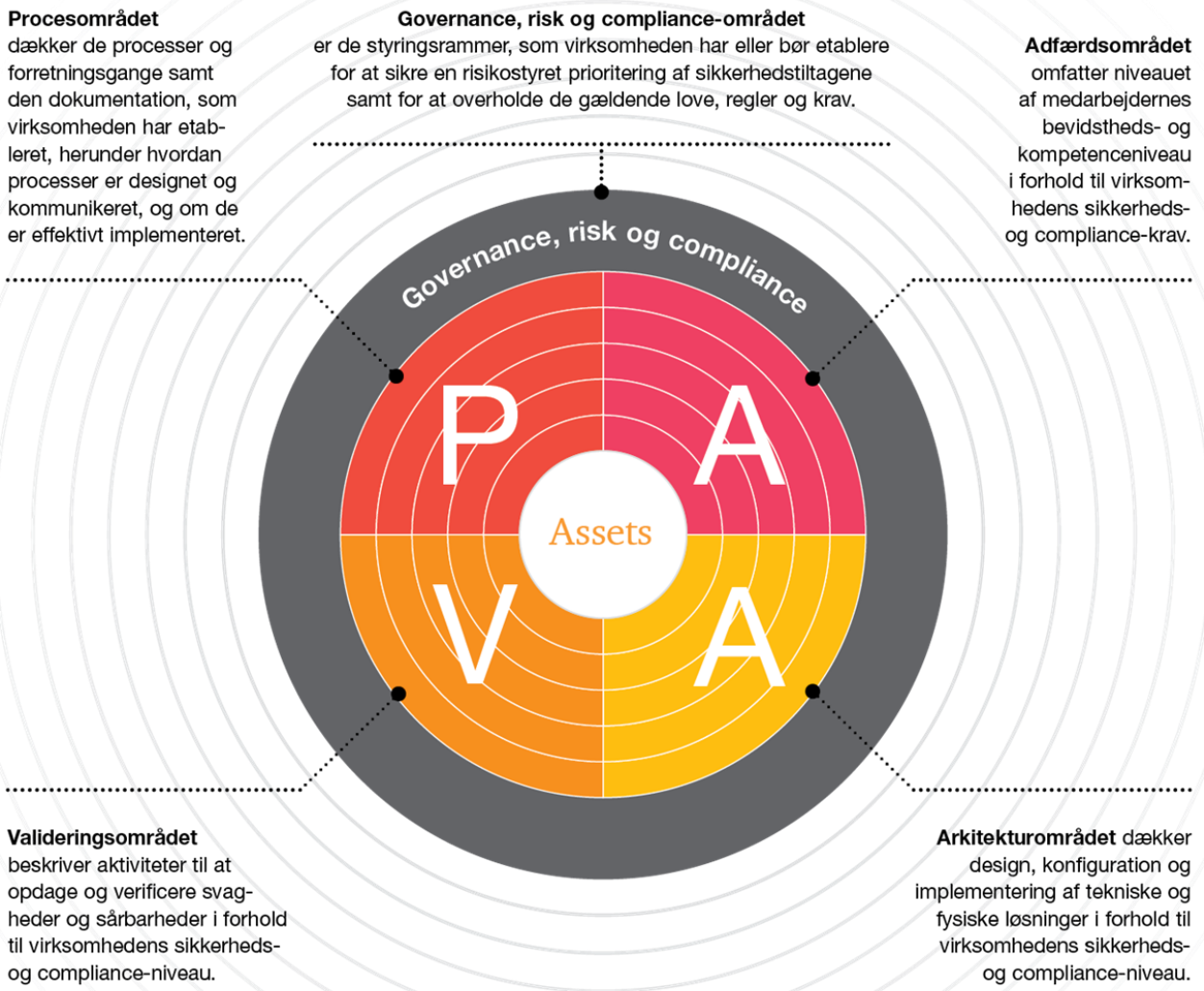
# Risikostyring og rapportering om cybersikkerhed

Morten Friis
Partner, PwC Technology & Security
For Bestyrelsesforeningen, nov. 2022

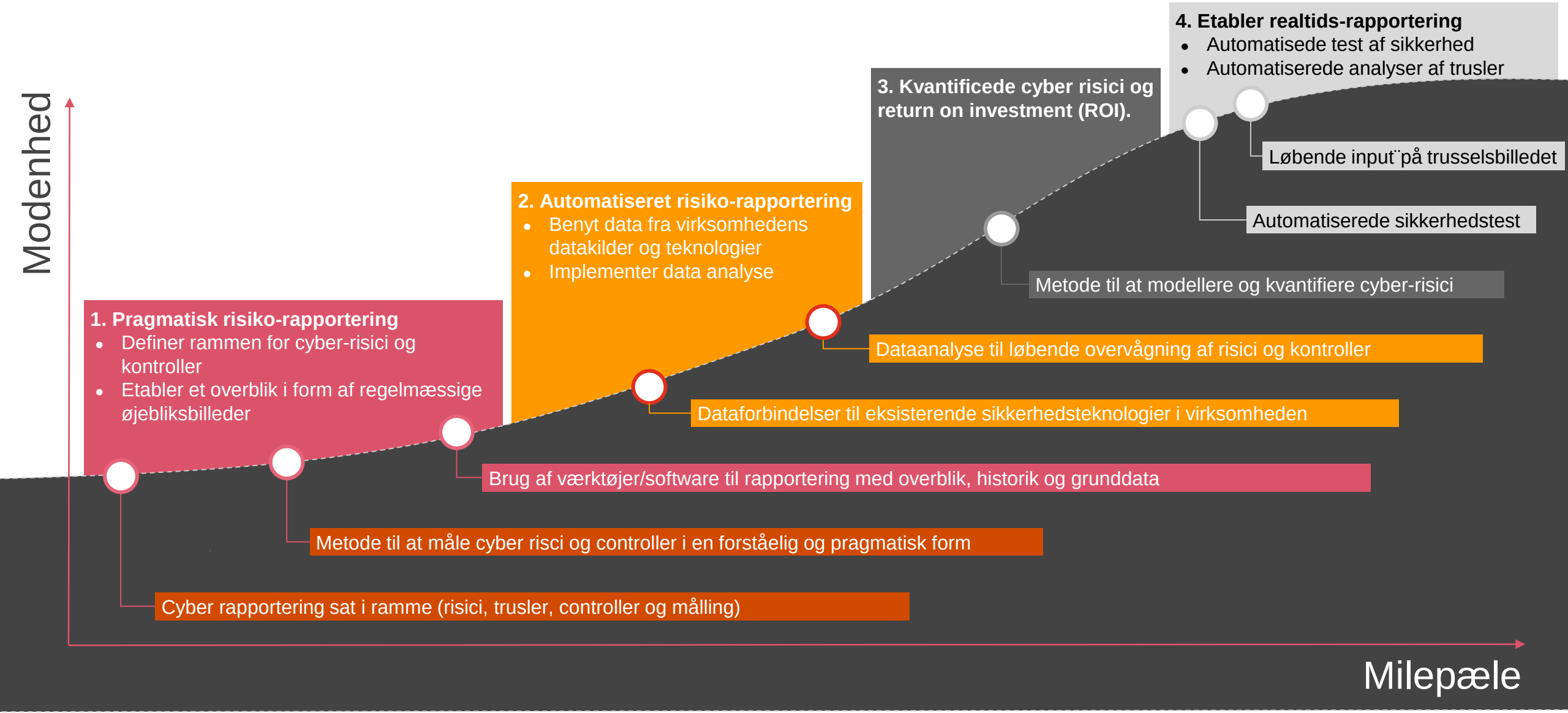
# PAVA – et forståeligt sikkerhedskoncept

PAVA-konceptet er et generisk kommunikations-, vurderings-og rapporteringskoncept, som virksomheder kan bruge til bl.a. at vurdere og rapportere deres parathed og robusthed over for forskellige typer af cyberrisici og -trusler.



# Cyber risiko-rapportering – en rejse

**Forstå hvor virkomsheden er i forhold til risikorapportering. Er der et fundament i form af en forståelse af konsekvenser, trusselsbilledet og modstandsdygtigheden og måling heraf?**



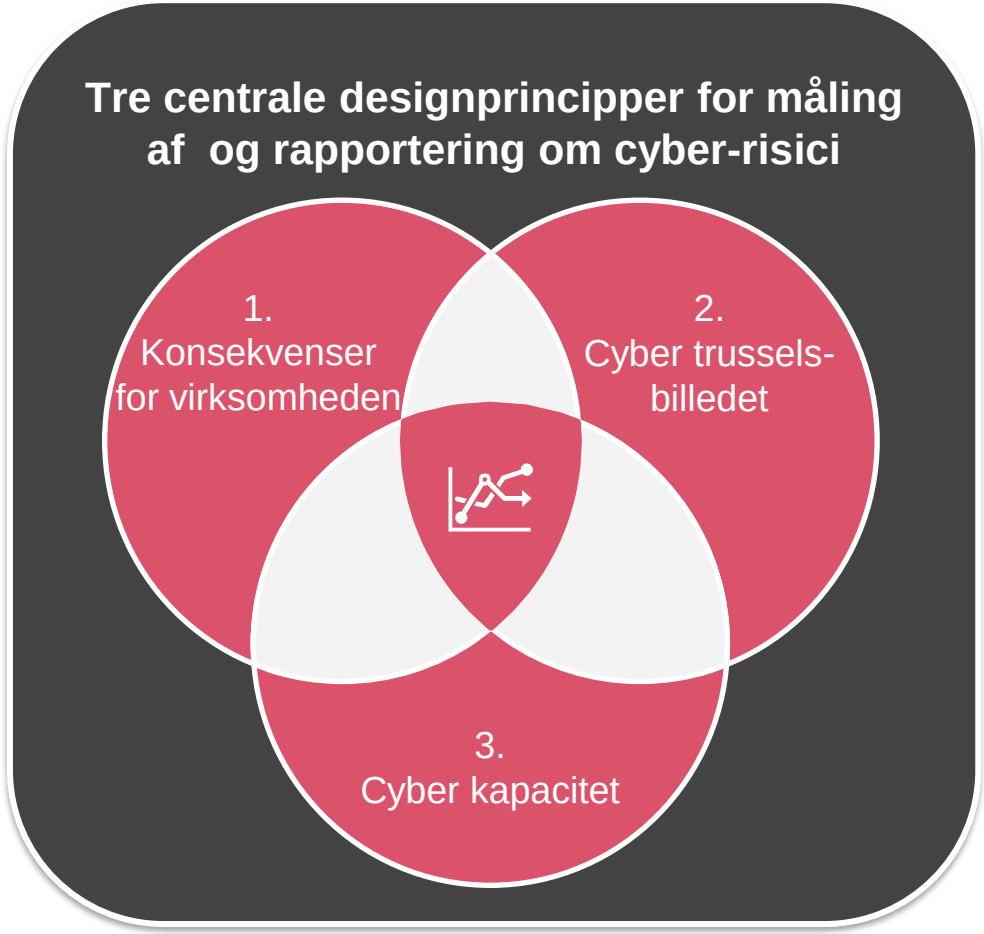
# Designprincipper for cyberrisikorapportering

**Det helt grundlæggende i cyberrisici**

**En stærk ledelsesrapportering om cyberrisici bør på i overskuelig form vise nuværende situation og den fremtidige ønskede modstandsdygtighed, samt hvordan det opnås.**

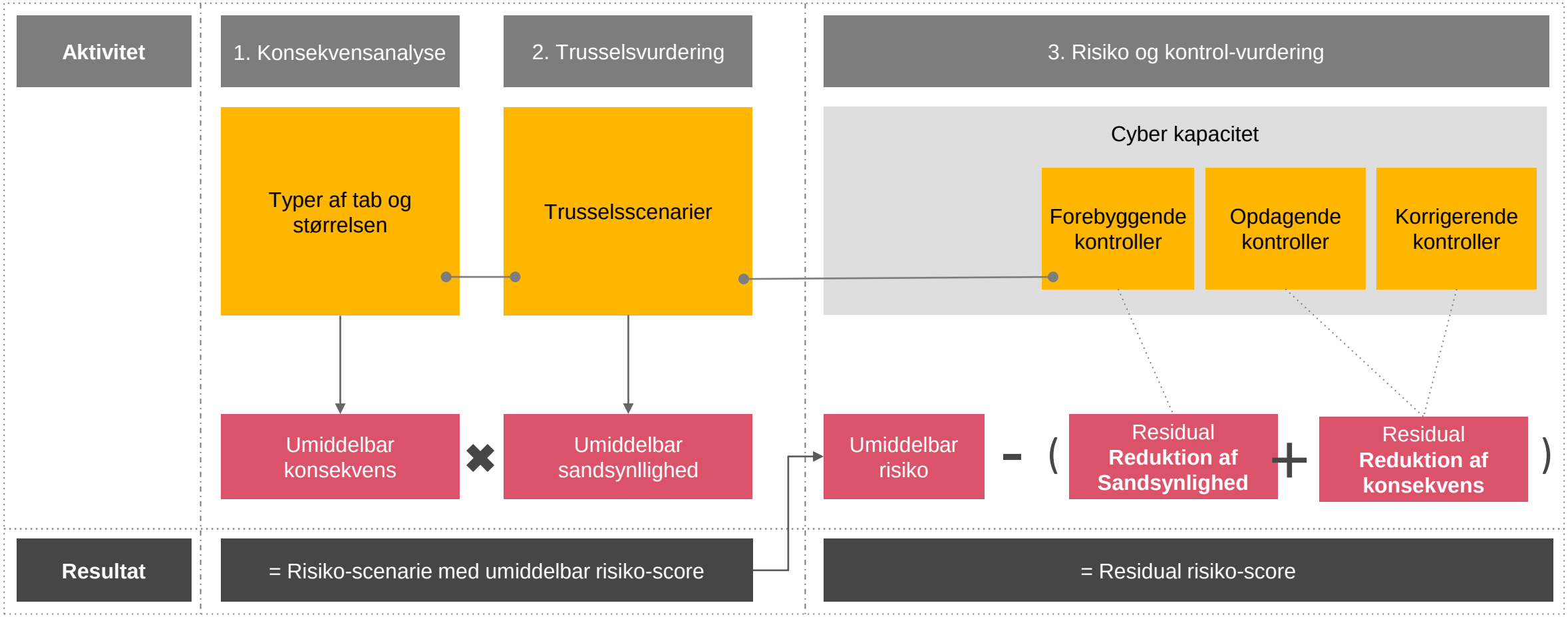
**De tre designprincipper**

1. **Analyser konsekvenser for virksomheden** – på de væsentligste cyberrisici. De bør beskrive hvordan det på virker viksomheden enten i kvalitative eller kvantitative termer.
2. **Analyser cyber trusselsbilledet** – i form af centrale trussels-scenarier eller -kategorier, der driver sandsynligheden for en cyberhændelse.
3. **Vurder cyber kapacitet** – virksomhedens evne til at forebygge, opdage og håndtere en cyberhændelse.



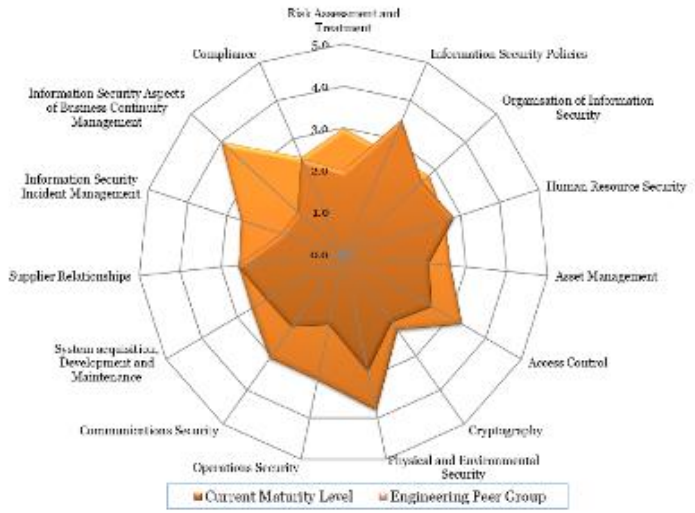
# God praksis| Analyse af virksomhedens cyber-risici

**Cyber-risici kan måles med en enkel beregning**

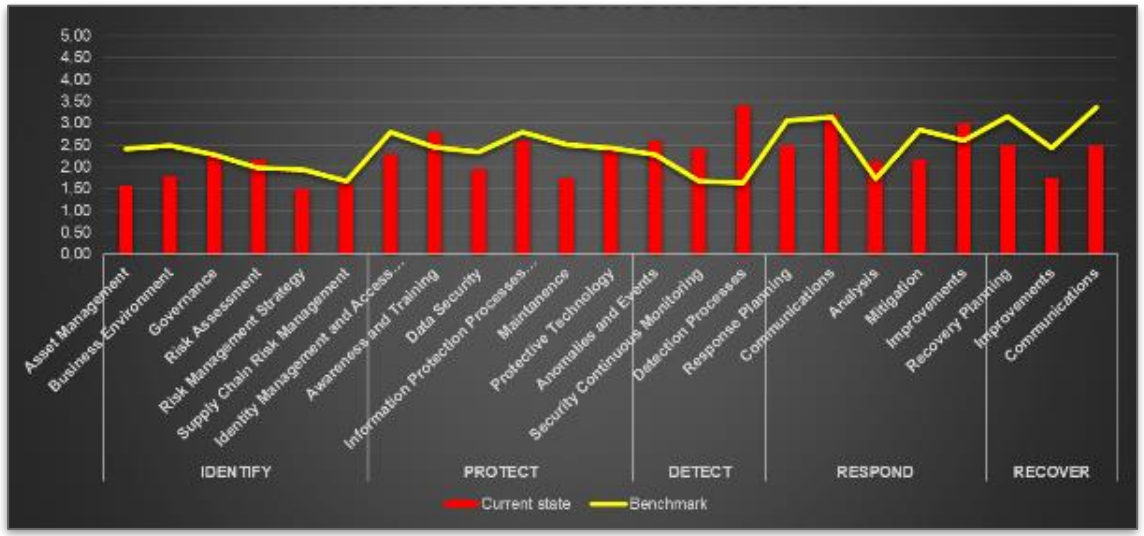


# Rapportering i henhold til anerkendte standarder mv.

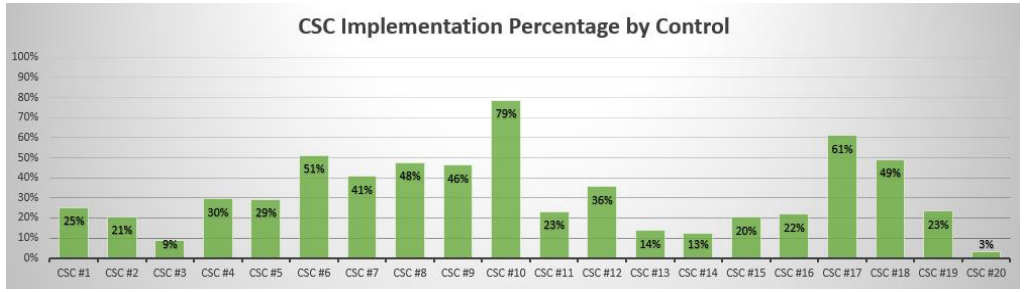
**Eksempler på rapportering og modenhedsmålinger i henhold til enten ISO-standard, National Institute of Standards and Technology (USA) eller Center for Internet Security (non-profit organisation)**




ISO27001




NIST Cybersecurity Framework




CIS18 – Critical Security Controls

# Ledelsesrapportering og risikoappetit

| Out of Appetite | Within risk tolerance | Within Appetite |
|---|---|---|

| **Enterprise Cyber Risks** with business impact-based descriptions | **Impact level** (worst case, enterprise-wide impact) |
|---|---|
| **R1. Accidental Leakage of Customer Information** | 3 |
| **R2. Theft of Confidential Information** | 2 |
| **R3. Theft of Customer Information** | 3 |
| **R4. Disruption to Business Operations** | 3 |
| **R5. Disruption to Online Services** | 1 |
| **R6. Theft of Funds** | 3 |
| **R7. Loss of Digital Trust** | 1 |

Example data

| Impact Level | Example Risk Assessment Matrix | | | |
|---|---|---|---|---|
| 4. Severe >25M | | | | |
| 3. Major 5M-25M | | | | |
| 2. Significant 500k-5m | | | | |
| 1. Minor <500K | | | | |
| Example Likelihood | 1. Remote (0-10%) | 2. Low (10-25%) | 3. Possible (25-50%) | 4. Likely (>50%) |

# Ledelsesrapportering - den store model …

**Risk Posture**
How well are we securing ourselves?

Reset

All

1

## Risks

| Accidental Leakage of Customer Information | Theft of Confidential Business Information | Theft of Customer Information | Disruption to Business Operations | Disruption to Online Services | Theft of Funds | Loss of Digital Trust |
|---|---|---|---|---|---|---|
| H Trend: ▲ | H Trend: -- | M Trend: -- | H Trend: -- | H Trend: -- | H Trend: -- | M Trend: -- |

2

## Threats

| Threat Category | Exposure | Prevent | Detect/ Correct |
|---|---|---|---|
| Accidental Insider Leak | H ▲ | 2.3 | 2.9 |
| External Cyber Attack | M ▲ | 2.1 | 2.6 |
| Malicious Insider Cyber Attack | H ▲ | 2.2 | 2.6 |
| Supply Chain Compromise | M ▲ | 2.1 | 2.6 |
| Denial of Service Attack | H ▲ | 1.9 | 2.5 |
| External Information Manipulation | M -- | 2.3 | 2.3 |
| Customer Compromise | H ▲ | 1.7 | 2.8 |

3

## Capabilities

| | Capability | Type | Assessed | Derived | Target |
|---|---|---|---|---|---|
| ASM.2 | Vulnerability Management … | P | 3.0 | 2.5 | 4.0 |
| ASM.3 | AppSec / DevSecOps (SA… | P | 2.0 | 1.3 | 4.0 |
| ASM.4 | Asset Management (Attack… | P | 2.0 | 1.5 | 4.0 |
| IAM.1 | Privileged Access Manage… | P | 2.0 | 1.5 | 4.0 |
| IAM.2 | Identity Governance | P | 2.0 | 1.3 | 4.0 |
| IAM.3 | Authentication & Authorisat… | P | 2.0 | 1.3 | 3.5 |
| IIP.1 | Data Loss Prevention | P | 2.0 | 1.3 | 4.0 |
| IIP.2 | Data Encryption | P | 2.0 | 1.3 | 4.0 |
| IIP.3 | Data Backup & Recovery | C | 3.0 | 3.3 | 4.0 |
| IIP.4 | Secure Data Disposal | P | 3.0 | 3.3 | 3.5 |
| IS.1 | Network Security (inc. Seg… | P | 3.0 | 3.3 | 4.0 |
| IS.2 | Endpoint Protection | P | 3.0 | 3.3 | 4.5 |
| IS.3 | DDOS Mitigation / Protection | P | 2.0 | 1.3 | 4.0 |
| IS.4 | Email / Web Access & Filte… | P | 3.0 | 3.3 | 4.0 |
| IS.5 | Secure Connectivity (inc. R… | P | 2.0 | 1.5 | 4.0 |
| SGL.1 | Security Culture & Training | P | 4.0 | 3.0 | 4.5 |
| SGL.2 | Cyber Crisis Management | C | 2.0 | 1.0 | 4.5 |
| SRC.1 | Supply Chain Risk Manage… | P | 2.0 | 1.5 | 3.5 |
| TDR.1 | Incident Response | C | 4.0 | 3.5 | 4.5 |
| TDR.2 | Continuous Monitoring (inc… | D | 3.0 | 3.3 | 4.0 |
| TDR.3 | Anomaly Analysis & Detect… | D | 4.0 | 3.5 | 4.5 |
| TDR.4 | Threat Intelligence | D | 2.0 | 1.0 | 3.5 |
| TDR.5 | Digital Brand Protection | P | 3.0 | 2.3 | 4.0 |

4

## Metrics

| Metrics | Effectiveness | Coverage |
|---|---|---|
| % of open critical vulnerabilities identified more than 30 days old | 7.0% ▲ | 77.5% ▼ |
| % of new apps promoted into live pen tested with all sec findings fixed | 75.0% ▲ | 65.3% ▲ |
| % of endpoints not in the asset inventory | 10.0% ▼ | 71.5% ▼ |
| % privileged accounts on boarded into PAM solution with regular passwo… | 92.0% ▲ | 59.5% ▼ |
| % of critical apps where all access is certified at least every 6 months | 90.0% ▼ | 52.5% ▲ |
| % of externally facing critical apps with multi-factor authentication | 87.0% ▼ | 41.5% ▼ |
| % of users covered by DLP, USB and mobile device mgt controls | 96.0% ▲ | 33.0% ▲ |
| % of critical apps with all sensitive fields / records encrypted | 81.0% ▲ | 43.0% ▼ |
| % of critical apps (BCM / DR) tested | 10.0% ▲ | 86.5% ▼ |
| % of LoBs that have an approved data destruction process and have the… | 90.0% ▲ | 93.0% ▼ |
| % of network devices not located on dedicated VLANs | 9.0% ▲ | 88.5% -- |
| % of endpoints with EPP solution installed with the latest threat indicators | 10.0% ▼ | 91.5% ▼ |
| % of critical external facing systems protected by a DDoS mitigation solu… | 55.0% ▲ | 64.5% ▲ |
| % of systems / end users being scanned by web proxies | 90.0% ▲ | 89.5% ▲ |
| % of remote user access connections with key controls implemented | 93.0% ▲ | 70.0% ▼ |
| % of employees targeted in a phishing campaign who reported the phishi… | 5.0% ▲ | 42.5% ▼ |
| % outstanding findings from post incident reports (for major incidents) | 9.0% ▼ | 16.5% ▼ |
| % of critical suppliers with outstanding issues still to resolve. | 98.0% ▲ | 73.0% ▼ |
| % deviation from target time btw SOC engagement and containment | 9.0% ▲ | 65.0% ▼ |
| % of all systems with logs enabled and capturing events into SIEM tool | 95.0% -- | 87.5% ▼ |
| % of endpoints with an EDR solution installed | 90.0% ▼ | 75.0% ▼ |
| % of incidents where the criticality has been informed by threat intelligence | 96.0% ▲ | 25.0% ▼ |
| % company domains spoofed | 80.0% ▲ | 35.0% ▼ |

*Eksempel på dashboard*

# Cybercrime Survey 2022

**73 %**

af CXO'er og it-fagfolk angiver, at deres øgede bekymring for cybertrusler i nogen eller i høj grad skyldes konflikten mellem Rusland og Vesten.

**47 %**

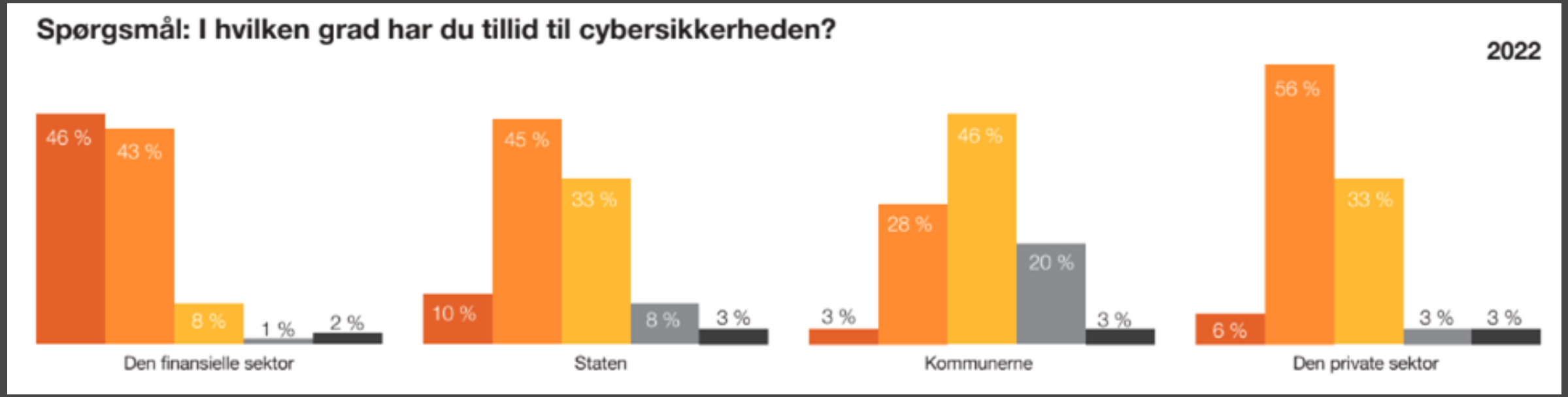
regner hacktivister blandt de største trusler. Det er 11 %-point flere end sidste år og den største andel nogensinde.

**51 %**

angiver, at deres virksomhed har været udsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår. Det er fjerde år i træk, at mere end hver anden virksomhed har været ramt.

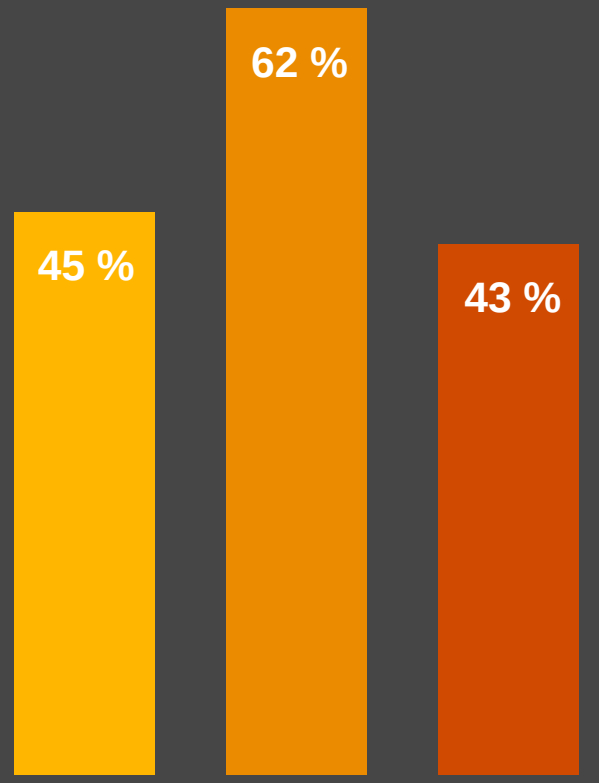
Revision. Skat. Rådgivning.

# Tillid til cybersikkerhed på tværs af sektorer




*PwC Cybercrime Survey 2022*

## Har din virksomhed planlagt eller implementeret nye cyber-sikkerhedstiltag som følge af konflikten mellem Rusland og Vesten?




Finansielle sektor

Offentlig sektor

Privat sektor

*PwC Cybercrime Survey 2022*

# Thank you!


**Læs mere om PwCs anbefalinger til cybersikkerhed og beredskab i Cybercrime Survey 2022.**

Our vision is to become the leading consulting partner, helping clients to solve complex business problems - focused on the human experience, fueled by innovation, and enabled through the latest technology.

**Your trusted advisor for the IT transformation journey**

Morten Friis

Partner, Technology & Security

T: +45 5215 0258

M: morten.friis@pwc.com