ISO/IEC 27001 Online

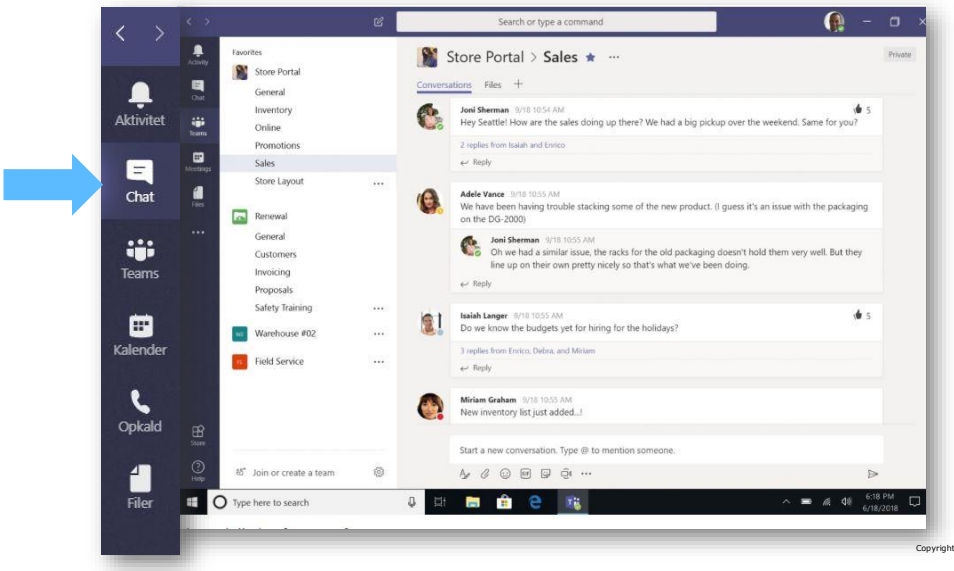
- få gratis overblik over standardens krav!

April 2020

DANSK STANDARD

1

Microsoft Teams: chat-funktion

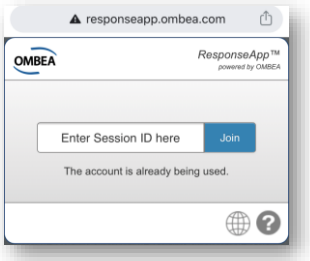


DANSK STANDARD

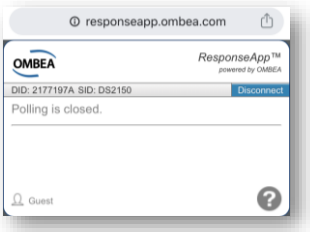
2

Ombea: Besvarelse af spørgsmål

1. Åben en browser på mobiltelefon (eller pc)
2. Gå til **responseapp.ombea.com**



3. Tast "**ISO27001**" som session ID og tryk *Join*



4. Vent på forbindelse og beskeden "Waiting for the poll to open" eller "Polling is closed."

5. Besvar ved at trykke på en svarmuligheden

3

Agenda

ISO/IEC 27001 Online
09:00 Introduktion til dagsorden
09:10 Introduktion til ISO/IEC 27001
09:25 Planlægning af et ISMS
09:45 Risikovurdering
10:10 Pause
10:20 Risikohåndtering
10:35 SoA-dokument
10:45 Implementering af et ISMS
11:00 Evaluering
11:20 Opsamling
11:30 På gensyn!

4

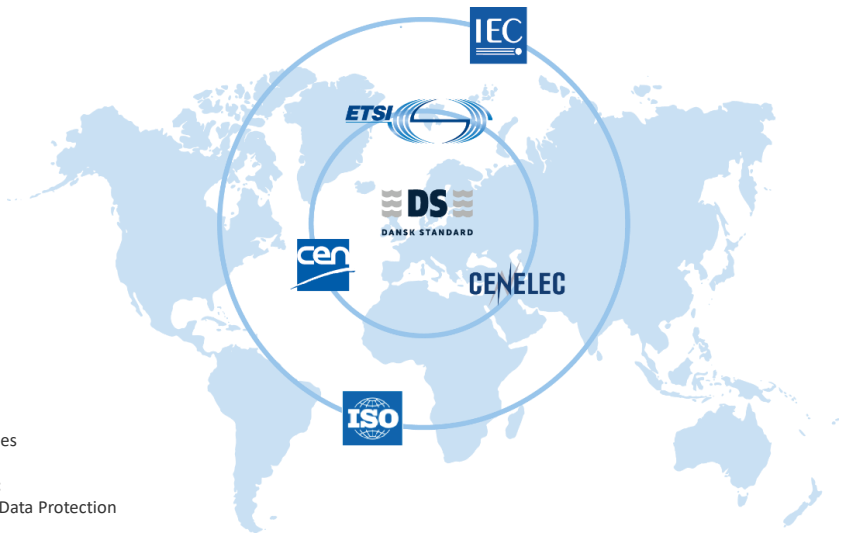
ISO/IEC 27001 Online

Introduktion til ISO/IEC 27001

DANSK STANDARD

5

International og europæisk standardisering



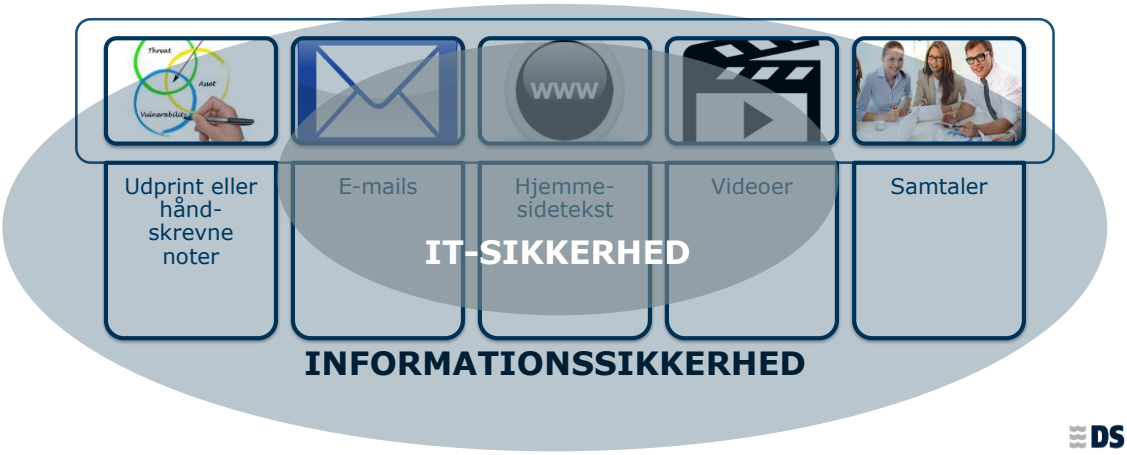
1. ISO/IEC JTC 1/SC 27:
- IT Security techniques

2. CEN-CENELEC JTC 13:
- Cyber Security and Data Protection

DANSK STANDARD

6

Informationer som skal beskyttes



7

Et ledelsessystem for informationssikkerhed

- Læk af interne strategier
- Ledere deler oplysninger om ansattes sygdomsforløb
- Ansatte taler åbent om sagsbehandling

Tab af fortrolighed

- Fejlbehæftet opdatering af systemer
- Fejl i udprint af filer
- Hackers ændring af kundedata

Tab af integritet

- Oversvømmelse af arkiver i kælderen
- Overbelastningsangreb
- Ransomware rammer sagsbehandlingssystem

Tab af tilgængelighed

"Ledelsessystemet for informationssikkerhed bevarer fortrolighed, integritet og tilgængelighed af information ved hjælp af en risikostyringsproces og sikrer, at interessenter har tillid til, at risici håndteres på en ordentlig måde."

ISO/IEC 27001:2017, Indledning, 01

8

Den nationale agenda

Den fællesoffentlige digitaliseringsstrategi, 2016-2020: regioner og kommuner skal følge ISO/IEC 27001's principper.

National strategi for cyber- og informationssikkerhed, 2018: Efterlevelse af minimumskrav til ISO/IEC 27001.

§

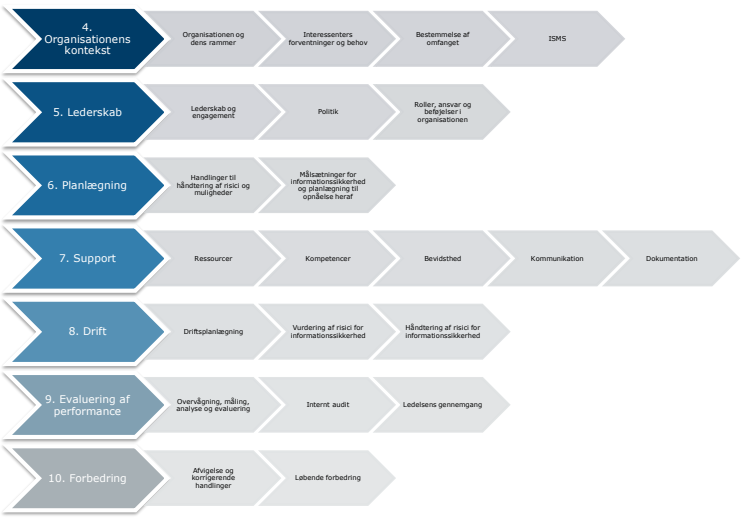
Databeskyttelsesforordningen 2016: Ny persondatalovgivning fra maj 2018 med krav om dokumentation af processer, politikker, organisering og konsekvensvurderinger.

Strategi for Danmarks digitale vækst, 2018: SMV-hjælp. Privacy-kompas, Sikkerhedstjek baseret på ISO/IEC 27001. En samlet portal på sikkerdigital.dk.

DS DANSK STANDARD

9

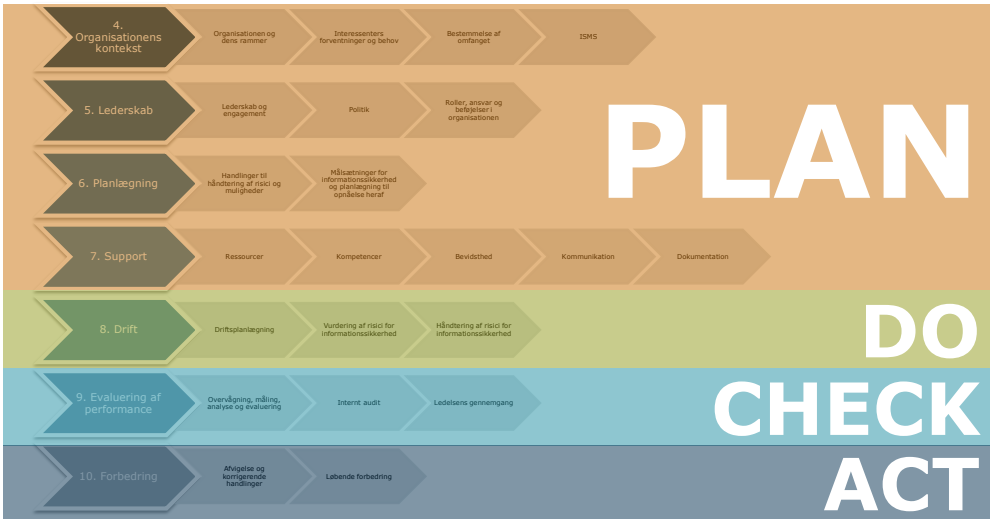
ISO/IEC 27001 Oversigt



DS DANSK STANDARD

10

ISO/IEC 27001 Oversigt



11

ISO/IEC 27001: Dokumentationskrav for informationssikkerhed

POLITIK OG MÅLSÆTNINGER (5.2; 6.2):	En dokumenteret informationssikkerhedspolitik, der indeholder målsætninger for informationssikkerhed
ANVENDELSESOMRÅDE (4.3):	En dokumenteret afgrænsning af ISMS'et
RISIKOMETODE (6.1.2):	En beskrivelse af risikovurderings- og håndteringsprocessen
RISIKOVURDERING (6.1.2, 8.2):	En risikovurderingsrapport
RISIKOHÅNDTERINGSPLAN (6.1.3, 8.3):	En plan for håndtering af risici
SOA-DOKUMENT (6.1.3):	Et "Statement of Applicability"
MEDARBEJDERKOMPETENCER (7.2d):	Dokumentation for kvalifikationer, erfaring og uddannelse
MÅLING (9.1):	Proces for og resultat af måling af foranstaltningers effektivitet
INTERNE AUDITS (9.2):	Programmer og rapporter for interne audit eringer
LEDELSENS GENNEMGANG (9.3):	Rapportering til ledelsen om evaluering af inf.sikkerhed og effekten af ISMS, afvigelser og opfølgende handlinger
AFVIGELSER OG KORRIGERENDE HANDLINGER (10.1):	Registrering og håndtering af afvigelser og implementering af korrigerende handlinger

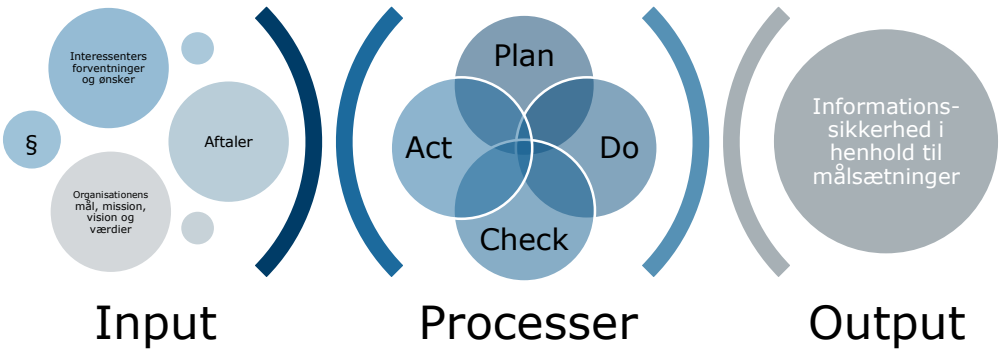
12

ISO/IEC 27001 Online

Planlægning af et ISMS

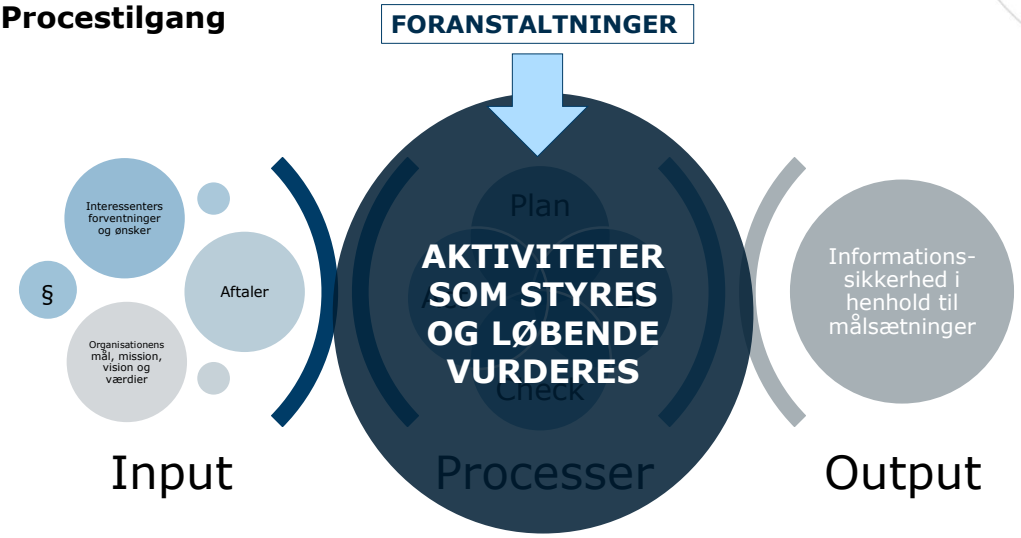
13

Procestilgang



14

Procestilgang



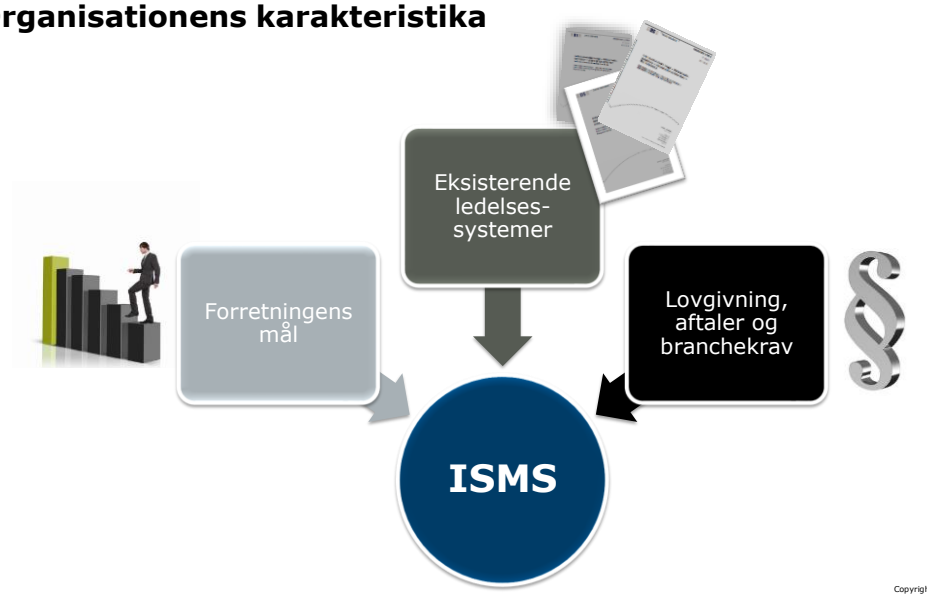
15

5 råd ved implementering

- Få ledelsens opbakning og forståelse for projektet
- Udnævn en ISMS-projektleder
- Integrer ISMS med de eksisterende processer
- Undgå integration af nye tekniske løsninger
- Involver interessenter fra hele organisationen – fra starten af projektet

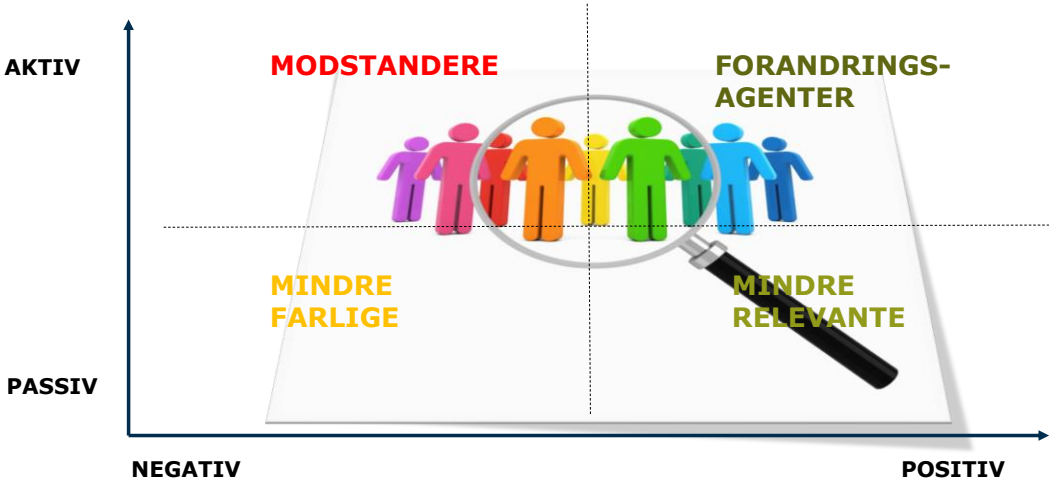
16

Organisationens karakteristika



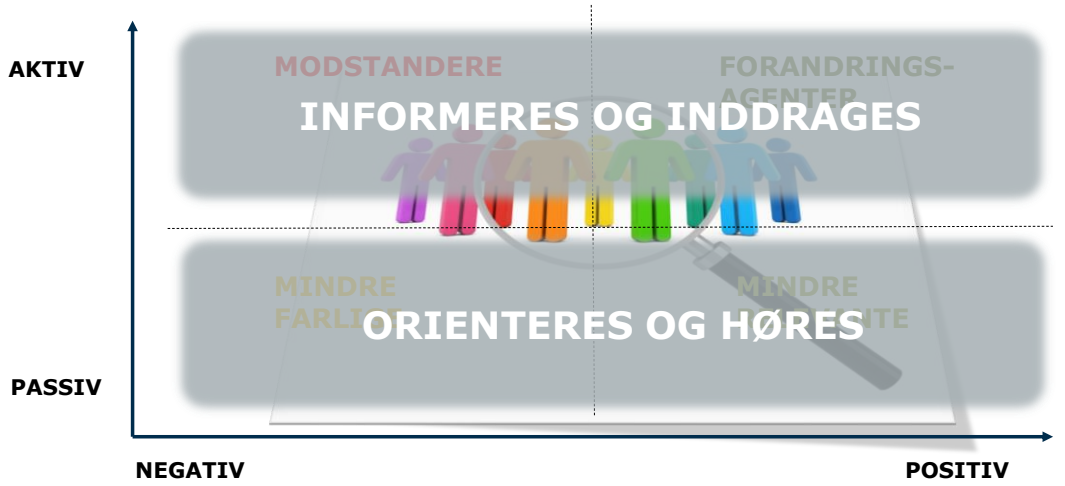
17

Interessentanalyse



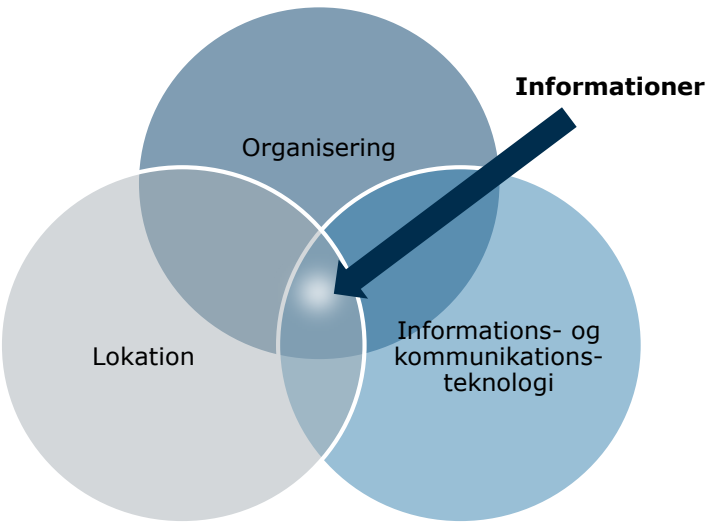
18

Interessentanalyse



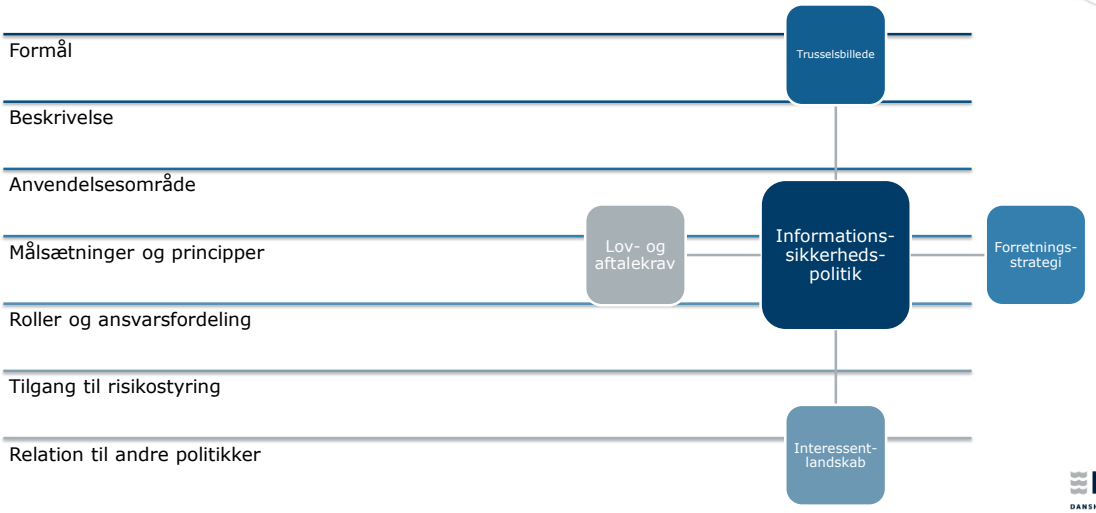
19

Definition af anvendelsesområde og afgrænsning



20

Beskrivelse af politik for informationssikkerhed



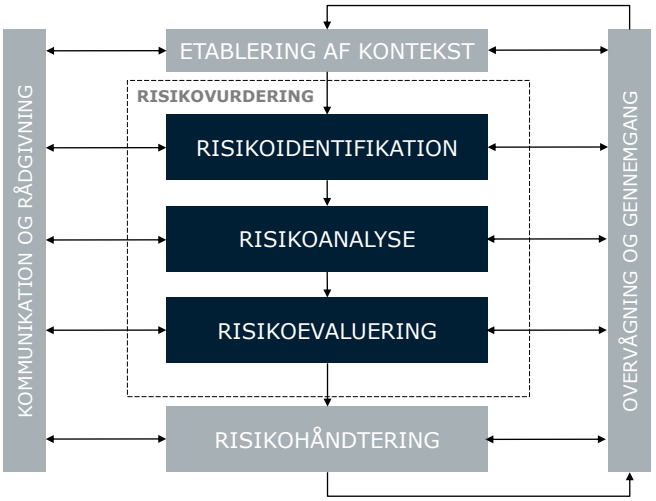
21

ISO/IEC 27001 Online

Risikovurdering

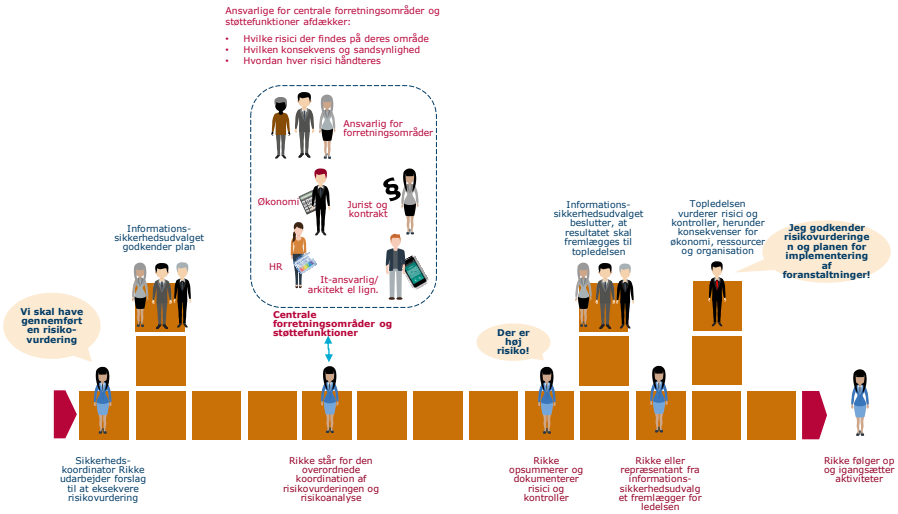
22

Risikovurdering, jf. ISO/IEC 27005



23

Organisering af risikostyringsproces



Https://sikkerdigital.dk/media/10839/leverandoerstyring-en-rejsefortaelling-om-krav-og-opfoelgning-paa-sikkerhed.pptx

24

Risikovurdering

Identifikation

Find aktiver, trusler, sårbarheder og foranstaltninger

Strømafbrud

↓

ingen diesel til generator

Analyse

Beregn sandsynlighed og konsekvens

4. Meget sandsynligt
3. Sandsynligt
2. Ret usandsynligt
1. Meget usandsynligt

Evaluering

Sammenhold risici med acceptkriterier

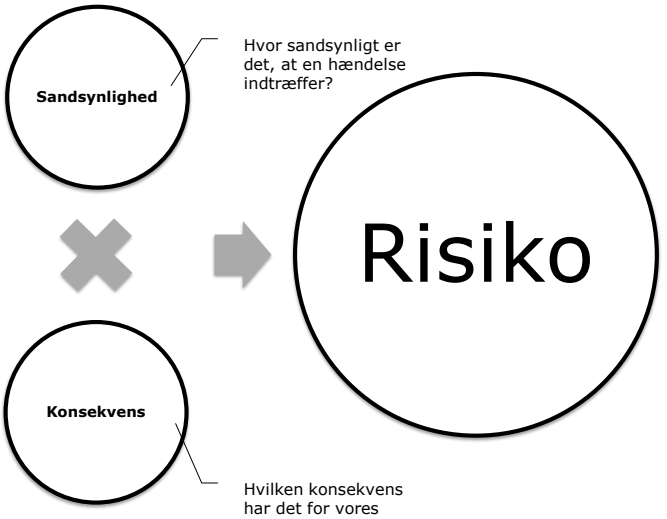
25

Udpegning af informationer

Ledelse	Salg og marketing	HR	Regnskab	Indkøb/jura	Drift	Udvikling
Politikker og planer	Kunder: navne, adresser, tlf.	Medarbejderoplysninger - navne, adresser, tlf.	Kontooplysninger	Leverandørinformation og leverandøraftaler	Proces- og opgavedokumentation	Kildekode for udviklede programmer
Strategier	Kunder: aktiviteter og adfærd	Forsikringer	Fakturaer, regninger og transaktioner	Indkøbsplaner	IPR	Softwareudviklinger og -udgivelser
Budgetter	Kunder kreditkort- og bankoplysninger	Helbredsoplysninger	Revision	Handelsbetingelser	Ressourceplanlægning	Produktspecifikationer
	Kunder: korrespondancer og klager	Løn- og bankoplysninger		Kundeaftaler	It-revision	
	Hjemmesidetekst	Efteruddannelse		Ejendomsleasing	Eksterne revisionsrapporter	
		Rekrutteringsoplysninger		Kreditaftaler	Risikovurderinger	
		Sikkerhedsgodkendelser		Forsikringspolicer		
		Ansættelseskontrakter				
		Klage- og disciplinærsager				

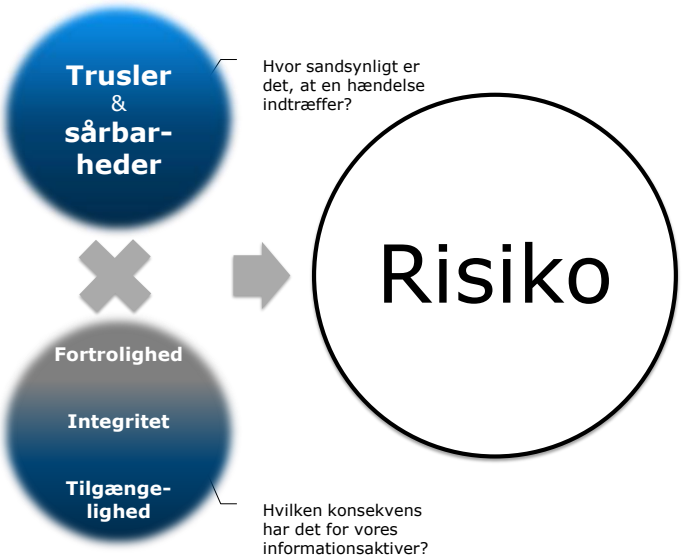
26

Risikometode



27

Risikometode



28

Risikoevaluering

TRUSSEL Scenarie	**SANDSYNLIGHED** Trussel + sårbarhed	**KONSEKVENS** F.I.T. for aktiv	**RISIKO** Score
Scenarie I	2	5	**10**
Scenarie II	5	1	**5**
Scenarie III	5	4	**20**
Scenarie IV	2	2	**4**
Scenarie V	5	3	**15**

29

Risikoevaluering

	SANDSYNLIGHED FOR SCENARIE	Meget usandsynligt	Usandsynligt	Muligt	Sandsynligt	Meget sandsynligt
KONSEKVENS IFT. AKTIV	Meget lille	1	2	3	4	5
	Lille	2	4	6	8	10
	Middel	3	6	9	12	15
	Stor	4	8	12	16	20
	Meget stor	5	10	15	20	25

30

ISO/IEC 27001 Online

Pause – vi starter igen 10:20

DANSK STANDARD

31

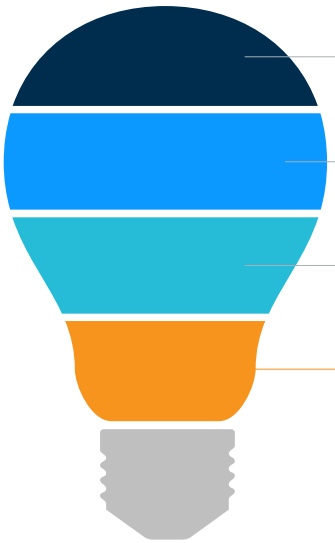
ISO/IEC 27001 Online

Risikohåndtering

DANSK STANDARD

32

Risikohåndtering: valgmuligheder



D Forøg/mindsk
At håndtere risikoen

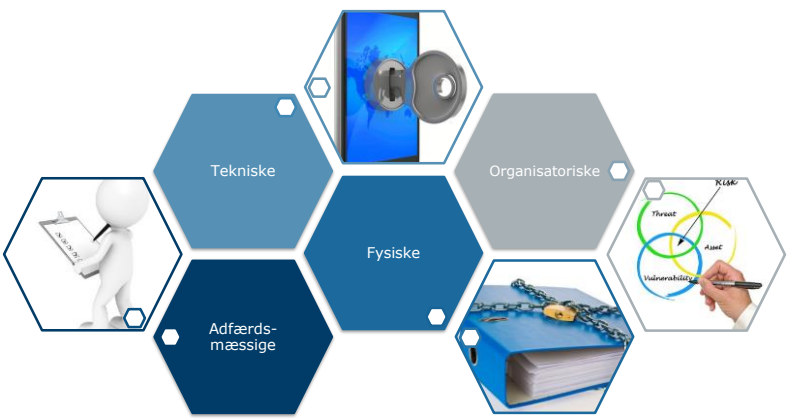
C Undgå
At undgå eksponering for risikoen

B Accepter
At vælge at leve med risikoen

A Flyt
At lade 3. part overtage håndtering af risikoen

33

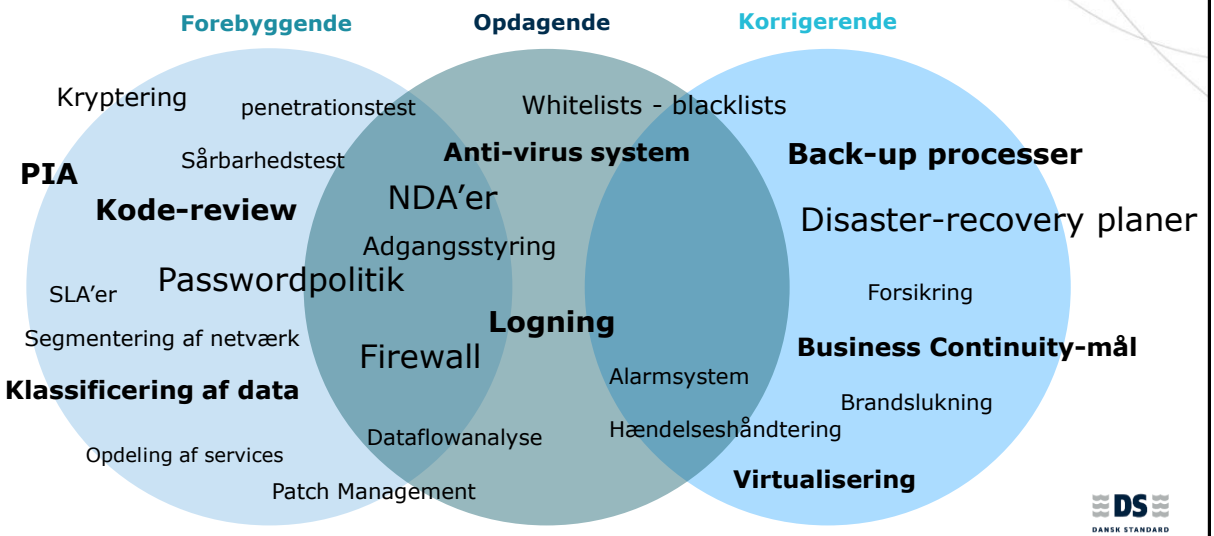
Foranstaltninger - typer



"Measure that is modifying risk"
[ISO/IEC 27005, 3.2]

34

Foranstaltninger - kategorier



35

ISO/IEC 27001 Online

SoA-dokument

36

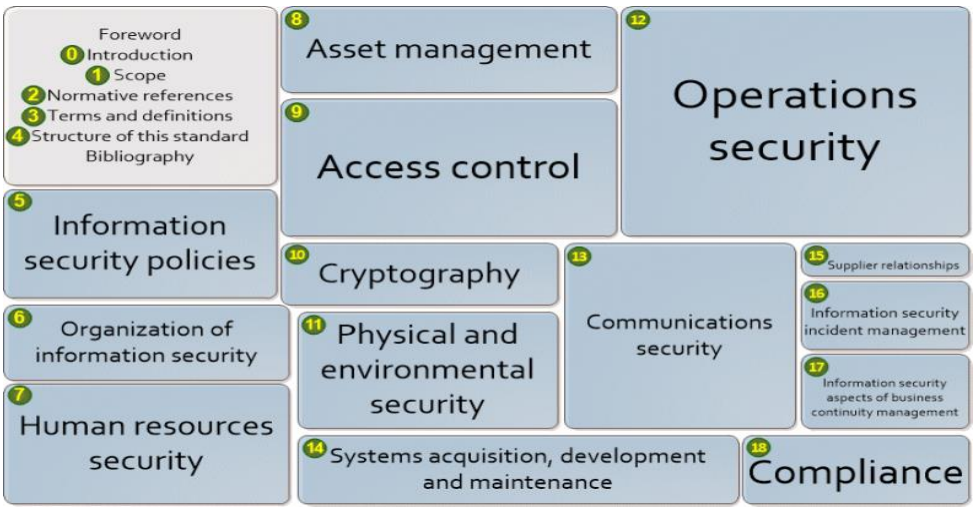
Statement of Applicability (SoA)

- 114 foranstaltninger fra Anneks A
- Organisationen skal gennemgå alle og begrunde til- og fravalg
- Lav tilføjelser og fravalg!
- Risikohåndteringsplanen er hovedbegrundelse for til- og fravalg
- Gældende lovgivning, aftaler og compliance-krav inddrages

DS DANSK STANDARD

37

ISO/IEC 27001, Anneks A

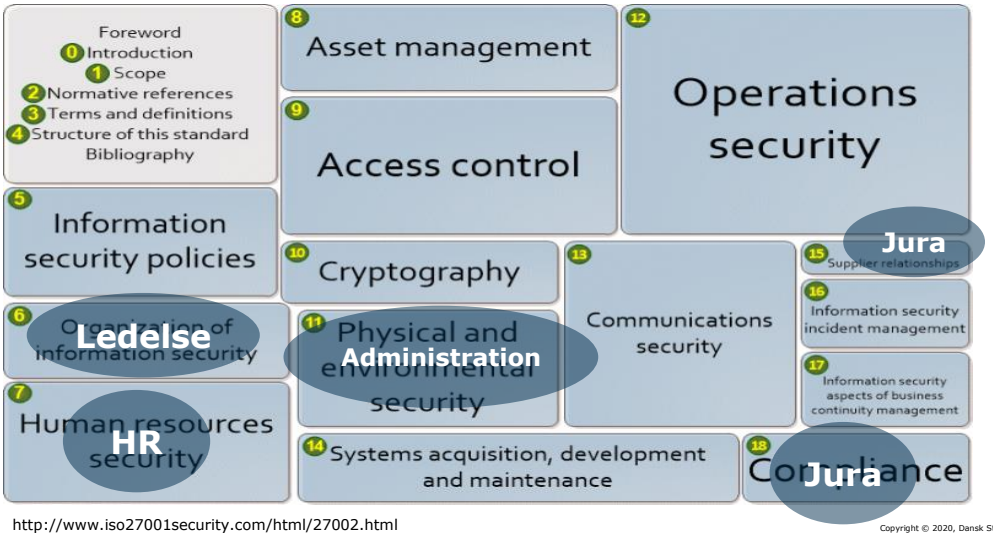


http://www.iso27001security.com/html/27002.html

DS DANSK STANDARD

38

ISO/IEC 27001, Anneks A



http://www.iso27001security.com/html/27002.html

39

Eksempel på SoA-struktur

FORANSTALTNING	TIL-/FRAVALGT?	BESKRIVELSE	BEGRUNDELSE	ANSVARLIG	REF. TIL DOKUMENTATION
Område / Afsnit / Kontrol	Best practice - BP Valg jf. risikovurdering - RV Lovgivning o.lign. - LOV		Planlagt ny/under forbedring - PL I drift - DR I drift og evalueres i forbedringsproces - EV		
A.5 Informationssikkerhedspolitikker					
Informationssikkerheds-politikker	5.1 Retningslinjer for styring af informationssikkerhed				
5.1.1 Politikker for informationssikkerhed					
5.1.2 Gennemgang af politikker for informationssikkerhed					
A.6 Organisering af informationssikkerhed					
Organisering af informationssikkerhed	6.1 Intern organisering				
6.1.1 Roller og ansvarsområder for informationssikkerhed					
6.1.2 Funktionsadskillelse					
6.1.3 Kontakt med myndigheder					
6.1.4 Kontakt med særlige interessegrupper					
6.1.5 Informationssikkerhed ved projektstyring					
6.2 Mobilt udstyr og fjernarbejdspladser					
6.2.1 Politik for mobilt udstyr					
6.2.2 Fjernarbejdspladser					

Kilde: https://digst.dk/media/13725/soa_skabelon_marts2016.xlsx

40

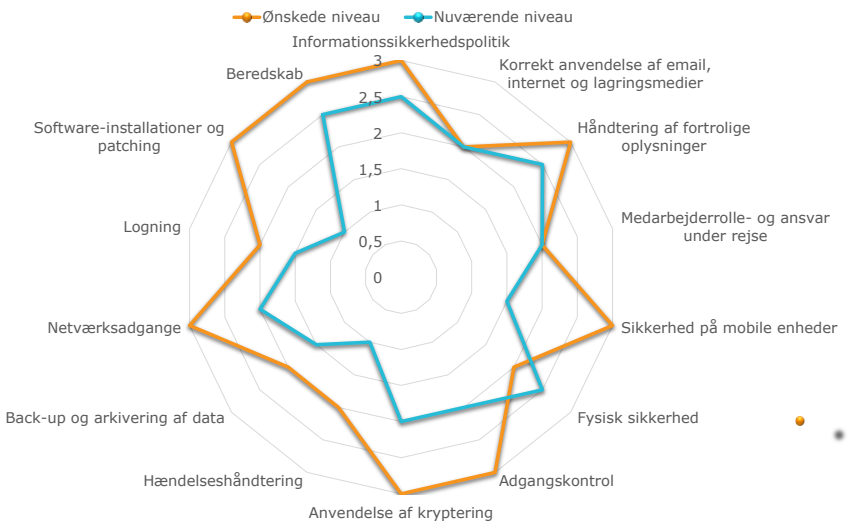
ISO/IEC 27001 Online

Implementering af et ISMS

DANSK STANDARD

41

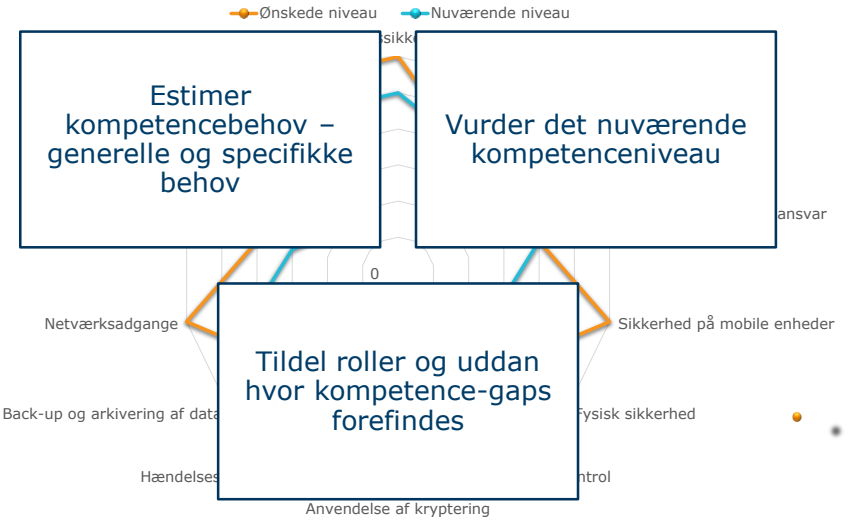
Kompetencegaps



DANSK STANDARD

42

Kompetencegaps



43

Awareness

1. Kende politikken for informationssikkerhed

2. Deres bidrag til organisationens informationssikkerhed

3. Konsekvenserne af ikke at efterleve kravene

44

Redskaber

45

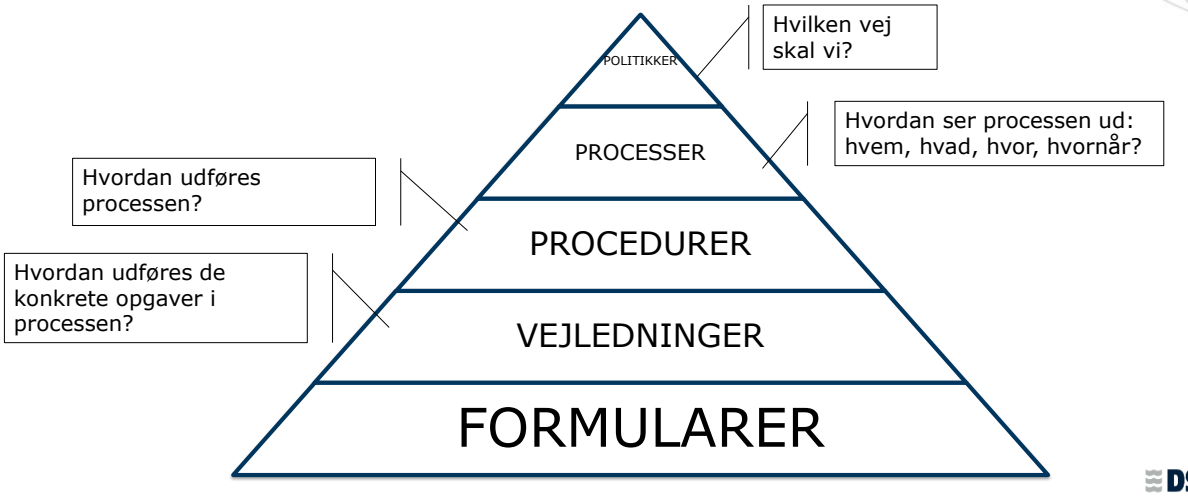
Kommunikationsplan

- Skabe troværdighed og tillid
- Sikre overholdelse af lovgivning og aftaler
- Demonstrere efterlevelse af interessenters krav
- Øve indflydelse på politikker omkring ISO/IEC 27001

1. Hvilket indhold skal kommunikeres?
2. Hvornår?
3. Til og fra hvem?
4. Hvordan? – hvilke platforme og medier

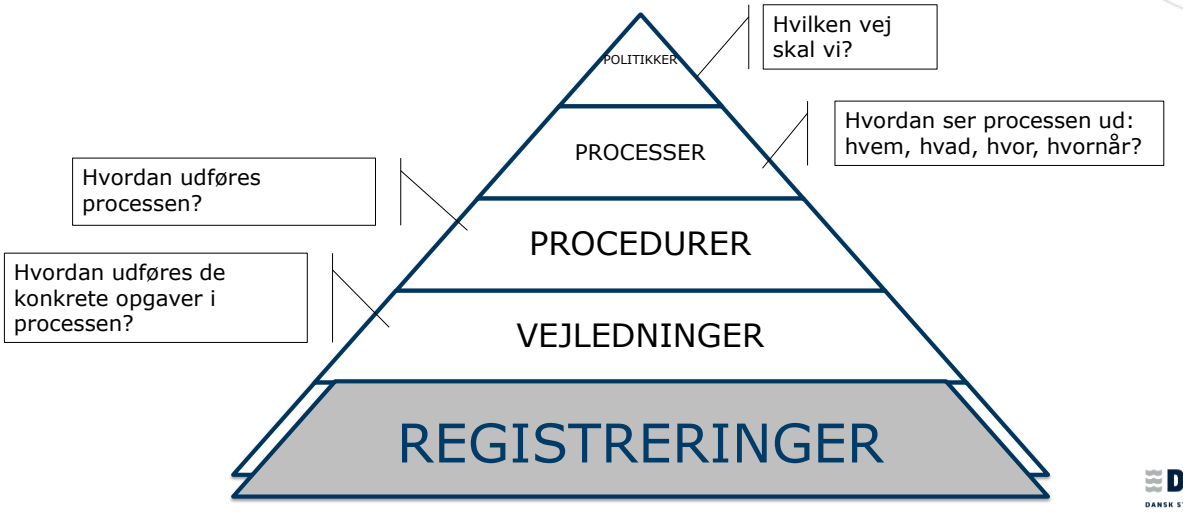
46

The paper exercise



47

The paper exercise



48

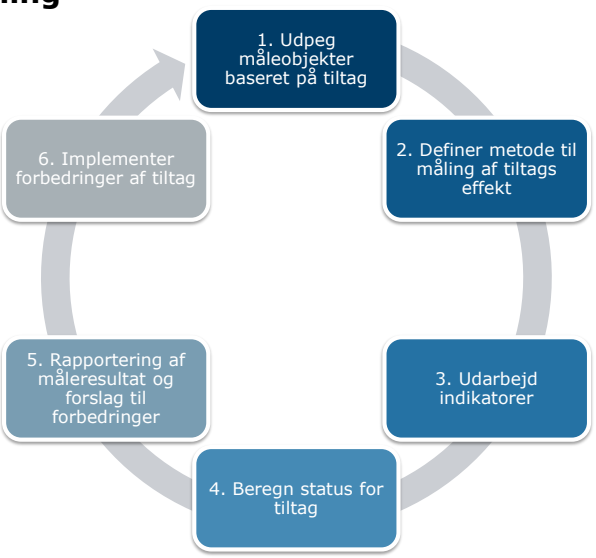
ISO/IEC 27001 Online

Evaluering

DANSK STANDARD

49

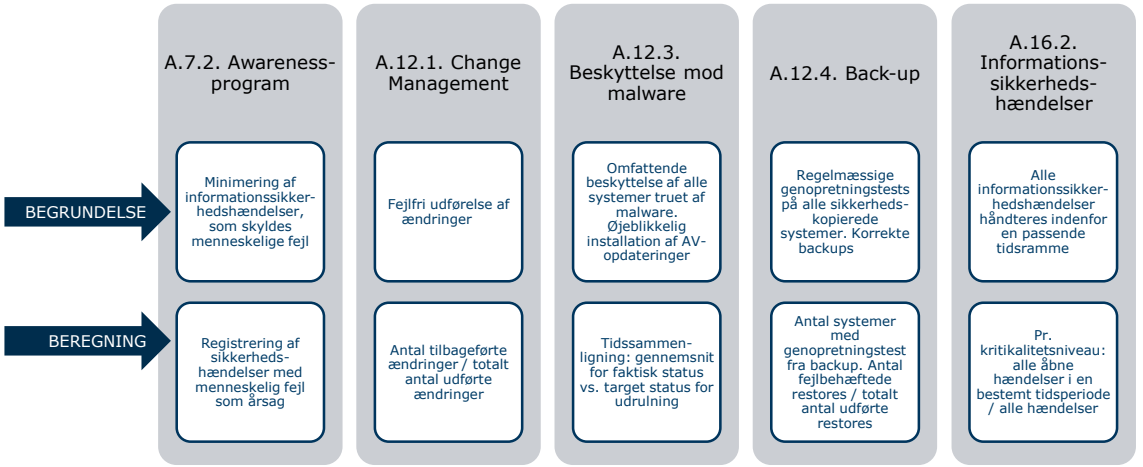
1-6 trin for måling



DANSK STANDARD

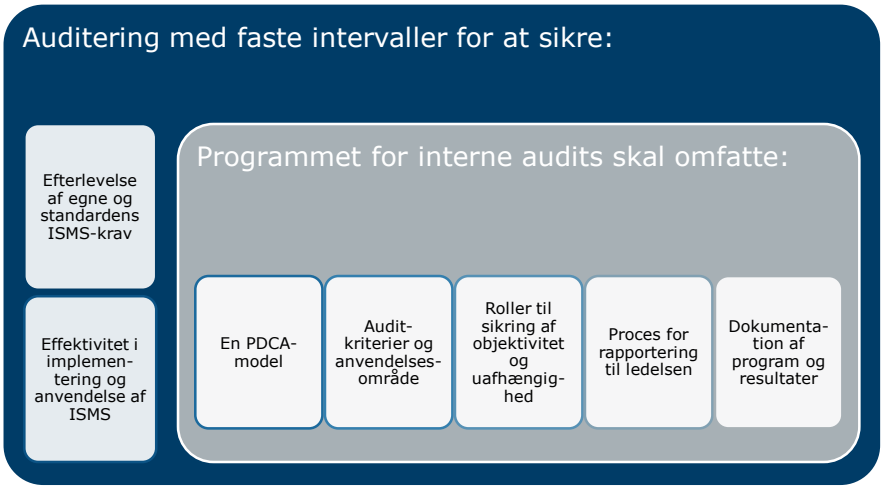
50

Måleeksempler



51

Internt audit



52

Ledelsens gennemgang

Gennemgang af ISMS med faste intervaller for at sikre:

- Egnethed
- Tilstrækkelighed
- Effektivitet

Programmet for ledelsens gennemgang skal omfatte:

- Status fra sidst
- Interne/eksterne ændringer af relevans for ISMS
- Feedback fra interessenter, resultater og trends
- Internt auditrapport
- Resultater fra risikovurdering og status på risikohåndteringsplan
- Muligheder for løbende forbedringer

53

ISO/IEC 27001 Online

Opsamling

54

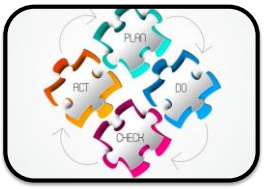
Opsummering

Vi beskytter informationer imod tab af:

- Fortrolighed, integritet og tilgængelighed

Det handler ikke blot om it-sikkerhed

- It-systemer, de fysiske rammer og medarbejdere er alle understøttende for beskyttelse af informationer



Plan, Do, Check, Act!

- Til enhver sikkerhedsforanstaltning knytter sig en proces, som vi styrer og løbende forbedrer på

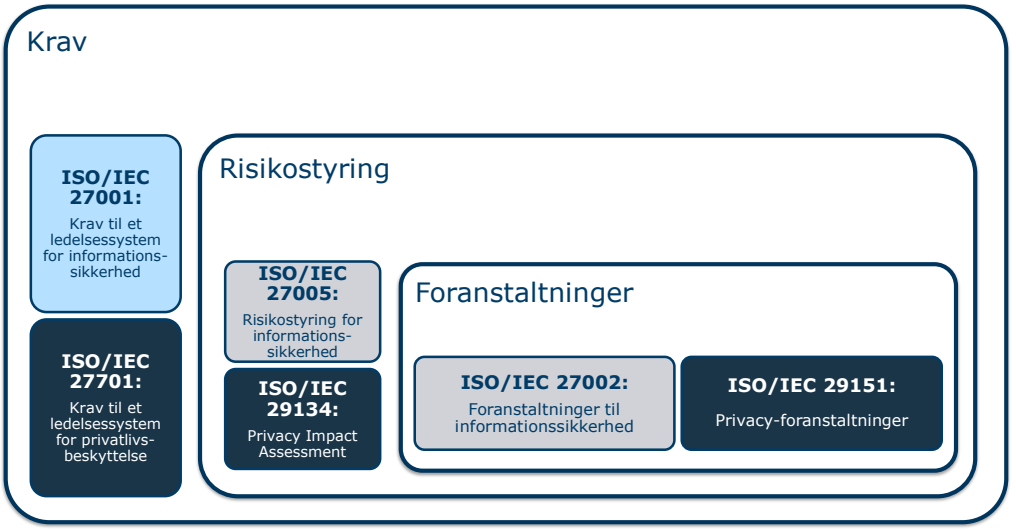
Say it, do it, prove it!

- Der forestår en paper exercise, som forklarer, hvad vi gør og som indeholder dokumentation for at, det bliver gjort

DS DANSK STANDARD

55

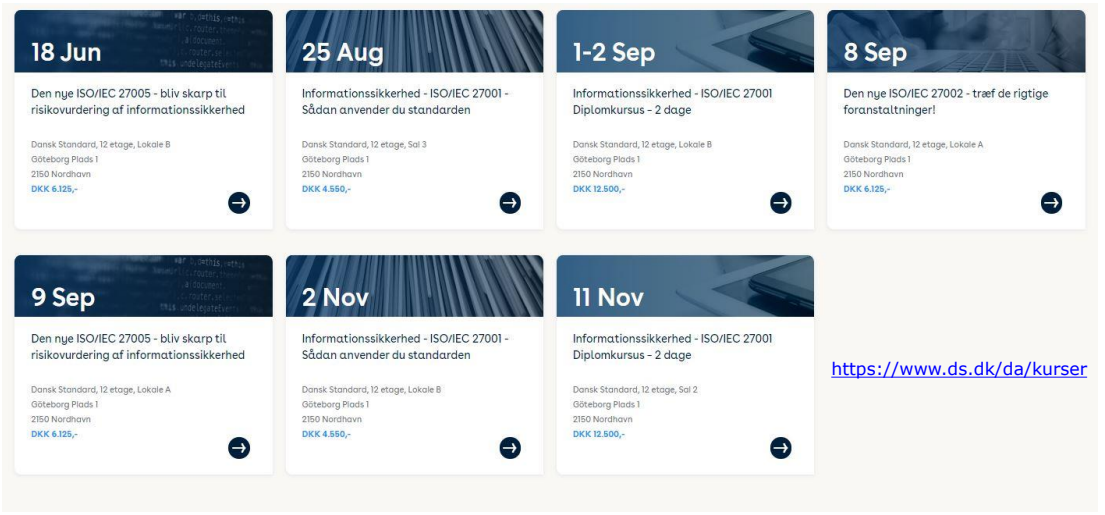
Informationssikkerhedsstandarder



DS DANSK STANDARD

56

Videre kompetenceudvikling



https://www.ds.dk/da/kurser

DS DANSK STANDARD

57

På gensyn!

Anders Linde
Tlf.: 6162 1500
E-mail: ali@ds.dk

DS DANSK STANDARD

58