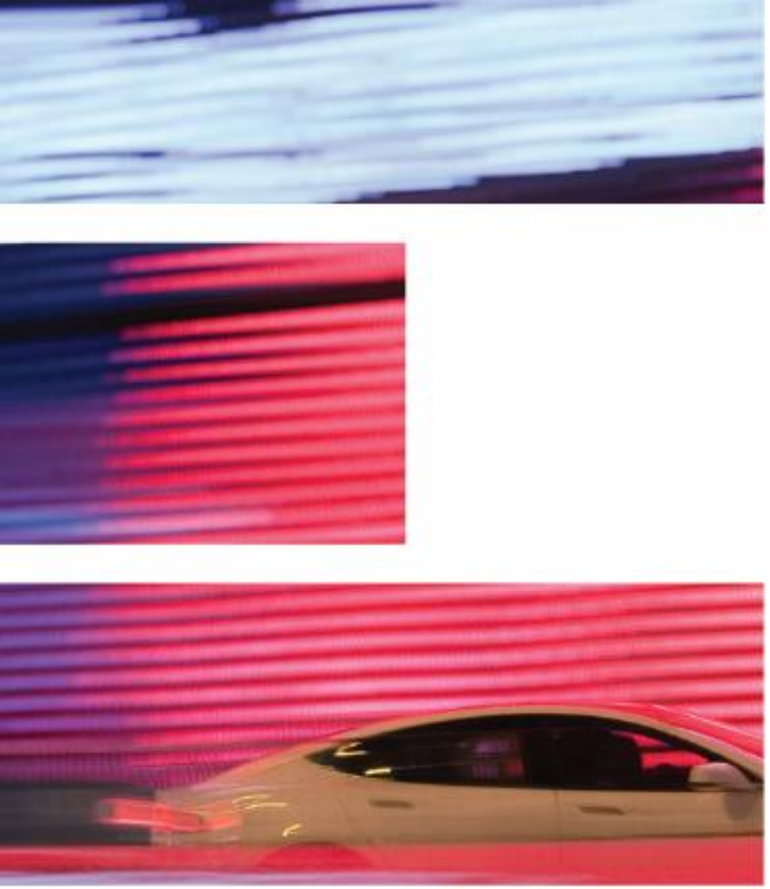
60 %

er mere bekymrede for cybertrusler i dag end for 12 måneder siden

Cybercrime Survey 2024

41 %

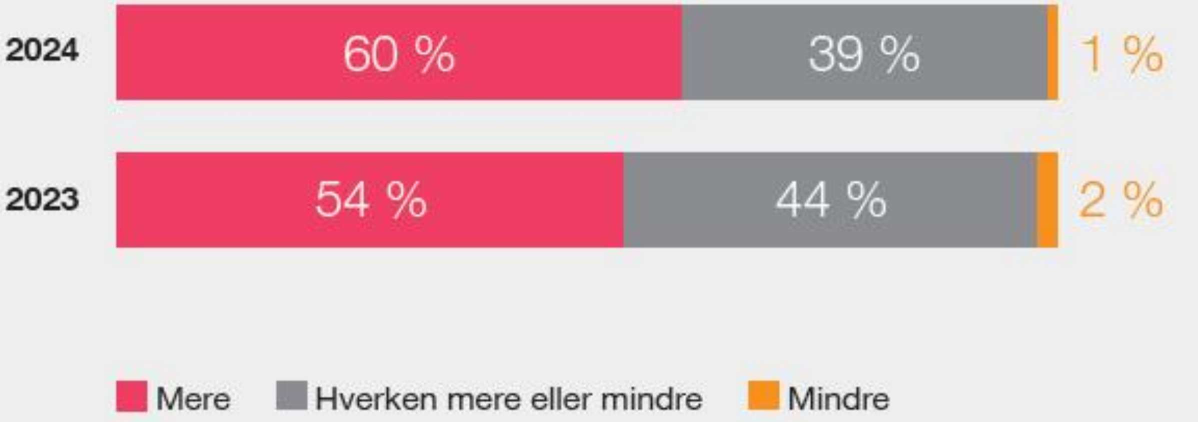
af virksomhederne har beredskab som højest prioriterede investering



Øget bekymring for cyberangreb i dansk erhvervsliv og den offentlige sektor

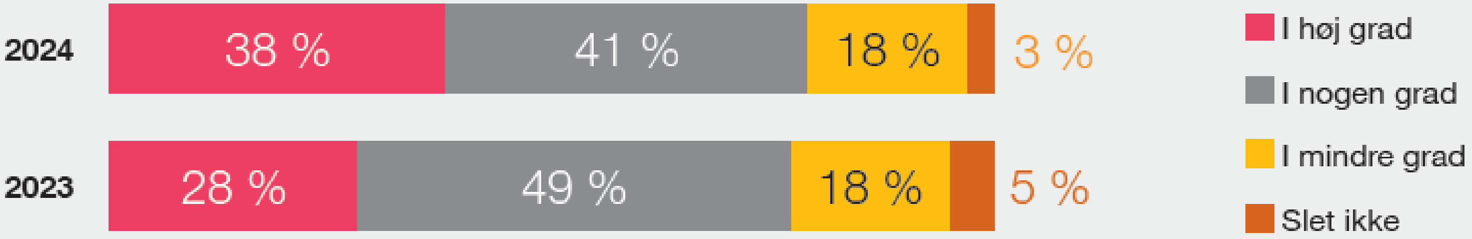
Bekymringen for cybertrusler fortsætter med at vokse i det danske erhvervsliv og den offentlige sektor. Hele 60 % af de adspurgte virksomheder angiver, at de er mere bekymrede for de cybertrusler, de står over for i dag, sammenlignet med for 12 måneder siden. 39 % vurderer, at deres bekymringsniveau er uændret, mens blot 1 % føler sig mindre bekymrede end for et år siden.

Spørgsmål: Bekymrer du dig i dag mere eller mindre om de cybertrusler, din virksomhed oplever, end du gjorde for 12 måneder siden?

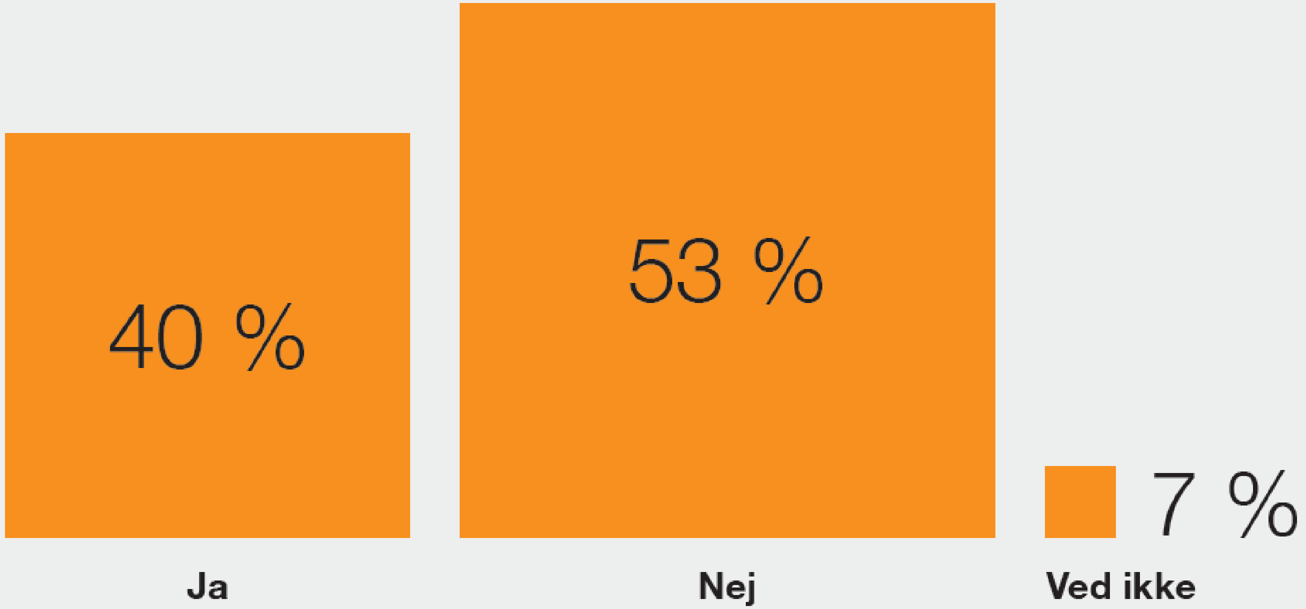


> På tre år er der sket en femdobling i andelen af virksomheder, der har AI som højt prioriteret investering inden for cybersikkerhed.

Spørgsmål: I hvilken grad er denne bekymring relateret til konflikten mellem Rusland og Vesten?

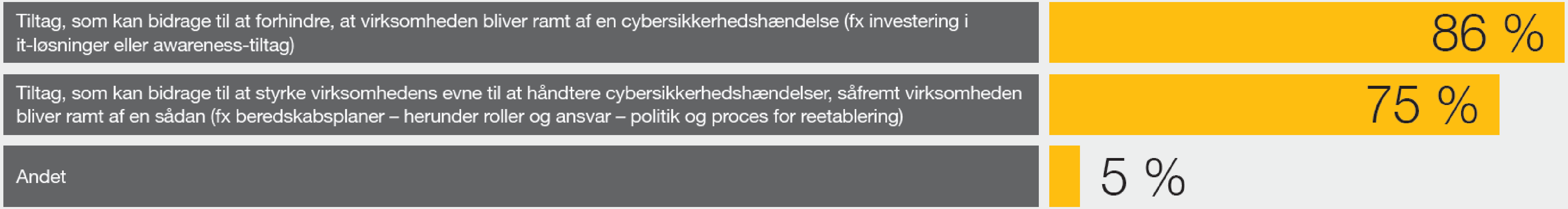


Spørgsmål: Har din virksomhed planlagt eller implementeret nye cybersikkerhedstiltag som følge af konflikten mellem Rusland og Vesten?



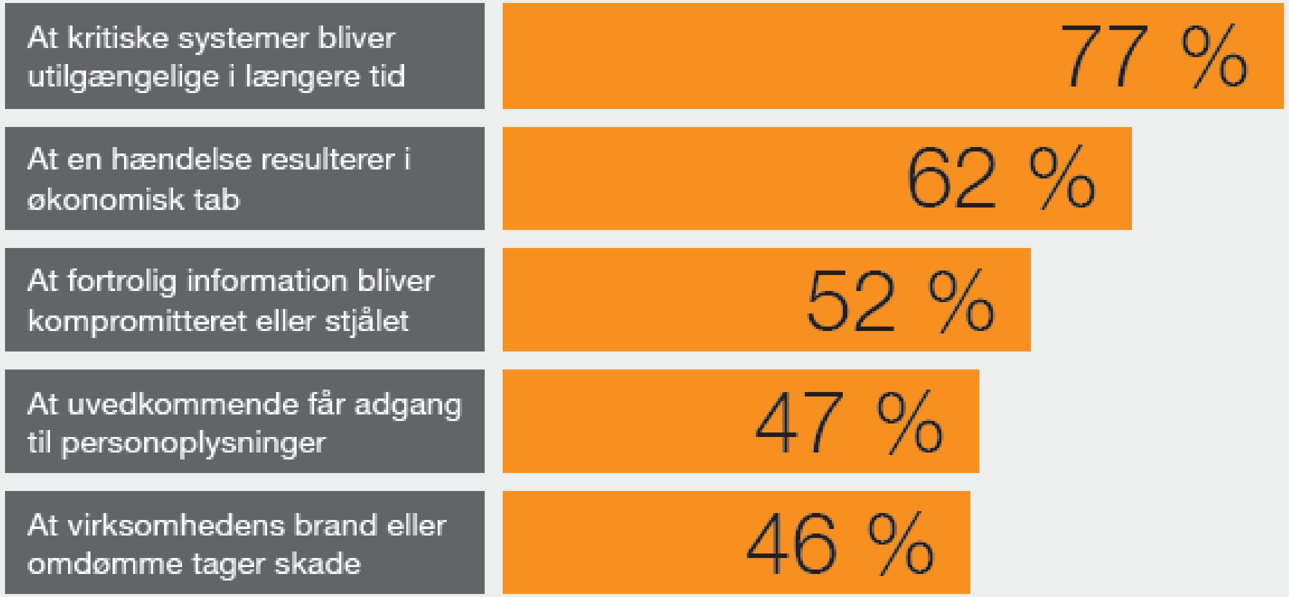
Som reaktion på den forøgede trussel har 40 % af virksomhederne implementeret nye cybersikkerhedstiltag. Disse omfatter både forebyggende foranstaltninger til at forhindre hændelser og beredskabsforanstaltninger, der styrker virksomhedernes evne til hurtigt og effektivt at reagere, hvis de bliver ramt af et cyberangreb.

Spørgsmål: Hvilke tiltag drejer det sig om?

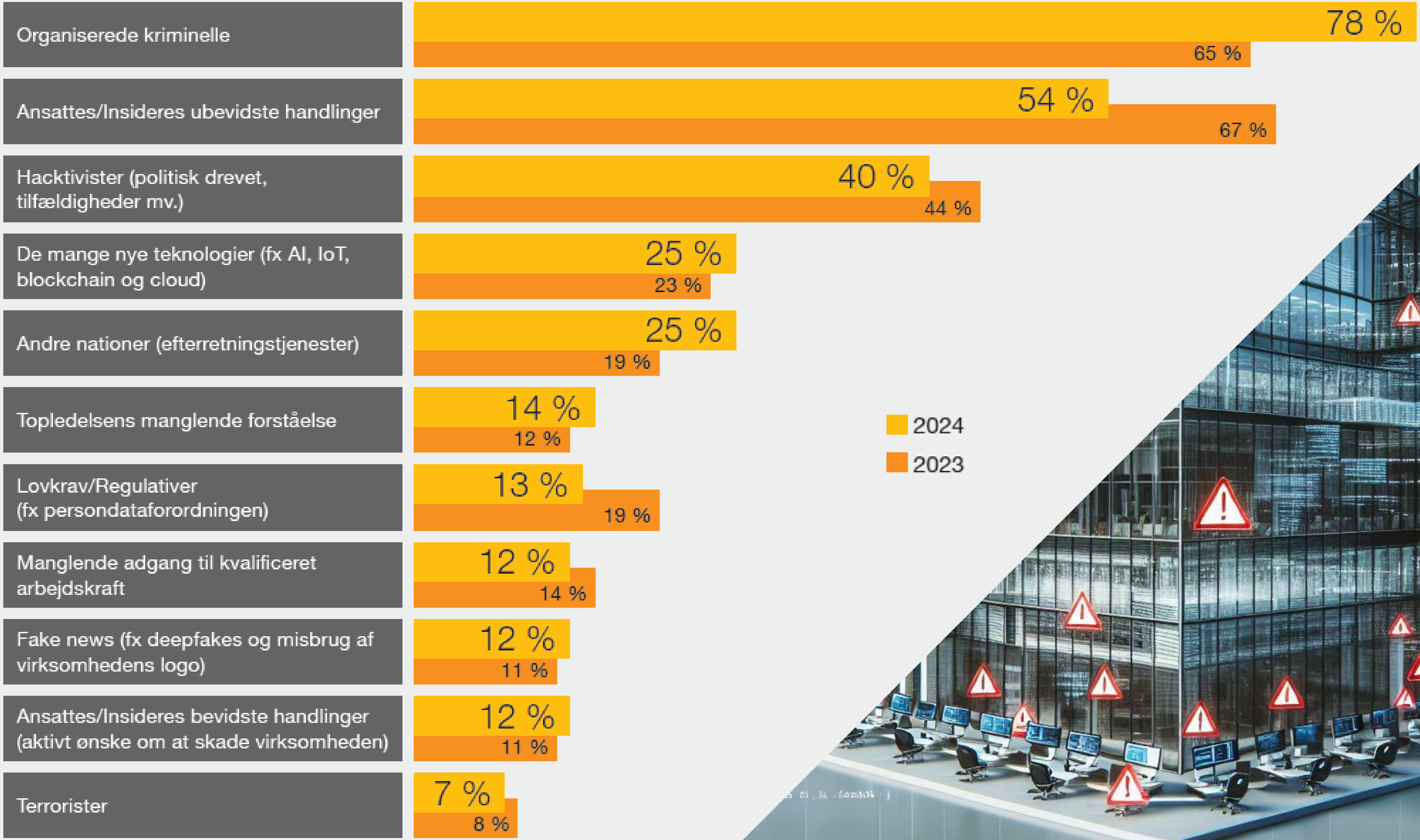


Tiltag, som kan bidrage til at forhindre, at virksomheden bliver ramt af en cybersikkerhedshændelse (fx investering i it-løsninger eller awareness-tiltag)	86 %
Tiltag, som kan bidrage til at styrke virksomhedens evne til at håndtere cybersikkerhedshændelser, såfremt virksomheden bliver ramt af en sådan (fx beredskabsplaner – herunder roller og ansvar – politik og proces for reetablering)	75 %
Andet	5 %

Spørgsmål: Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse?

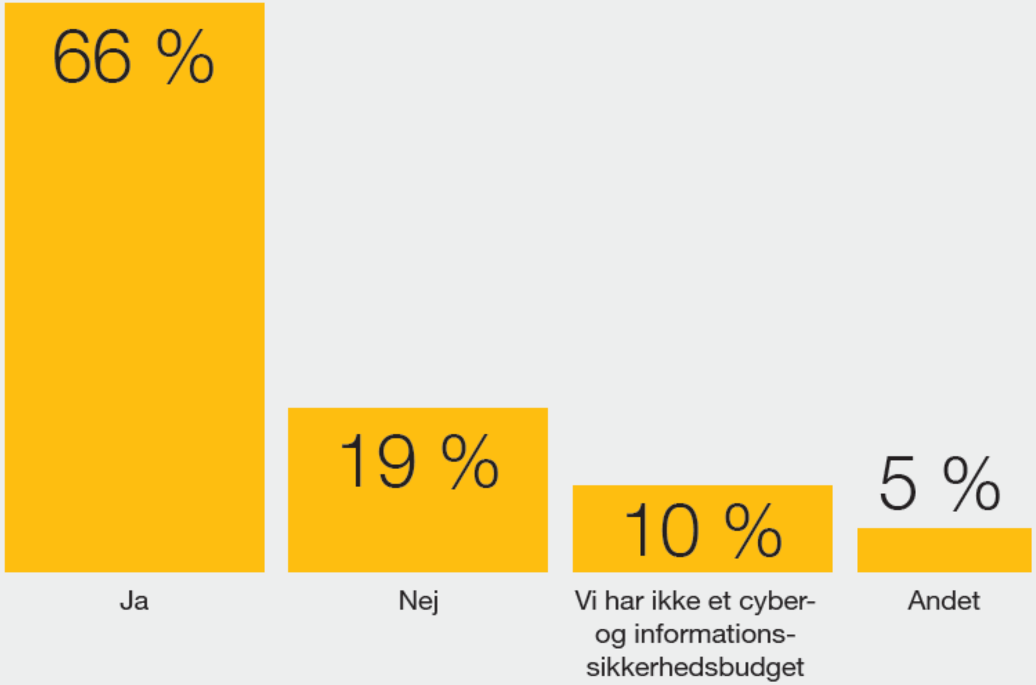


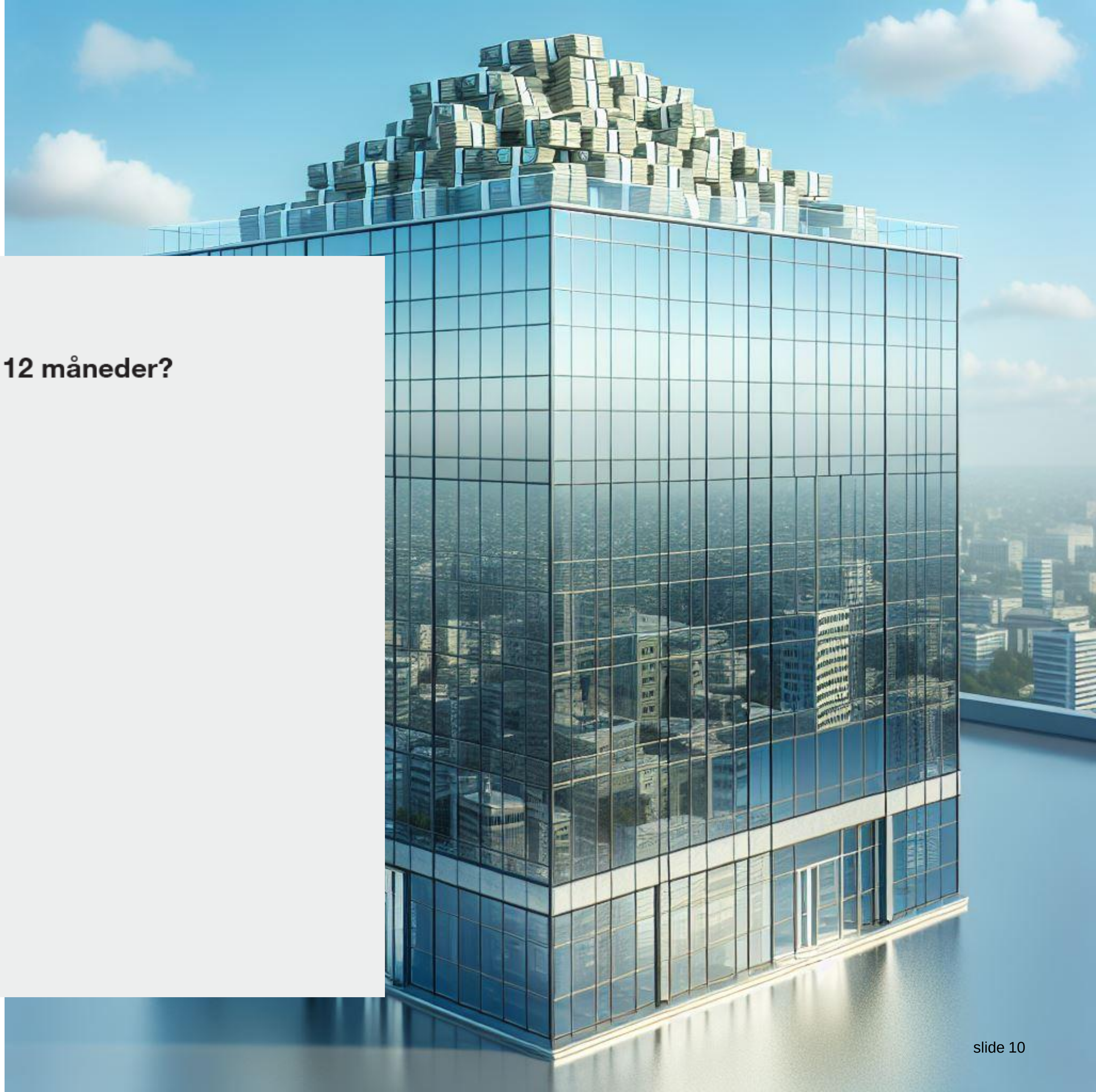
Spørgsmål: Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?



De danske virksomheder fortsætter med at øge budgetterne inden for cyber- og informationssikkerhed. Således forventer 66 % af virksomhederne at bruge endnu flere midler på bekæmpelse af cyberangreb.

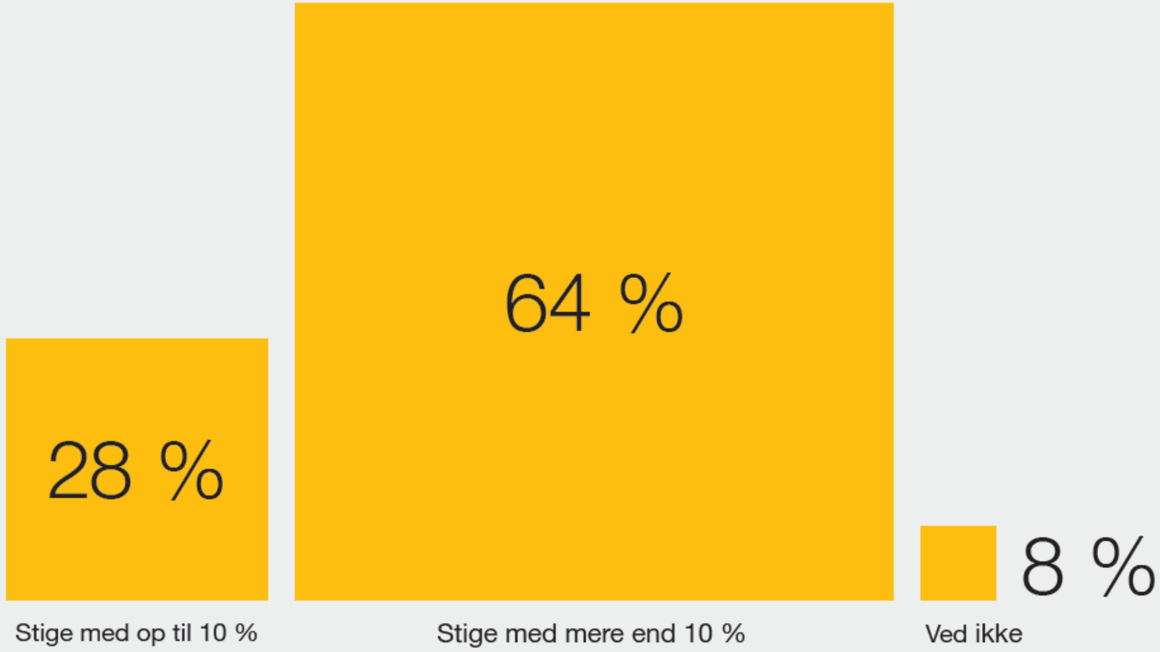
Spørgsmål: Forventer/Tror du, at virksomhedens cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder?



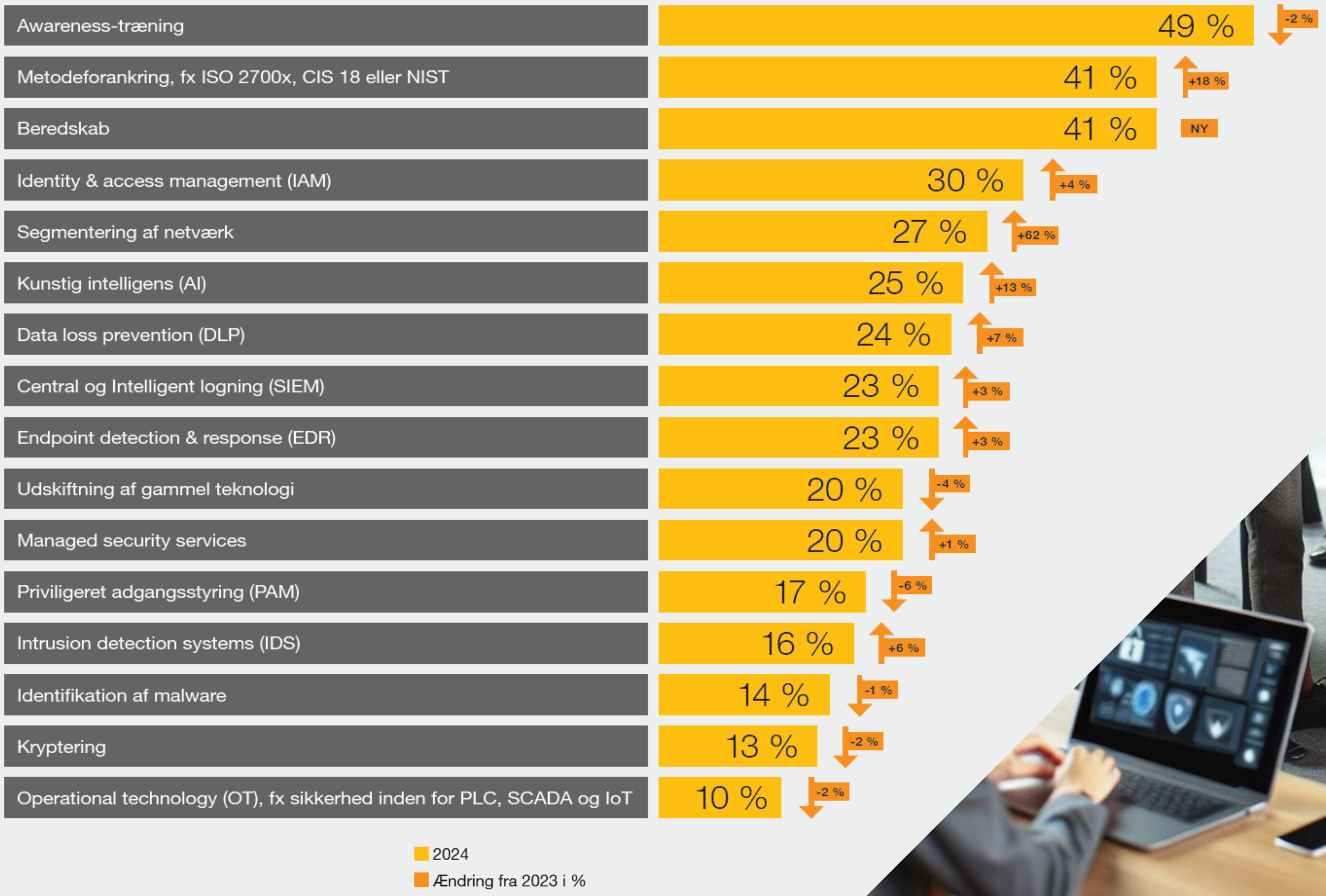


Awareness-træning topper virksomhedernes liste over prioriterede investeringer. I årets undersøgelse har man som noget nyt kunnet vælge beredskab, og denne kategori går direkte ind på en delt andenplads over de mest prioriterede investeringer. På en delt andenplads finder vi også metodeforankring, som går fra 23 % i 2023 til 41 % i 2024. Det skyldes bl.a., at flere virksomheder i stigende grad læner sig op ad diverse metoder til at strukturere deres sikkerhedsarbejde for at imødekomme kravene fra ny lovgivning, fx NIS 2 og DORA.

Spørgsmål: Hvor meget forventer du, at cyber- og informationssikkerhedsbudgettet vil stige inden for de næste 12 måneder?

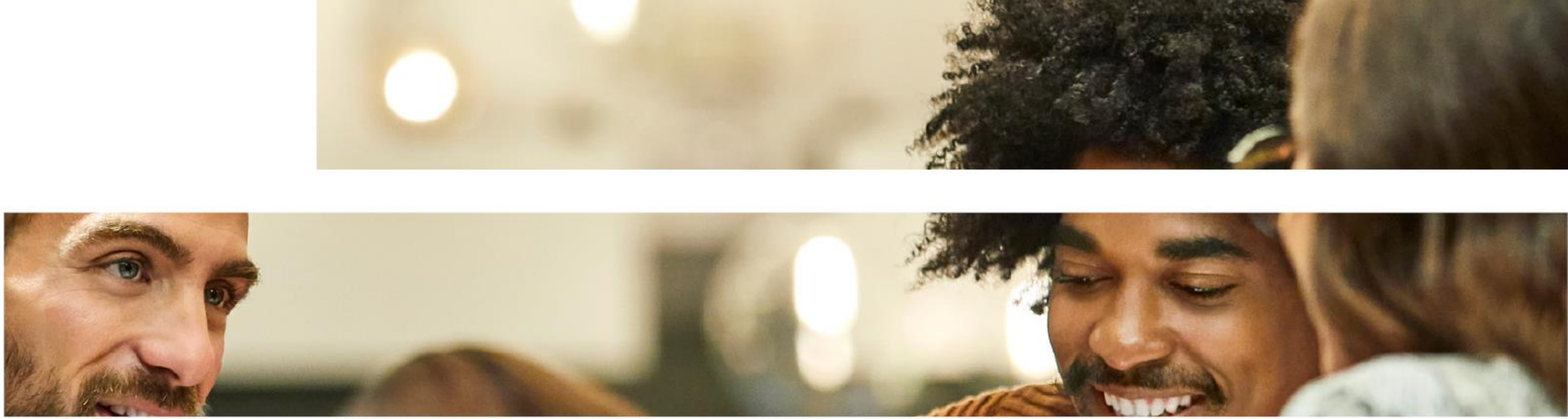


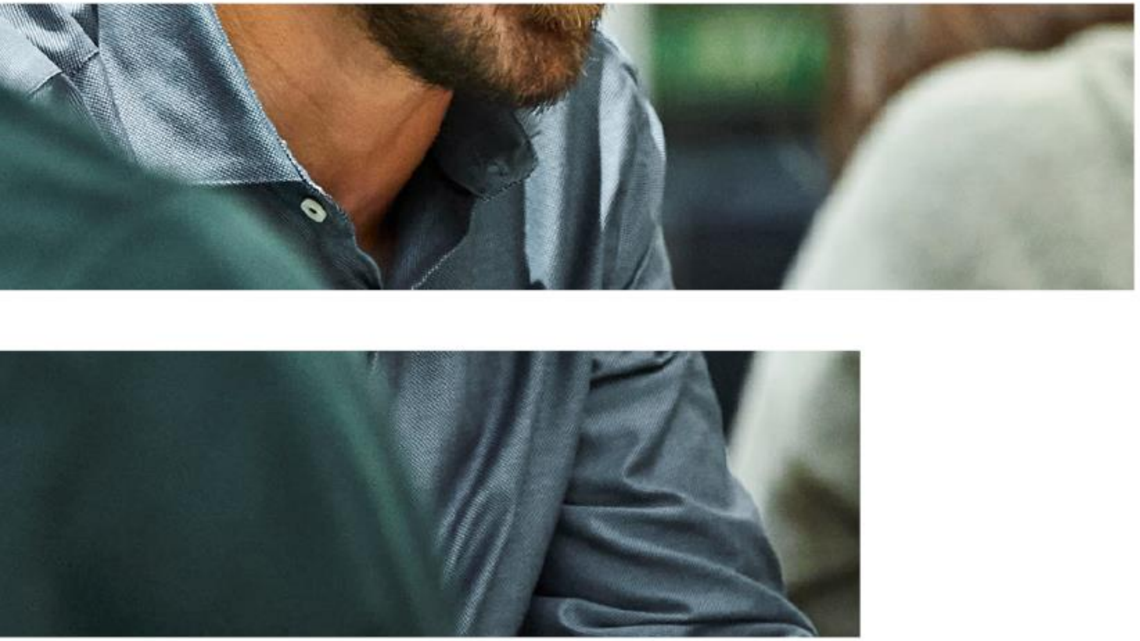
Spørgsmål: Hvad er din virksomheds højst prioriterede investeringer inden for it-sikkerhed de næste 12 måneder?



2

Fokus på bestyrelsen



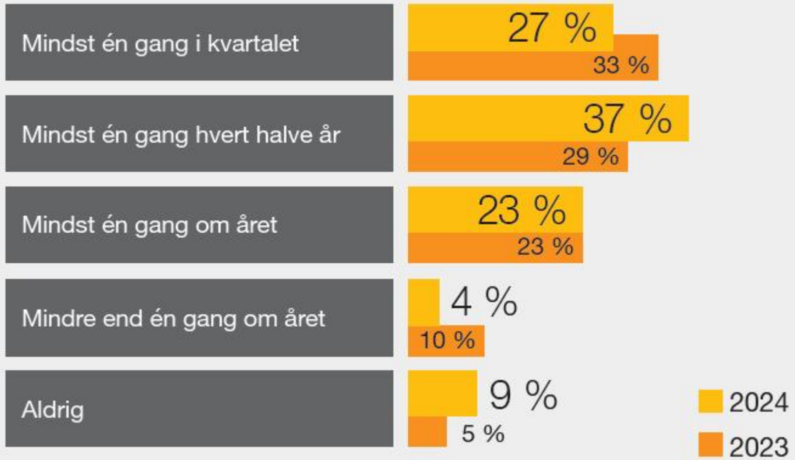


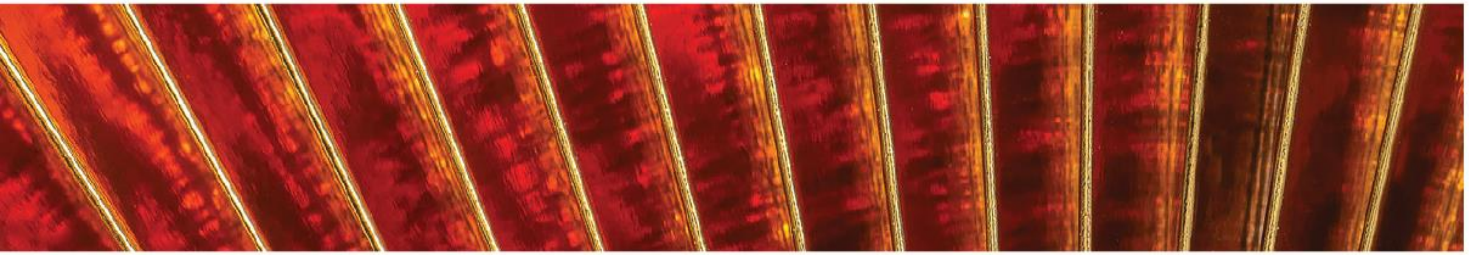
7 ud af 10

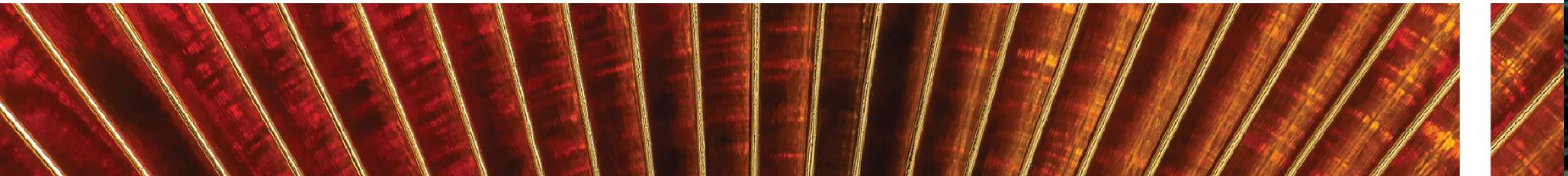
bestyrelsesmedlemmer har cybersikkerhed som en fast del af deres årshjul

Trods dette strategiske fokus viser undersøgelsen, at der er områder, hvor udviklingen stagnerer. Løbende opfølgning på cyberrisici og behandling af hændelser drøftes eksempelvis ikke oftere i bestyrelserne end tidligere. Derudover fortæller færre bestyrelsesmedlemmer, at de modtager træning i cyber- og informationssikkerhed sammenlignet med tidligere år, hvilket kan pege på en udfordring, i forhold til at sikre at bestyrelsen har de nødvendige kompetencer til at håndtere de stigende trusler. Flere medlemmer end tidligere fortæller også, at bestyrelsens samlede kompetencer på dette område ikke er tilstrækkeligt dybdegående.

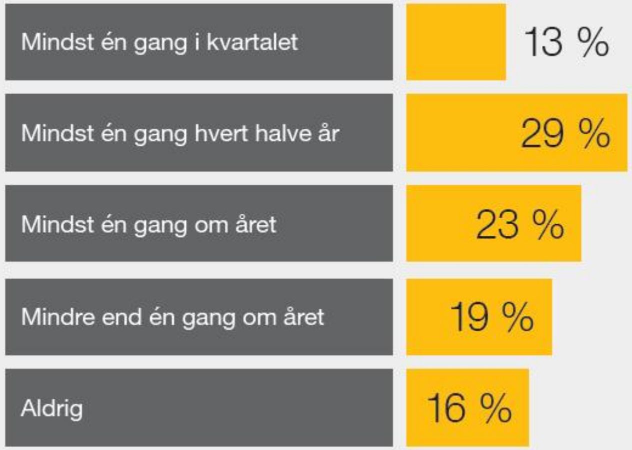
Spørgsmål: Hvor ofte modtager og behandler bestyrelsen information vedrørende cyberrisici?



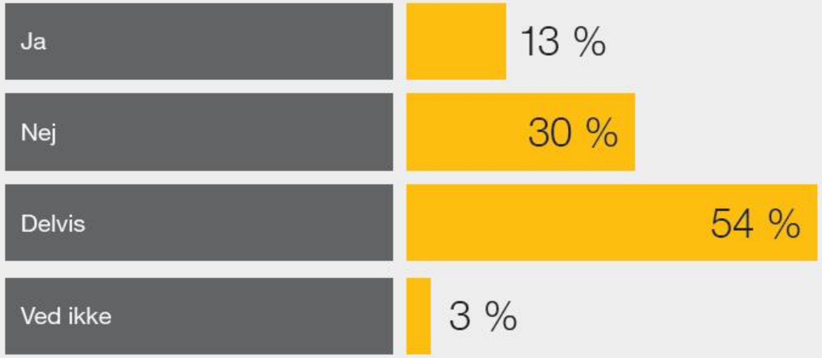


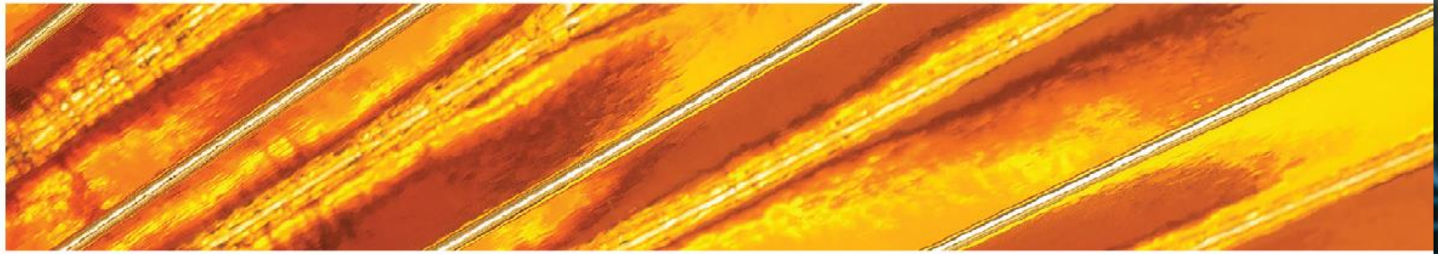


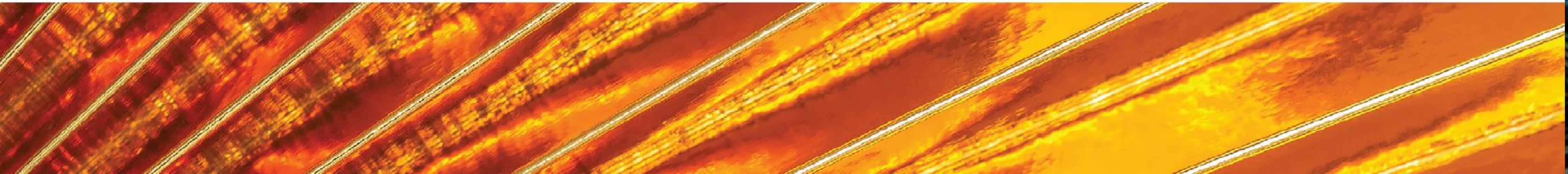
Spørgsmål: Hvor ofte behandler bestyrelsen cyberhændelser?



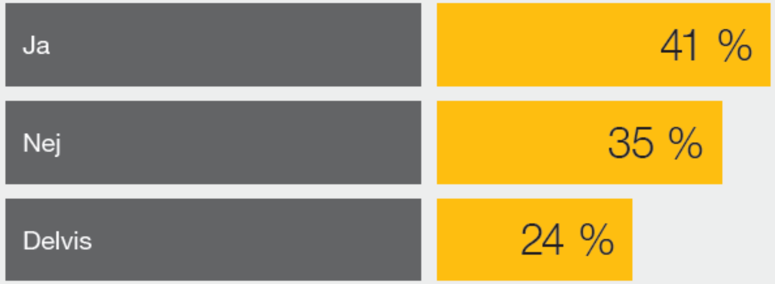
Spørgsmål: Modtager bestyrelsen træning i cyber- og informationssikkerhed?



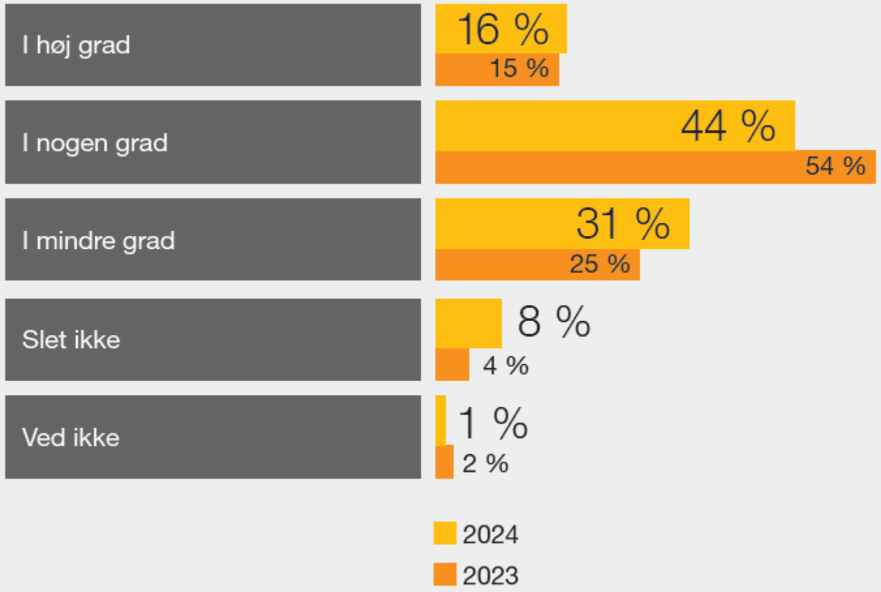




Spørgsmål: **Fører bestyrelsen kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af hackerangreb, strømnedbrud mv.?**



Spørgsmål: **I hvilken grad vurderer du, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed?**



ANBEFALINGER OG TJEKLISTE

Til styrkelse af strategiske cyberkompetencer i danske bestyrelser

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

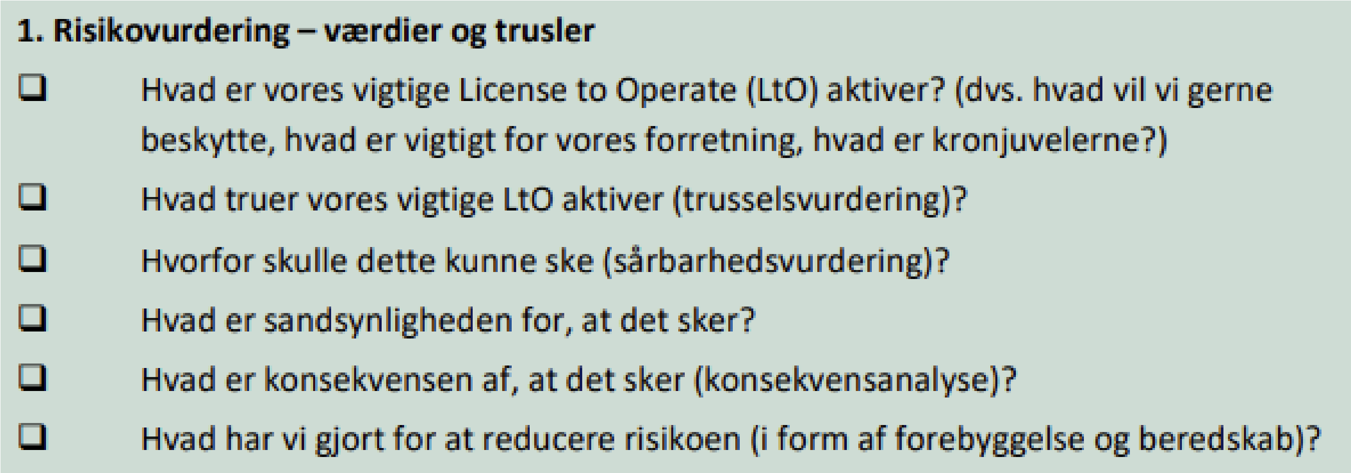
KROMANN REUMERT

Dubex:

FE CENTER FOR CYBERSIKKERHED

Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. Bestyrelsesforeningen eller dens samarbejdspartnere påtager sig ikke ansvar for tab som følge af handlinger eller undladelser baseret på publikationens indhold. Alle rettigheder forbeholdes.

Udpluk fra Bestyrelsesforeningens checkliste



1. Risikovurdering – værdier og trusler

❑ Hvad er vores vigtige License to Operate (LtO) aktiver? (dvs. hvad vil vi gerne beskytte, hvad er vigtigt for vores forretning, hvad er kronjuvelerne?)

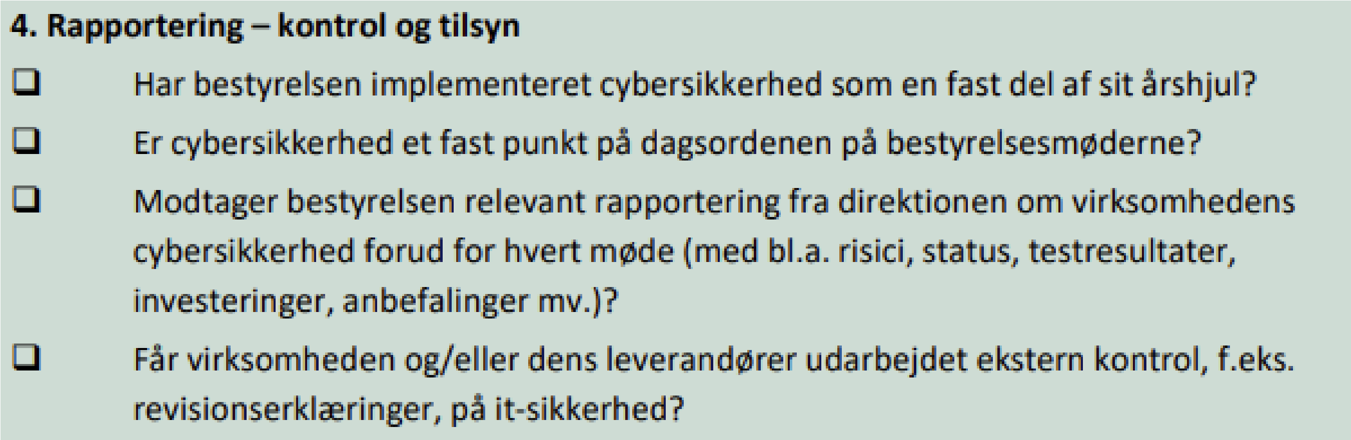
❑ Hvad truer vores vigtige LtO aktiver (trusselsvurdering)?

❑ Hvorfor skulle dette kunne ske (sårbarhedsvurdering)?

❑ Hvad er sandsynligheden for, at det sker?

❑ Hvad er konsekvensen af, at det sker (konsekvensanalyse)?

❑ Hvad har vi gjort for at reducere risikoen (i form af forebyggelse og beredskab)?



4. Rapportering – kontrol og tilsyn

❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?

❑ Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?

❑ Modtager bestyrelsen relevant rapportering fra direktionen om virksomhedens cybersikkerhed forud for hvert møde (med bl.a. risici, status, testresultater, investeringer, anbefalinger mv.)?

❑ Får virksomheden og/eller dens leverandører udarbejdet ekstern kontrol, f.eks. revisionserklæringer, på it-sikkerhed?

3

Cyber Risk Reporting

Cyber Risk Management – summed up

The business

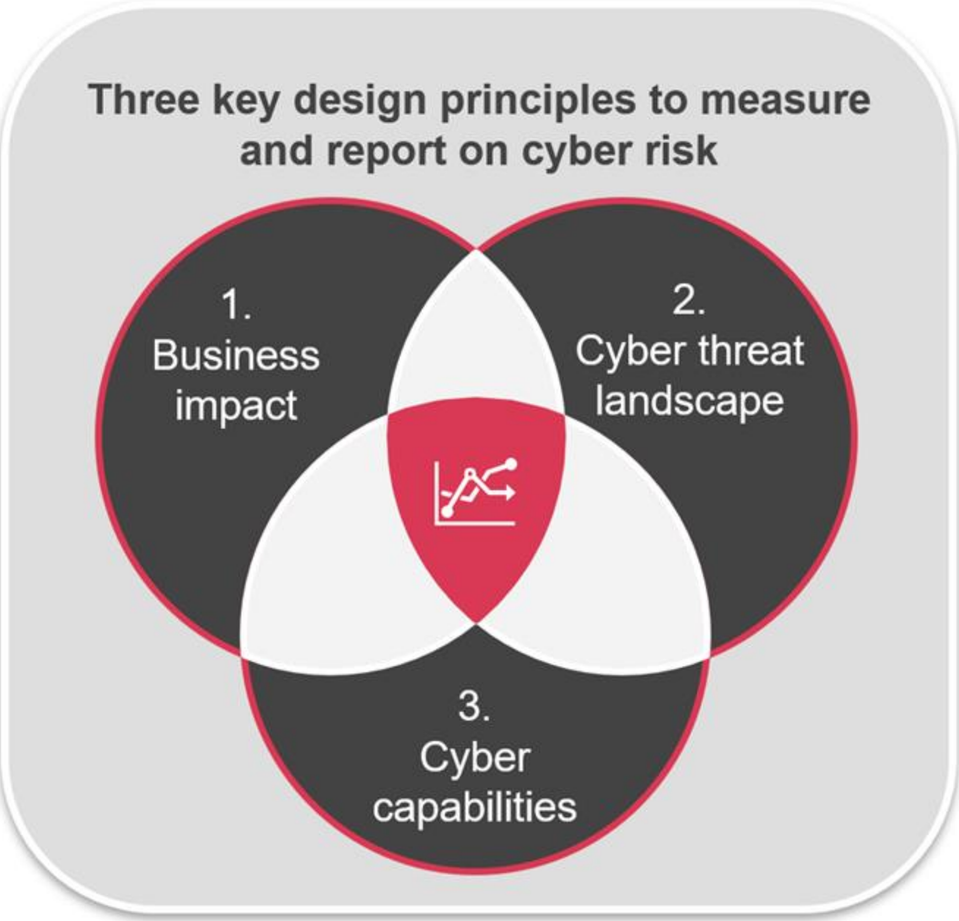
- What do we absolutely need to secure and protect from harm?
- What is the impact of a security incident if protection fails?

The threat landscape

- Who would potentially try to hurt our business?
- How real is the threat and scenarios we are facing?

The security capabilities

- How well are we securing ourselves today?
- Where do we need to improve and in what order/priority?



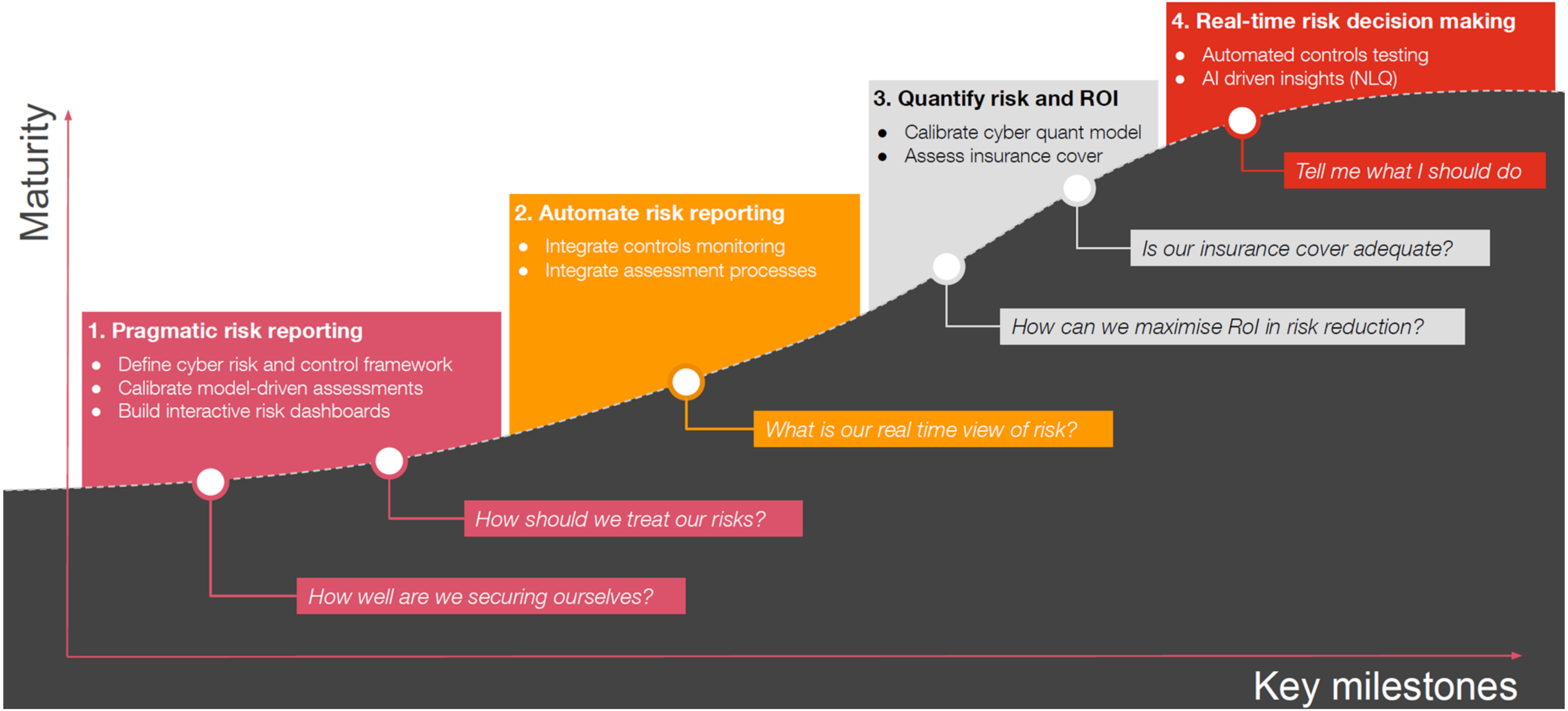
Three key design principles to measure and report on cyber risk

1. Business impact

2. Cyber threat landscape

3. Cyber capabilities

Proposed journey towards fact-based insights



1. Pragmatic risk reporting

- Define cyber risk and control framework
- Calibrate model-driven assessments
- Build interactive risk dashboards

2. Automate risk reporting

- Integrate controls monitoring
- Integrate assessment processes

3. Quantify risk and ROI

- Calibrate cyber quant model
- Assess insurance cover

4. Real-time risk decision making

- Automated controls testing
- AI driven insights (NLQ)

How well are we securing ourselves?

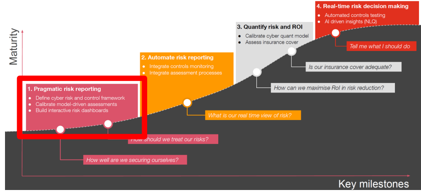
How should we treat our risks?

What is our real time view of risk?

How can we maximise RoI in risk reduction?

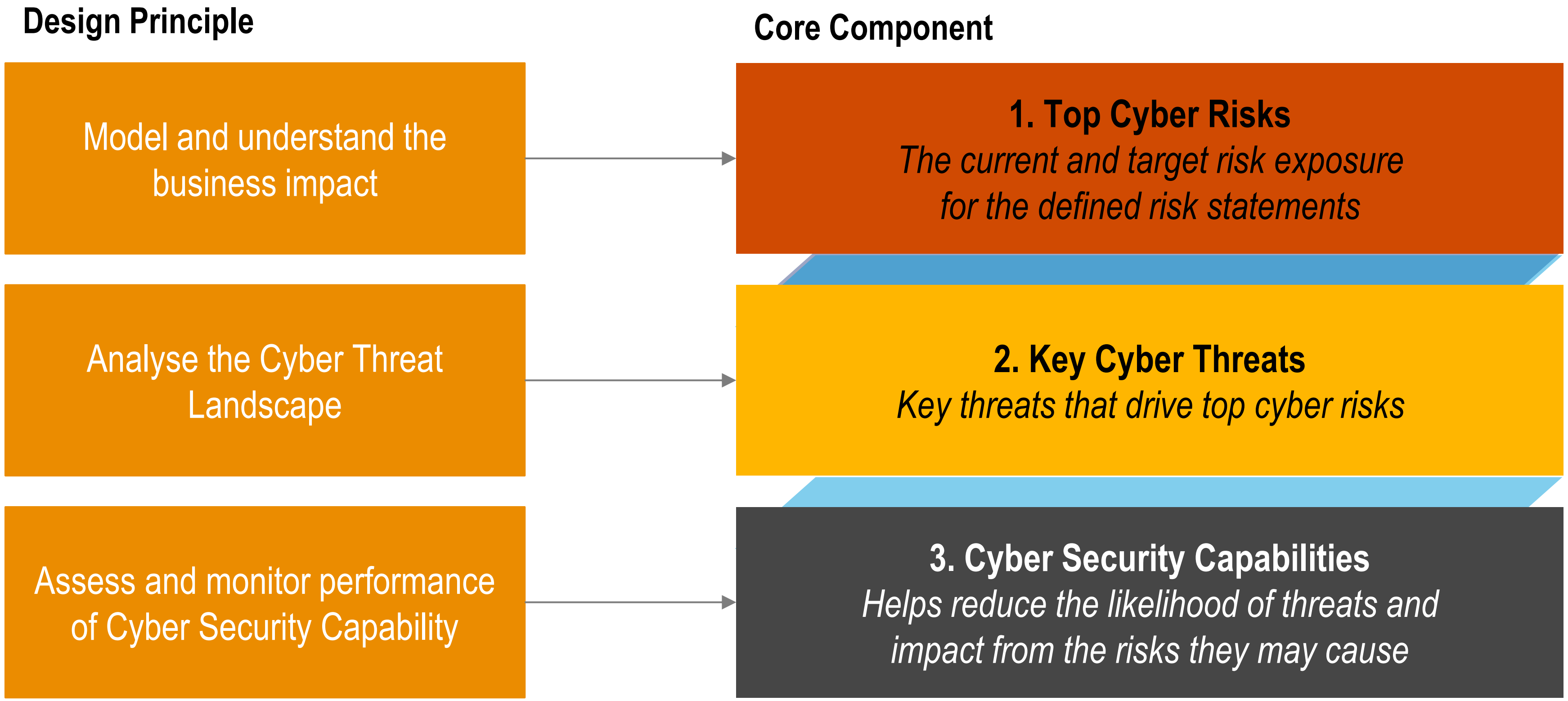
Is our insurance cover adequate?

Tell me what I should do


4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
Maturity
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
Tell me what I should do
Is our insurance cover adequate?
How can we maximise RoI in risk reduction?
What is our real time view of risk?
How should we treat our risks?
How well are we securing ourselves?
Key milestones

Agreeing on taxonomy

A Cybersecurity Risk Management Framework requires a common taxonomy of cyber security risks, its relationship to threats and the mitigating capabilities that need to be in place to ensure cyber security risks are prudently and consistently managed.



Design Principle

Core Component

Model and understand the business impact

1. Top Cyber Risks
The current and target risk exposure for the defined risk statements

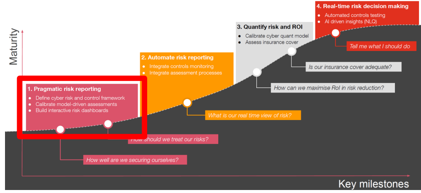
Analyse the Cyber Threat Landscape

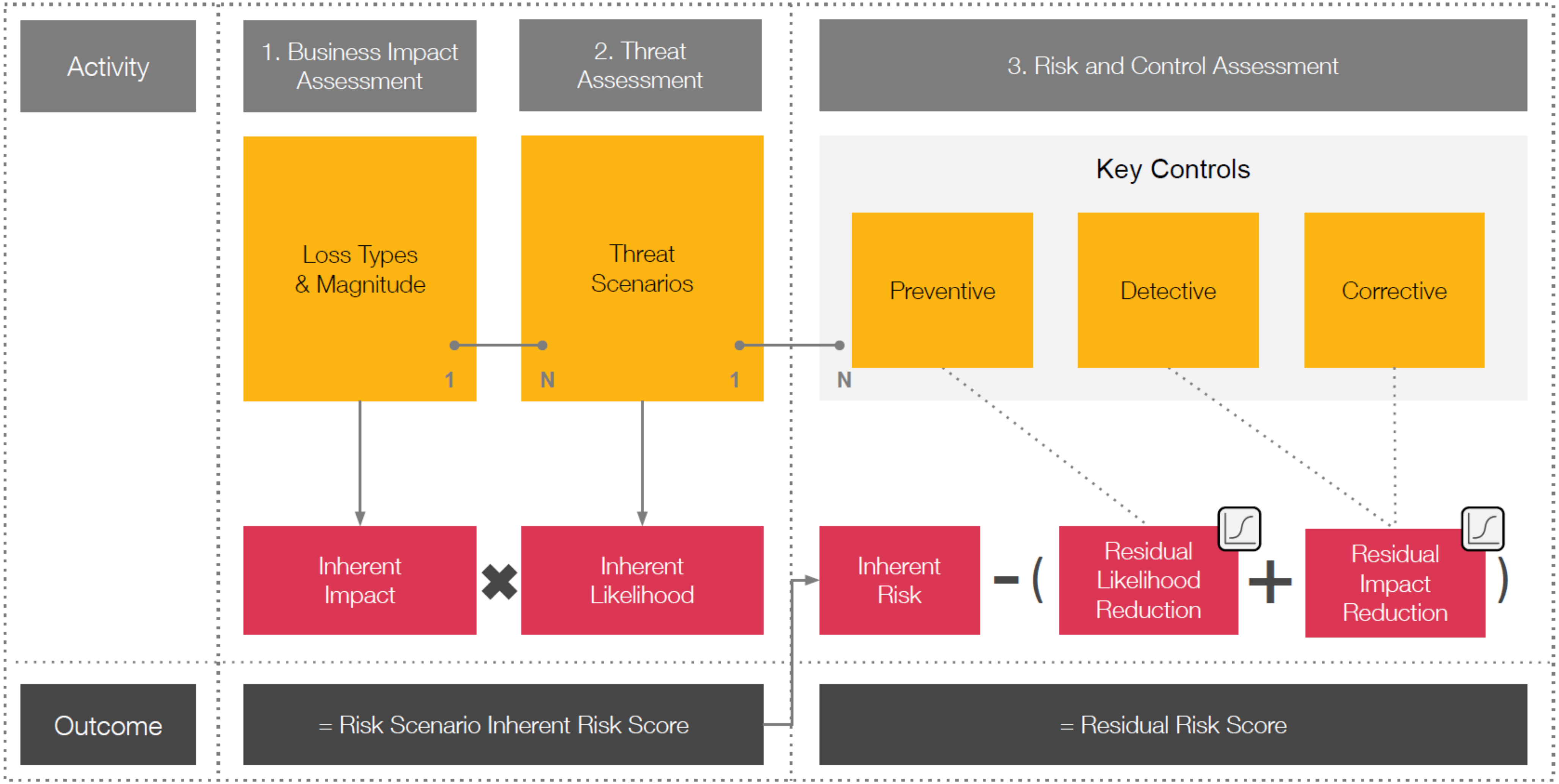
2. Key Cyber Threats
Key threats that drive top cyber risks

Assess and monitor performance of Cyber Security Capability

3. Cyber Security Capabilities
Helps reduce the likelihood of threats and impact from the risks they may cause

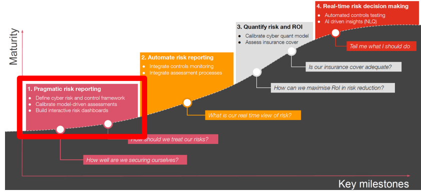
Using a ‘basic’ risk model


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

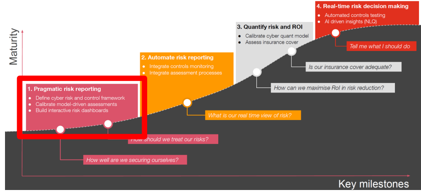


- The risk model is calibrated using a logistic s-curve to better reflect reality (e.g. CMMI level 5 controls does not mean zero residual risk)

Deterministic Risk Calculation Logic

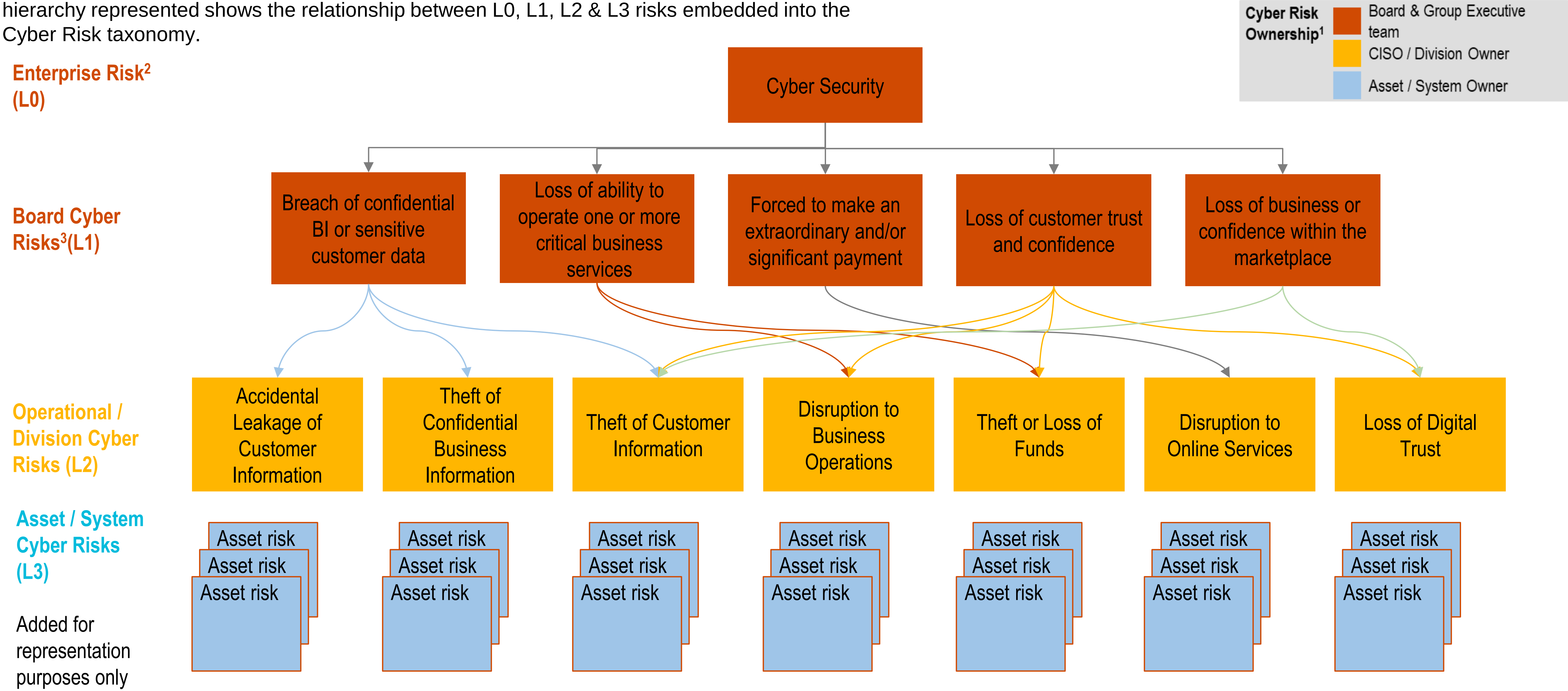

4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
Maturity
Tell me what I should do
Is our insurance cover adequate?
How can we maximise RoI in risk reduction?
What is our real time view of risk?
How should we treat our risks?
How well are we securing ourselves?
Key milestones

	Impact assessment	Threat identification & assessment	Control assessment		Risk assessment				Reporting
	1. Calculate inherent impact	2. Calculate inherent likelihood	3. Calculate controls derived scores	4. Aggregate and weight controls scores	5. Calculate likelihood reduction factor	6. Calculate residual likelihood	7. Calculate impact reduction factor	8. Calculate residual impact	9. Determine residual risk rating
Scope	per risk per OU	per threat scenario per OU	per control per OU	per control type per OU	per threat scenario per OU	per threat scenario per OU	per risk per OU	per risk per OU	per risk per OU
Input	BIA assessment, ERM impact framework	sophistication, proximity, frequency	control assessed score, metrics score, metrics RAG, control effectiveness factorisation	control derived score, control weighting	overall prevent derived score, impact reduction factor curve	inherent likelihood score, likelihood reduction factor	overall detect and correct derived score, impact reduction factor curve	inherent impact score, impact reduction factor	residual impact, residual likelihood, ERM heatmap
Output	inherent impact rating	inherent likelihood rating	control derived score	overall control type derived score (prevent, detect, correct)	likelihood reduction factor (%)	residual likelihood rating	impact reduction factor (%)	residual impact rating	residual risk rating


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

Cyber Risk Hierarchy

A Cyber Risk hierarchy allows for risk aggregation and clear assignment of risk ownership. The hierarchy represented shows the relationship between L0, L1, L2 & L3 risks embedded into the Cyber Risk taxonomy.



Cyber Risk Ownership[1]

🟥	Board & Group Executive team
🟨	CISO / Division Owner
🟦	Asset / System Owner

Enterprise Risk[2] **(L0)**

- Cyber Security

Board Cyber Risks[3]**(L1)**

- Breach of confidential BI or sensitive customer data
- Loss of ability to operate one or more critical business services
- Forced to make an extraordinary and/or significant payment
- Loss of customer trust and confidence
- Loss of business or confidence within the marketplace

Operational / Division Cyber Risks (L2)

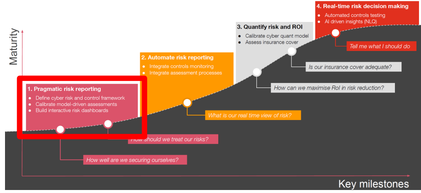
- Accidental Leakage of Customer Information
- Theft of Confidential Business Information
- Theft of Customer Information
- Disruption to Business Operations
- Theft or Loss of Funds
- Disruption to Online Services
- Loss of Digital Trust

Asset / System Cyber Risks (L3)

Asset risk
Asset risk
Asset risk

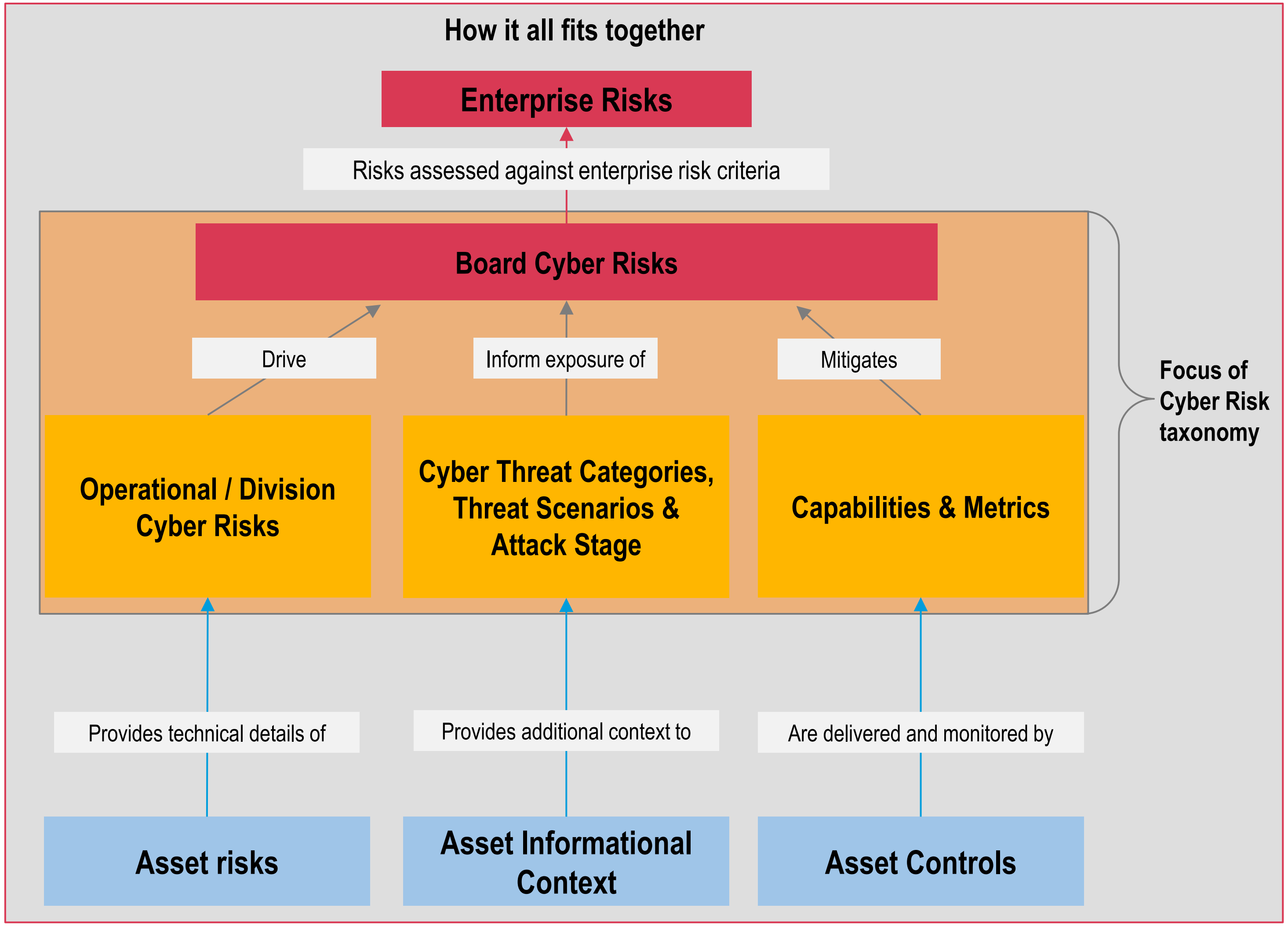
Added for representation purposes only

[1] Cyber Risk Ownership is defined as part of the Cyber Security Risk Management Framework; [2] Corporate Risk Register (Cyber Security as risk #xx); [3] Cyber Risks reported by Group CISO to the Board


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

Cyber Risk & Control Levels

	Level	Cyber Risk taxonomy core component
Enterprise Level	L0	Enterprise Risks[1]
Strategic Level	L1	Board Cyber Risks[2]
Operational Level	L2	Operational / Division Cyber Risks
		Threat Categories, Threat Scenarios & Attack Stage
		Capabilities & Metrics
Asset / System Level	L3	Asset Risks
		Asset Informational Context
		Asset Controls



How it all fits together

Enterprise Risks

Risks assessed against enterprise risk criteria

Board Cyber Risks

Drive

Inform exposure of

Mitigates

Operational / Division Cyber Risks

Cyber Threat Categories, Threat Scenarios & Attack Stage

Capabilities & Metrics

Focus of Cyber Risk taxonomy

Provides technical details of

Provides additional context to

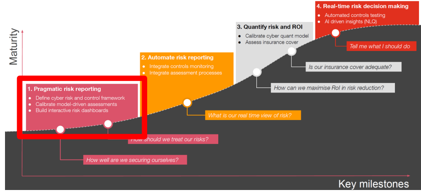
Are delivered and monitored by

Asset risks

Asset Informational Context

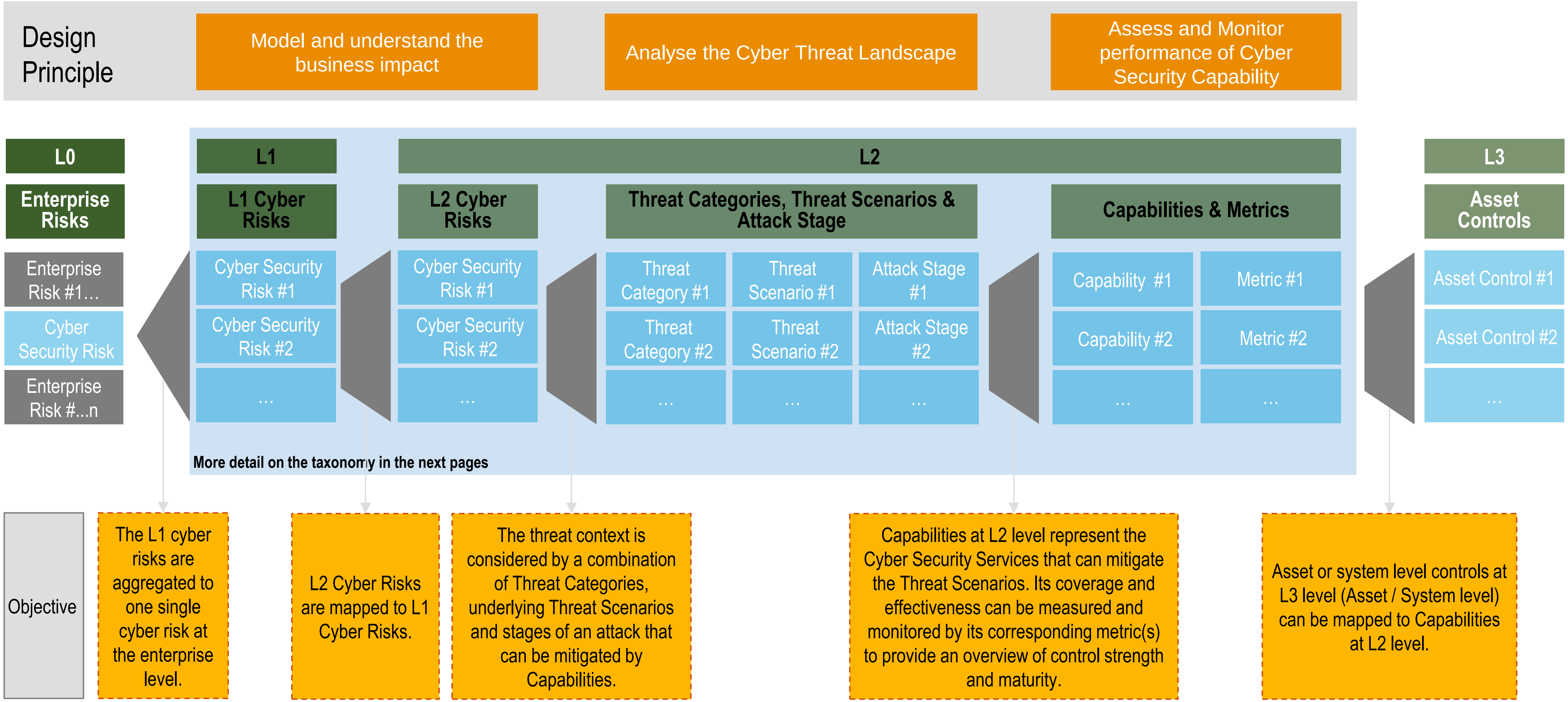
Asset Controls

1: Corporate Risk Register (Cyber Security as risk #xx); 2: Cyber Risks reported by the Group CISO to the Board


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

Mapping approach for Cyber risks and objectives

The Cyber Risk taxonomy and underlying reporting approach is based on the mapping between the L1 Cyber Risks to L2 Cyber Risks, to the threat context that contributes to them and the capabilities in place to mitigate those threats.



Design Principle

Model and understand the business impact

Analyse the Cyber Threat Landscape

Assess and Monitor performance of Cyber Security Capability

L0

Enterprise Risks

Enterprise Risk #1…

Cyber Security Risk

Enterprise Risk #…n

L1

L1 Cyber Risks

Cyber Security Risk #1

Cyber Security Risk #2

…

L2

L2 Cyber Risks

Cyber Security Risk #1

Cyber Security Risk #2

…

Threat Categories, Threat Scenarios & Attack Stage

Threat Category #1

Threat Scenario #1

Attack Stage #1

Threat Category #2

Threat Scenario #2

Attack Stage #2

…

…

…

Capabilities & Metrics

Capability #1

Metric #1

Capability #2

Metric #2

…

…

L3

Asset Controls

Asset Control #1

Asset Control #2

…

More detail on the taxonomy in the next pages

Objective

The L1 cyber risks are aggregated to one single cyber risk at the enterprise level.

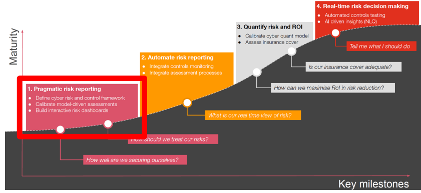
L2 Cyber Risks are mapped to L1 Cyber Risks.

The threat context is considered by a combination of Threat Categories, underlying Threat Scenarios and stages of an attack that can be mitigated by Capabilities.

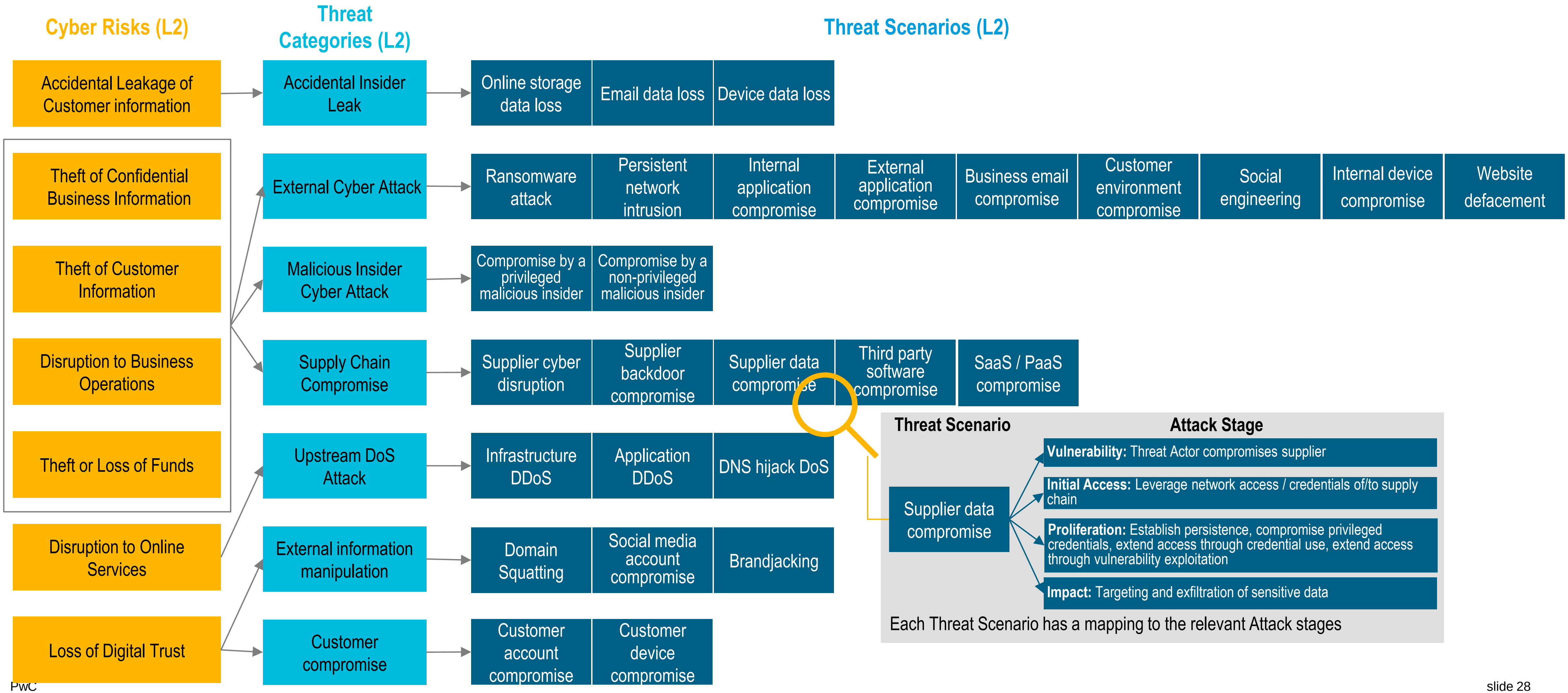
Capabilities at L2 level represent the Cyber Security Services that can mitigate the Threat Scenarios. Its coverage and effectiveness can be measured and monitored by its corresponding metric(s) to provide an overview of control strength and maturity.

Asset or system level controls at L3 level (Asset / System level) can be mapped to Capabilities at L2 level.

Threat Categories, Threat Scenarios & Attack Stages


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

A clear taxonomy and relationship between Operational / Divisional Cyber Risks (L2), the relevant Threat Categories and the underlying Threat Scenarios for each Threat Category is defined as follows.



Cyber Risks (L2)

Threat Categories (L2)

Threat Scenarios (L2)

Accidental Leakage of Customer information → Accidental Insider Leak → Online storage data loss | Email data loss | Device data loss

Theft of Confidential Business Information

Theft of Customer Information

Disruption to Business Operations

Theft or Loss of Funds

External Cyber Attack → Ransomware attack | Persistent network intrusion | Internal application compromise | External application compromise | Business email compromise | Customer environment compromise | Social engineering | Internal device compromise | Website defacement

Malicious Insider Cyber Attack → Compromise by a privileged malicious insider | Compromise by a non-privileged malicious insider

Supply Chain Compromise → Supplier cyber disruption | Supplier backdoor compromise | Supplier data compromise | Third party software compromise | SaaS / PaaS compromise

Disruption to Online Services

Upstream DoS Attack → Infrastructure DDoS | Application DDoS | DNS hijack DoS

Loss of Digital Trust

External information manipulation → Domain Squatting | Social media account compromise | Brandjacking

Customer account compromise → Customer account compromise | Customer device compromise

Threat Scenario

Attack Stage

Supplier data compromise

Vulnerability: Threat Actor compromises supplier

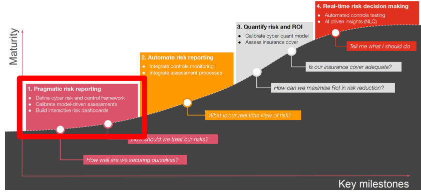
Initial Access: Leverage network access / credentials of/to supply chain

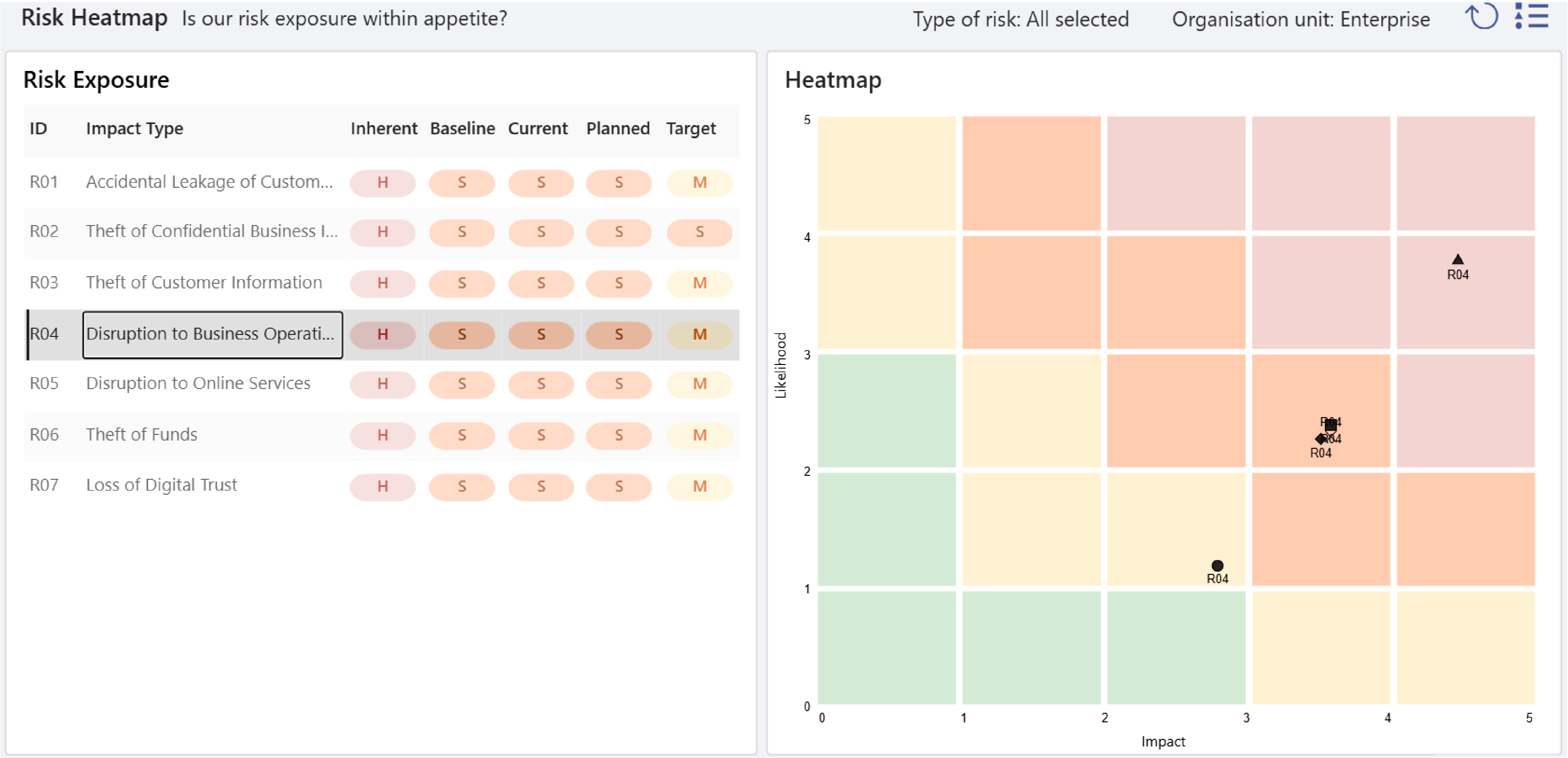
Proliferation: Establish persistence, compromise privileged credentials, extend access through credential use, extend access through vulnerability exploitation

Impact: Targeting and exfiltration of sensitive data

Each Threat Scenario has a mapping to the relevant Attack stages

Using pragmatic dashboards *(BoD-level)*


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones



Risk Heatmap Is our risk exposure within appetite?

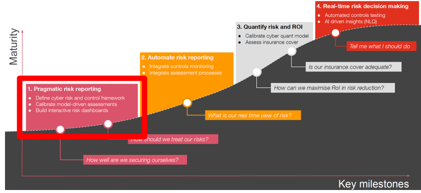
Type of risk: All selected   Organisation unit: Enterprise

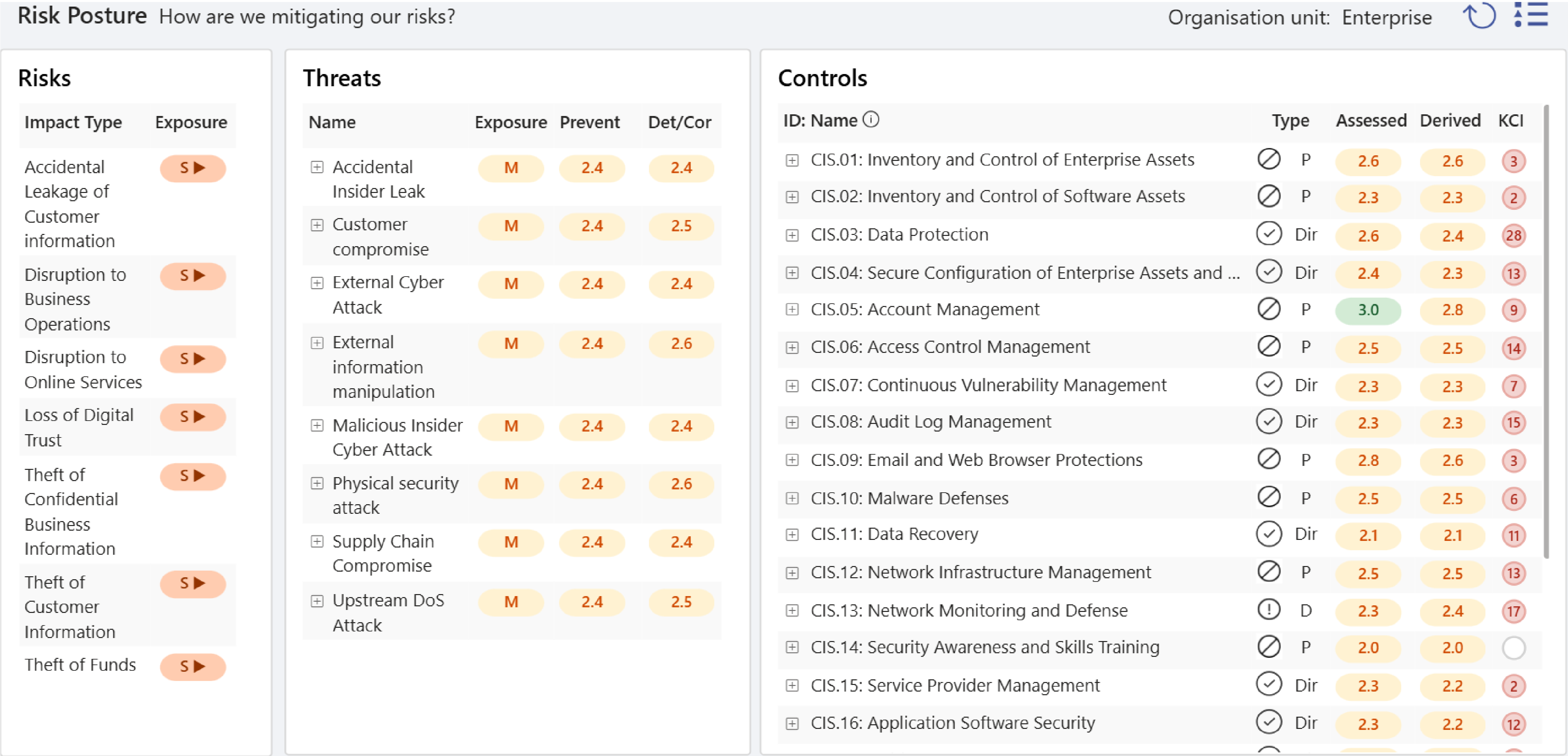
Risk Exposure

ID	Impact Type	Inherent	Baseline	Current	Planned	Target
R01	Accidental Leakage of Custom...	H	S	S	S	M
R02	Theft of Confidential Business I...	H	S	S	S	S
R03	Theft of Customer Information	H	S	S	S	M
R04	Disruption to Business Operati...	H	S	S	S	M
R05	Disruption to Online Services	H	S	S	S	M
R06	Theft of Funds	H	S	S	S	M
R07	Loss of Digital Trust	H	S	S	S	M

Heatmap

Using pragmatic dashboards *(Risk Owner-level)*


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
Tell me what I should do
Is our insurance cover adequate?
How can we maximise RoI in risk reduction?
What is our real time view of risk?
How should we treat our risks?
How well are we securing ourselves?
Key milestones



Risk Posture How are we mitigating our risks? Organisation unit: Enterprise

Risks

Impact Type	Exposure
Accidental Leakage of Customer information	S ▶
Disruption to Business Operations	S ▶
Disruption to Online Services	S ▶
Loss of Digital Trust	S ▶
Theft of Confidential Business Information	S ▶
Theft of Customer Information	S ▶
Theft of Funds	S ▶

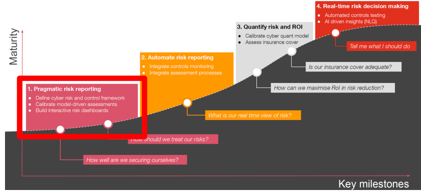
Threats

Name	Exposure	Prevent	Det/Cor
⊞ Accidental Insider Leak	M	2.4	2.4
⊞ Customer compromise	M	2.4	2.5
⊞ External Cyber Attack	M	2.4	2.4
⊞ External information manipulation	M	2.4	2.6
⊞ Malicious Insider Cyber Attack	M	2.4	2.4
⊞ Physical security attack	M	2.4	2.6
⊞ Supply Chain Compromise	M	2.4	2.4
⊞ Upstream DoS Attack	M	2.4	2.5

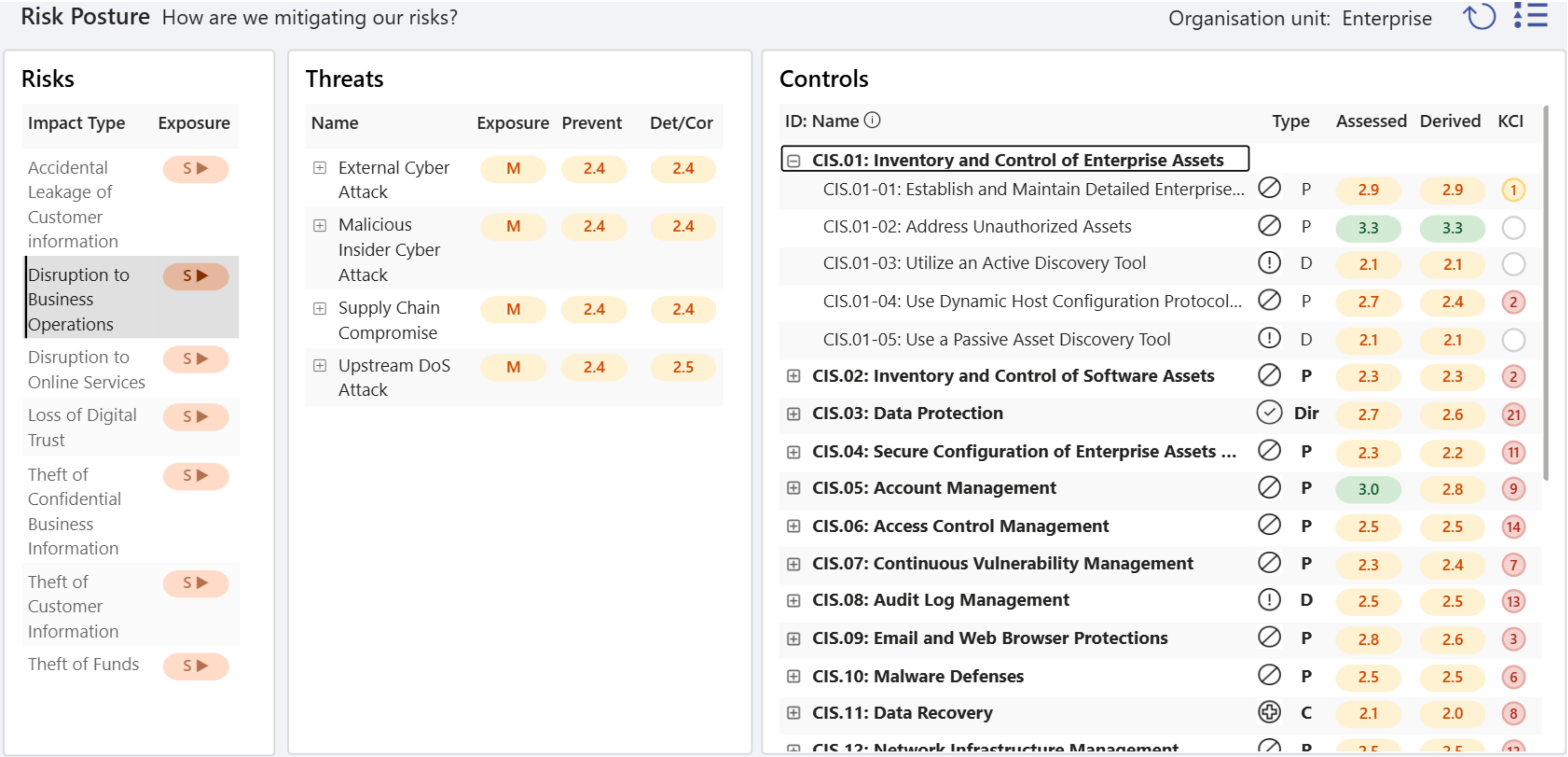
Controls

ID: Name ⓘ	Type		Assessed	Derived	KCI
⊞ CIS.01: Inventory and Control of Enterprise Assets	⊘	P	2.6	2.6	3
⊞ CIS.02: Inventory and Control of Software Assets	⊘	P	2.3	2.3	2
⊞ CIS.03: Data Protection	✓	Dir	2.6	2.4	28
⊞ CIS.04: Secure Configuration of Enterprise Assets and ...	✓	Dir	2.4	2.3	13
⊞ CIS.05: Account Management	⊘	P	3.0	2.8	9
⊞ CIS.06: Access Control Management	⊘	P	2.5	2.5	14
⊞ CIS.07: Continuous Vulnerability Management	✓	Dir	2.3	2.3	7
⊞ CIS.08: Audit Log Management	✓	Dir	2.3	2.3	15
⊞ CIS.09: Email and Web Browser Protections	⊘	P	2.8	2.6	3
⊞ CIS.10: Malware Defenses	⊘	P	2.5	2.5	6
⊞ CIS.11: Data Recovery	✓	Dir	2.1	2.1	11
⊞ CIS.12: Network Infrastructure Management	⊘	P	2.5	2.5	13
⊞ CIS.13: Network Monitoring and Defense	!	D	2.3	2.4	17
⊞ CIS.14: Security Awareness and Skills Training	⊘	P	2.0	2.0	○
⊞ CIS.15: Service Provider Management	✓	Dir	2.3	2.2	2
⊞ CIS.16: Application Software Security	✓	Dir	2.3	2.2	12

Using pragmatic dashboards *(Risk Owner-level)*



Maturity
Key milestones
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do



Risk Posture How are we mitigating our risks?

Organisation unit: Enterprise

Risks

Impact Type	Exposure
Accidental Leakage of Customer information	S ▶
Disruption to Business Operations	S ▶
Disruption to Online Services	S ▶
Loss of Digital Trust	S ▶
Theft of Confidential Business Information	S ▶
Theft of Customer Information	S ▶
Theft of Funds	S ▶

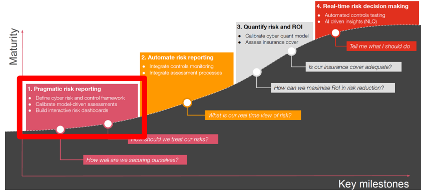
Threats

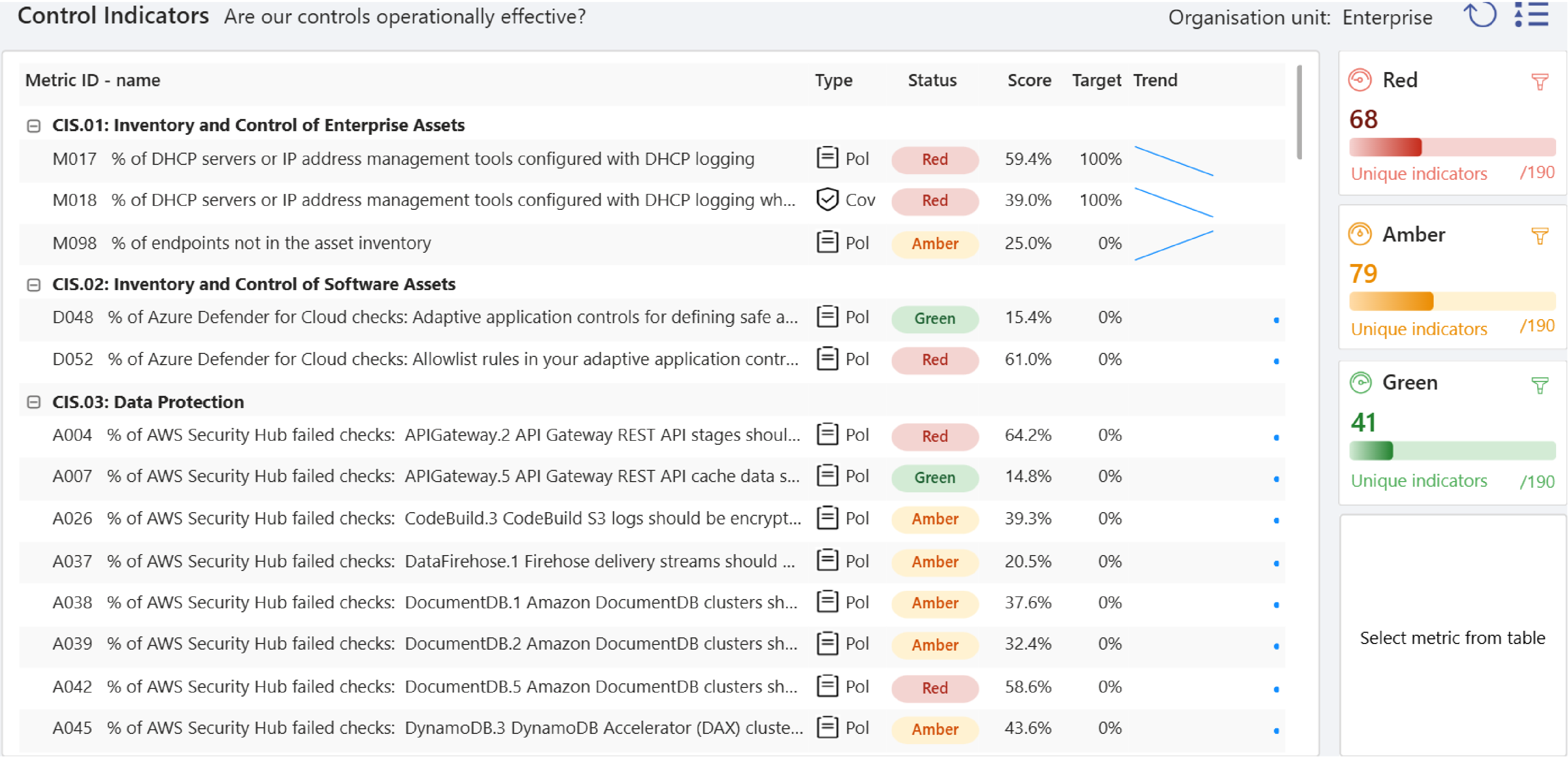
Name	Exposure	Prevent	Det/Cor
⊞ External Cyber Attack	M	2.4	2.4
⊞ Malicious Insider Cyber Attack	M	2.4	2.4
⊞ Supply Chain Compromise	M	2.4	2.4
⊞ Upstream DoS Attack	M	2.4	2.5

Controls

ID: Name ⓘ	Type	Assessed	Derived	KCI
⊟ **CIS.01: Inventory and Control of Enterprise Assets**				
CIS.01-01: Establish and Maintain Detailed Enterprise...	⊘ P	2.9	2.9	1
CIS.01-02: Address Unauthorized Assets	⊘ P	3.3	3.3	○
CIS.01-03: Utilize an Active Discovery Tool	ⓘ D	2.1	2.1	○
CIS.01-04: Use Dynamic Host Configuration Protocol...	⊘ P	2.7	2.4	2
CIS.01-05: Use a Passive Asset Discovery Tool	ⓘ D	2.1	2.1	○
⊞ **CIS.02: Inventory and Control of Software Assets**	⊘ **P**	2.3	2.3	2
⊞ **CIS.03: Data Protection**	✓ **Dir**	2.7	2.6	21
⊞ **CIS.04: Secure Configuration of Enterprise Assets ...**	⊘ **P**	2.3	2.2	11
⊞ **CIS.05: Account Management**	⊘ **P**	3.0	2.8	9
⊞ **CIS.06: Access Control Management**	⊘ **P**	2.5	2.5	14
⊞ **CIS.07: Continuous Vulnerability Management**	⊘ **P**	2.3	2.4	7
⊞ **CIS.08: Audit Log Management**	ⓘ **D**	2.5	2.5	13
⊞ **CIS.09: Email and Web Browser Protections**	⊘ **P**	2.8	2.6	3
⊞ **CIS.10: Malware Defenses**	⊘ **P**	2.5	2.5	6
⊞ **CIS.11: Data Recovery**	⊕ **C**	2.1	2.0	8
⊞ **CIS.12: Network Infrastructure Management**	⊘ **P**	2.5	2.5	12

Using pragmatic dashboards *(Risk Owner-level)*


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones



Control Indicators Are our controls operationally effective?

Organisation unit: Enterprise

Metric ID - name	Type	Status	Score	Target	Trend
CIS.01: Inventory and Control of Enterprise Assets					
M017 % of DHCP servers or IP address management tools configured with DHCP logging	Pol	Red	59.4%	100%	
M018 % of DHCP servers or IP address management tools configured with DHCP logging wh...	Cov	Red	39.0%	100%	
M098 % of endpoints not in the asset inventory	Pol	Amber	25.0%	0%	
CIS.02: Inventory and Control of Software Assets					
D048 % of Azure Defender for Cloud checks: Adaptive application controls for defining safe a...	Pol	Green	15.4%	0%	
D052 % of Azure Defender for Cloud checks: Allowlist rules in your adaptive application contr...	Pol	Red	61.0%	0%	
CIS.03: Data Protection					
A004 % of AWS Security Hub failed checks: APIGateway.2 API Gateway REST API stages shoul...	Pol	Red	64.2%	0%	
A007 % of AWS Security Hub failed checks: APIGateway.5 API Gateway REST API cache data s...	Pol	Green	14.8%	0%	
A026 % of AWS Security Hub failed checks: CodeBuild.3 CodeBuild S3 logs should be encrypt...	Pol	Amber	39.3%	0%	
A037 % of AWS Security Hub failed checks: DataFirehose.1 Firehose delivery streams should ...	Pol	Amber	20.5%	0%	
A038 % of AWS Security Hub failed checks: DocumentDB.1 Amazon DocumentDB clusters sh...	Pol	Amber	37.6%	0%	
A039 % of AWS Security Hub failed checks: DocumentDB.2 Amazon DocumentDB clusters sh...	Pol	Amber	32.4%	0%	
A042 % of AWS Security Hub failed checks: DocumentDB.5 Amazon DocumentDB clusters sh...	Pol	Red	58.6%	0%	
A045 % of AWS Security Hub failed checks: DynamoDB.3 DynamoDB Accelerator (DAX) cluste...	Pol	Amber	43.6%	0%	

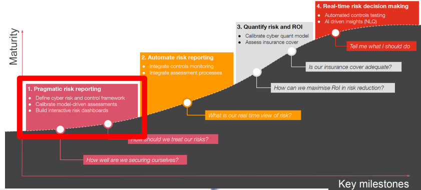
Red
68
Unique indicators /190

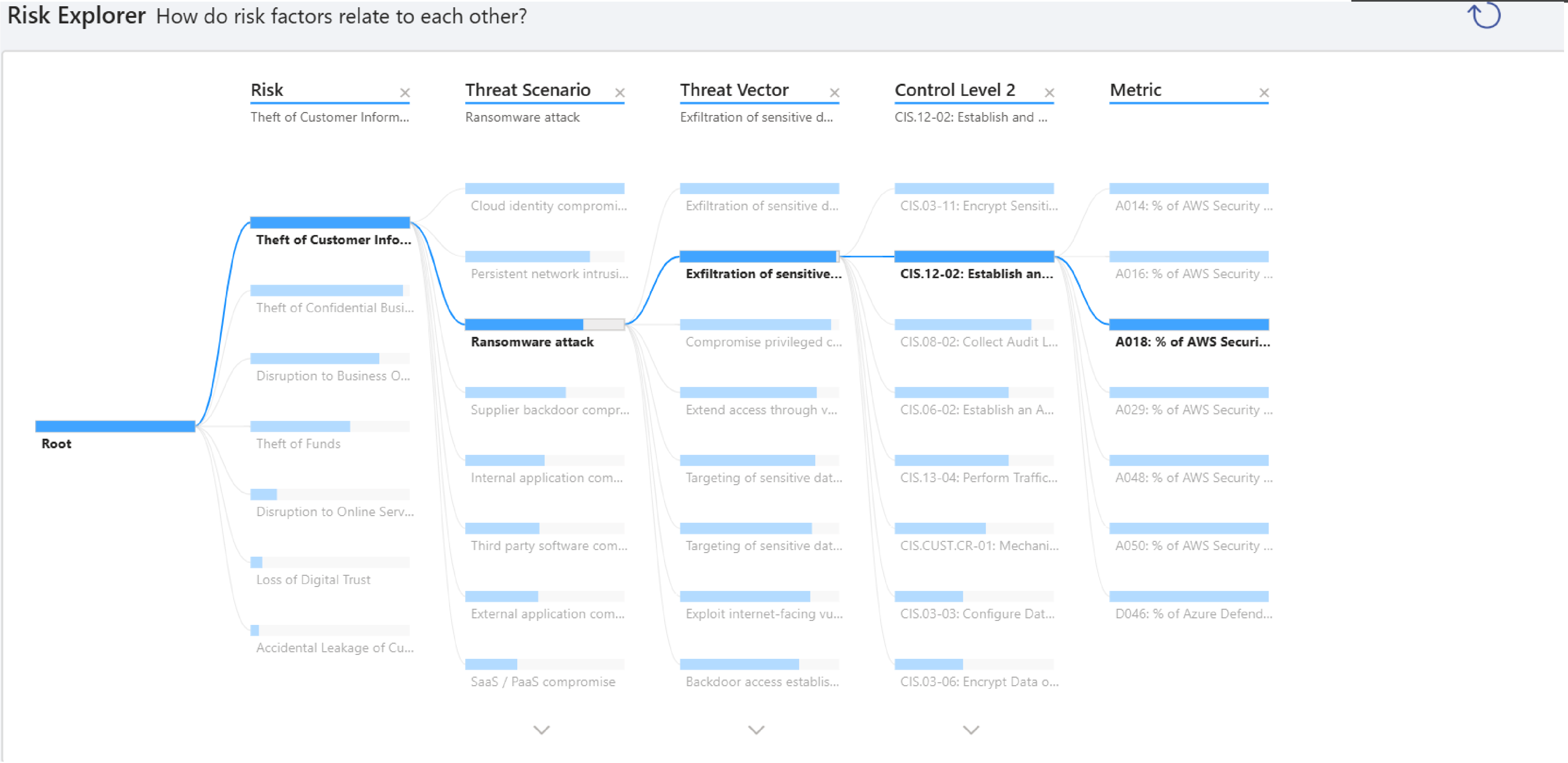
Amber
79
Unique indicators /190

Green
41
Unique indicators /190

Select metric from table

Using pragmatic dashboards *(Operations-level)*


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
How should we treat our risks?
How well are we securing ourselves?
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
What is our real time view of risk?
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
Tell me what I should do
Key milestones


Risk Explorer How do risk factors relate to each other?

Risk	Threat Scenario	Threat Vector	Control Level 2	Metric
Theft of Customer Inform...	Ransomware attack	Exfiltration of sensitive d...	CIS.12-02: Establish and ...	

Root

Risk:
- **Theft of Customer Info...**
- Theft of Confidential Busi...
- Disruption to Business O...
- Theft of Funds
- Disruption to Online Serv...
- Loss of Digital Trust
- Accidental Leakage of Cu...

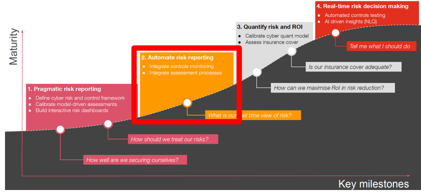
Threat Scenario:
- Cloud identity compromi...
- Persistent network intrusi...
- **Ransomware attack**
- Supplier backdoor compr...
- Internal application com...
- Third party software com...
- External application com...
- SaaS / PaaS compromise

Threat Vector:
- Exfiltration of sensitive d...
- **Exfiltration of sensitive...**
- Compromise privileged c...
- Extend access through v...
- Targeting of sensitive dat...
- Targeting of sensitive dat...
- Exploit internet-facing vu...
- Backdoor access establis...

Control Level 2:
- CIS.03-11: Encrypt Sensiti...
- **CIS.12-02: Establish an...**
- CIS.08-02: Collect Audit L...
- CIS.06-02: Establish an A...
- CIS.13-04: Perform Traffic...
- CIS.CUST.CR-01: Mechani...
- CIS.03-03: Configure Dat...
- CIS.03-06: Encrypt Data o...

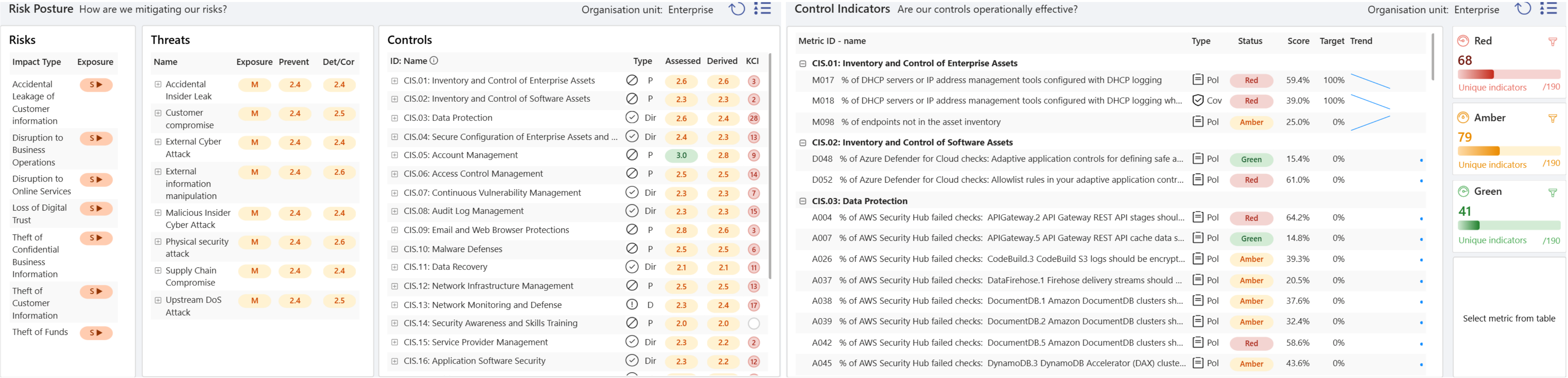
Metric:
- A014: % of AWS Security ...
- A016: % of AWS Security ...
- **A018: % of AWS Securi...**
- A029: % of AWS Security ...
- A048: % of AWS Security ...
- A050: % of AWS Security ...
- D046: % of Azure Defend...

Moving towards automation


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our eal time view of risk?
How can we maximise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

Now imagine updating these risks, threats, controls and particularly control indicators on a quarterly basis to allow for frequent reporting to the Board of Directors.

Start out small – find a reasonable metric for a control and find a way to pull that metric automatically from your infrastructure.



Risk Posture How are we mitigating our risks? Organisation unit: Enterprise

Risks

Impact Type	Exposure
Accidental Leakage of Customer information	S ▶
Disruption to Business Operations	S ▶
Disruption to Online Services	S ▶
Loss of Digital Trust	S ▶
Theft of Confidential Business Information	S ▶
Theft of Customer Information	S ▶
Theft of Funds	S ▶

Threats

Name	Exposure	Prevent	Det/Cor
⊞ Accidental Insider Leak	M	2.4	2.4
⊞ Customer compromise	M	2.4	2.5
⊞ External Cyber Attack	M	2.4	2.4
⊞ External information manipulation	M	2.4	2.6
⊞ Malicious Insider Cyber Attack	M	2.4	2.4
⊞ Physical security attack	M	2.4	2.6
⊞ Supply Chain Compromise	M	2.4	2.4
⊞ Upstream DoS Attack	M	2.4	2.5

Controls

ID: Name ⓘ	Type	Assessed	Derived	KCI
⊞ CIS.01: Inventory and Control of Enterprise Assets	⊘ P	2.6	2.6	3
⊞ CIS.02: Inventory and Control of Software Assets	⊘ P	2.3	2.3	2
⊞ CIS.03: Data Protection	✓ Dir	2.6	2.4	28
⊞ CIS.04: Secure Configuration of Enterprise Assets and ...	✓ Dir	2.4	2.3	13
⊞ CIS.05: Account Management	⊘ P	3.0	2.8	9
⊞ CIS.06: Access Control Management	⊘ P	2.5	2.5	14
⊞ CIS.07: Continuous Vulnerability Management	✓ Dir	2.3	2.3	7
⊞ CIS.08: Audit Log Management	✓ Dir	2.3	2.3	15
⊞ CIS.09: Email and Web Browser Protections	⊘ P	2.8	2.6	3
⊞ CIS.10: Malware Defenses	⊘ P	2.5	2.5	6
⊞ CIS.11: Data Recovery	✓ Dir	2.1	2.1	11
⊞ CIS.12: Network Infrastructure Management	⊘ P	2.5	2.5	13
⊞ CIS.13: Network Monitoring and Defense	! D	2.3	2.4	17
⊞ CIS.14: Security Awareness and Skills Training	⊘ P	2.0	2.0	○
⊞ CIS.15: Service Provider Management	✓ Dir	2.3	2.2	2
⊞ CIS.16: Application Software Security	✓ Dir	2.3	2.2	12

Control Indicators Are our controls operationally effective? Organisation unit: Enterprise

Metric ID - name	Type	Status	Score	Target	Trend
⊟ **CIS.01: Inventory and Control of Enterprise Assets**					
M017 % of DHCP servers or IP address management tools configured with DHCP logging	Pol	Red	59.4%	100%	
M018 % of DHCP servers or IP address management tools configured with DHCP logging wh...	Cov	Red	39.0%	100%	
M098 % of endpoints not in the asset inventory	Pol	Amber	25.0%	0%	
⊟ **CIS.02: Inventory and Control of Software Assets**					
D048 % of Azure Defender for Cloud checks: Adaptive application controls for defining safe a...	Pol	Green	15.4%	0%	•
D052 % of Azure Defender for Cloud checks: Allowlist rules in your adaptive application contr...	Pol	Red	61.0%	0%	•
⊟ **CIS.03: Data Protection**					
A004 % of AWS Security Hub failed checks: APIGateway.2 API Gateway REST API stages shoul...	Pol	Red	64.2%	0%	•
A007 % of AWS Security Hub failed checks: APIGateway.5 API Gateway REST API cache data s...	Pol	Green	14.8%	0%	•
A026 % of AWS Security Hub failed checks: CodeBuild.3 CodeBuild S3 logs should be encrypt...	Pol	Amber	39.3%	0%	•
A037 % of AWS Security Hub failed checks: DataFirehose.1 Firehose delivery streams should ...	Pol	Amber	20.5%	0%	•
A038 % of AWS Security Hub failed checks: DocumentDB.1 Amazon DocumentDB clusters sh...	Pol	Amber	37.6%	0%	•
A039 % of AWS Security Hub failed checks: DocumentDB.2 Amazon DocumentDB clusters sh...	Pol	Amber	32.4%	0%	•
A042 % of AWS Security Hub failed checks: DocumentDB.5 Amazon DocumentDB clusters sh...	Pol	Red	58.6%	0%	•
A045 % of AWS Security Hub failed checks: DynamoDB.3 DynamoDB Accelerator (DAX) cluste...	Pol	Amber	43.6%	0%	•

Red
68
Unique indicators /190

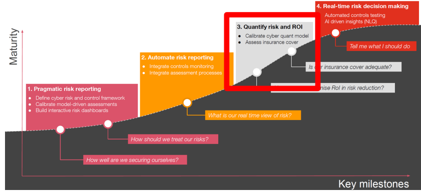
Amber
79
Unique indicators /190

Green
41
Unique indicators /190

Select metric from table

Touching upon quantification

Some questions to get started

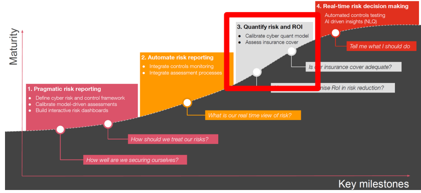

Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
mise RoI in risk reduction?
Is our insurance cover adequate?
Tell me what I should do
Key milestones

Why doesn’t everyone quantify?

Does cyber risk quantification need to be very complicated?

How do you get started?

Why is quantification of IT-risks relevant


Maturity

1. Pragmatic risk reporting
- Define cyber risk and control framework
- Calibrate model-driven assessments
- Build interactive risk dashboards

2. Automate risk reporting
- Integrate controls monitoring
- Integrate assessment processes

3. Quantify risk and ROI
- Calibrate cyber quant model
- Assess insurance cover

4. Real-time risk decision making

Automated controls testing
AI driven insights (NLQ)

How well are we securing ourselves?

How should we treat our risks?

What is our real time view of risk?

mise RoI in risk reduction?

Is our insurance cover adequate?

Tell me what I should do

Key milestones

Quantification of IT-risks are required and relevant both for regulatory and general enterprise risk management purposes

DORA incident reporting

It is a requirement to report the total amount of gross and indirect costs and losses incurred by the financial entity stemming from a major incident under DORA as part of the final report.

Due to the time restraints imposed in DORA a calculation framework and governance need to be established in order to adequately estimate the impact when a major incident occurs.

Calculation of emerging risks in ORSA and ICAAP

As part of the ORSA and ICAAP processes, IT-risks are highly relevant given its status as an emerging risk and not necessarily captured adequately in the capital models.

The impact of Cyber on your business could be calculated in different scenarios, such as a best estimate, 200 year event, etc.

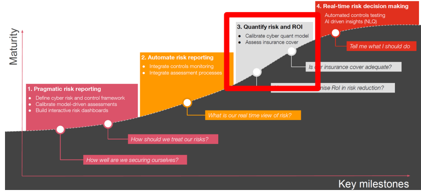
Business insights

Quantification can help inform decision makers about what Cyber scenarios are truly material to the business, thus empowering the business to spend time on mitigating the risk drivers that truly matter to the business and less on others.

Management reporting

Quantifying IT-risks can be a key tool for the board to challenge whether the actual IT-risks are aligned with the risk appetite.

Furthermore, it can help inform the CISO and other stakeholders on relevant mitigation activities and to assess the cost of these against the IT-risk reduction.



4. Real-time risk decision making

Automated controls testing
AI driven insights (NLQ)

3. Quantify risk and ROI

- Calibrate cyber quant model
- Assess insurance cover

2. Automate risk reporting

- Integrate controls monitoring
- Integrate assessment processes

1. Pragmatic risk reporting

- Define cyber risk and control framework
- Calibrate model-driven assessments
- Build interactive risk dashboards

Tell me what I should do

Is o r insurance cover adequate?

[illegible] mise RoI in risk reduction?

What is our real time view of risk?

How should we treat our risks?

How well are we securing ourselves?

Challenges in quantifying cyber risks

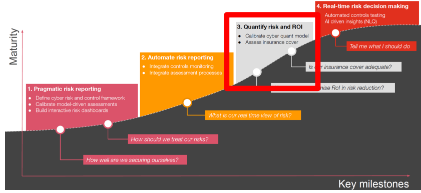
Cyber risk is a so-called ‘Emerging Risk’. This presents numerous challenges when modelling quantitative impacts

Lack of data: There is only very sparse public databases available that provide insight into the impact of cyber attacks and these are largely biased, as they are based on self-reporting. Most companies do not disclose the impact of successful attacks nor the frequency of attempted attacks against them.

Lack of modeling expertise: Since losses due to cyber attacks are so new and the amount of data is so small, there has also not been any consensus around 'best practice' within the modeling of these, neither in the industry nor in the scientific literature.

Insufficient domain knowledge: It is only in rare cases that cyber risk modelers and cyber risk experts are the same person.

Overview of Cyber Risk Model and DORA metrics


Maturity
1. Pragmatic risk reporting
Define cyber risk and control framework
Calibrate model-driven assessments
Build interactive risk dashboards
2. Automate risk reporting
Integrate controls monitoring
Integrate assessment processes
3. Quantify risk and ROI
Calibrate cyber quant model
Assess insurance cover
4. Real-time risk decision making
Automated controls testing
AI driven insights (NLQ)
How well are we securing ourselves?
How should we treat our risks?
What is our real time view of risk?
mise RoI in risk reduction?
Is r insurance cover adequate?
Tell me what I should do
Key milestones

Metrics

Model Inputs

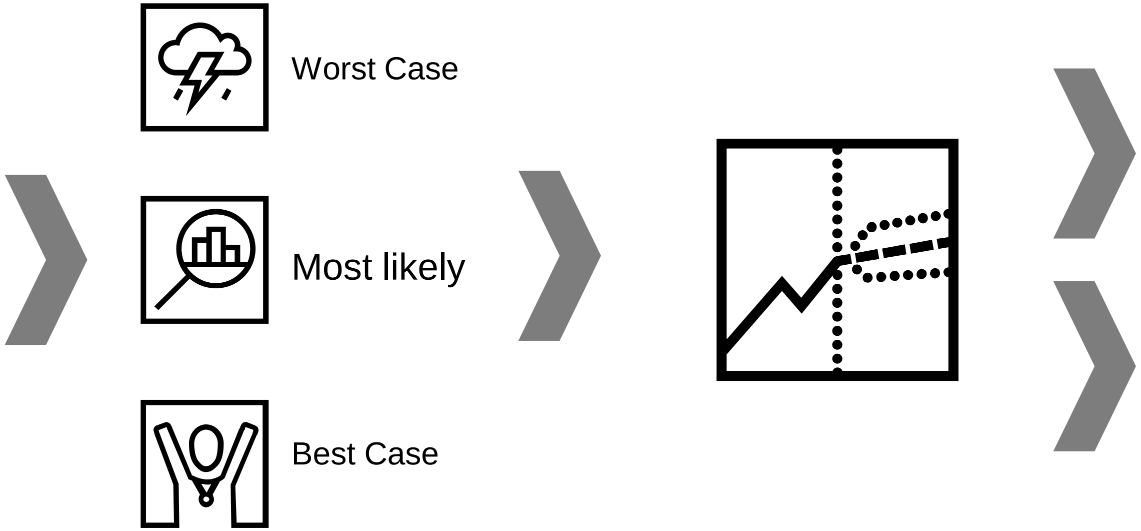
Cyber Risk Model

Model Outputs

Total amount of gross direct and indirect costs and losses incurred by the financial entity stemming from the major incident

Amount of expropriated funds or financial assets for which the financial entity is liable	Amount of replacement or relocation costs of software, hardware or infrastructure
Amount other specified costs and losses	Amount of fees due to non-compliance with contractual obligations
Amount of customer redress and compensation costs	Amount of losses due to forgone revenues
Amount of costs associated with internal and external communication	Amount of advisory costs, including costs associated with legal counselling, forensic and remediation services

Amount of staff costs, including costs associated to replacing or relocating staff, hiring extra staff, remuneration of overtime and recovering lost or impaired skills of staff



Cyber Scenario Impacts (Cyber Stress Tests)

DORA costs and losses

Utilizing expert judgement data

Expert Judgement Data
Model distribution

Currently Cyber Risk models utilize a high amount of expert judgement data. One common approach, such as the one outlined in the FAIR framework, is to have business experts supply their inputs on the **Best Case, Most Likely** and **Worst Case** outcomes.
Best Case: 19 out of 20 events, **Most Likely**: Average, **Worst Case:** 1 out of 20 events.

One easy way to use this for modelling purposes is to fit a log – normal distribution to these inputs using the ***method of moments estimator (MoM)*** like so:

$X \sim LN(\mu_{MoM}, \sigma^2_{MoM})$
where $\sigma_{MoM} = \frac{\log(\text{Worst Case}) - \log(Best\ case)}{2 * \alpha_{95\%}}$ and $\mu_{MoM} = \log(\text{mean}) - \frac{\sigma^2_{MoM}}{2}$

4

Spørgsmål