

ISO/IEC 27001 Online

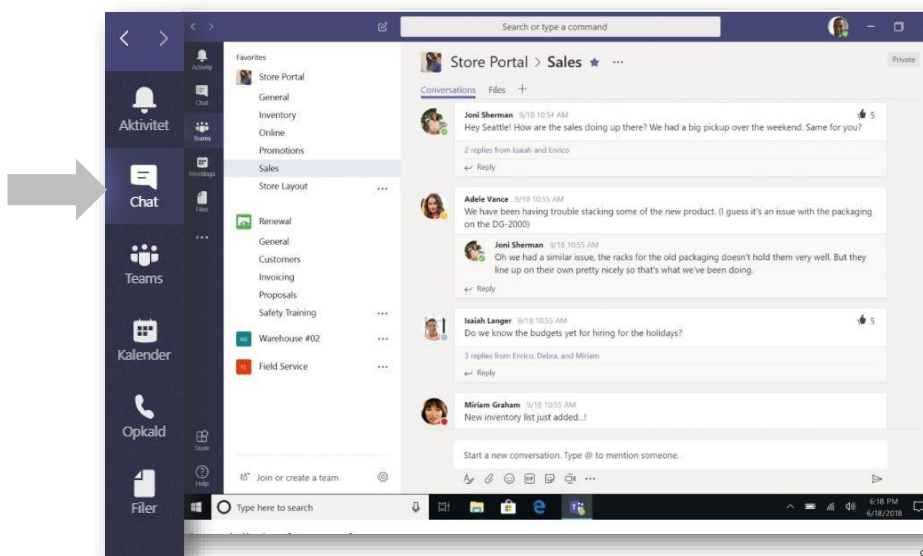
- få gratis overblik over standardens krav!

April 2020



1

Microsoft Teams: chat-funktion

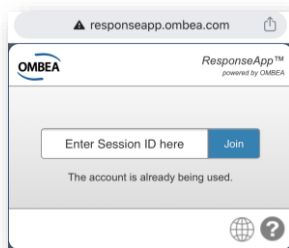


Copyright © 2020, Dansk Standard. All rights reserved

2

Ombea: Besvarelse af spørgsmål

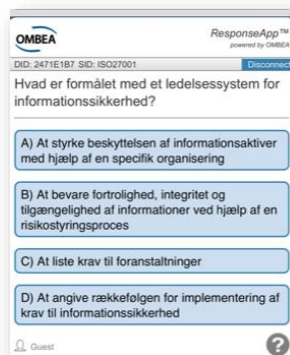
1. Åben en browser på mobiltelefon (eller pc)
2. Gå til **responseapp.ombea.com**



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



Copyright © 2020, Dansk Standard. All rights reserved

3

Agenda

ISO/IEC 27001 Online

- 13:00 Introduktion til dagsorden
- 13:10 Introduktion til ISO/IEC 27001
- 13:25 Planlægning af et ISMS
- 13:45 Risikovurdering
- 14:10 Pause
- 14:20 Risikohåndtering
- 14:35 SoA-dokument
- 14:45 Implementering af et ISMS
- 15:00 Evaluering
- 15:20 Opsamling
- 15:30 På gensyn!



Copyright © 2020, Dansk Standard. All rights reserved

4

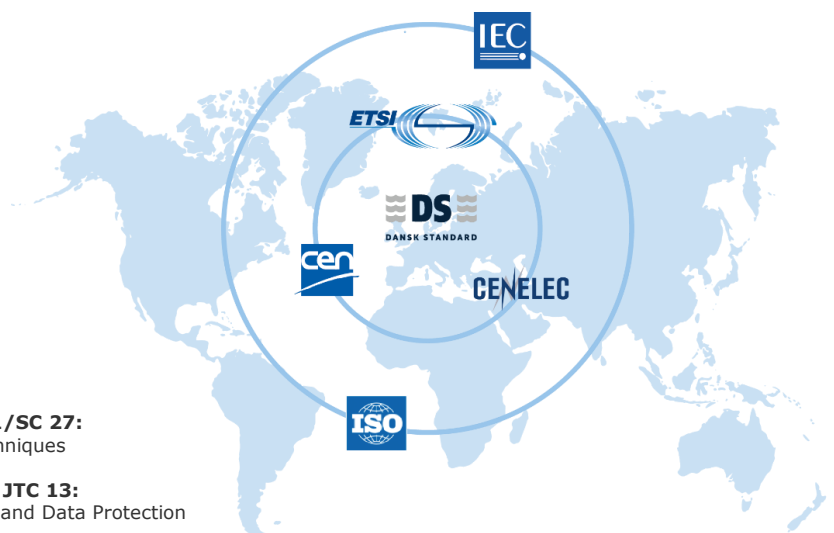
ISO/IEC 27001 Online

Introduktion til ISO/IEC 27001



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



Copyright © 2020, Dansk Standard. All rights reserved

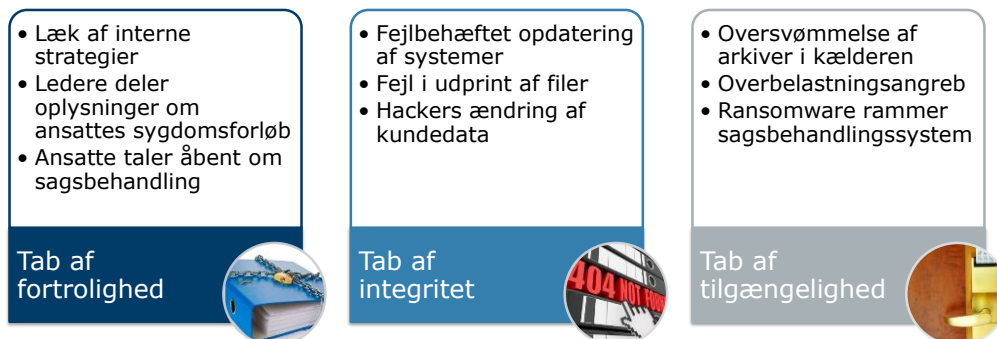
6

Informationer som skal beskyttes



7

Et ledelsessystem for informationssikkerhed



"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."

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.

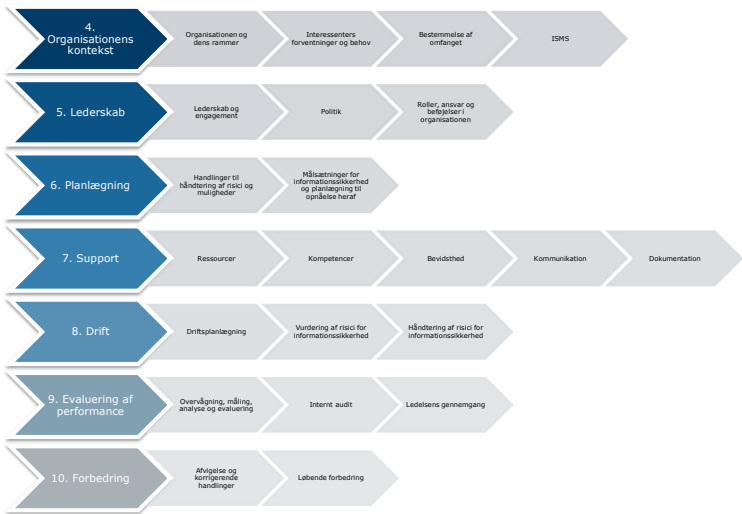


Strategi for Danmarks digitale vækst, 2018: SMV-hjælp. Privacy-kompas, Sikkerhedstjek baseret på ISO/IEC 27001. En samlet portal på sikkerdigital.dk.



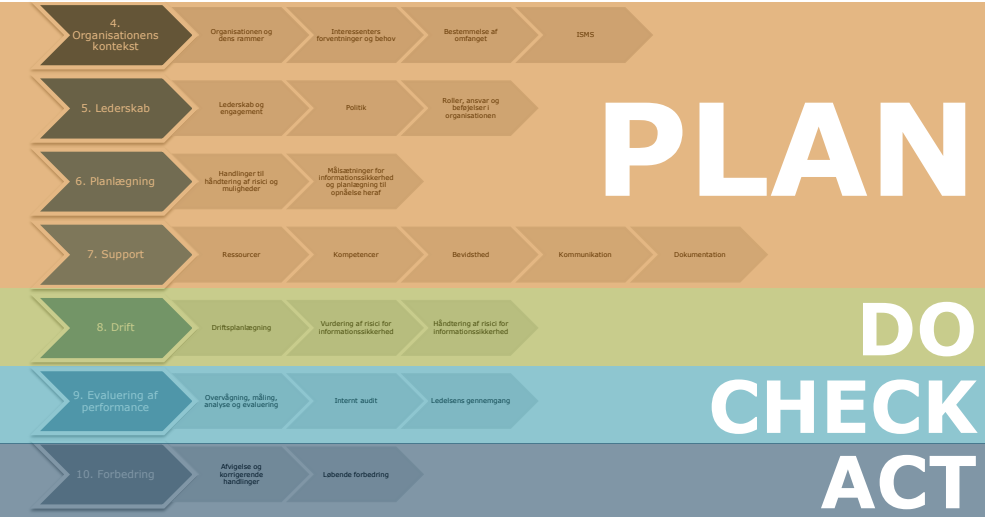
Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001 Oversigt



Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001 Oversigt



Copyright © 2020, Dansk Standard. All rights reserved



ISO/IEC 27001: Dokumentationskrav for informationssikkerhed

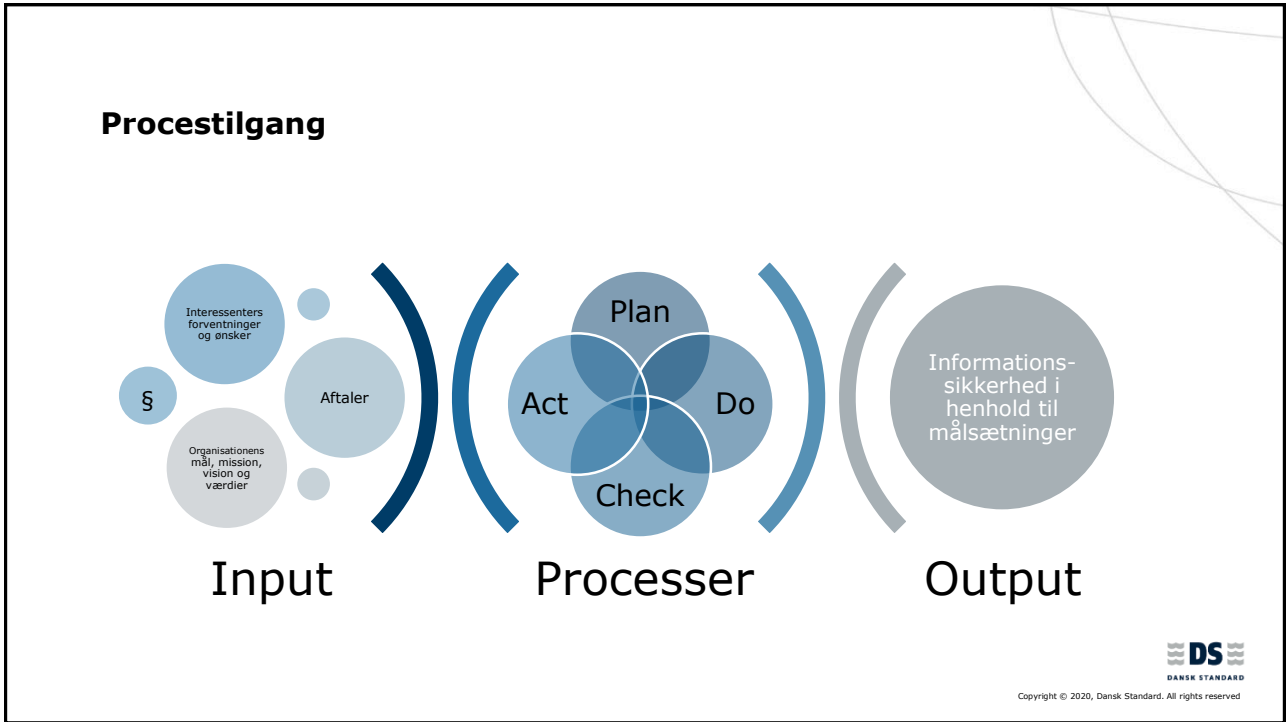
POLITIK OG MÅLSÆTNINGER (5.2; 6.2):	En dokumenteret informationssikkerhedspolitik, der indeholder målsætninger for informationssikkerhed
ANVENDELSESOMRÅDE (4.3):	En dokumenteret afgrænsning af ISMS'et
RISIKOMETODE (6.1.2):	En beskrivelse af risikovurderings- og håndteringsprocessen
RISIKOVURDERING (6.1.2, 8.2):	En risikovurderingsrapport
RISIKOHÅNTERINGSPLAN (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 auditeringer
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

Copyright © 2020, Dansk Standard. All rights reserved



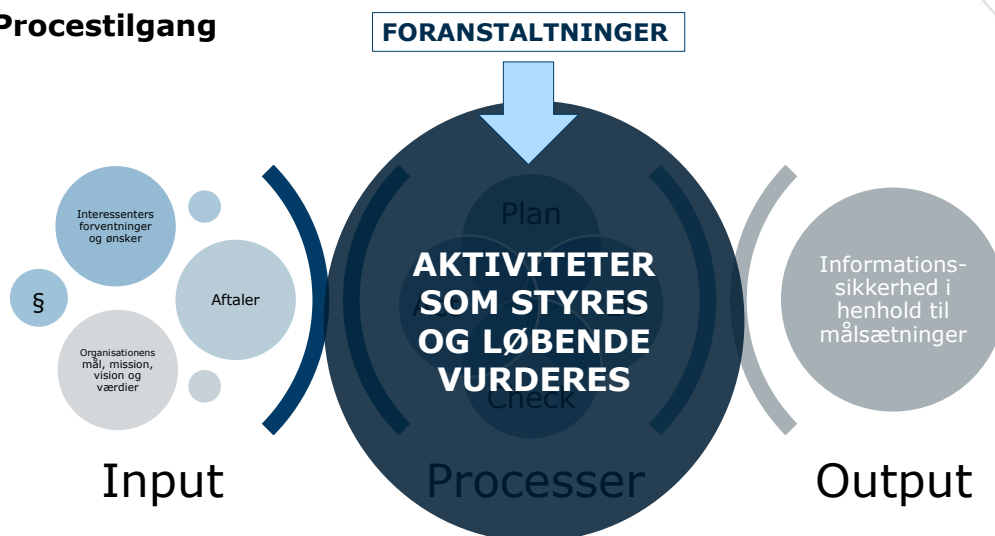


13



14

Procestilgang



15

5 råd ved implementering



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

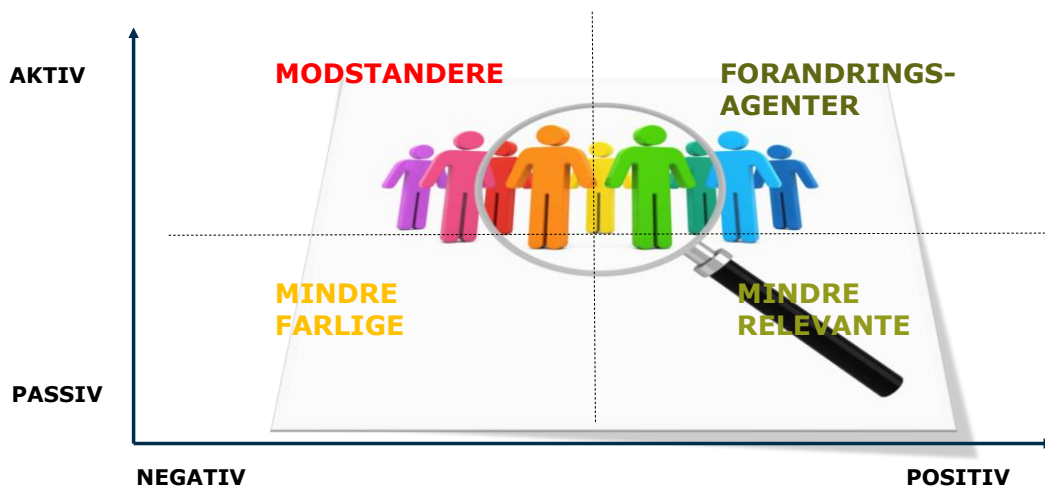
16

Organisationens karakteristika

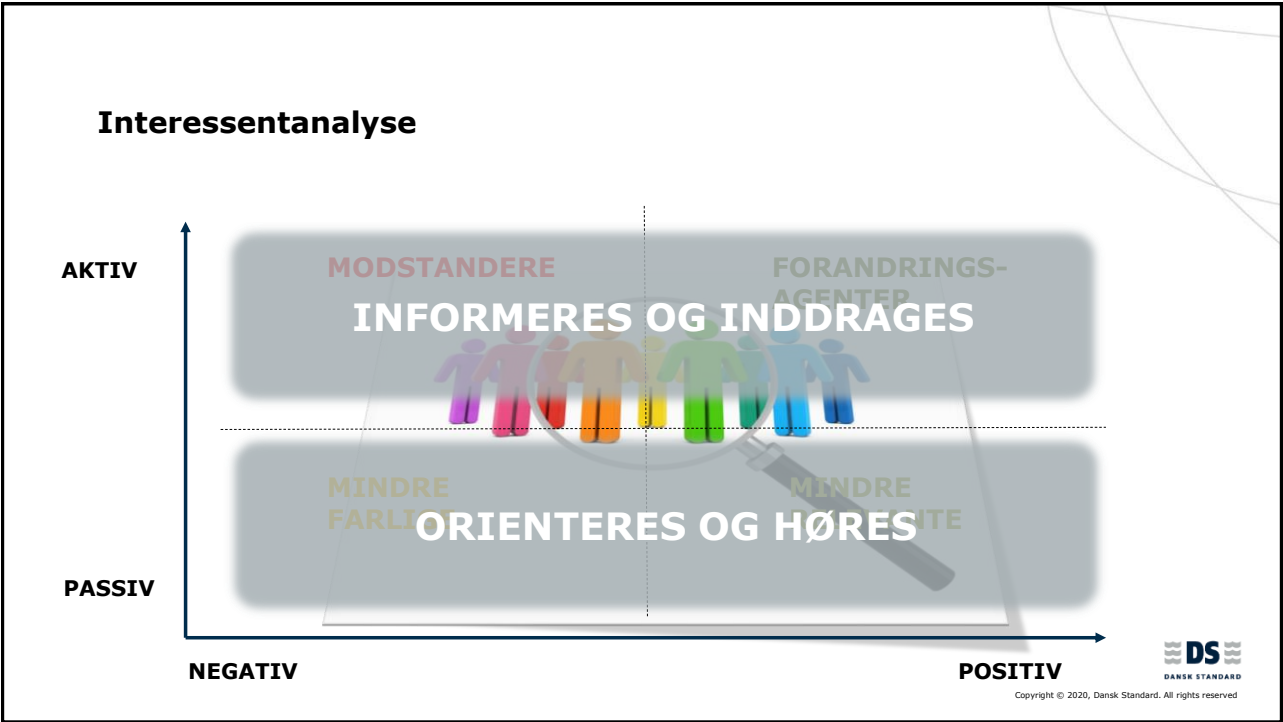


17

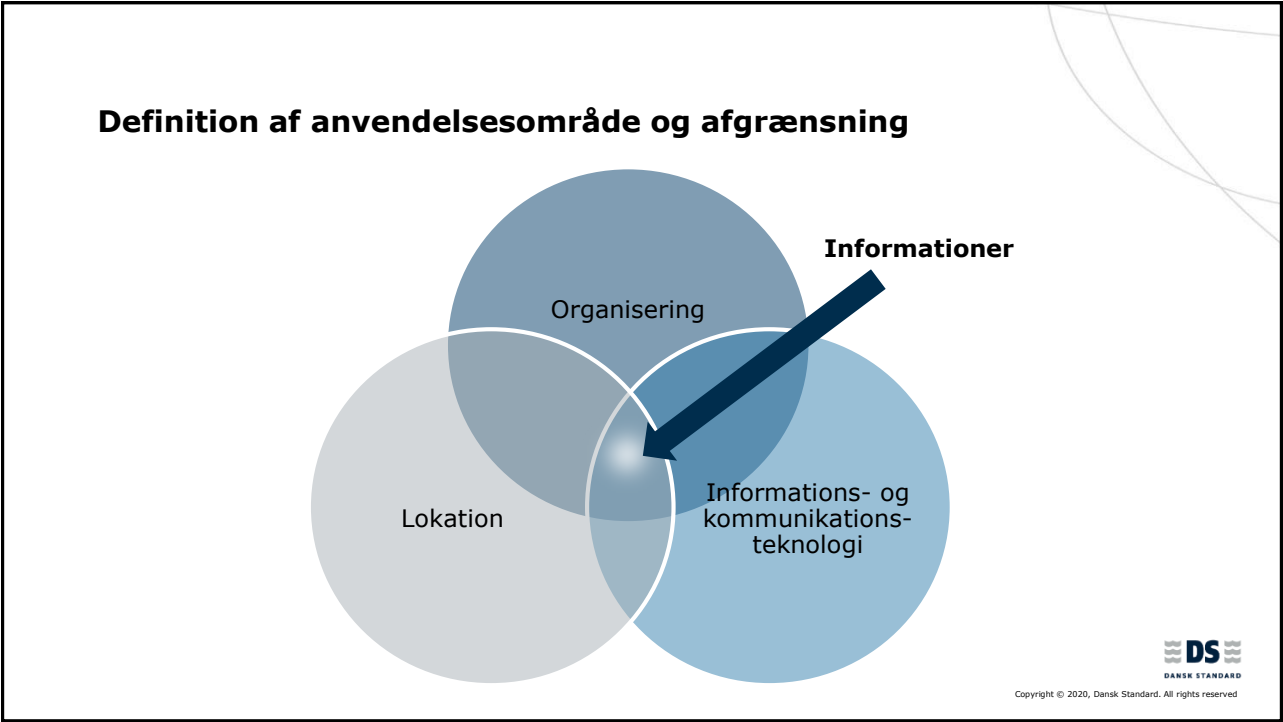
Interessentanalyse



18

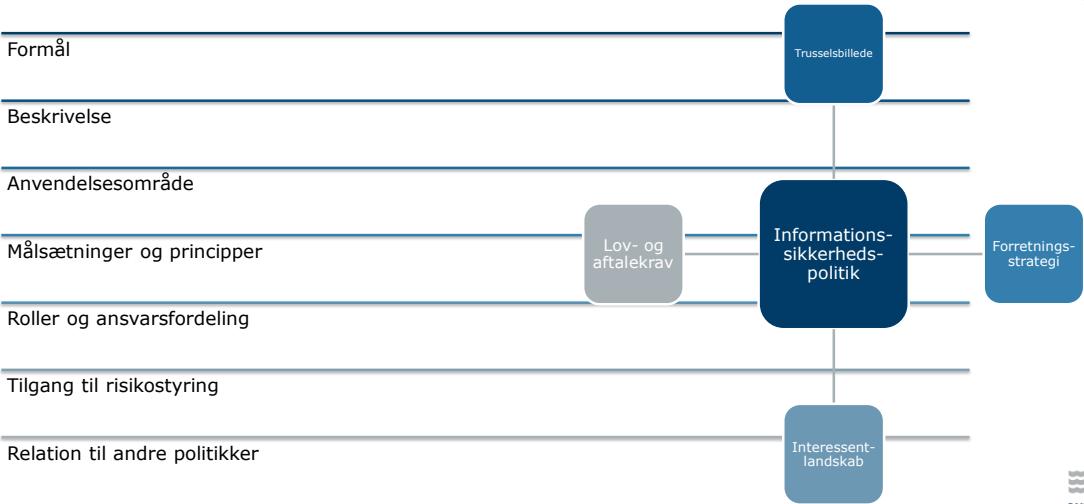


19



20

Beskrivelse af politik for informationssikkerhed

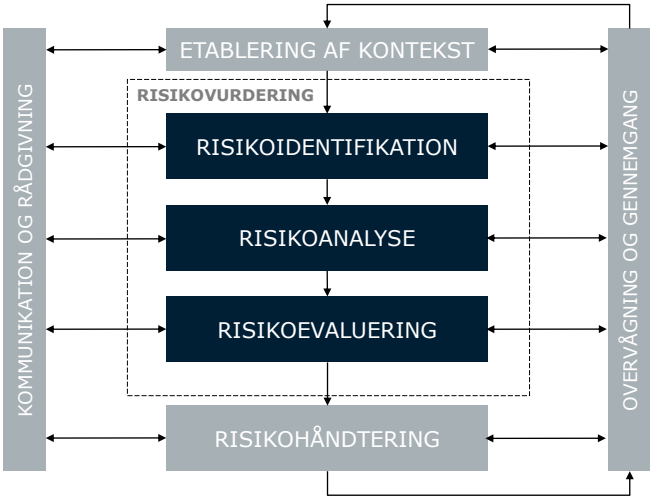


Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001 Online
Risikovurdering

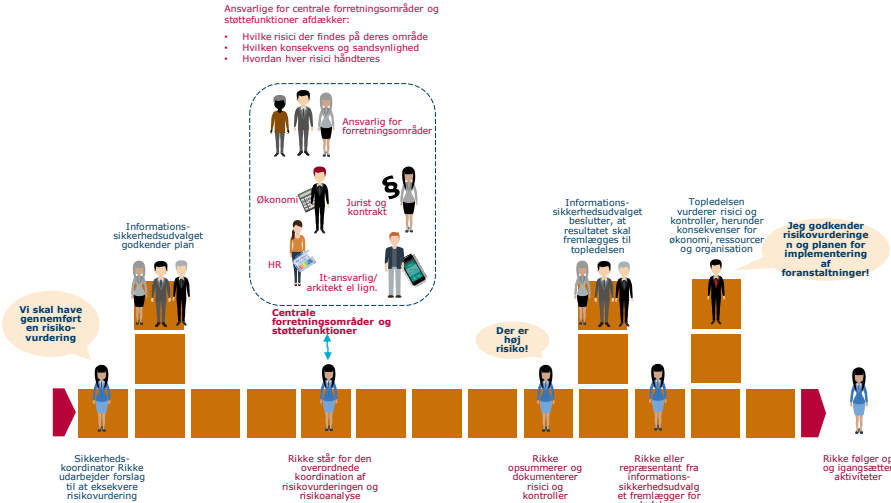


Risikovurdering, jf. ISO/IEC 27005



Copyright © 2020, Dansk Standard. All rights reserved

Organisering af risikostyringsproces



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

Copyright © 2020, Dansk Standard. All rights reserved

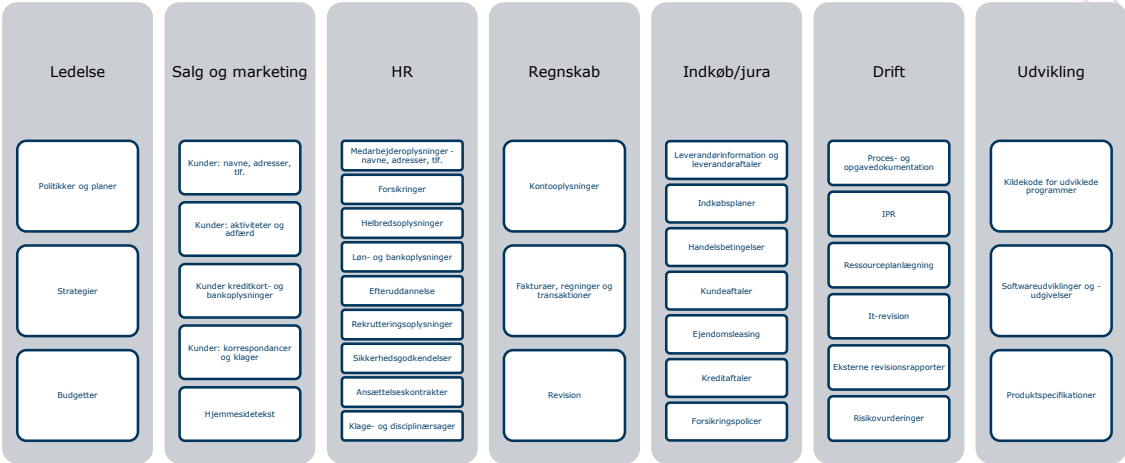
Risikovurdering



Copyright © 2020, Dansk Standard. All rights reserved

25

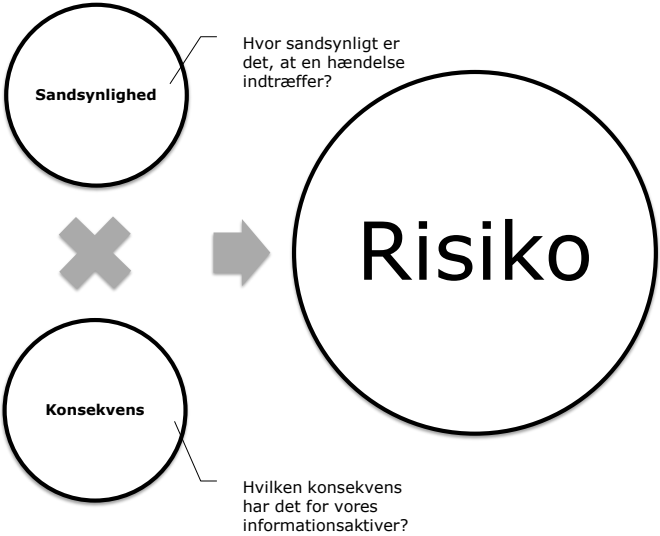
Udpegning af informationer



Copyright © 2020, Dansk Standard. All rights reserved

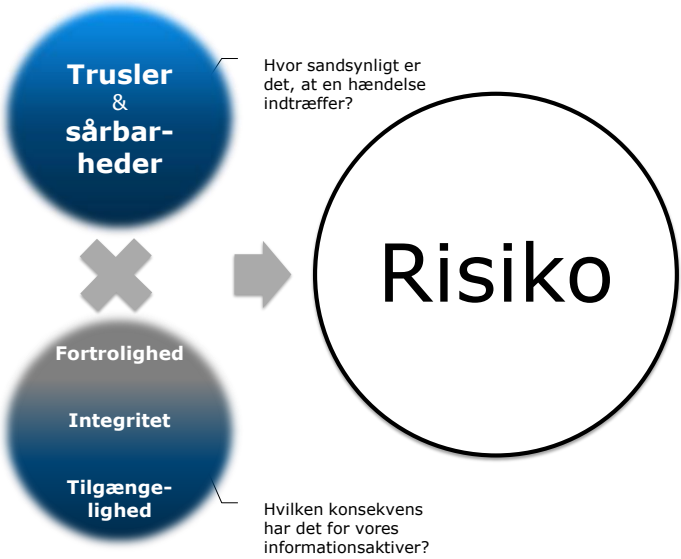
26

Risikometode



27

Risikometode



28

Risikoevaluering

TRUSSEL Scenarie	SANDSYNLIGHED Trussel + sårbarhed	KONSEKVENNS 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



Copyright © 2020, Dansk Standard. All rights reserved

29

Risikoevaluering

		SANDSYNLIGHED FOR SCENARIO				
		Meget usandsynligt	Usandsynligt	Muligt	Sandsynligt	Meget sandsynligt
KONSEKVENNS 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



Copyright © 2020, Dansk Standard. All rights reserved

30

ISO/IEC 27001 Online

Pause – vi starter igen 14:20



31

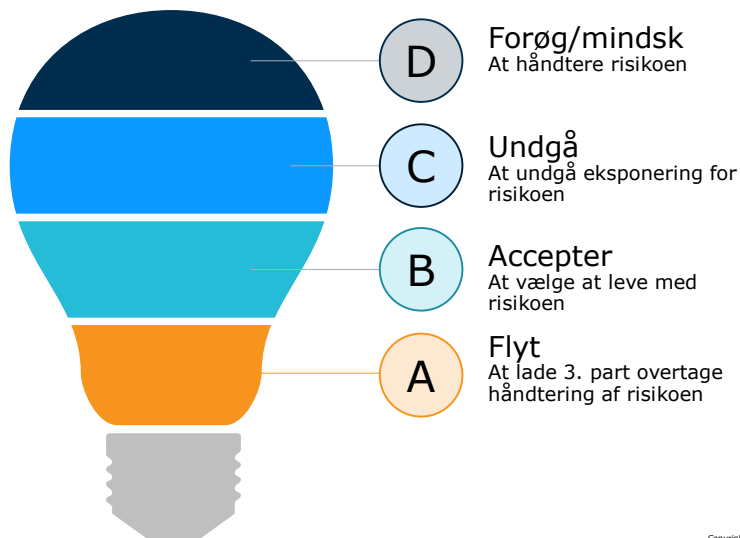
ISO/IEC 27001 Online

Risikohåndtering



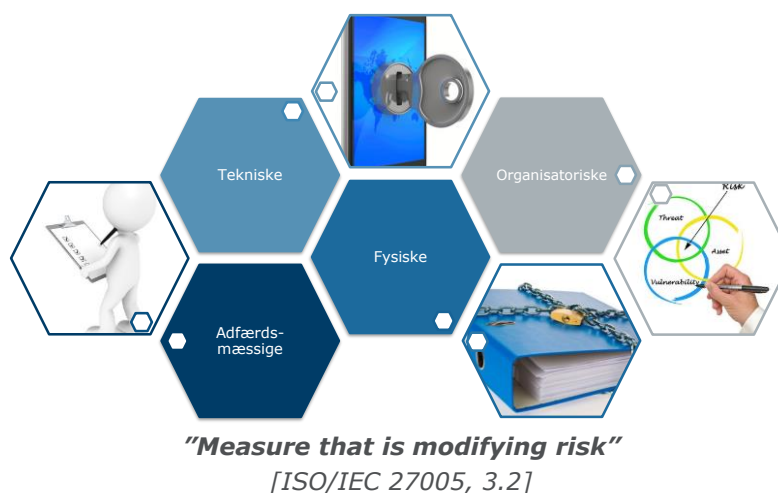
32

Risikohåndtering: valgmuligheder



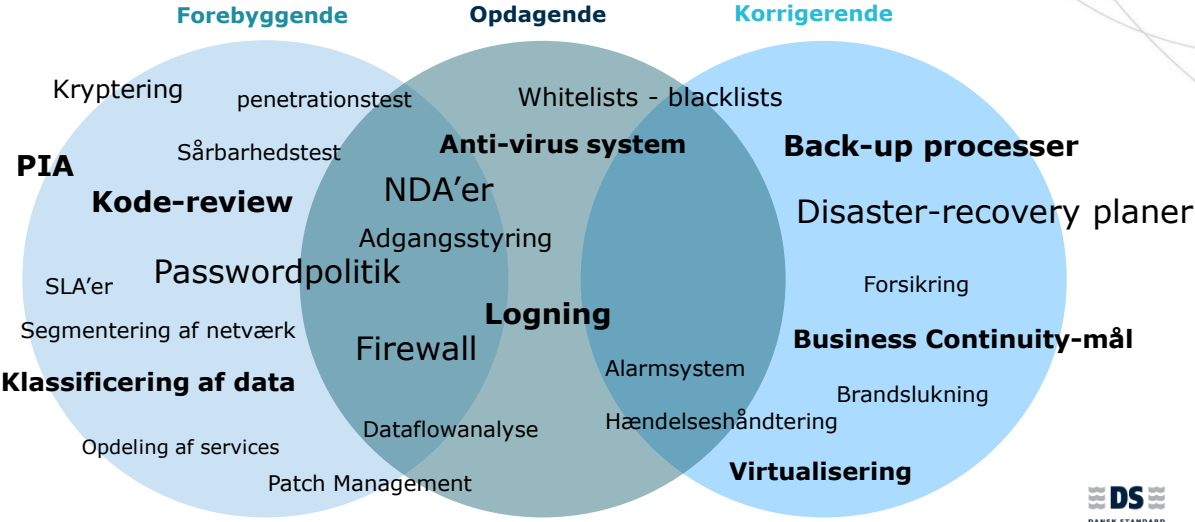
33

Foranstaltninger - typer



34

Foranstaltninger - kategorier



35

ISO/IEC 27001 Online

SoA-dokument

36

Statement of Applicability (SoA)

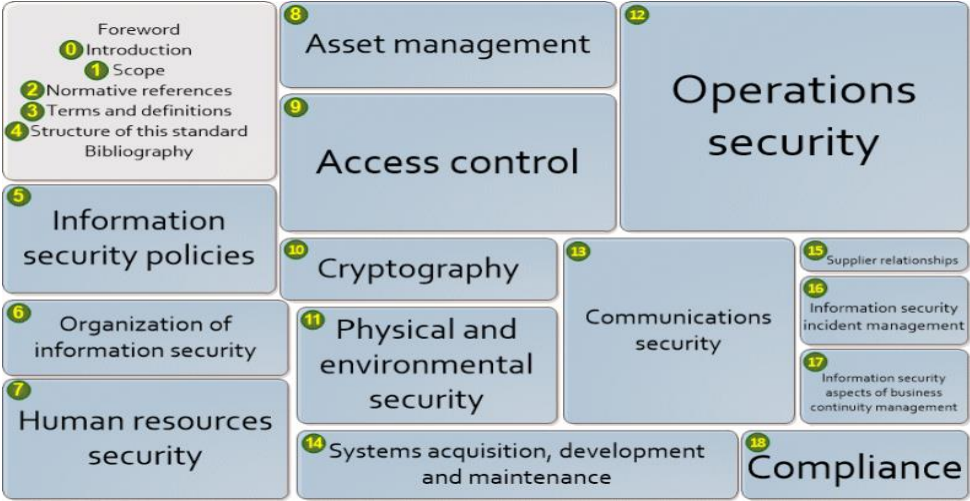
STATEMENT OF APPLICABILITY	
OBJECTIVE The Statement of Applicability is a requirement of ISO/IEC 27001, as specified in clause 8.2.14 of ISO 27001, and is a document that describes the scope of the Information Security Management System (ISMS) and the controls that are selected to meet the requirements of the ISMS. It is a document that is used to demonstrate the effectiveness of the ISMS and to provide evidence of the ISMS's performance.	
Reference	Application or Not Applicable
8.2.14	Yes
8.2.15	Yes
8.2.16	Yes
8.2.17	Yes
8.2.18	Yes
8.2.19	Yes
8.2.20	Yes
8.2.21	Yes
8.2.22	Yes
8.2.23	Yes
8.2.24	Yes
8.2.25	Yes
8.2.26	Yes
8.2.27	Yes
8.2.28	Yes
8.2.29	Yes
8.2.30	Yes
8.2.31	Yes
8.2.32	Yes
8.2.33	Yes
8.2.34	Yes
8.2.35	Yes
8.2.36	Yes
8.2.37	Yes
8.2.38	Yes
8.2.39	Yes
8.2.40	Yes
8.2.41	Yes
8.2.42	Yes
8.2.43	Yes
8.2.44	Yes
8.2.45	Yes
8.2.46	Yes
8.2.47	Yes
8.2.48	Yes
8.2.49	Yes
8.2.50	Yes
8.2.51	Yes
8.2.52	Yes
8.2.53	Yes
8.2.54	Yes
8.2.55	Yes
8.2.56	Yes
8.2.57	Yes
8.2.58	Yes
8.2.59	Yes
8.2.60	Yes
8.2.61	Yes
8.2.62	Yes
8.2.63	Yes
8.2.64	Yes
8.2.65	Yes
8.2.66	Yes
8.2.67	Yes
8.2.68	Yes
8.2.69	Yes
8.2.70	Yes
8.2.71	Yes
8.2.72	Yes
8.2.73	Yes
8.2.74	Yes
8.2.75	Yes
8.2.76	Yes
8.2.77	Yes
8.2.78	Yes
8.2.79	Yes
8.2.80	Yes
8.2.81	Yes
8.2.82	Yes
8.2.83	Yes
8.2.84	Yes
8.2.85	Yes
8.2.86	Yes
8.2.87	Yes
8.2.88	Yes
8.2.89	Yes
8.2.90	Yes
8.2.91	Yes
8.2.92	Yes
8.2.93	Yes
8.2.94	Yes
8.2.95	Yes
8.2.96	Yes
8.2.97	Yes
8.2.98	Yes
8.2.99	Yes
8.2.100	Yes

- 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



Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001, Anneks A

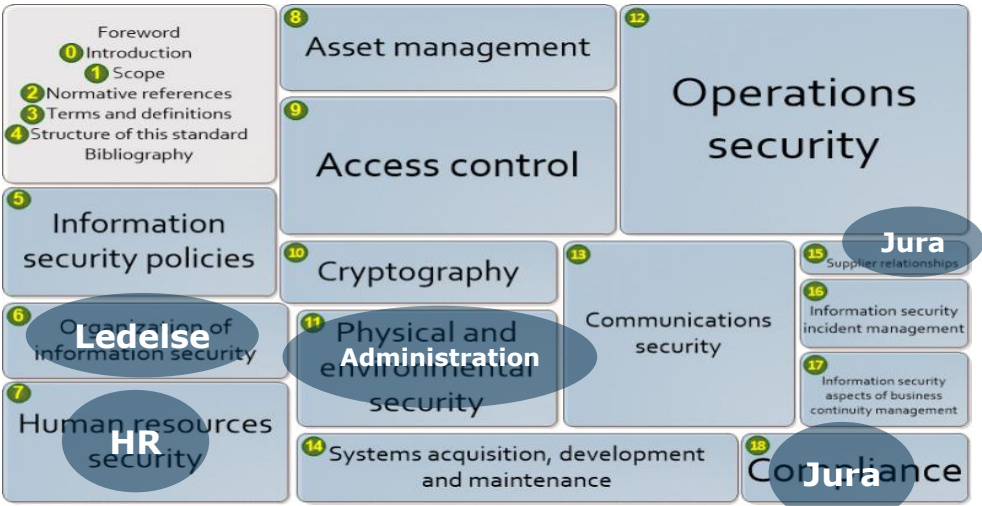


<http://www.iso27001security.com/html/27002.html>



Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001, Anneks A



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

Copyright © 2020, Dansk Standard. All rights reserved

39

Eksempel på SoA-struktur

FORANSTALTNING		TIL- FRAVALGT?	BESKRIVELSE	BEGRUNDELSE	ANSVARLIG	REF. TIL DOKUMENTATION
Område	Afsnit	Kontrol	best practice Valg jf. risikovurdering Lovgivning o.lign.	Planlagt ny/under forbedring I drift 1 drift og evalueres i forbedringsproces	- PL - DR - EV	
Informationssikkerheds- politikker	A.5 Informationssikkerhedspolitikker					
	5.1 Retningslinjer for styring af informationssikkerhed					
	5.1.1	Politikker for informationssikkerhed				
Organisering af informationssikkerhed	5.1.2	Gennemgang af politikker for informationssikkerhed				
	A.6 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 projektsstyring				
	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

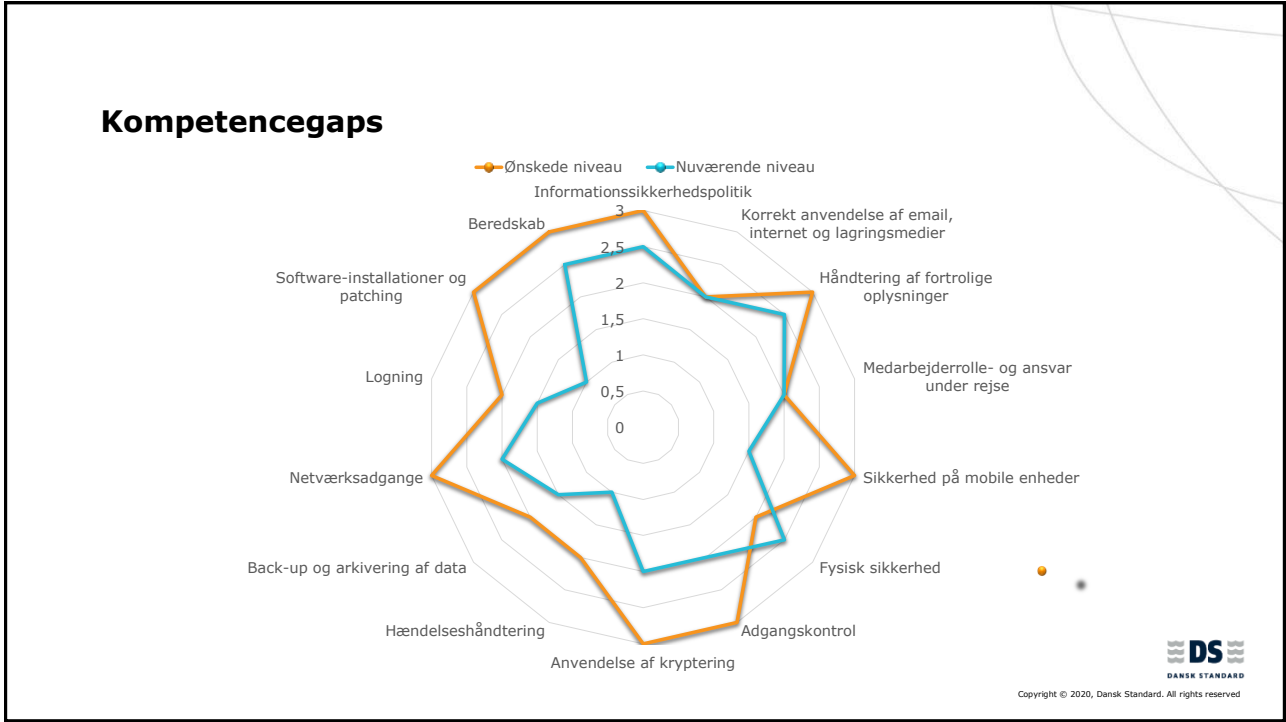
Copyright © 2020, Dansk Standard. All rights reserved

40

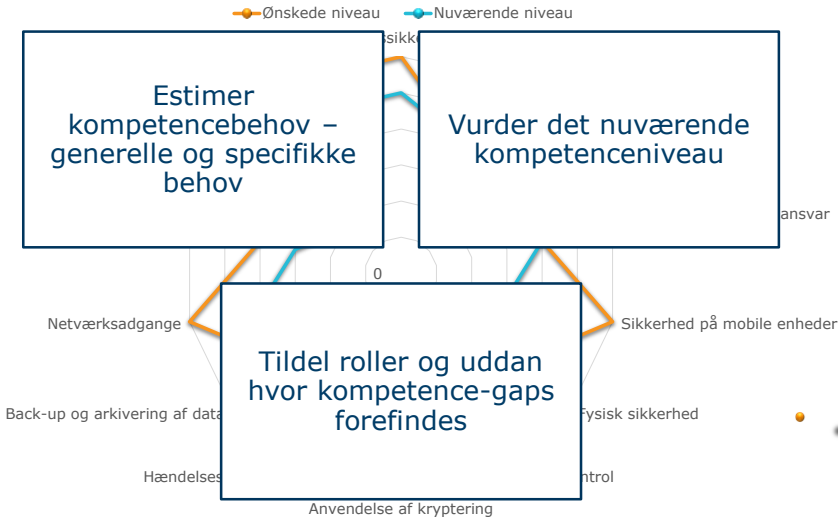
ISO/IEC 27001 Online

Implementering af et ISMS


DANSK STANDARD



Kompetencegaps



43

Awareness



1. Kende politikken for informationssikkerhed



2. Deres bidrag til organisationens informationssikkerhed



3. Konsekvenserne af ikke at efterleve kravene

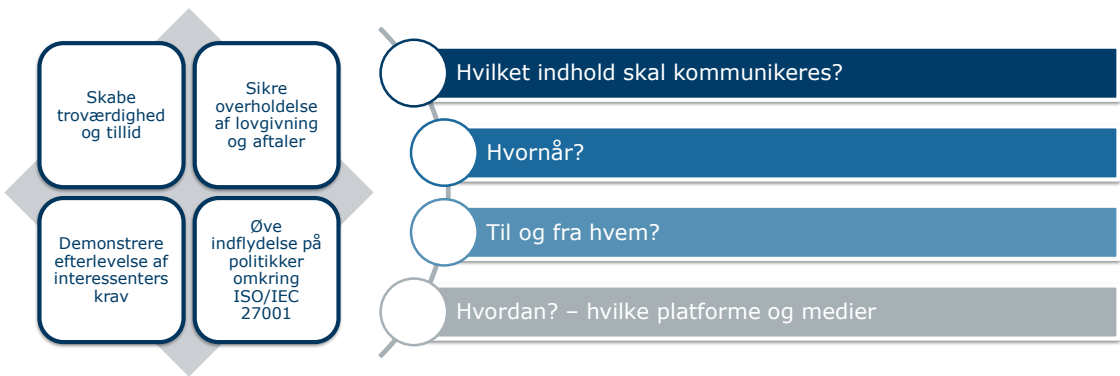
44

Redskaber



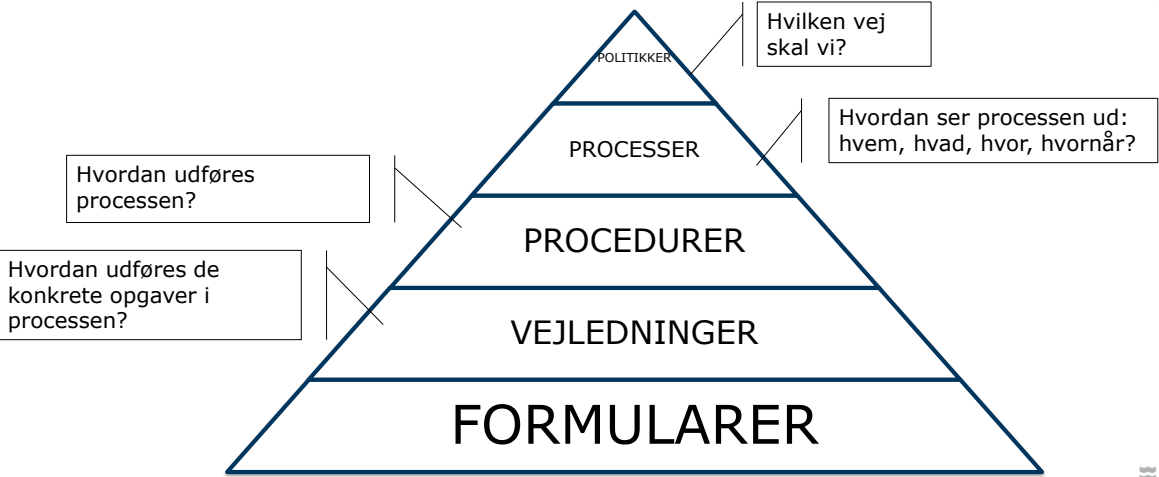
Copyright © 2020, Dansk Standard. All rights reserved

Kommunikationsplan

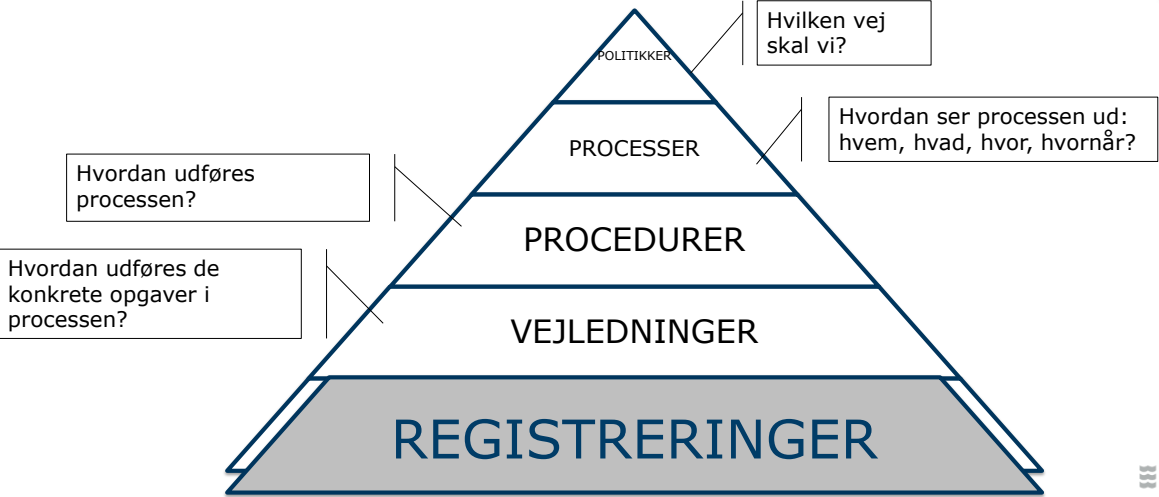


Copyright © 2020, Dansk Standard. All rights reserved

The paper exercise

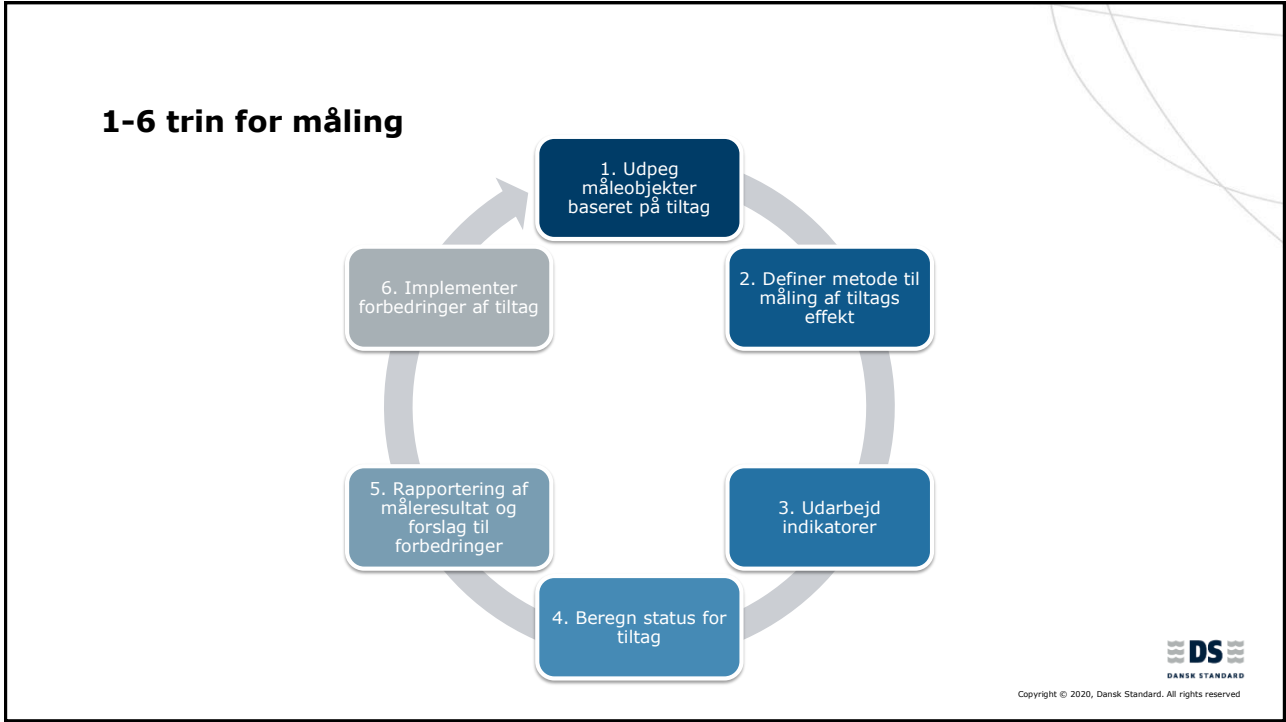


The paper exercise



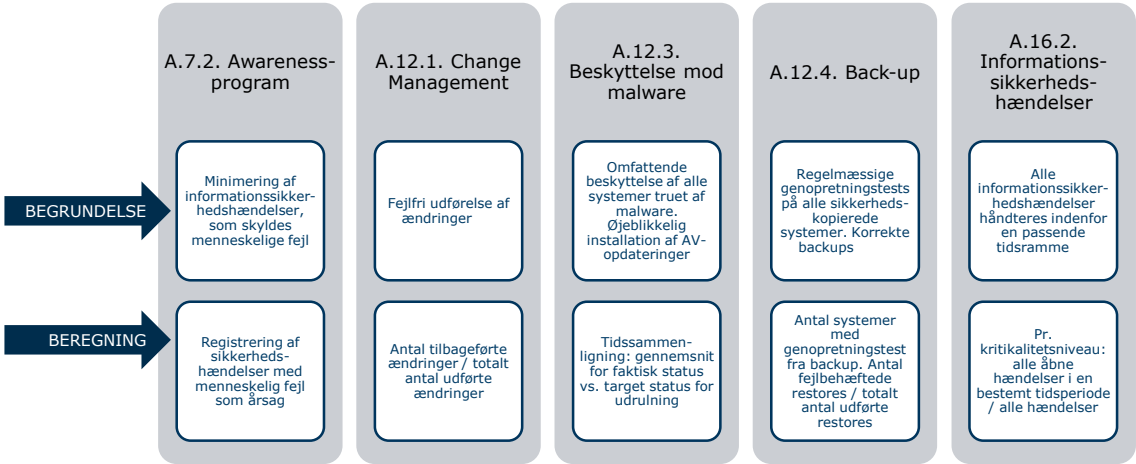


49



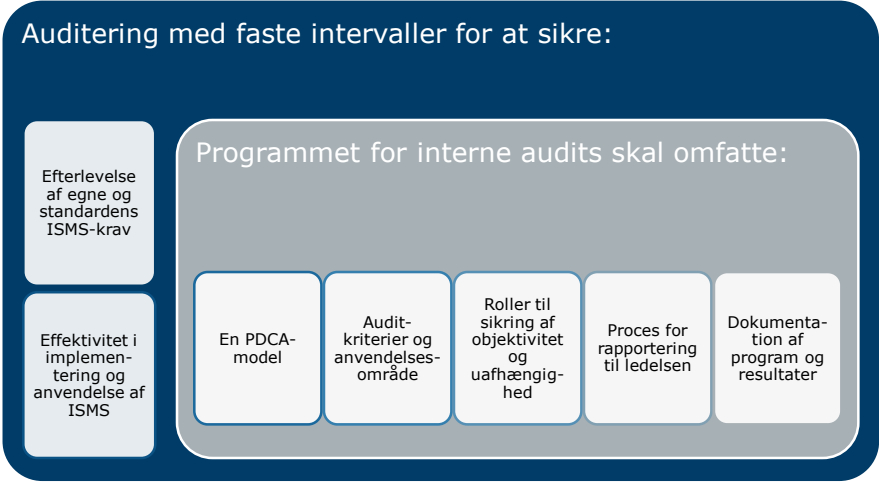
50

Måleeksempler



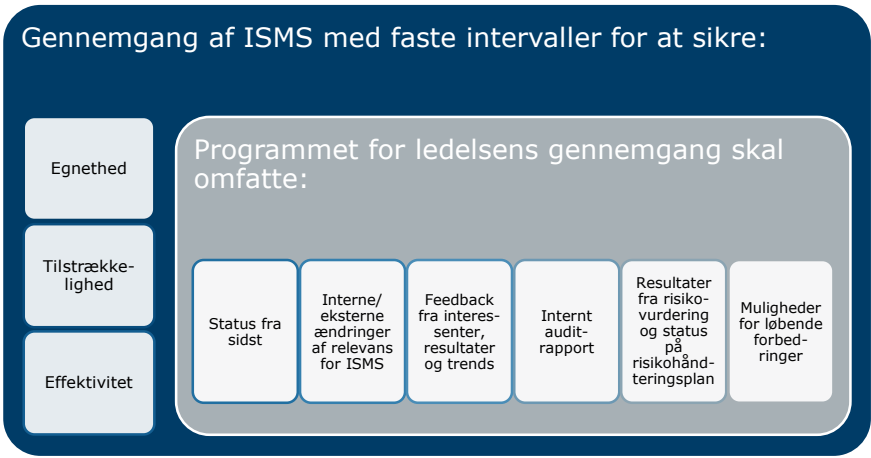
Copyright © 2020, Dansk Standard. All rights reserved

Internt audit



Copyright © 2020, Dansk Standard. All rights reserved

Ledelsens gennemgang



Copyright © 2020, Dansk Standard. All rights reserved

ISO/IEC 27001 Online

Opsamling

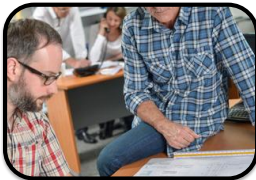


Opsummering



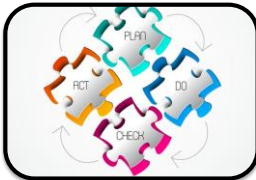
Vi beskytter informationer imod tab af:

- 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

Informationssikkerhedsstandarder

Krav

ISO/IEC 27001:

Krav til et ledelsessystem for informations-sikkerhed

ISO/IEC 27701:

Krav til et ledelsessystem for persondata-beskyttelse

Risikostyring

ISO/IEC 27005:

Risikostyring for informations-sikkerhed

ISO/IEC 29134:

Privacy Impact Assessment

Foranstaltninger

ISO/IEC 27002:

Foranstaltninger til informationssikkerhed

ISO/IEC 29151:

Privacy-foranstaltninger

Videre kompetenceudvikling

18 Jun

Den nye ISO/IEC 27005 - bliv skarp til risikovurdering af informationssikkerhed

Dansk Standard, 12 etage, Lokale B
Göteborg Plads 1
2150 Nordhavn
DKK 6.125,-



25 Aug

Informationssikkerhed - ISO/IEC 27001 - Sådan anvender du standarden

Dansk Standard, 12 etage, Sal 3
Göteborg Plads 1
2150 Nordhavn
DKK 4.850,-



1-2 Sep

Informationssikkerhed - ISO/IEC 27001
Diplomkursus - 2 dage

Dansk Standard, 12 etage, Lokale B
Göteborg Plads 1
2150 Nordhavn
DKK 12.500,-



8 Sep

Den nye ISO/IEC 27002 - træf de rigtige foranstaltninger!

Dansk Standard, 12 etage, Lokale A
Göteborg Plads 1
2150 Nordhavn
DKK 6.125,-



9 Sep

Den nye ISO/IEC 27005 - bliv skarp til risikovurdering af informationssikkerhed

Dansk Standard, 12 etage, Lokale A
Göteborg Plads 1
2150 Nordhavn
DKK 6.125,-



2 Nov

Informationssikkerhed - ISO/IEC 27001 - Sådan anvender du standarden

Dansk Standard, 12 etage, Lokale B
Göteborg Plads 1
2150 Nordhavn
DKK 4.850,-



11 Nov

Informationssikkerhed - ISO/IEC 27001
Diplomkursus - 2 dage

Dansk Standard, 12 etage, Sal 2
Göteborg Plads 1
2150 Nordhavn
DKK 12.500,-



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



Copyright © 2020, Dansk Standard. All rights reserved

57

På gensyn!

Anders Linde

Tlf.: 6162 1500

E-mail: ali@ds.dk



58