





ATV-konference Virksomhedernes cyber- tilstand

Klaus Kongsted, CEO, Dubex A/S
København, den 15. januar 2015

Moderne virksomheder bygger på information

 Zynga behandler over 1 petabyte data om dagen

 2 mia. videoer ses hver dag

 1,2 mio. beskeder via Twitter pr. sekund

Volume
Store mængder data

Velocity
Hurtig behandling

Variety
Forskellige typer

Samlet antal miles logget af Connect-brugere
3,309,821,694



Large Hadron Collider genererer 150 mio. petabytes pr. år - 99.999% smides væk

Voksende datamængde

- Global datamængde vokser med ca. 40% pr. år
- En harddisk til 3.000 kr. kan gemme al musik i verden

Ustruktureret data

- 80% af alle data er ustrukturerede
- Dynamisk kommunikation
- 30 mia. opdateringer på Facebook hver måned

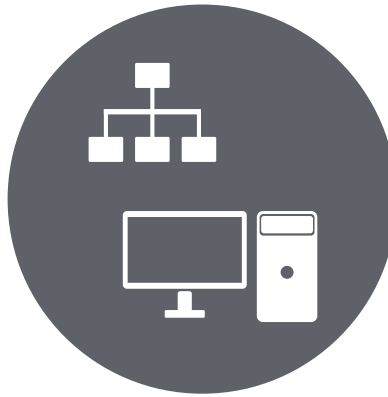
Applikationer og kommunikation

- Sociale medier
- Mobile enheder ~ ca. 5. mia. i verden
- Brugere, kunder, partnere
- Komplekse rettigheder

Cyber-udfordringer for virksomhederne



**Avanceret
infrastruktur**



**Stigende
kompleksitet**



**Et udfordrende
trussesbillede**



Forretningskrav

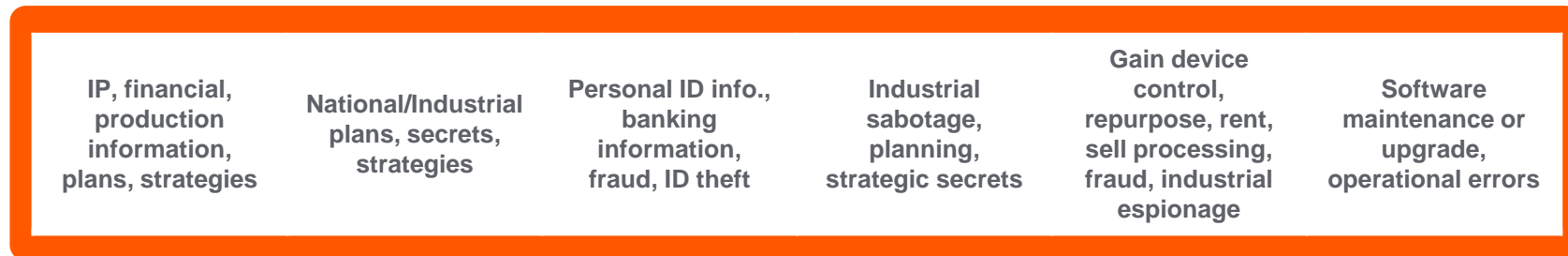
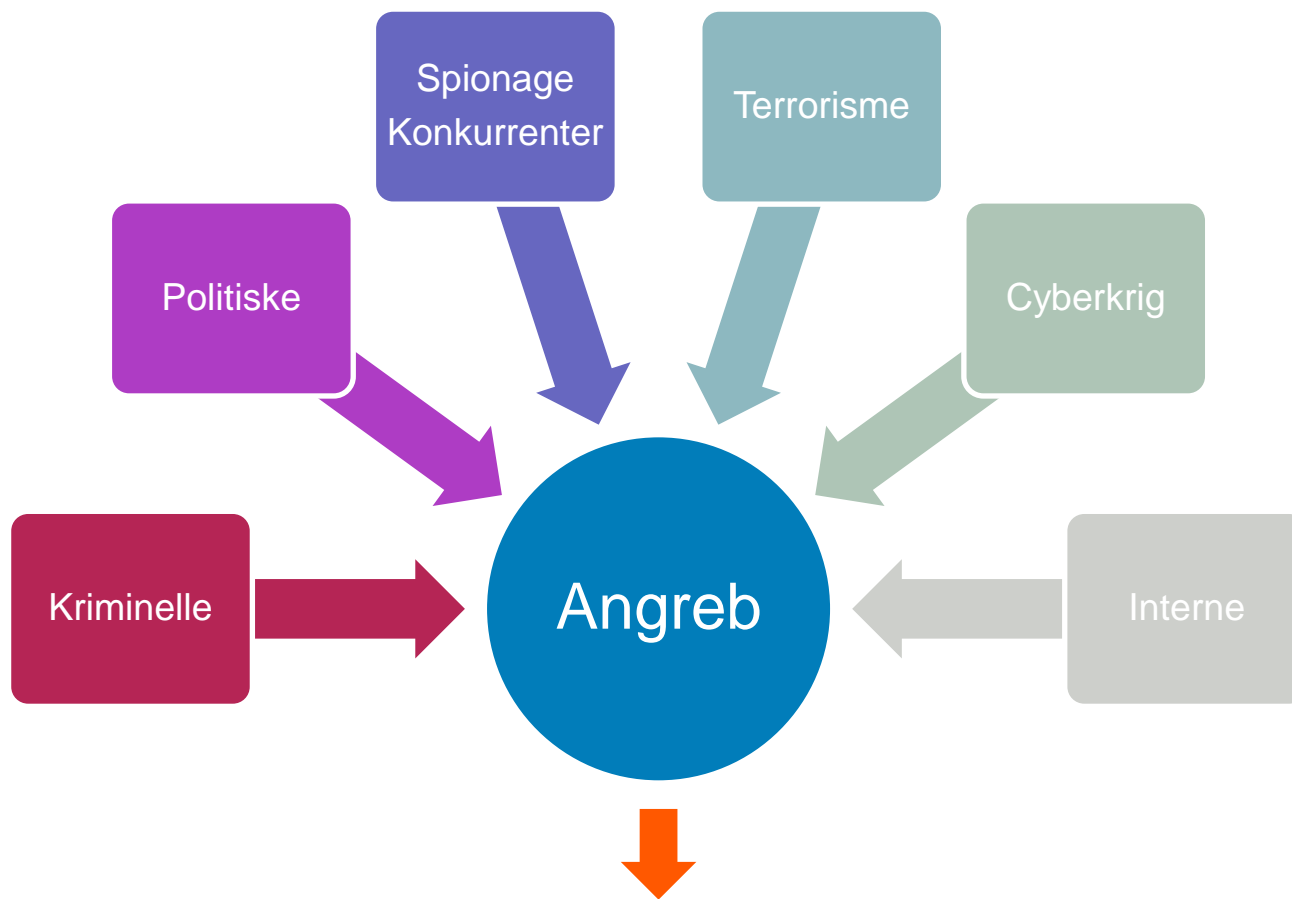


**Information er
blevet strategisk**



**Personale og
kvalifikationer**

Hvorfor bliver vi angrebet?

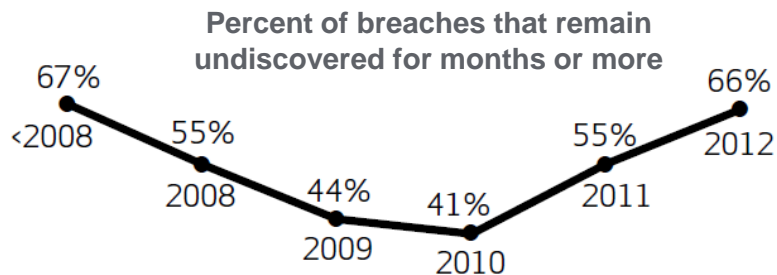


Angreb opdages langsomt og tilfældigt

Opdagelse af angreb - hastighed



66% af alle organisationer var flere måneder eller år om at opdage det initiale indbrud



Opdagelse af angreb - hvordan



82%

af alle hændelser blev opdaget af eksterne



12%

af alle hændelser blev tilfældigt opdaget internt



Kun 6%

af alle hændelser blev aktivt opdaget internt

... så det normale er, at der efter nogle måneder kommer nogle eksterne og fortæller, at vi er blevet hacket...

Den nye adaptive tilgang til avancerede trusler

Continuous Monitoring and Analytics

Predict &
identify

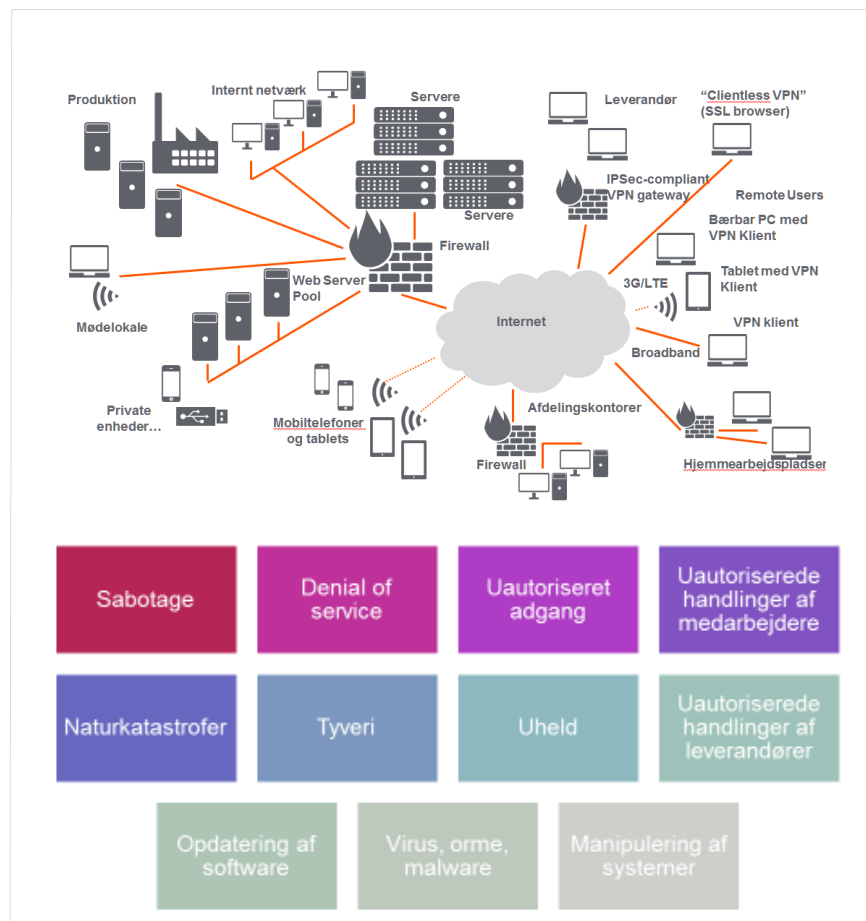
Prevent &
protect

Detect

Respond
& recover

Prioritering af cybersikkerhed

- Udfordringerne er mange
 - Der er trusler og behov
 - Der er krav og forventninger fra myndigheder, samarbejdspartnere og kunder
 - Man kan "drukne" i løsninger, muligheder og aktiviteter
 - Det er vigtigt at målrette sikkerheden til de "forretningsmæssige" behov
 - Ledelsesopbakning og brugerinddragelse er kritisk for successen
- Risikovurderinger er et vigtigt hjælpemiddel til prioritering af it-sikkerhed - også når man skal vælge mellem forskellige løsninger/muligheder



It-afdelingens dilemma

INFORMATION er blevet virksomheders vigtigste asset

Managing risk

Beskytte følsomme oplysninger for at forbedre og opretholde markedspostion og sikre overholdelse af regulativer samtidig med en kontrol af omkostningsniveauet



Enabling growth

Forbedre og sikre forretningens agilitet ved at give hurtig og intuitiv adgang til de rigtige informationer, værktøjer og applikationer

It er grundlaget for alle forretningsprocesser

Ledelsen og bestyrelsen skal beskytte værdien af virksomheden

Udfordring: Synliggørelse af den risiko som it-anvendelsen medfører

Risikostyring skal bruges til at beskytte værdien af virksomheden

Primære drivere for outsourcing

- Informationer om nuværende trusselsbillede er svært at **vedligeholde**
- **Kompetencer** til at udfylde de mange områder er svære at:
 - Få
 - Vedligeholde
 - Udnytte & betale
- **Hastighed** i implementering og forankringen i forretningen tager for lang tid
- **Omkostninger** er for høje ved køb og drift selv
 - Drift (8-17 eller 24x7)
 - Vedligehold
 - Administration
 - Fortolkning af data
- Virksomheden ønsker ikke at drive området selv, da det **ikke** er **forretningskritisk**
- **Outsourcing giver større fleksibilitet, omkostningskontrol samt værdi**

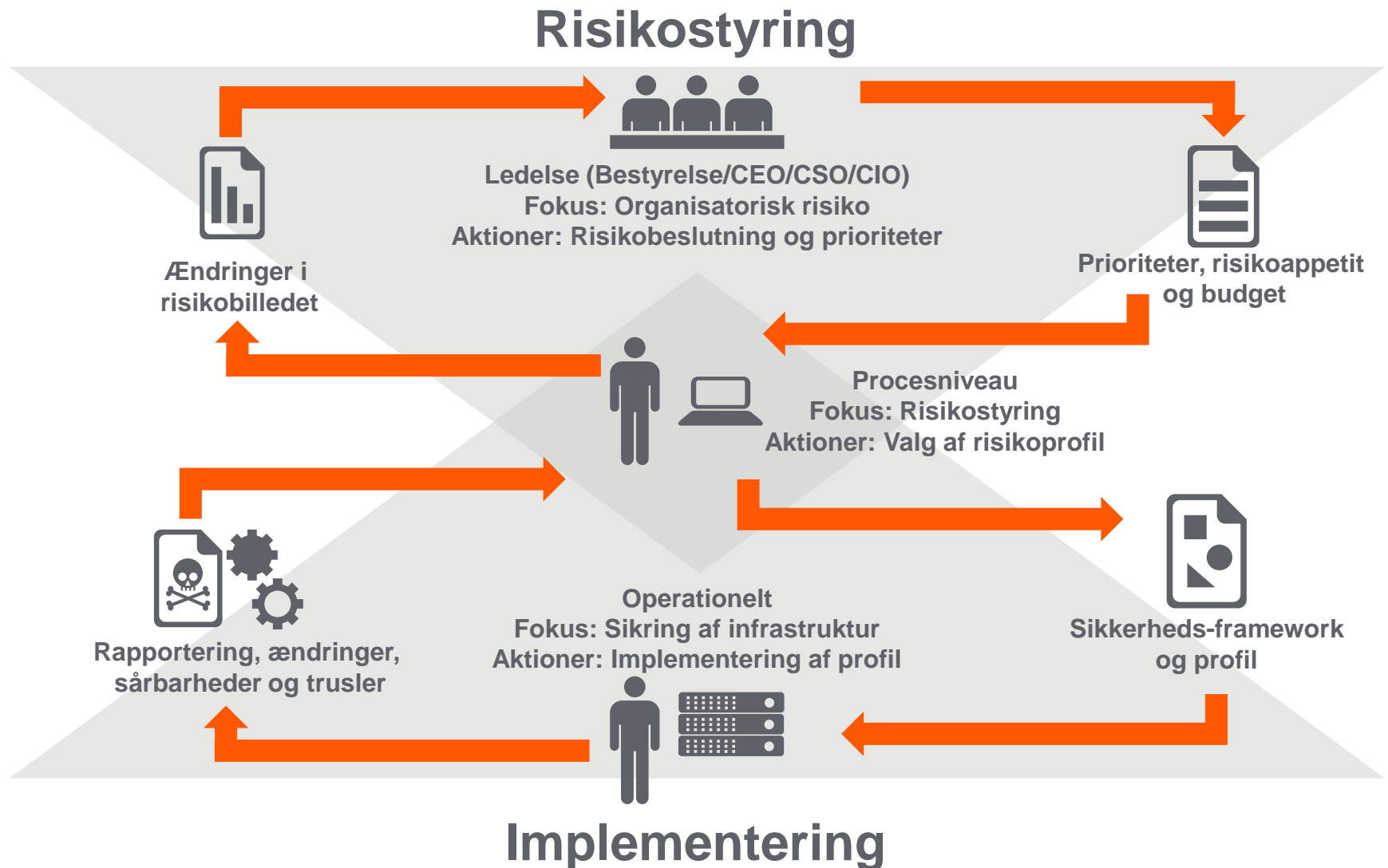


Høj fart...



... kræver gode bremser

Organisering af sikkerhedsprocessen



Risikostyring på ledelse- og bestyrelsesniveau

Risikostrategi

Tager vi de rigtige risici?

- Kender vi de betydeligste risici, vi tager?
- Er de risici vi tager på linje med vores forretningsmæssige mål og vækststrategier?
- Vil de risici, vi tager hjælpe os med at opnå konkurrencemæssige fordele?
- Hvordan passer de risici, vi tager med aktiviteter, der skaber værdi?
- Har vi rettidig og relevant information til at foretage strategiske valg?

Risikoappetit

Har vores risiko det rette omfang?

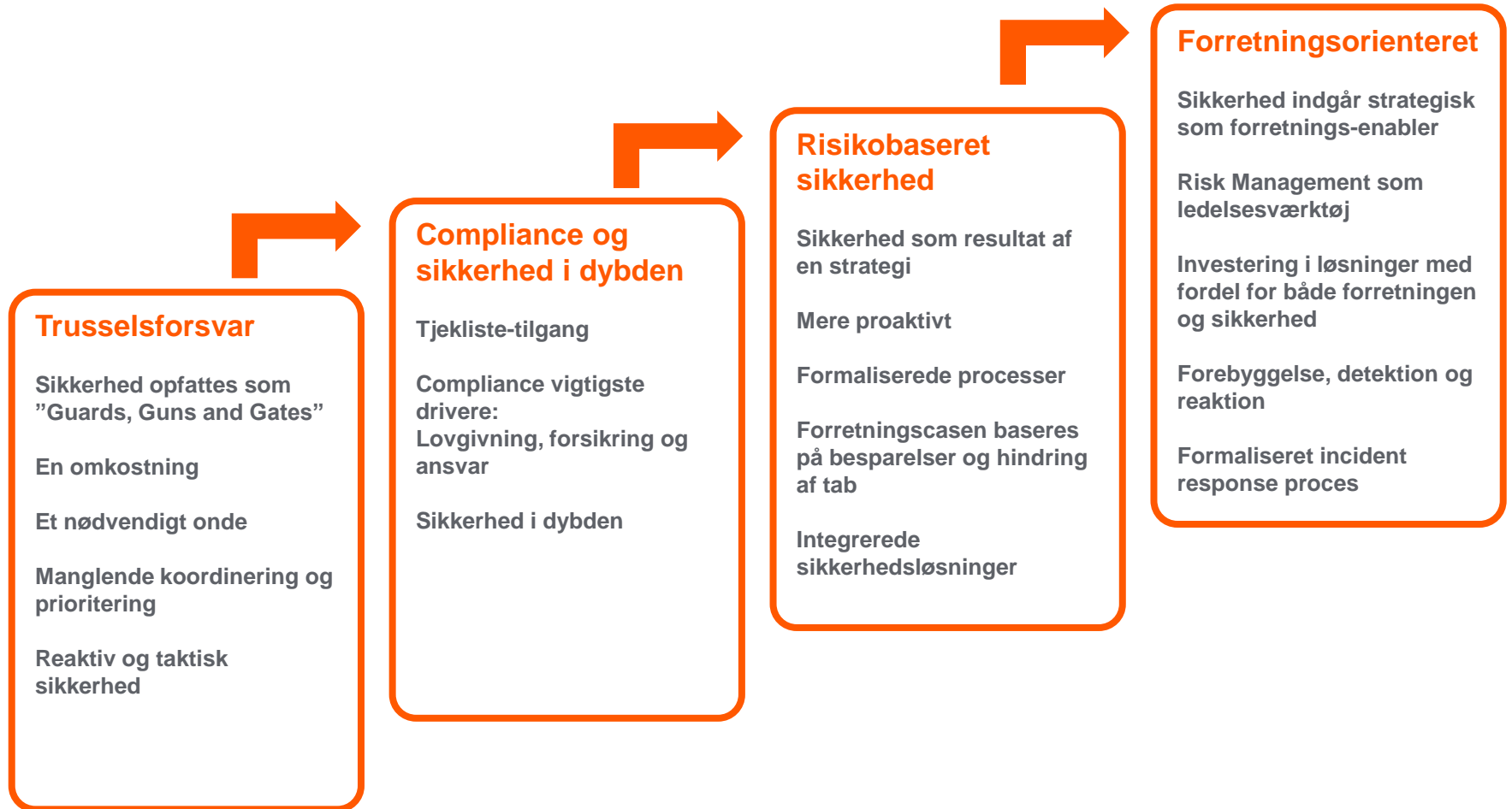
- Kan vi opnå et afkast, der er i overensstemmelse med vores overordnede risikoprofil?
- Fremmer eller hæmmer vores kultur det rette niveau af risikotagning adfærd og aktiviteter?
- Har vi en defineret, formidlet og forstået organisatorisk risikoappetit og tolerance?
- Er vores risikoappetit kvantificeret både samlet og per hændelse?
- Er vores reelle risikoprofil i overensstemmelse med vores risikovillighed?
- Er vores kapital er tilstrækkelig til at understøtte vores risikoprofil?

Evner

Er vi effektive til at styre risici?

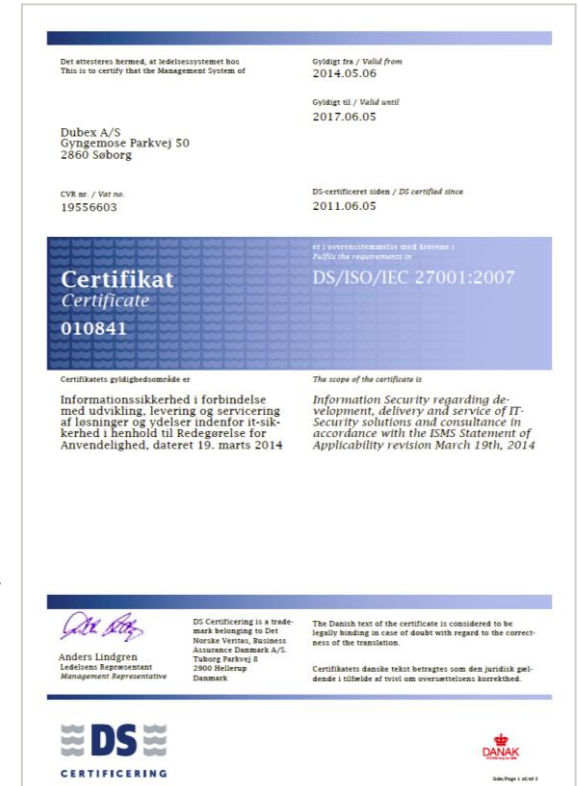
- Er vores risikostyringsproces "ensartet", på niveau med vores strategiske beslutningsproces og key performance foranstaltninger?
- Risikostyring - er der klarhed over bemyndigelse, afgrænsninger og ansvarsområder?
- Overvåges vores risikostyringsproces effektivt på tværs af hele virksomheden?
- Er vores ensartede risikostyringsproces omkostningseffektiv og effektiv?

Modenhedskurve



Hvad er ISO 27001?

- ISO 27001 er ikke bare en standard for et ledelsessystem
 - ISO 27001 er også en generel proces, der hjælper med forankring, behovsanalyse og prioritering af it-sikkerheden
- Ledelsessystem for informationssikkerhed (ISMS)
 - ISMS politik
 - Informationsaktiver og klassifikation
 - Risikovurdering og planer
 - Sikkerhedshåndbog
 - Awareness
 - Interne ISMS audits
 - Hændelser og forbedringer
 - Vedligeholdelse
- Grundlaget er ledelsens commitment og accept
- Fokus er på forretningen og de forretningskritiske aktiver
- Valg af kontroller baseret på risikovurdering
 - Udvælgelsen er en vigtig del af processen
- Procesorienteret (Plan-Do-Check-Act)
- Der lægges vægt på rapportering



Thank you

For more information please contact
kka@dubex.dk