

Modul 1

Basis indenfor
Cybersikkerhed

Modul 2

Teknisk Træning

Modul 3

Risikostyring

Modul 4

NIS-2

Modul 5

Beredskabs-
kommunikation

Modul 6

Certificering i SC-900
hos Microsoft



MODUL 3 AF 7

Risikostyring



Dagens program

- Præsentation af os og jer
- Hvad skal vi lærer de næste 2 dage
- Basal risikoteori
 - Hvad er risiko, konsekvens og sandsynlighed
 - Iboende risiko og residualrisiko
 - Risikostyringsproces
 - Break-out øvelse
- Frokost
- Informationssikkerhedsrisici
 - Risiko og trusler
 - Informationssikkerhedsstandarder
 - Break-out

Præsentation af underviser

KONSULENT - DELOITTE



Emilie Enné Lykkegaard

Konsulent | T&T Cyber strategy and Transformation

E-mail : elykkegaard@deloitte.dk
Mobil : +45 30 93 63 84

*Uddannet cand. Arch.
Tidligere kursist fra Fast track.
Arbejder primært med cyber strategier
og modenheds analyser.*

MANAGER - DELOITTE



Morten Staib

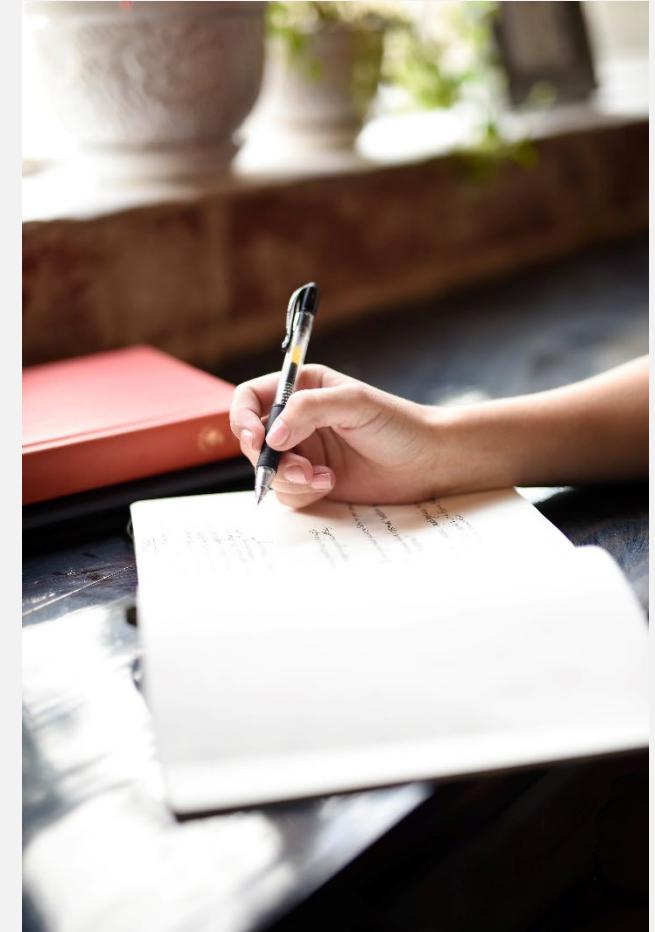
Manager | T&T Cyber strategy and Transformation

E-mail : mstaib@deloitte.dk
Mobil : +45 41 60 22 09

Projektleder og specialist på forskellige projekter i det offentlige og private indenfor cyber -og informationssikkerhedsområdet.

Præsentation af jer

- Navn samt din baggrund? (seneste uddannelse eller job)
- Hvad har motiveret dig til at tage dette kursus?
- Hvad ønsker du at opnå gennem kurset? (dine læringsmål).



Hvad vil I lære de næste 2 dage?

Basal risikotankegang

Informationssikkerhedsstandarder og rammeværk

Sikkerhed vs. compliance

Hvordan styres informationssikkerhedsrisici

Roller og ansvar vedrørende risikostyring

Forberedelse til casearbejde



Basal risikoteori



**En risiko er et udtryk for usikkerhed omkring en
forventet hændelse og dens mulige
konsekvenser.**

Hvad er en risiko?

Diskuter med sidemanden, hvilke risici I bevidst eller ubevidst har identificeret, vurderet og håndteret siden i morges.





**En konsekvens er det resultat eller den effekt,
der opstår som følge af en handling, beslutning
eller begivenhed.**

Hvad er en konsekvens?

Diskuter med sidemanden hvilke og hvor store konsekvenser, der er forbundet med de risici I lige har diskuteret.





Sandsynlighed er en kvantificering af, hvor ofte en begivenhed forventes at forekomme.

Hvad er en sandsynlighed?

Diskuter med sidemanden sandsynligheden for, at de risici, I diskutterede, realiseres, samt på hvilket grundlag I baserer jeres vurderede sandsynligheder.





**Pause
10 min**



En iboende risiko er en risiko, der findes, selvom du ikke gør noget specielt for at forårsage den.

Hvad er en iboende risiko?

Ofte den sværreste at forholde sig til, da man ubevidst kommer til at tænke kompenserende tiltag ind, når konsekvens og sandsynlighed vurderes for en iboende risiko.



Hvad er kompenserende tiltag?

Tiltag, der reducerer den iboende risikos sandsynlighed og konsekvens ved realisering.

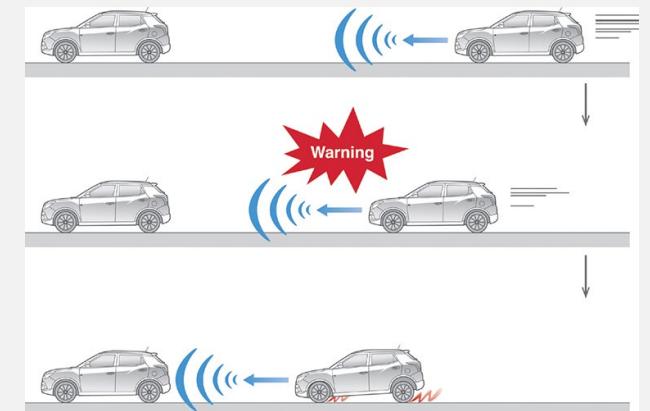
Reducering af konsekvens



Reducering af sandsynlighed



Reducering af både konsekvens
og sandsynlighed



Hvad er residual risiko

Diskuter med sidemanden hvilke kompenserende tiltag, der reducerer jeres identificerede risicis konsekvens, sandsynlighed eller begge.

Iboende risiko for trafikuheld

Høj			X
Mellem			
Lav			
K S	Lav	Mellem	Høj

Residual risiko for trafikuheld

Høj			
Mellem		X	
Lav			
K S	Lav	Mellem	Høj

Hvordan håndteres residualrisiko?

Baseret på residualrisikoen vurderes hvilke risikohåndteringsmuligheder, der bør anvendes.

Undgå risikoen



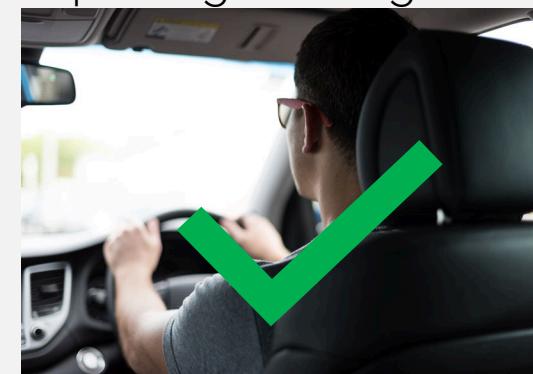
Overfør/del risikoen



Mitiger risikoen yderligere



Accepter og overvåg risikoen



Hvad er risikoappetit og -tolerance?

Risikoappetitten refererer til den mængde og type af risiko, som man er villig til at påtage sig. Risikotolerance er den mængde og type af risiko, som man er villig til at acceptere efter gennemførelsen af kompenserende foranstaltninger.

Iboende risiko for trafikuheld

Høj			X
Mellem			
Lav			
K S	Lav	Mellem	Høj

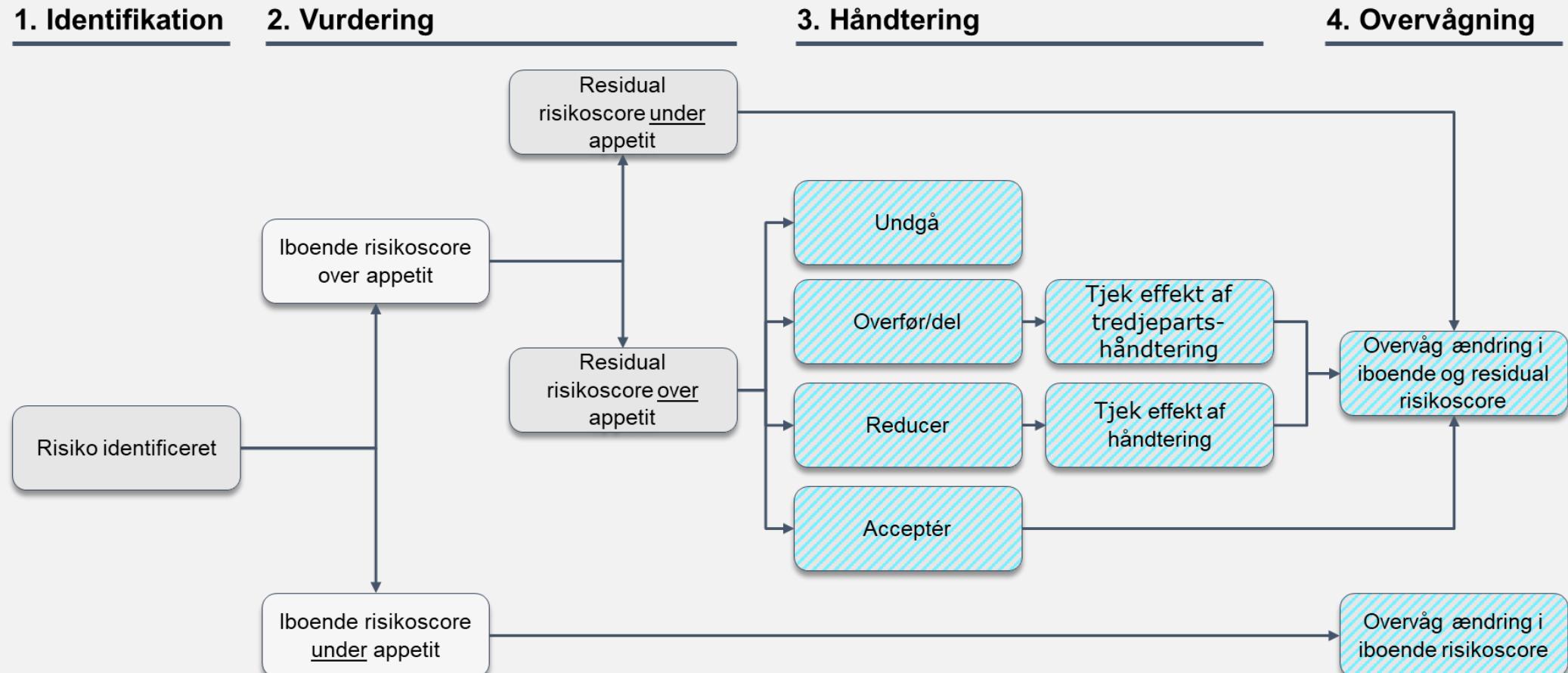
Residual risiko for trafikuheld

Høj			
Mellem	X		
Lav			
K S	Lav	Mellem	Høj

- Eksempel på håndteringsstrategi
- Undgå, reducer eller overfør
 - Reducer eller accepter og overvåg
 - Accepter og overvåg

Risikostyringsproces

Identificering og håndtering af risici kan illustreres via processen nedenfor.



Break-out - Risikoidentifikationsøvelse

Diskuter i grupper følgende trusselsscenerier, og identificer og analyser de potentielle risici, der er forbundet med jeres scenarier. Dette omfatter at vurdere konsekvenser og sandsynlighed for hvert identificeret risikoscenarie.

Scenarier:

- 1. Cyberangreb på en virksomheds it-infrastruktur:**

Eksempel på risikoscenarie: Et avanceret ransomware-angreb rammer virksomhedens netværk og stjæler potentielt følsomme kundedata.

- 2. Naturkatastrofe (f.eks. oversvømmelse eller jordskælv) på en virksomheds lokation:**

Eksempel på risikoscenarie: En pludselig naturkatastrofe rammer virksomhedens hovedkvarter og forårsager omfattende skader.

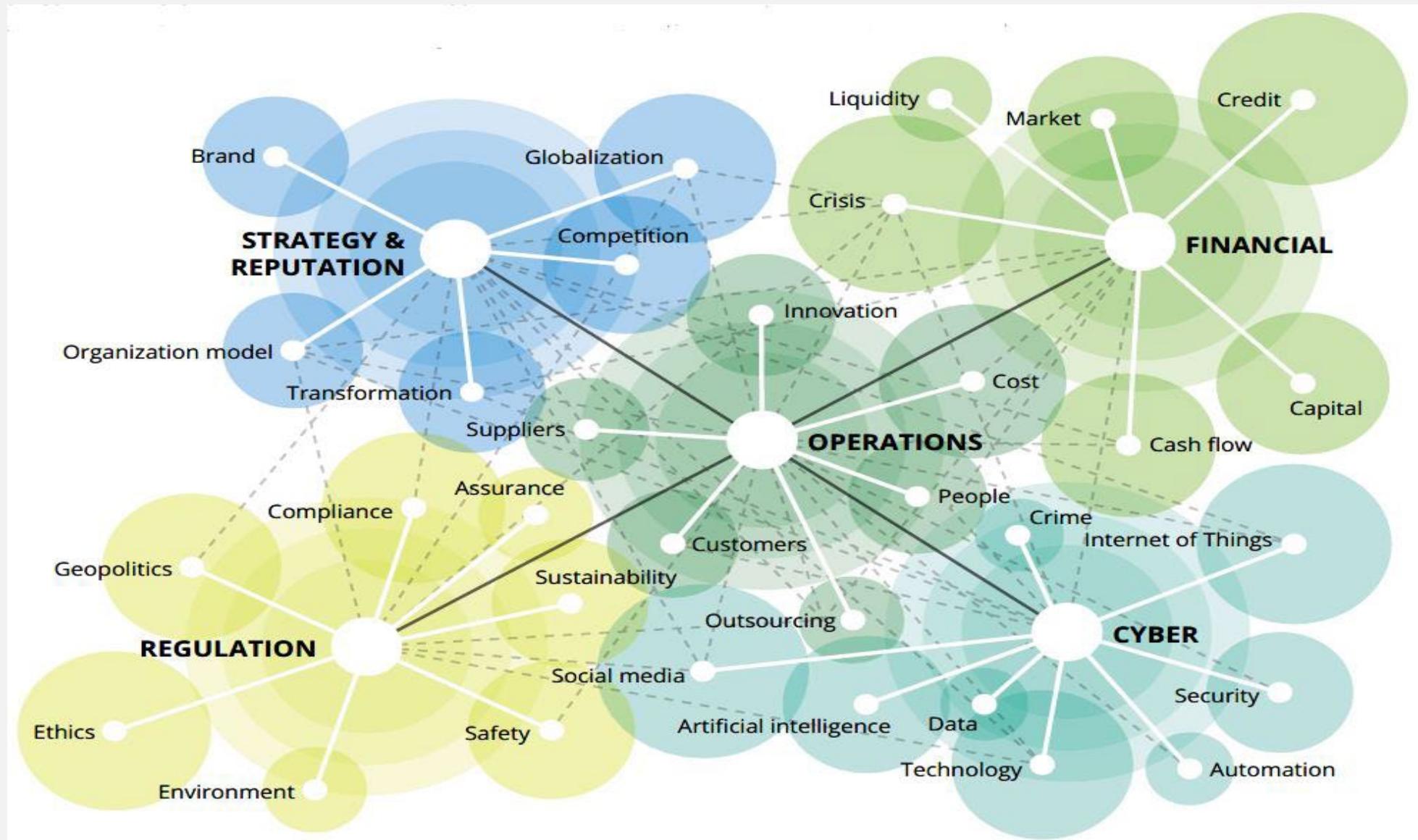
- 3. Menneskelig fejl (f.eks. uagtsomhed eller misbrug af adgangsrettigheder):**

Eksempel på risikoscenarie: En medarbejder løkker utilsigtet følsomme oplysninger eller misbruger adgangsrettigheder til systemer.



Informationssikkerheds- risici

Risici er alle steder!



Truslen er høj!

Diskuter med sidemanden, hvilke sager I kender til fra medierne vedrørende cyber- og informationssikkerhedsbrud.

Feb. 2024

FINANS LOG IN

26/02/2024 KL. 17:10

ERHVERV

Netcompany-værdi i milliardfald efter omfattende hackerangreb

Markedsværdien af Netcompany er højet ned med over 1 mia. kroner, siden det blev kendt, at landets største offentlige IT-leverandør er blevet hacket, det skriver Børsen.

[DEL ARTIKLEN](#) [GEM PÅ LÆSELISTE](#)



netcompany

Jul. 2024

En opdatering af store virksomheders antivirusprogram har fredag skabt et massivt IT-nedbrud, som har lammet kritisk infrastruktur verden over.

Aflyste flyafgange og lukkede lægejournaler: Her er et overblik over dagens enorme IT-kaos



Passagerer venter i kai i Gatwick lufthavn i London, efter at flyene er aflyst eller forsinkede. Foto: Benjamin Cremel/Ritzau Scanpix

MADS SPANGGAARD Journalist

LYT TIL ARTIKLEN [GEM ARTIKLEN](#)

TECH 18. JULI 2024, 17:35

Det var en fejlslag opdatering af antivirusprogrammet CrowdStrike, der fredag forudsagede et stort, globalt IT-nedbrud. Leger har ikke kunnet tilgå patientjournaler, flyafgange er blevet aflyst i massevis, og supermarkeder og andre virksomheder har lidt under nedbruddet. Selskabet bag CrowdStrike har fundet frem til fejlen, men det er stadig uvist, hvornår systemerne er oppe at køre igen. Her får du et overblik over, hvor nedbruddet slakte størst problemer.

Beredskabet og sundhedsvæsenet

CROWDSTRIKE

Okt. 2024

VIRKSOMHEDER

Europas største atomaffaldsanlæg får millionbøde for hullet IT-sikkerhed

Sellafield-anlægget opdaterede ikke sine IT-systemer og stod derfor som åbent mål for hækkere. Flere lande sendte hemmelige advarsler til den britiske regering.



Atomaffaldsanlægget Sellafield ligger på grænsen til Skotland og er Europas største. Men IT-sikkerheden har været så hullet, at den blev kaldt «oldemor» med henvisning til den onde trollmandsunk (Harry Potter) i legenden. Foto: Oliwier Zielinski/PA Wire/Scanpix

ANNONCE



nemlig

Trustpilot 4.4 31.589 anmeldelser

THOMAS BRENNSTRUP Journalist

Fredag d. 04. oktober 2024, kl. 14:20
Der denne artikel

 Sellafield Ltd



Hvordan håndtere man informationssikkerheds risici?

Informationssikkerhed i staten



Trusselsvurdering

- » Truslen for cyberspionage er meget høj
- » Truslen for cyberkriminalitet er meget høj
- » Truslen for cyberaktivisme er høj



Øget digitalisering i samfundet

- » Digitalisering i alle organisationslag og forretningsområder
- » Brug af ny teknologi til at fremme vækst og velstand
- » Øget digitalisering til serviceforbedringer og effektiviseringer i den offentlige sektor



Faste krav til statslige myndigheder

- » ISO 27001
- » Tekniske minimumskrav
- » Statens It-råds reviews af store it-projekter
- » Sikkerhedscirkulæret og klassificeret information



Statslige strategier med elementer af sikkerhed

- » Den fællesoffentlige digitaliseringsstrategi
- » National strategi for cyber- og informationssikkerhed
- » National strategi for kunstig intelligens
- » Strategi for it-styring i staten

Tekniske minimumskrav til statslige myndigheder

Kravene er udvalgt under hensyntagen til effekt og implementeringsomkostninger og følger af eksisterende vejledninger hvor af nogle er udtryk for udbredt best-practice.

Klienter/PC'er



Der skal implementeres firewall på alle klienter

Mail



DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden

Mobiltelefoner



Anvend numerisk adgangskode på minimum 6 cifre eller biometrisk identifikation

Netværk



Krav om logging, log på alle systemer og tjenester på netværksservere

Websider



Der skal benyttes regelmæssigt opdateret serversoftware på webservere



**Pause
10 min**

Informationssikkerhedsstandarder

Der findes flere internationale anerkendte standarder til styring af informationssikkerhed. De mest kendte er ISO/IEC 27001 - 27002, NIST Cybersecurity Framework, CIS Controls mfl.



ISO/IEC 27001 & ISO/IEC 27002

Hvad er ISO/IEC 27001?

ISO 27001 er en international ledelsesstandard for informationssikkerhed. Standarden er et styringsværktøj, der hjælper virksomheder til at beskytte værdifulde informationer - herunder persondata - på en sikker og troværdig måde. ISO 27001 opstiller blandt andet krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed.

Hvad er et ISMS?

Et ISMS (Information Security Management System) er et ledelsessystem til styring af informationssikkerhed. Kravene til ledelsessystemet er beskrevet i ISO 27001.

Et ISMS er et samlet udtryk for de politikker, procedurer, processer, organisatoriske beslutningsgange og aktiviteter, som udgør komponenterne i organisationens styring af informationssikkerhed.

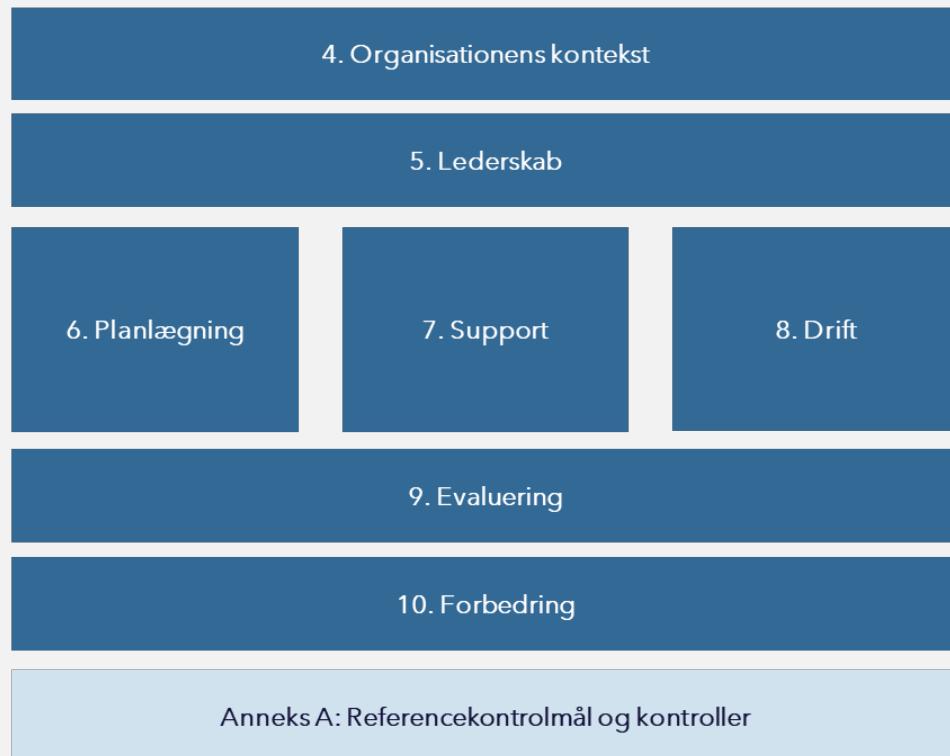
Hvad er ISO/IEC 27002?

Det er en vejledende standard, der kan hjælpe organisationer med at udvikle deres eget informationssikkerhedssystem.

Formålet med ISO/IEC 27002 er at give vejledning og anbefalinger til implementering af sikkerhedsforanstaltninger og -kontroller for at beskytte organisationers information og datasystemer.

ISO/IEC 27001 og ISO/IEC 27002

ISO 27001: Ledelsessystem for informationssikkerhed

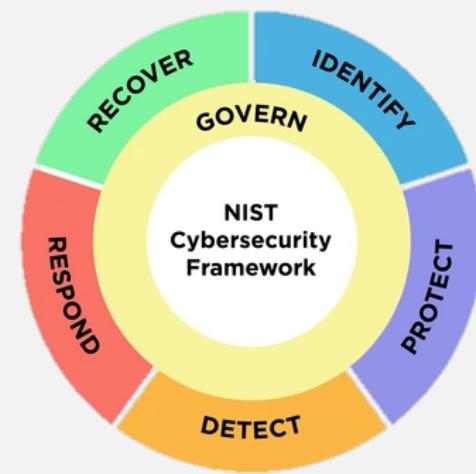
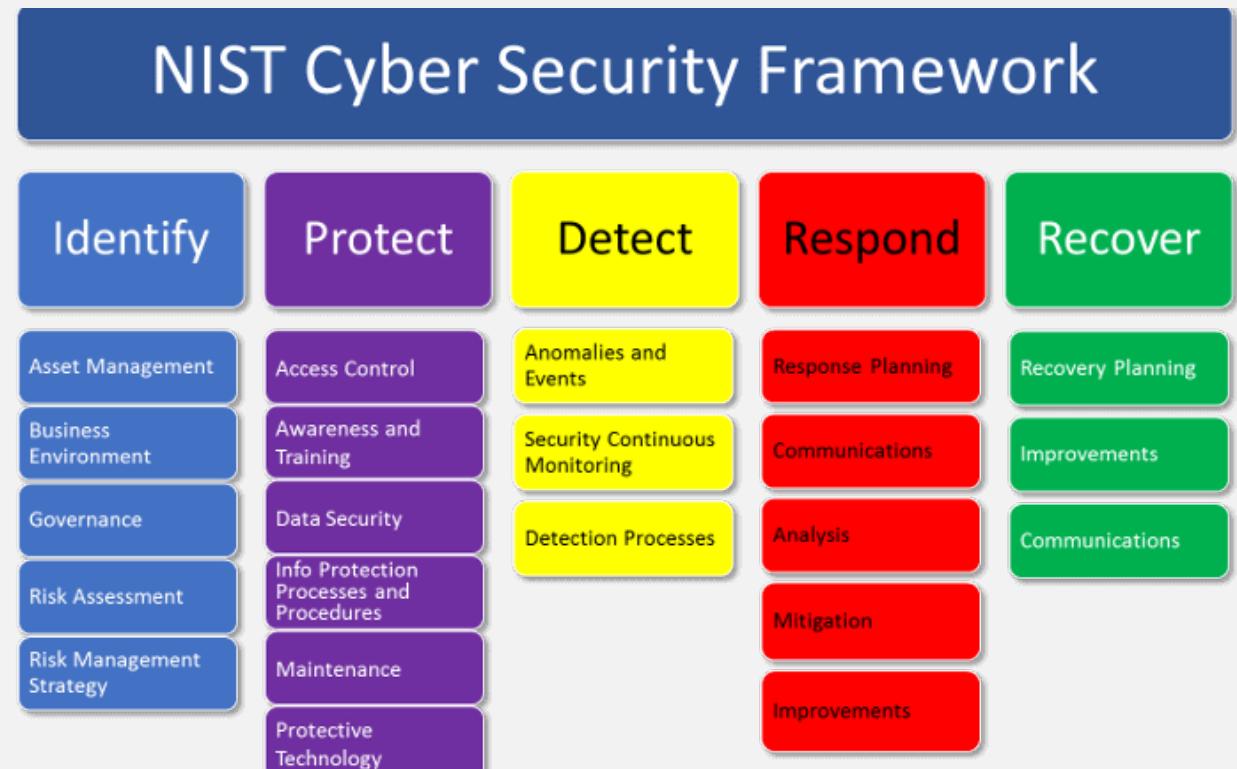


ISO 27002: Foranstaltninger til informationssikkerhed



NIST 2.0

National Institute of Standards and Technology (NIST)-rammeverket er en retningslinje udviklet af det amerikanske National Institute of Standards and Technology for at hjælpe organisationer med at forbedre deres cybersikkerhedspraksis og håndtere risici relateret til informationssikkerhed.



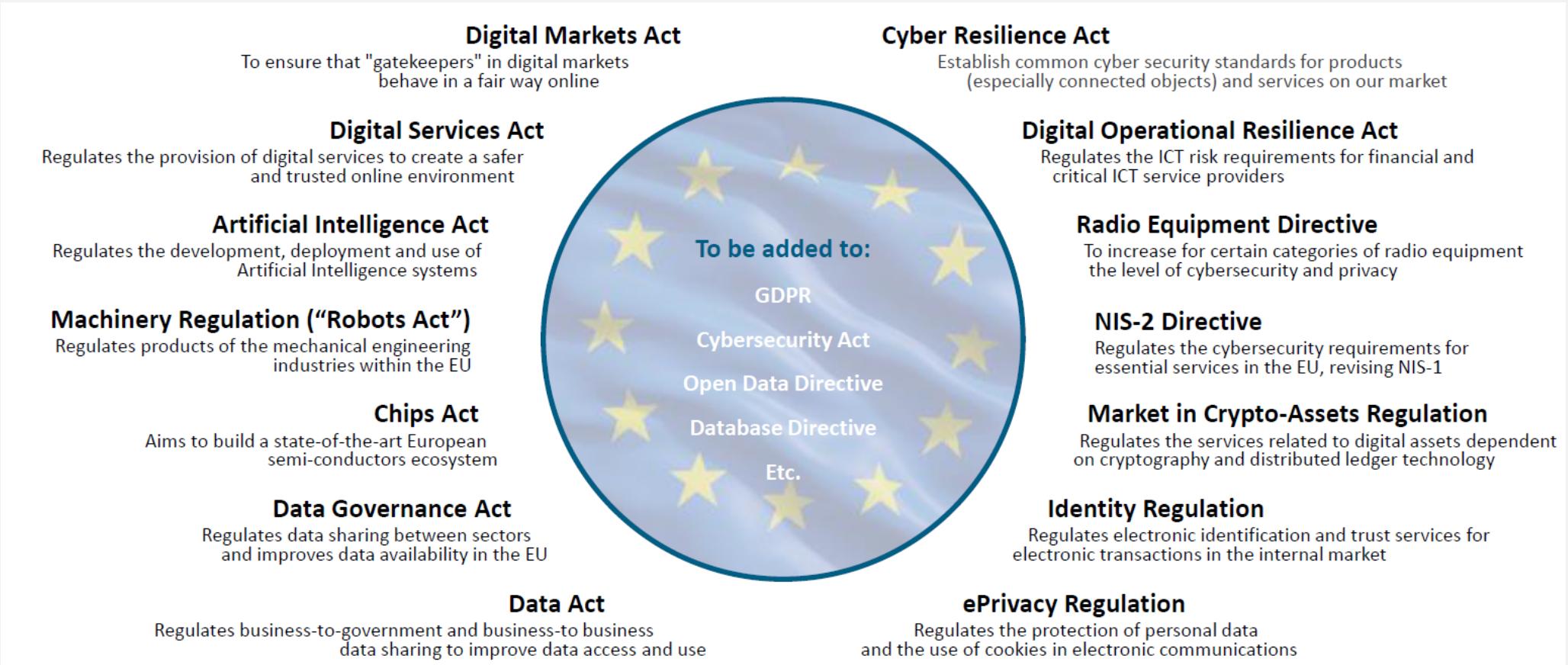
CIS18 Controls

CIS (Center for Internet Security)
Controls er en omfattende liste over sikkerhedsforanstaltninger og -kontroller udviklet af Center for Internet Security. Disse kontroller er designet til at hjælpe organisationer med at beskytte deres informationssystemer mod cybertrusler og angreb ved at implementere bedste praksis inden for cybersikkerhed.

Below is a list of the CIS Controls in v8, and how many Safeguards in each are applicable to each Implementation Group.

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards (IG1 2/5) (IG2 4/5) (IG3 5/5)	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards (IG1 3/7) (IG2 6/7) (IG3 7/7)	CONTROL 03 Data Protection 14 Safeguards (IG1 6/14) (IG2 12/14) (IG3 14/14)
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards (IG1 7/12) (IG2 11/12) (IG3 12/12)	CONTROL 05 Account Management 6 Safeguards (IG1 4/6) (IG2 6/6) (IG3 6/6)	CONTROL 06 Access Control Management 8 Safeguards (IG1 5/8) (IG2 7/8) (IG3 8/8)
CONTROL 07 Continuous Vulnerability Management 7 Safeguards (IG1 4/7) (IG2 7/7) (IG3 7/7)	CONTROL 08 Audit Log Management 12 Safeguards (IG1 3/12) (IG2 11/12) (IG3 12/12)	CONTROL 09 Email and Web Browser Protections 7 Safeguards (IG1 2/7) (IG2 6/7) (IG3 7/7)
CONTROL 10 Malware Defenses 7 Safeguards (IG1 3/7) (IG2 7/7) (IG3 7/7)	CONTROL 11 Data Recovery 5 Safeguards (IG1 4/5) (IG2 5/5) (IG3 5/5)	CONTROL 12 Network Infrastructure Management 8 Safeguards (IG1 1/8) (IG2 7/8) (IG3 8/8)
CONTROL 13 Network Monitoring and Defense 11 Safeguards (IG1 0/11) (IG2 6/11) (IG3 11/11)	CONTROL 14 Security Awareness and Skills Training 9 Safeguards (IG1 8/9) (IG2 9/9) (IG3 9/9)	CONTROL 15 Service Provider Management 7 Safeguards (IG1 1/7) (IG2 4/7) (IG3 7/7)
CONTROL 16 Applications Software Security 14 Safeguards (IG1 0/14) (IG2 11/14) (IG3 14/14)	CONTROL 17 Incident Response Management 9 Safeguards (IG1 3/9) (IG2 8/9) (IG3 9/9)	CONTROL 18 Penetration Testing 5 Safeguards (IG1 0/5) (IG2 3/5) (IG3 5/5)

Et Europa klar til den digitale tidsalder: EU's digitale strategi



GDPR

GDPR står for General Data Protection Regulation og er en EU-forordning, der regulerer beskyttelsen af persondata og privatlivets fred for enkeltpersoner inden for EU og Det Europæiske Økonomiske Samarbejdsområde (EØS).

GDPR indeholder syv grundlæggende principper for behandling af persondata.



NIS2 og national strategi for cyber- og informationssikkerhed

NIS2 står for Network and Information Security Directive og er et EU-direktiv, der sigter mod at styrke cybersikkerheden og beskytte kritisk infrastruktur og digitale tjenester i EU.

Derudover har vi en national strategi for cyber- og informationssikkerhed, som sigter efter at løfte den digitale sikkerhed på tværs af samfundet.

Kan I nævne nogle virksomheder omfattet af NIS2?

Sectors in scope of NIS2 directive*

*Source: [Publications Office \(europa.eu\)](https://publications.europa.eu)

HIGHLY CRITICAL

OTHER CRITICAL

 Energy	 Health	 ICT service management (business-to-business)
 Transport	 Drinking water	 Public administration
 Banking	 Wastewater	 Space
 Financial market infrastructures	 Digital infrastructure	
 Postal and courier services	 Manufacture, production and distribution of chemicals	 Manufacturing
 Waste management	 Production, processing and distribution of food	 Research
		 Digital providers

Nye EU-regler for kunstig intelligens

Den nye reguleringsordning går videre end blot AI-loven

De nye forordninger

AI-forordningen

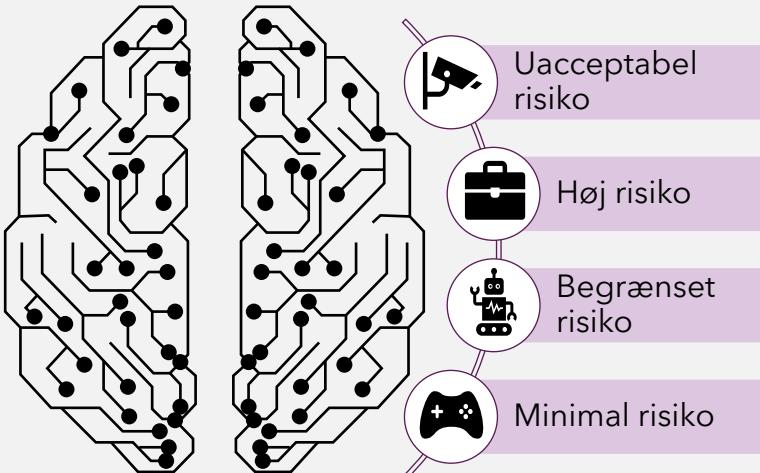
- Retsakten om kunstig intelligens vil sikre, at europæerne kan have tillid til kunstig intelligens. Forholdsmaessige og fleksible regler vil imødegå de **specifikke risici, som AI-systemer udgør**, og fastsætte den højeste standard på verdensplan.
- AI Act klassificerer risiko i fire niveauer: uacceptabel risiko, høj risiko, begrænset risiko og minimal risiko.

Direktiv om ansvar for kunstig intelligens

- Formålet med direktivet om AI-ansvar er at fastsætte ensartede regler for **adgang til oplysninger** og **lettelse af bevisbyrden** i forbindelse med skader forårsaget af AI-systemer.

Baggrund

Retsakten om kunstig intelligens og direktivet om ansvar for kunstig intelligens er en del af den **europæiske strategi for kunstig intelligens**, som har til formål at gøre EU til et knudepunkt for kunstig intelligens i verdensklasse og sikre, at kunstig intelligens er menneskecenteret og pålidelig. **AI-ansvarspakken** supplerer AI-forordningen ved at lette culpabaserede erstatningskrav og fastsætte en ny standard for tillid til erstatning.



AI Act risikobaseret tilgang

Biometrisk fjernidentifikation i
realtid

CV-sorteringsssoftware til
rekruttering

Chatbots

Videospil

Næste skridt

Efter ikrafttrædelsen foreslår loven om kunstig intelligens en periode på **24 måneder**, før loven finder anvendelse.

Det foreslås, at Kommissionen fem år efter ikrafttrædelsen af **direktivet om AI-ansvar** vurderer behovet for regler om objektivt ansvar for AI-relatedede krav.

Break-out - Sikkerhed vs. Compliance

I grupper, hvor nogle fokuserer på sikkerhed, mens andre har fokus på compliance, skal vi diskutere følgende scenarie og identificere de specifikke sikkerhedsforanstaltninger, der skal implementeres for at adressere henholdsvis sikkerhed og compliance.

Scenarie: Beskyttelse af følsomme kundedata og overholdelse af GDPR:

En virksomhed behandler persondata fra EU-borgere uden at have implementeret tilstrækkelige sikkerhedsforanstaltninger, f.eks. manglende kryptering af data og utilstrækkelig adgangskontrol.

- 1) Hvilke risici opstår for henholdsvis sikkerhed og compliance i dette scenarie?
- 2) Beskriv de identificerede sikkerhedsforanstaltninger, der er nødvendige for at imødekomme compliance og/eller øge sikkerhed.
- 3) Diskuter jeres risici og valgte sikkerhedsforanstaltninger med en anden gruppe som har et andet fokus end jer.

Break-out - Sikkerhed vs. Compliance





Tak for i dag



MODUL 3 AF 7

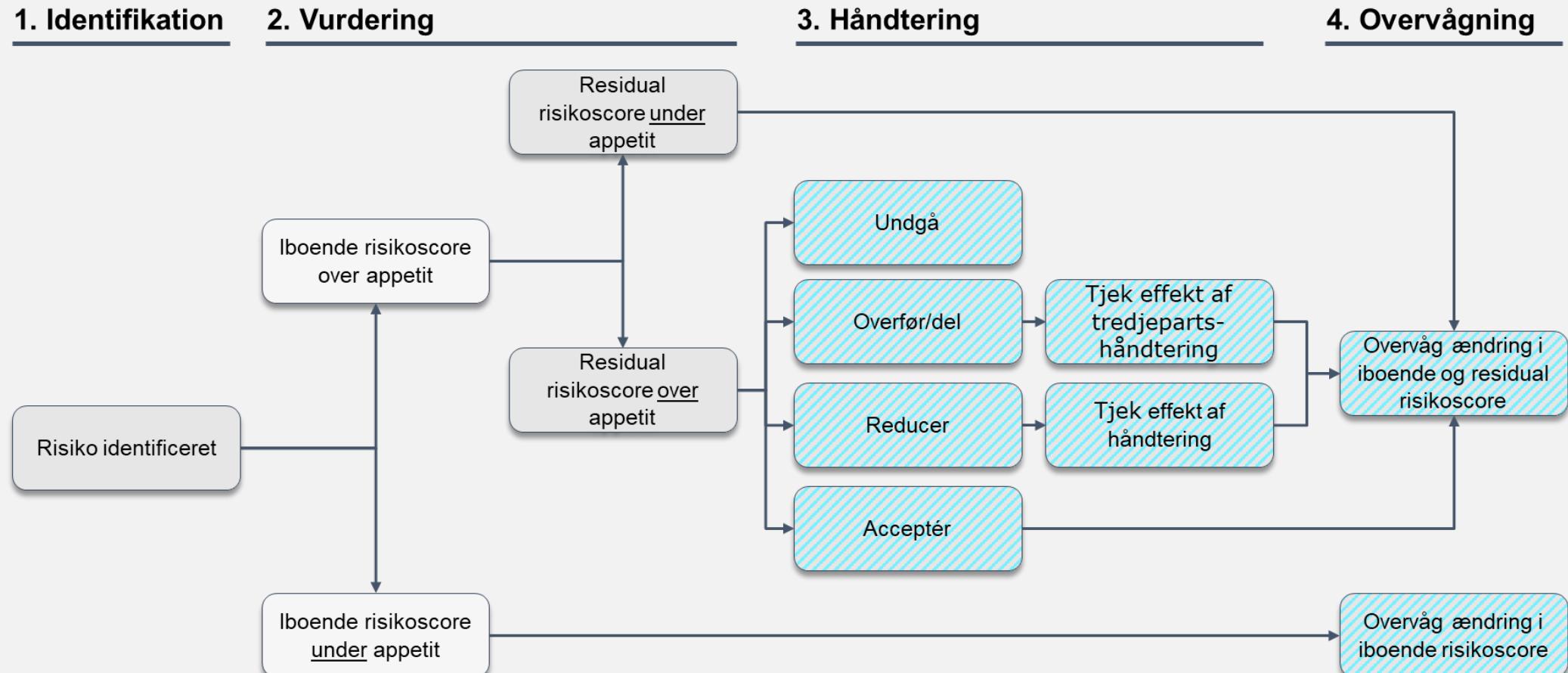
Risikostyring

Dagens program

- Recap og refleksion
- Styring af informationssikkerhedsrisici
- Break out - It-risikovurdering af virksomhed
- **Frokost**
- Opsamling på break out
- Governance og Risk Management
- Præsentation af Case-opgave

Recap og præsentation af dagens emne

Identificering og håndtering af risici kan illustreres via processen nedenfor.





Styring af informations- sikkerhedsrisici

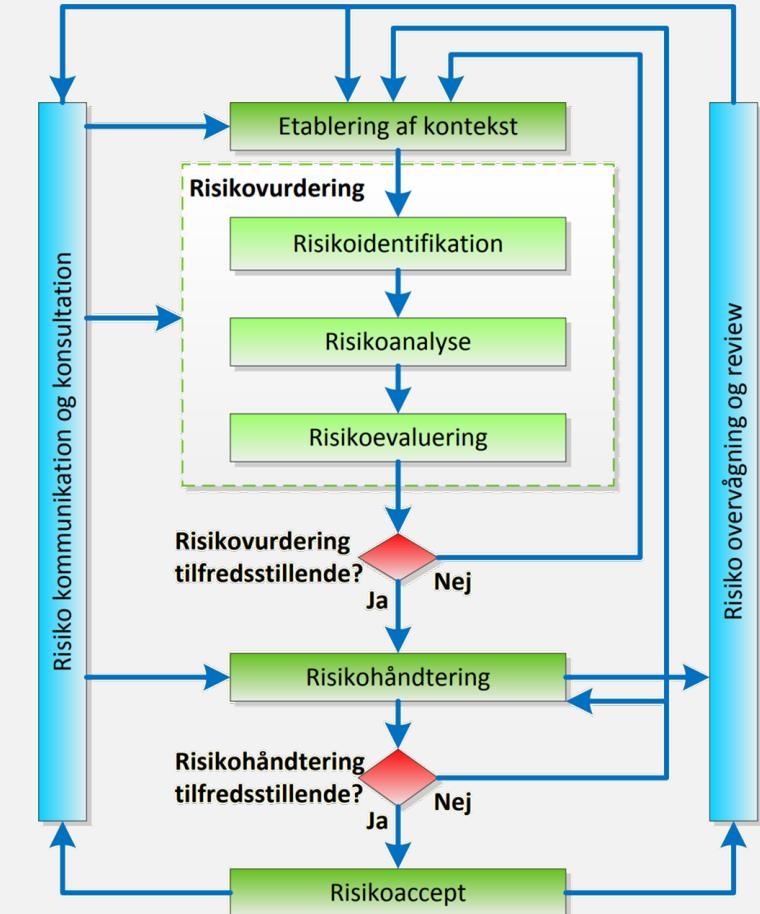
ISO/IEC 27005 - risikobaseret tilgang

ISO27005 - Information security risk management
Spiller sammen med den meget udbredte ISO27001

Risikostyring består af fire grundelementer

1. Etablering af kontekst
2. Risikovurdering
3. Risikohåndtering
4. Risikoaccept

Hvilke elementer, mener I, er vigtigst at prioritere?



Styring af informationssikkerhedsrisici



1. Identificering

Identificering af risici, som kan have en effekt på organisationens efterlevelse af strategi og opnåelse af mål

2. Analysering

Vurdering af den potentielle effekt (sandsynlighed og konsekvens) af de identificerede risici

3. Håndtering

Vurdering af risici og identificering samt valg af håndteringstiltag

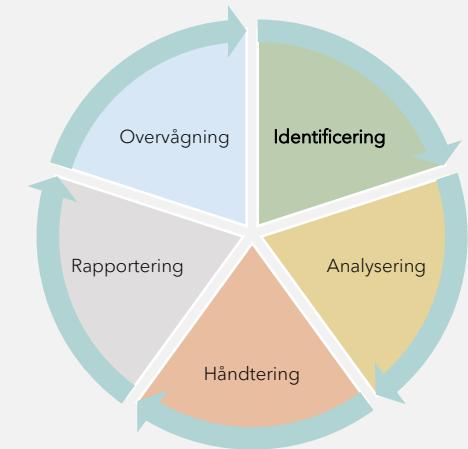
4. Rapportering

Rapportering til ledelsen om status og fremdrift på risici og håndteringstiltag

5. Overvågning

Opfølgning og overvågning af risici og håndteringstiltag

Styring af informationssikkerhedsrisici



Step 1) - Identificering af primære og understøttende aktiver:

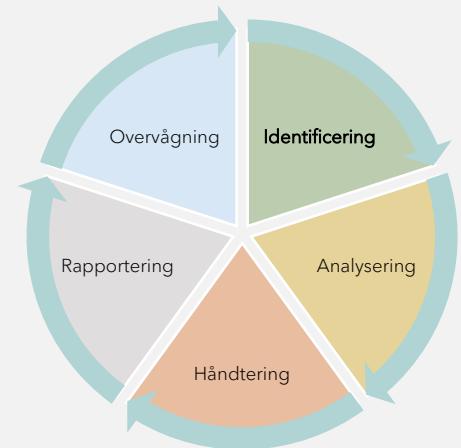
Primære aktiver er forretningsprocesser, aktiviteter og information, der støtter organisationens kerneydelser/hovedprocesser.

Understøttende aktiver er, i modsætning til primære aktiver, aktiver som kan skiftes ud. De understøttende aktiver kan være it-systemer, netværk, personel, udstyr mfl., som understøtter det primære aktiv.

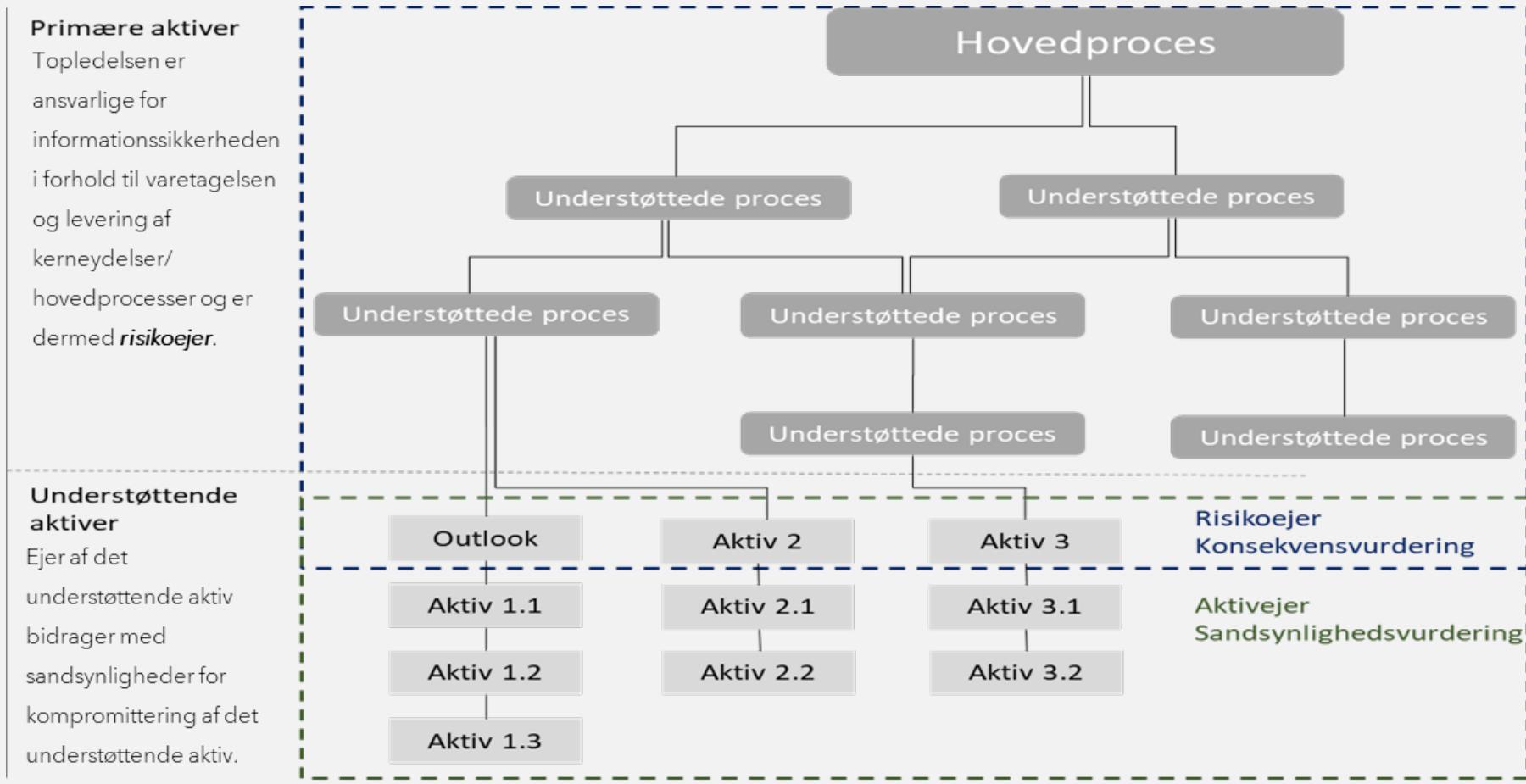
Ideelt bør alle aktiver identificeres og analyseres. Ressourcer og kompleksitet kan dog gøre denne øvelse særdeles vanskelig. For at arbejde risikobaseret bør en organisation som minimum identificere og kende til deres "*kronjuveler*", som er de aktiver, der er mest kritiske for organisationen.

Øvelse: Identificer jeres tidligere arbejdsgivers "*kronjuveler*", og diskuter hvilke aktiver, der understøtter disse. Evt. tænk på en kendt virksomhed.

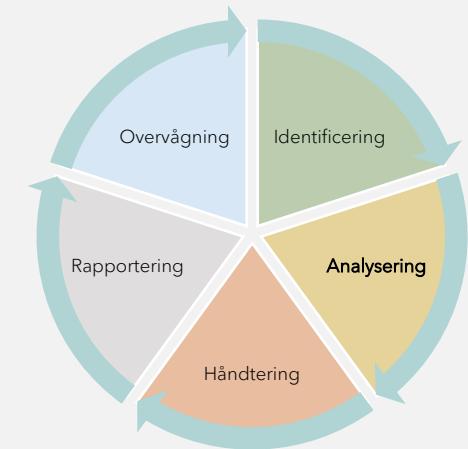
Styring af informationssikkerhedsrisici



Step 1) - Identificering af primære- og understøttende aktiver:



Styring af informationssikkerhedsrisici



Step 2) - Konsekvensanalyse for primære aktiver

Tekniske implikationer:

Beskyttelse af FIT:

- *Fortrolighed* - sikrer, at data kun er tilgængelige for de autoriserede personer eller systemer.
- *Integritet* - sikrer, at data forbliver uændrede og pålidelige gennem hele deres livscyklus.
- *Tilgængelighed* - sikrer, at data og systemer er tilgængelige for autoriserede brugere, når de har brug for det.
- *Uafviselighed* - sikrer, at en part ikke kan benægte at have udført en handling. Bruges typisk i forbindelse med digitale signaturen og transaktioner for at sikre, at en part ikke senere kan benægte at have foretaget en handling eller accepteret en aftale.
- *Autenticitet* - sikrer, at data, brugere eller systemer er dem, de hævder at være.

Forretningsmæssige implikationer:

Kan variere, men vil oftest omfatte finansiel skade, skade på omdømme, juridiske konsekvenser mfl.

Styring af informationssikkerhedsrisici



Step 2) - Analysere forretningskritikalitet:

Forretningskonsekvensanalysen, også kaldet Business Impact Assessment (BIA), analyserer de forretningsmæssige konsekvenser et informationssikkerhedsbrud på fortrolighed, integritet og tilgængelighed vil have for det primære aktiv (forretningsprocessen).

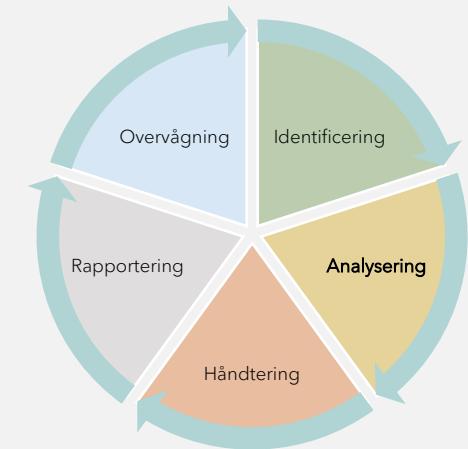
De understøttende aktiver analyseres yderligere for at finde frem til deres risikoværdi. Dette step indeholder følgende:

- Identificering af relevante trusler
- Identificering af relaterede sårbarheder
- Identificering af relevante implementerede kontroller

Ud fra ovenstående vurderes sandsynligheden og konsekvensen for, at en given trussel udnytter en sårbarhed til at forsage et informationssikkerhedsbrud på fortrolighed, integritet eller tilgængelighed.

Kombinationen af sandsynligheden og konsekvenser afspejler risikoværdien for residual risikoen.

Styring af informationssikkerhedsrisici

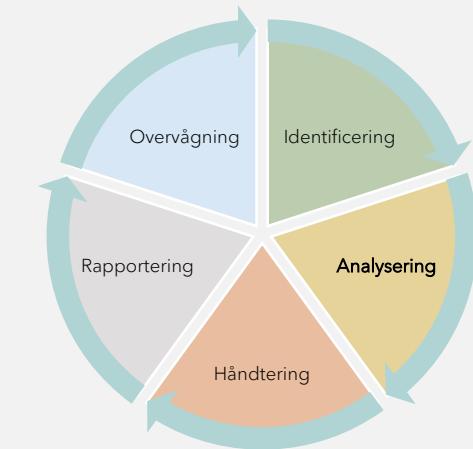


Step 2) - Trusselsvurdering

Eksempler på trusler:

1.	Fysisk skade	4.	Ubevidste menneskelige fejl
1.1	Brand	4.1	Utilsigtet brug af hardware/software
1.2	Vandskade	4.2	Utilsigtet offentliggørelse af data
1.3	Tyveri af it-udstyr	4.3	Utilsigtet sletning/ændring af data
1.4	Hærværk/vandalisme	4.4	Utilstrækkelig sikkerhed hos underleverandører
1.5	Terrorangreb		
1.6	Tab af dataforbindelse som følge af overgravet kabel		
1.7	Anden fysisk skade på it-udstyr		
2.	Naturkatastrofer	5.	Ondsindet menneskelig skade
2.1	Oversvømmelse i datacenter	5.1	Intern - Misbrug af egne rettigheder
2.2	Strømafbrydelse	5.2	Intern - Misbrug af andre/privilegerede rettigheder
2.3	Stormskade	5.3	Cyberangreb - Phishing/malware/ransomware
3.	Tekniske fejl	5.4	Cyberangreb - Spionage / Tyveri af fortrolig data
3.1	It-nedbrud pga. hardwarefejl	5.5	Cyberangreb - Destruktive angreb (DDoS, Terrorismus)
3.2	It-nedbrud pga. softwarefejl		
3.3	Software er fejlbehæftet		

Styring af informationssikkerhedsrisici



Step 2) - Sårbarheder

Eksempler på sårbarheder:

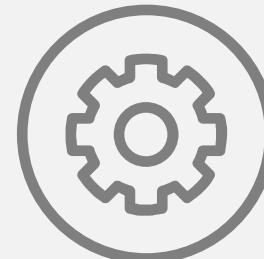
Mennesker (People):

- Utilstrækkelig sikkerhedsuddannelse og opmærksomhed.
- Manglende ansvar og bevidsthed om sikkerhed.
- Uopdaterede adgangsrettigheder.



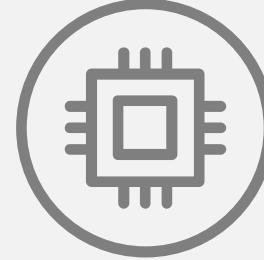
Processer (Process):

- Manglende sikkerhedsprocedurer og retningslinjer.
- Svagheder i datahåndtering.
- Manglende opdatering af software og systemer.



Teknologi (Technology):

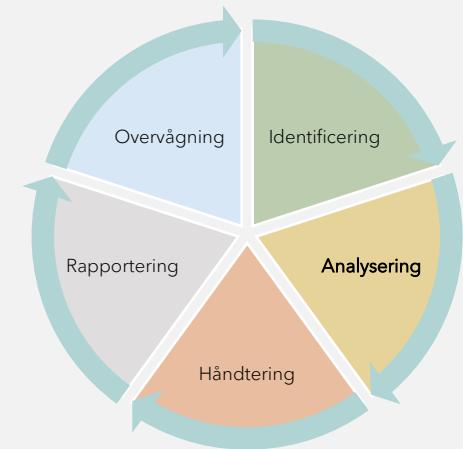
- Sårbarheder i software og applikationer.
- Manglende sikkerhedsopdateringer.
- Utilstrækkelig adgangskontrol.





**Pause
10 min**

Styring af informationssikkerhedsrisici



Step 2) - Implementerede kontroller

Eksempler på forebyggende kontroller:

Tekniske kontroller:

- Firewall
- Antivirussoftware
- Kryptering:

Administrative kontroller:

- Politikker og procedurer
- Træning og opmærksomhed
- Adgangskontrol baseret på brugerroller

Eksempler på udbedrende kontroller:

Tekniske kontroller:

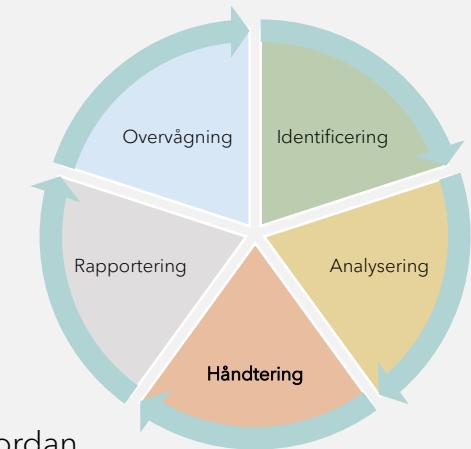
- Sikkerhedsopdateringer (Patching)
- Logning
- Backup

Administrative kontroller:

- Krisestyringsplan
- It-beredskabsplaner
- Disaster recovery-plan

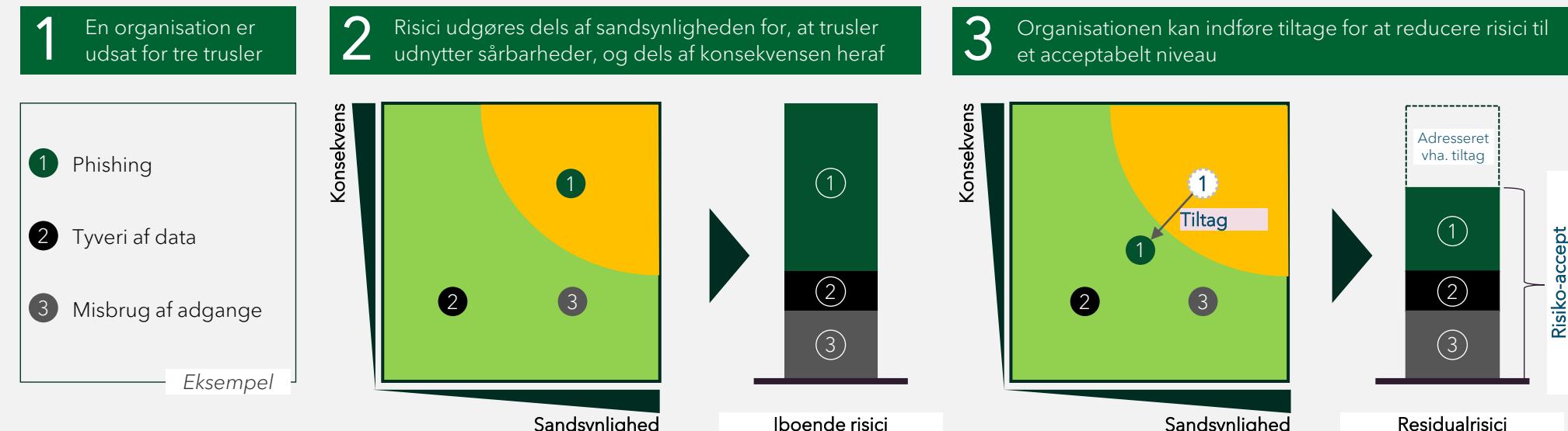


Styring af informationssikkerhedsrisici



Step. 3) – Vurdering og håndtering af risici

Efter analysen skal risici vurderes og håndteres. Det bør være en risikostyringsstrategi, der fastsætter rammerne for, hvordan identificerede risici skal håndteres. Ved mitigering (reducering) af risici implementeres nye eller eksisterende kontroller forbedres for at reducere sandsynligheden for, eller reducere konsekvensen af et informationssikkerhedsbrud. Processen fortsætter indtil residualrisikoen accepteres.



Styring af informationssikkerhedsrisici



Step. 3) – Risikohåndteringsplan

De identificerede risici og håndteringstiltag registreres og opdateres løbende.

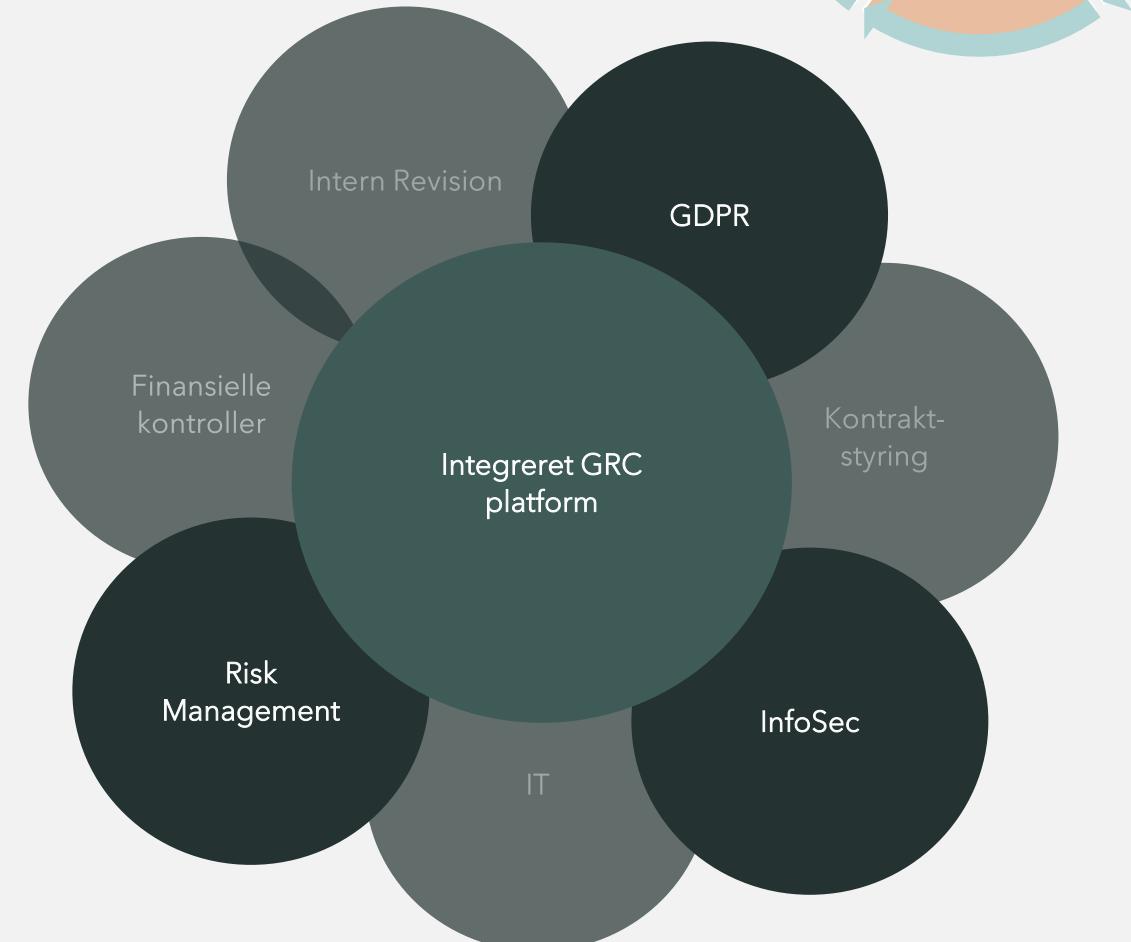
Stamoplysninger							Vurdering af iboende risiko					Vurdering af kontroller og håndteringstiltag					Vurdering af residual risiko					Planlagte kontroller og håndteringstiltag				
Risk ID	Stamoplysninger						Vurdering af iboende risiko						Vurdering af kontroller og håndteringstiltag			Vurdering af residual risiko										
	Risikonavn	Risikobeskrivelse	Risikotype	Årsag	Risikosjær	Iboende sandsynlighed	Iboende konsekvens	Primær konsekvensdimension	Iboende score	Mnav og beskrivelse	Design	Effektivitet	Score	Residual sandsynlighed	Residual konsekvens	Residual score	Mnav og beskrivelse2	Forrestet residual score	Deadline for implementering							
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										

Styring af informationssikkerhedsrisici

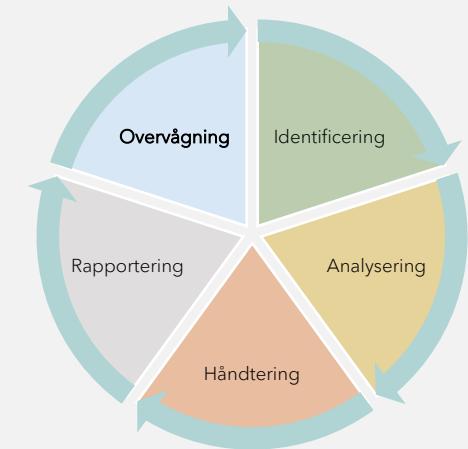
Step. 4) - Rapportering

Når risikoplanerne er udarbejdet, konsolideres samtlige risici og en rapport bestående af eks. risikohåndteringsplaner, analyser, risikoappetit mfl. udarbejdes og rapporteres til ledelsen.

Man kan med fordel integrere rapportering af risici i et samlet GRC (Governance, Risk & Compliance) -værktøj, som samler og håndterer alle typer af risici i en organisation.



Styring af informationssikkerhedsrisici



Step. 5) - Monitorering og overvågning

Risici og deres tilhørende faktorer, såsom relaterede trusler, sårbarheder, sandsynligheder, konsekvenser mfl., bør monitoreres og overvåges for at sikre et ajourført overblik over risikobilledet. Dette gøres ved eksempelvis følgende tiltag:

- Intern/ekstern auditering
- Review af formelle processkrivelser, procedurer, instrukser mfl.
- Risici- og hændelsesrapportering
- Ajourføring og tilpasning til trusselslandskabet
- Ajourføring og tilpasning af kontekst og omfang ved eksempelvis ændringer af eksternt/internt miljø, lovmæssige krav, organisation og struktur mfl.

Styring af informationssikkerhedsrisici



Step. 5) - Monitorering og overvågning

KPI'er (Key Performance Indicators) i informationssikkerhed kan omfatte målinger af effektiviteten af eksempelvis sikkerhedskontroller.

Eksempler på målbare KPI'er kan være:

- Procentdel af systemer med opdaterede sikkerhedsopdateringer
- Gennemførelsesgrad af sikkerhedstræning for medarbejdere
- Antal brud på datasikkerhedspolitikker

KRI'er (Key Risk Indicators) i informationssikkerhed er målinger, der identificerer og overvåger potentielle risici for informationsaktiver og systemer. Disse indikatorer kan omfatte ændringer i trusselslandskabet, antallet af vellykkede angreb eller forsøg, og sårbarheder i systemer, der ikke er blevet adresseret.

Eksempler på kvantitative KRI'er kan være:

- Antal malware-angreb mod virksomhedens systemer
- Hyppigheden af phishing-forsøg mod medarbejdere
- Antal dataovertrædelser eller lækager

Break-out - It-risikovurdering af din virksomhed

Vælg i grupper en reel eller fiktiv virksomhed og udfyld dernæst it-risikovurderingsværktøjet fra Virksomhedsguiden.dk [IT-risikovurderingsværktøj | Virksomhedsguiden.](#)

Analyser og diskuter det efterfølgende resultat i regnearket, herunder hvilke forbehold man bør forholde sig til vedrørende resultaterne, samt hvad de næste skridt er.



Governance og Risk Management

Risikostyring som en del af ISMS'et - SOA

Statement of applicability (SOA)

SOA-dokumentet er en vigtig del af ISO/IEC 27001-certificeringen, da det demonstrerer organisationens forståelse af dens informationssikkerhedsrisici, valg af passende sikkerhedskontroller og engagement i at implementere og opretholde et effektivt informationssikkerhedssystem.

SOA består af følgende:

- Omfang af ISMS:** SOA-dokumentet angiver omfanget af ISMS, herunder de aktiviteter, processer, afdelinger og information, der er omfattet af standarden.
- Identificerede risici:** Det inkluderer gennemgang af de identificerede informationssikkerhedsrisici baseret på risikovurderinger, og hvordan organisationen har til hensigt at håndtere disse risici.
- Valg af kontroller:** SOA-dokumentet angiver de specifikke sikkerhedskontroller (fra ISO/IEC 27002), som organisationen overordnet har valgt at implementere for at tackle de identificerede risici.
- Rationale for valg af kontroller:** Begrundelse for hvorfor bestemte kontroller er valgt, herunder deres relevans og effektivitet i forhold til organisationens behov og risikoprofil.
- Kontrolstatus:** SOA-dokumentet inkluderer ofte en status for implementeringen af de valgte kontroller, herunder om de er fuldt implementeret, delvist implementeret eller endnu ikke implementeret.
- Undtagelser og begrundelser:** Hvis der er kontroller, som organisationen har valgt ikke at implementere, skal SOA-dokumentet også inkludere begrundelserne for disse undtagelser.



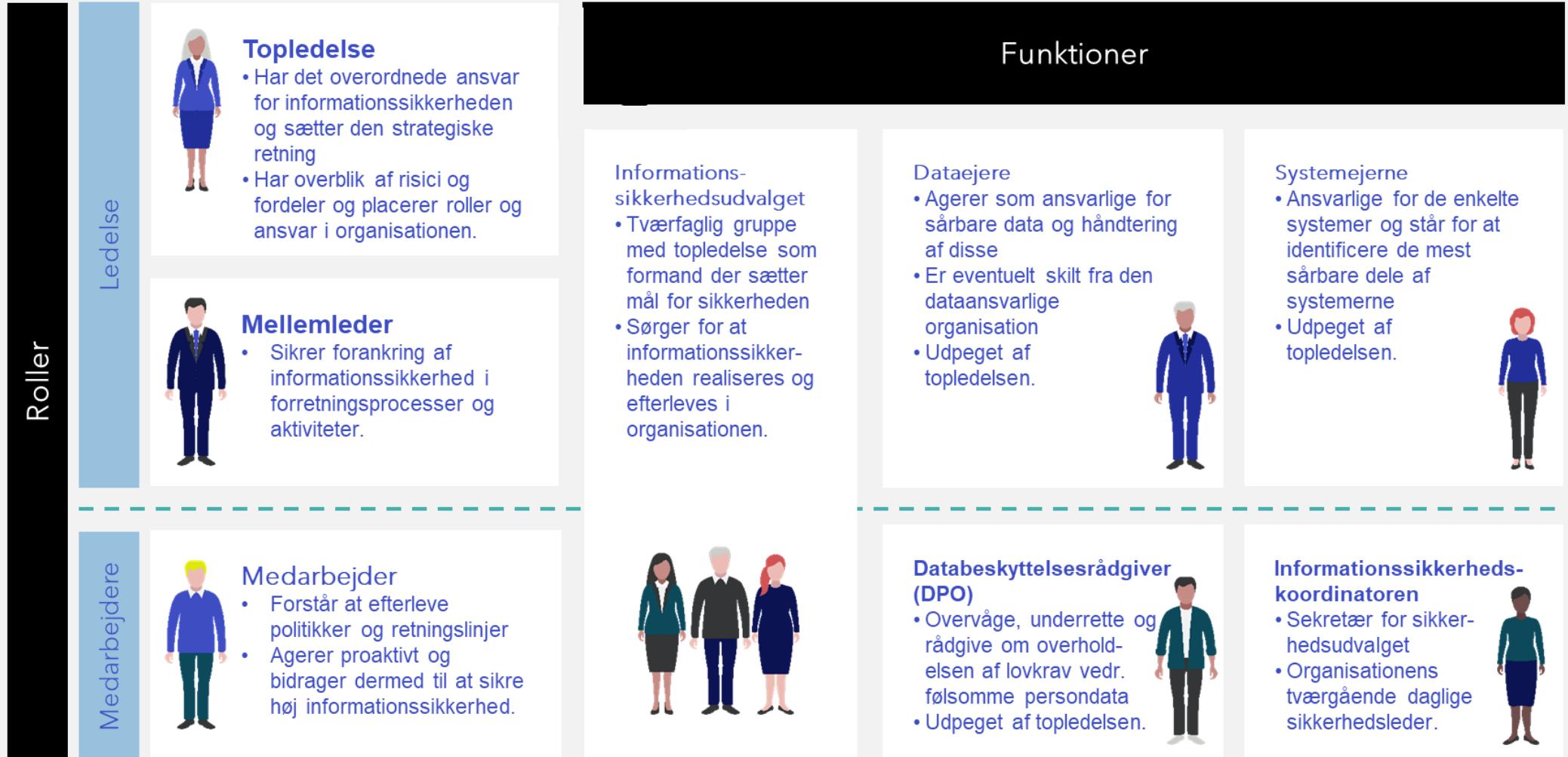
Risikostyringspolitik

Risikostyringspolitik for informationssikkerhedsrisici

Foruden typiske elementer som formål, mål og anvendelsesområde indeholder sådan en politik følgende:

- Roller og ansvarsområder
- Risikovurderingsproces
- Risikobehandlingsstrategi
- Kommunikation og rapportering
- Overvågning og revision
- Overholdelse af lovgivning og standarder

Roller og ansvar - informationssikkerhedsaktiviteter - eksempler



Roller og ansvar - informationssikkerhedsaktiviteter - eksempler

Typiske kerneopgaver

Typiske opgaver i relation til informations-sikkerhed

HR

Varetager:



- Specialistopgaver, trivselsproblemer
- Administrative opgaver såsom ansættelser, funktionsskifte, afskedigelser og vedligehold af stamdata
- Forretningsorienterede opgaver, fx ressourcebemanding, jf. strategi.

Økonomi

Varetager:



- Økonomiske forhold, herunder bogføring, udarbejdelse af interne og eksterne regnskaber, budgettering, ind- og udbetalinger, samt løn- og gageudbetalinger mv.

Jura/kontrakt

Varetager:



- Kunde- og leverandørkontakt, omsætningsfastholdelse og -udvikling samt kontraktstyring
- Rådgivning om indkøb i lyset af juridiske og kontraktuelle forhold.

It-ansvarlig/arkitekt

Varetager:



- Koblingen mellem forretning/forvaltning er it-understøttet, således der er den nødvendige sammenhæng mellem forretnings- og it-arkitektur
- Sikringen af principper for systemernes design og udvikling og for deres indbyrdes sammenhæng.

Støttefunktioner

- Forvaltning af sikkerhedsgodkendelser samt udarbejdelse og gennemførelse af awareness-program.
- Udarbejdelsen af brugerrettede sikkerhedspolitikker og HR-beredskabsplaner.
- Budgettering og opfølging af informations-sikkerhedsaktiviteter
- Økonomisk konkretisering af konsekvenser af risici
- Evt. hensættelser af midler.

- Fortolkning af love og direktiver for persondata og informationssikkerhed generelt
- Sikringen af kontrakter og juridisk bistand ved leverandørstyring.

- Etablering af sikkerhedsarkitektur og valg af sikkerhedsløsninger, herunder løsninger til monitorering, logning og rapportering
- Beredskabsplan for it-arkitekturen.

Roller og ansvar - informationssikkerhedsaktiviteter - eksempler

	Styring af informations-sikkerhed	Udvikling af politik for informations-sikkerhed	Risikovurdering og håndtering	Leverandør-styring	Hændelseshåndtering	Beredskabsplanlægning	Uddannelse og oplysning	Planer for sikkerhedsaktiviteter	SOA-dokumentet
Roller	Topledelsen	A	A	A	A	A	A	A	A
Funktioner	Mellemledere	A	A	A	A	A	A	A	A
Medarbejdere					I	I	I	I	
Informations-sikkerheds-udvalget	R	R	R	I	R	R	R	R	R
Informations-sikkerhedskoordinatoren	S	S	S	S	S	S	S	S	S
Systemejere			C	C	C	C	C	C	C
Dataejere			C	I	C	C	I	C	C
DPO		C	C	C	C	C	C	I	C
Jura/kontrakt		C	C	C	C	I	I	I	I
HR		C	C		C	I	S	I	I
It-ansvarlige, it-arkitekter		C	C	R	C	I	C	I	C
Økonomi		C	C	I	C	I	I	I	I

RACI (RASCI)

R (Responsible): Er ansvarlig for, at opgaven udføres

A (Accountable): Kan træffe beslutninger og står til regnskab for opgaven

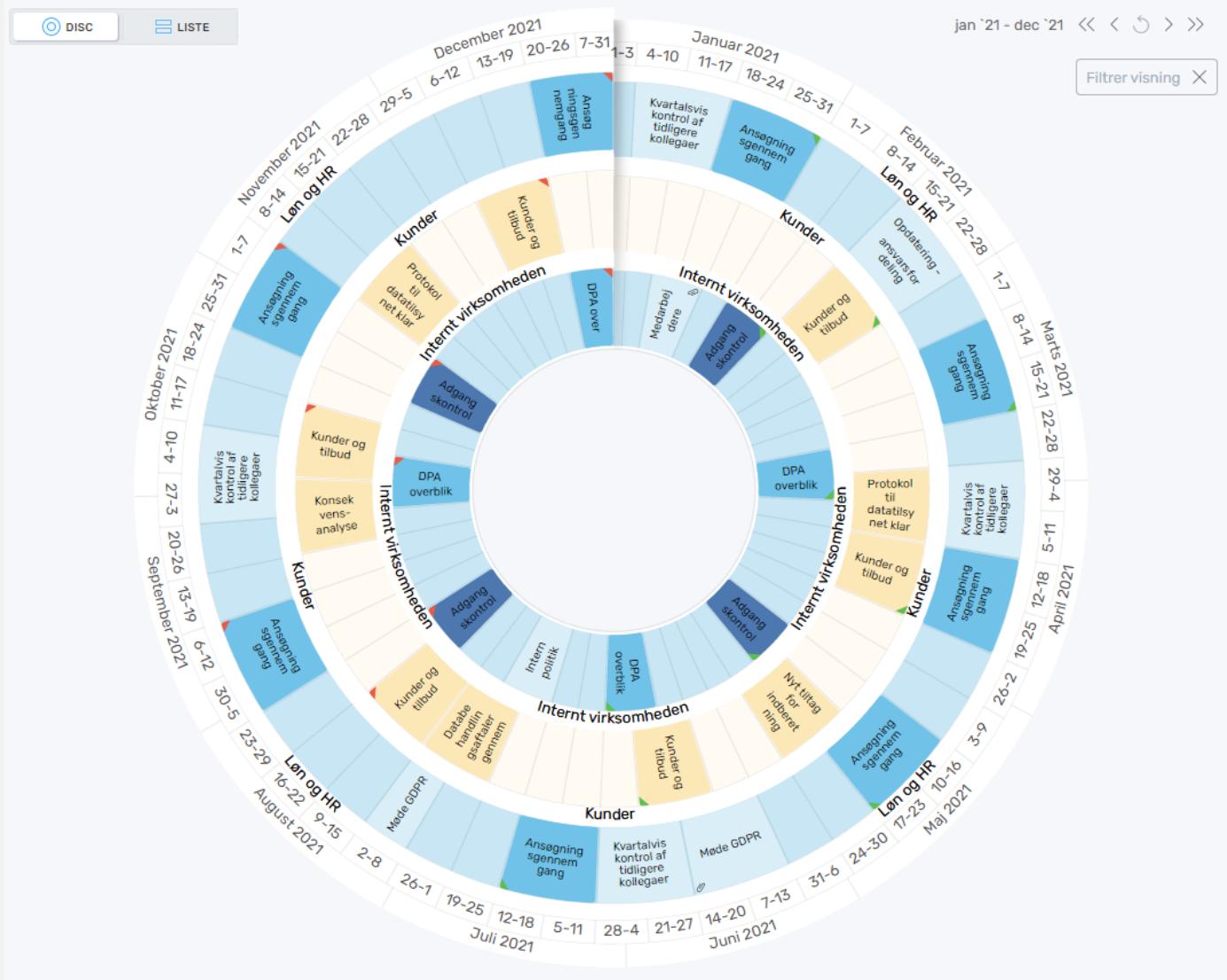
S (Supportive): Hjælper og supporterer opgaven

C (Consulted): Har vigtig information og bør derfor konsulteres under udførelsen

I (Informed): Skal holdes informeret og er formentlig afhængig af opgavens udfald

Årshjul - informationssikkerhedsaktiviteter

Eksempel på GDPR-årshjulsaktiviteter



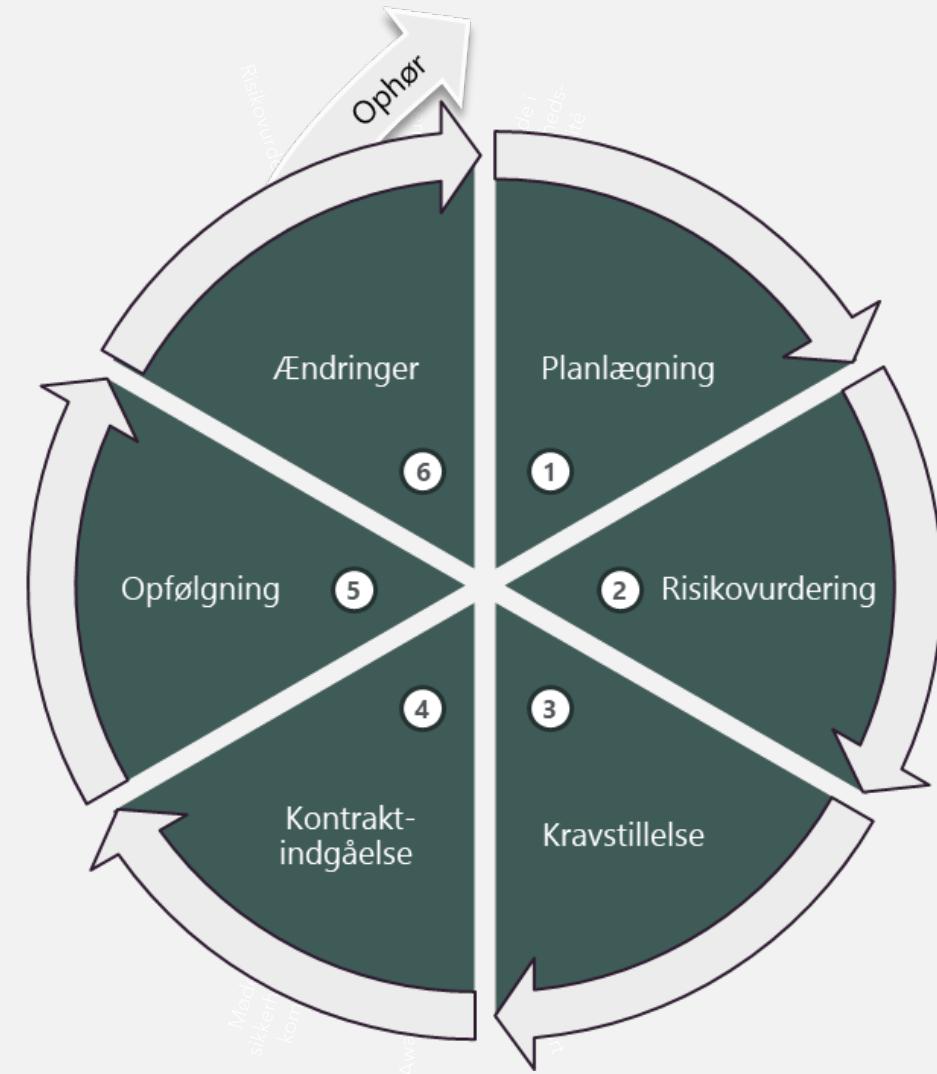


**Pause
10 min**

Risikostyring af leverandører

Eksempel på styring af leverandørrisici fra vugge til grav:

1. Afdække behov, herunder data, integrationer mfl.
2. Foretag risikovurdering
3. Stille krav efter identificeret risikoprofil
4. Indgå kontrakt samt formel kravstillelse
5. Følg op på efterlevelse af stillede krav
6. Vurder ændrede risici som følge af kontraktændringer, og juster herefter med tillæg til kontrakten.

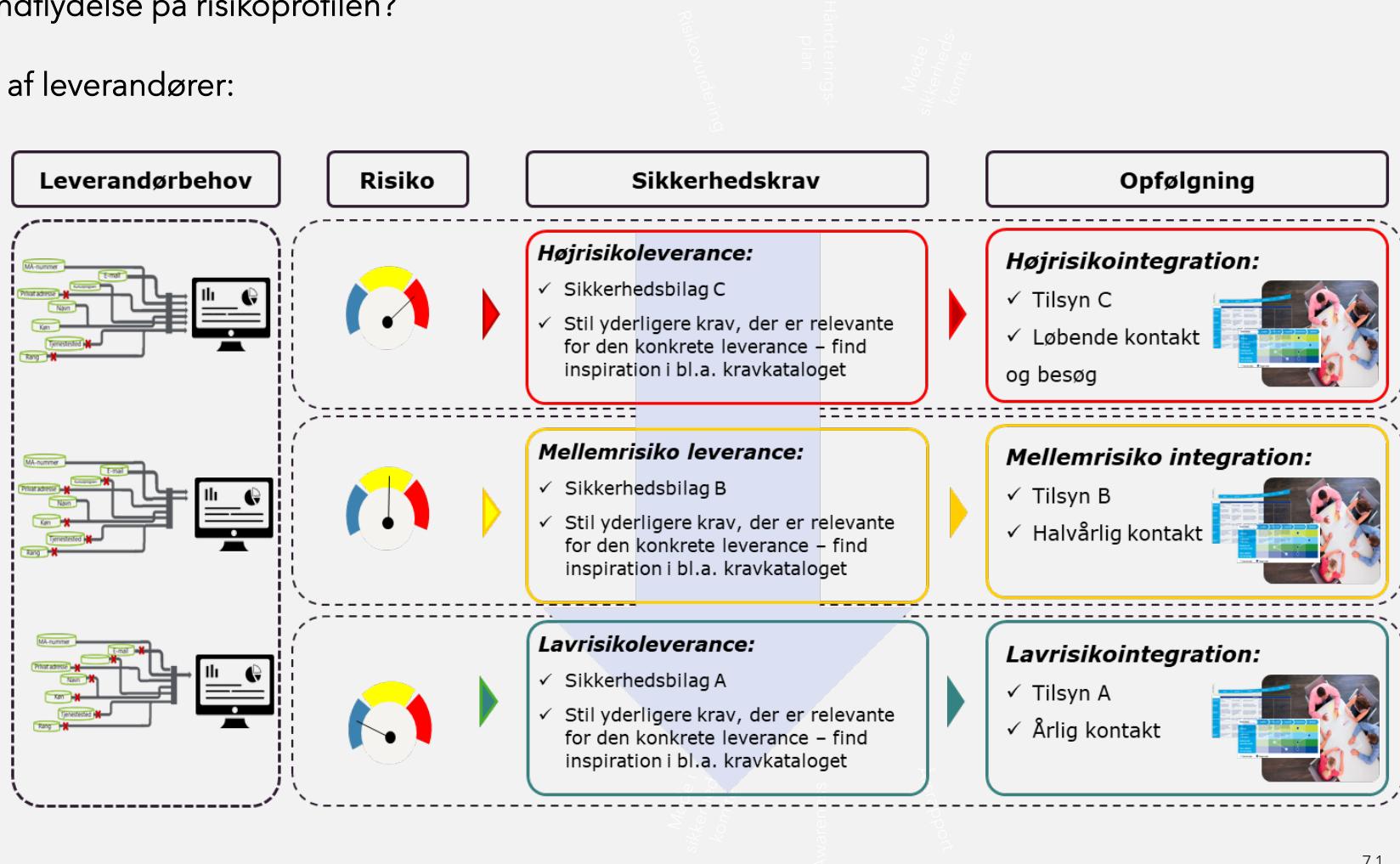


Risikostyring af leverandører

Hvilke aspekter kan have en indflydelse på risikoprofilen?

Eksempel på risikoprofilering af leverandører:

- Vurderingen kan tage udgangspunkt i leverandørens behov for data, både ift. mængde, type og adgangsrettigheder.
- Uover databehovet, kan diverse eksterne og interne faktorer medvirke til tildeling af risikoprofil for den potentielle integration.
- Risikoprofilen bør herefter udmøntes i specifikke sikkerhedskrav, rammer for opfølgning og grad af hændelsesinvolvering.



Governance, Risk Management og Compliance (GRC)



Governance ~ styring/ledelse



Risk Management ~ risikostyring



Compliance ~ kontroller og håndteringstiltag

Det overordnede formål med en central GRC-tilgang er at sikre en ensartet tilgang til de aktiviteter, der ligger indenfor risikostyring og interne kontroller, herunder:

- ✓ Skabe transparens på tværs
- ✓ Ensarte beskrivelser og dokumentation
- ✓ Effektivt identificere afvigelser
- ✓ Skabe et fundament for god datakvalitet
- ✓ Etablere fælles standardrapportering
- ✓ Styre roller og adgange

Governance: the three lines of defence





Case

CASE - risikoanalyse

Ud fra Digitaliseringsstyrelsens vejledning og metode til risikovurdering skal I:

1. Orientere jer og forstå vejledningsdokumenterne Bilag 1-7
2. Gennemføre en risikoanalyse af et centralt system på baggrund af en af virksomhedscasene ved hjælp af risikovurderingsmodel (regnarket) og de tilhørende vejledninger. Identificere kompenserende tiltag til at reducere de identificerede risici.
3. Udarbejde risikorapportering og dermed også forslag til risikohåndtering til ledelsen baseret på jeres risikoanalyser af det centrale system. Dette skal danne udgangspunkt for jeres præsentation fredag. Hvordan I ønsker at præsenterer rapportering og risikohåndtering er op til jer.

CASE - risikoanalyse

Som topledelse ønsker vi at se følgende i rapporteringen:

- **Resumé:**
 - En kortfattet opsummering af de vigtigste risici og anbefalede tiltag.
- **Oversigt over Risikovurdering:**
 - En visuel præsentation af identificerede risici (fx gennem en risikomatrix, diagram eller graf) baseret på sandsynlighed og konsekvens.
- **Detaljer om Risici:**
 - Hvad de centrale risici er.
 - Hvordan de påvirker forretningen og systemet.
 - Den eksisterende kontroltilstand for hver risiko.
- **Forslag til Risikohåndtering:**
 - Konkrete anbefalinger for at reducere risikoniveauet.
 - Vurdering af omkostninger eller ressourcer der kræves for risikohåndtering.
 - Realistiske tidsrammer for implementering.
- **Konklusion og Next Steps:**
 - Opsummering af prioriterede risici.
 - Klar handlingsplan til ledelsens beslutning.