Hvordan gjøre en risikoanalyse? - Slik starter du med ISO 27001

Roger Ison-Haug

PEDAB

Her er vi

- 26 års erfaring
- 9 land
- omsetning 2018: 1,4 mrd nok
- Vekst: 24,2% y/y
- 130 ansatte

3 FOKUSOMRÅDER

INFRASTRUCTURE

SECURITY

DATA & ANALYTICS

Hvordan overleve et cyberangrep?

- Velg en metode - Jobb mot en standard

    1. ISO / IEC sikkerhetskontrollstandarder
    2. FFIEC Cybersecurity Assessment
    3. SEC / OCIE Cybersecurity Initiative
    4. FCC Cyber Security Planning Guide
    5. NIST Cybersecurity Framework

Hvorfor velge en standard

jobb mot noe som er velprøvd

- ✓ Overblikk – sikrer at alt og alle er med
- ✓ Strukturert tilgang – ingenting glemmes
- ✓ Klar kommunikasjon – på tvers av hele organisasjonen, samt opp til styre
- ✓ Transparens vedrørende risiko om de beslutninger som tas
- ✓ Gjennomprøvde prosesser og beste praksis
- ✓ Tilbakevendende trening og bevisstgjøring
- ✓ Identifisering av hvilke oppgaver som skal løses in-house og de som kan flyttes ut
- ✓ Sertifisering så samarbeidspartnere kan forholde seg til deres sikkerhetssystem/-tankesett

ISO 27001 - *NS-EN ISO/IEC 27001:2017*

ISO 27001 er en spesifikasjon for et informasjonssikkerhetsstyringssystem (ISMS).

Et ISMS er et rammeverk av retningslinjer og prosedyrer som inkluderer alle juridiske, fysiske og tekniske kontroller involvert i en organisasjons informasjonssikkerhetsstyringsprosesser.

Faser i en 27001 implementasjon

1. Identifiser målene for virksomheten din
2. Få ledelsens støtte
3. Definer omfanget
4. Skriv en kort ISMS policy (Information Security Management System)
5. Definer risiko vurderingsmetode & strategi
6. Opprett en risikohåndteringsplan, håndter disse risikoene
7. Definer policyer og prosedyrer for å kontrollere risikoer
8. Tildele nødvendige ressurser samt gjennomfør opplæring og lag et oppfølgingsprogram
9. Kontinuerlig overvåke ISMS
10. Forbered deg på en intern revisjon
11. Periodisk ledelsesgjennomgang

ISO

Bruk PDCA-syklusen for å sikre kontinuerlig forbedring av QMS

ACT

Ta tak i avvik

Korrigerende tiltak

Risikostyring

PLAN

Vedlikehold QMS

Dokumenter QMS

Ledelse og lederskap

Legg planer

Fordel resurser

Kontroller styrings- og måleparametere

CHECK

Ledelsesanmeldelser

Måling og monitorering

Kundetilfredshet

Internrevisjon

Dataanalyse

DO

Sikre rett kompetanse

Designe, utvikle og realisere

Innkjøp

Produkt- og tjenestebestemmelser

ROS analyser

- Gjør analyser for delområder
- Aggreger opp til en overordnet analyse for hvert hovedområde
- Repeter prosessen med faste intervaller
- Juster din SOA etter din risiko

(statement of applicability/ anvendelighetserklæring)

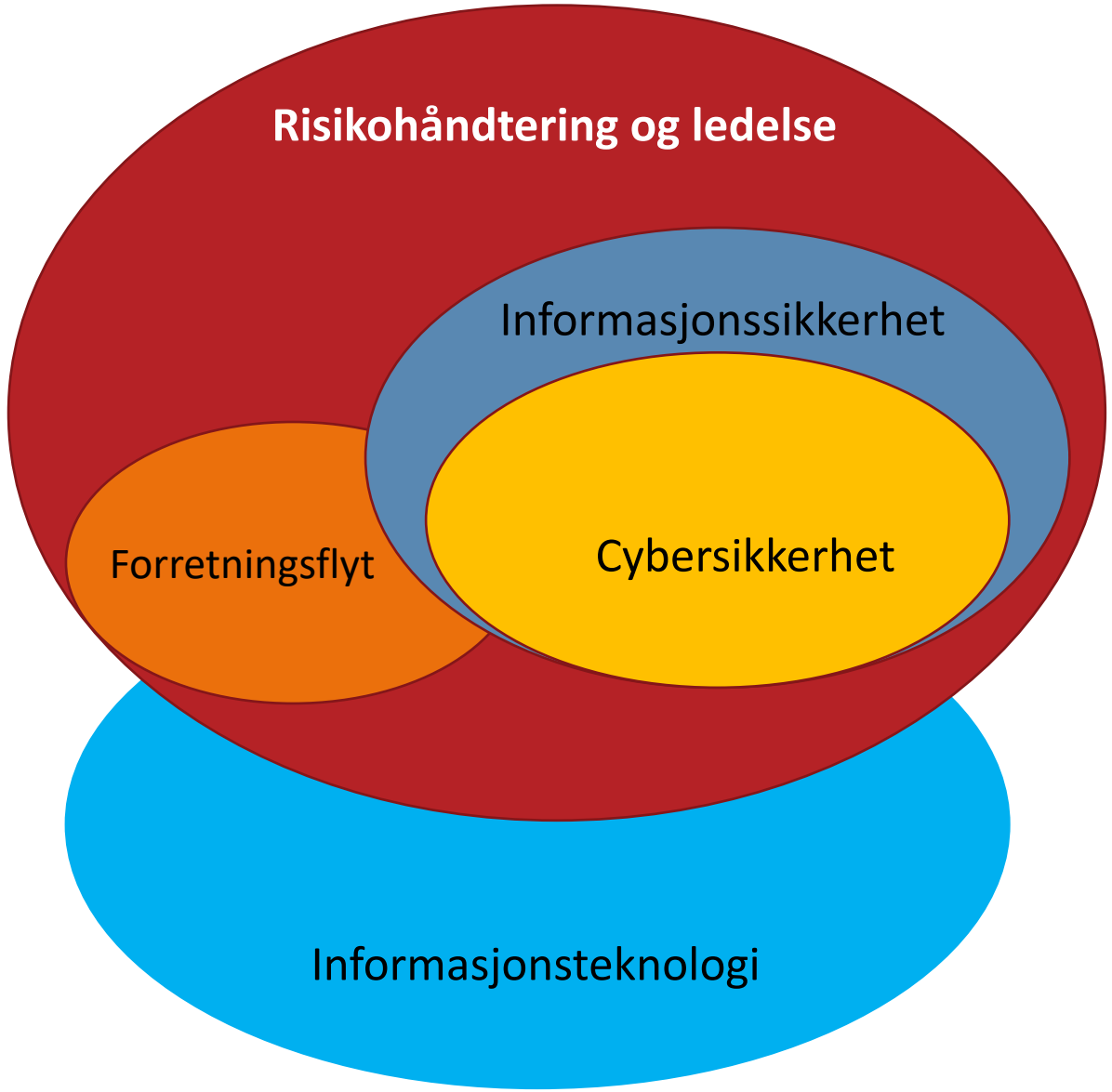
Konsekvens – hva er maksimal tenkelig konsekvens

Sannsynlighet

	Ubetydelig	Liten	Moderat	Stor	Katastrofe
Nesten sikkert	Medium	Medium	Høy	Ekstrem	Ekstrem
Trolig	Lav	Medium	Medium	Høy	Ekstrem
Mulig	Lav	Lav	Medium	Høy	Høy
Usannsynlig	Lav	Lav	Lav	Medium	Høy
Sjelden	Lav	Lav	Lav	Lav	Medium

Hva er ISO 27001

- Risikohåndtering og ledelse
- Informasjonssikkerhet
- Cybersikkerhet
- Forretningsflyt
- Informasjonsteknologi



Juster din SOA etter din risiko og dine behov

statement of applicability /anvendelighetserklæring

5. Informasjonssikkerhetspolicyer
6. Organisering av informasjonssikkerhet
7. Personellsikkerhet
8. Forvaltning av aktiva
9. Aksesskontroll
10. Kryptografi
11. Fysisk og miljø
12. Driftssikkerhet
13. Kommunikasjonssikkerhet
14. Anskaffelse, utvikling og vedlikehold av systemer
15. Leverandørforhold
16. Styring av informasjonssikkerhetsbrudd
17. Informasjonssikkerhetsaspekter ved styring av virksomhetskontinuitet
18. Samsvar

LK=Krav i lov eller forskrift.
KK= Kontraktuelle krav.
ISO: Obligatoriske krav i ISO 27001
RA: Etter etter risikoanalyse.

ISO 27001 Anvendelighetserklæring

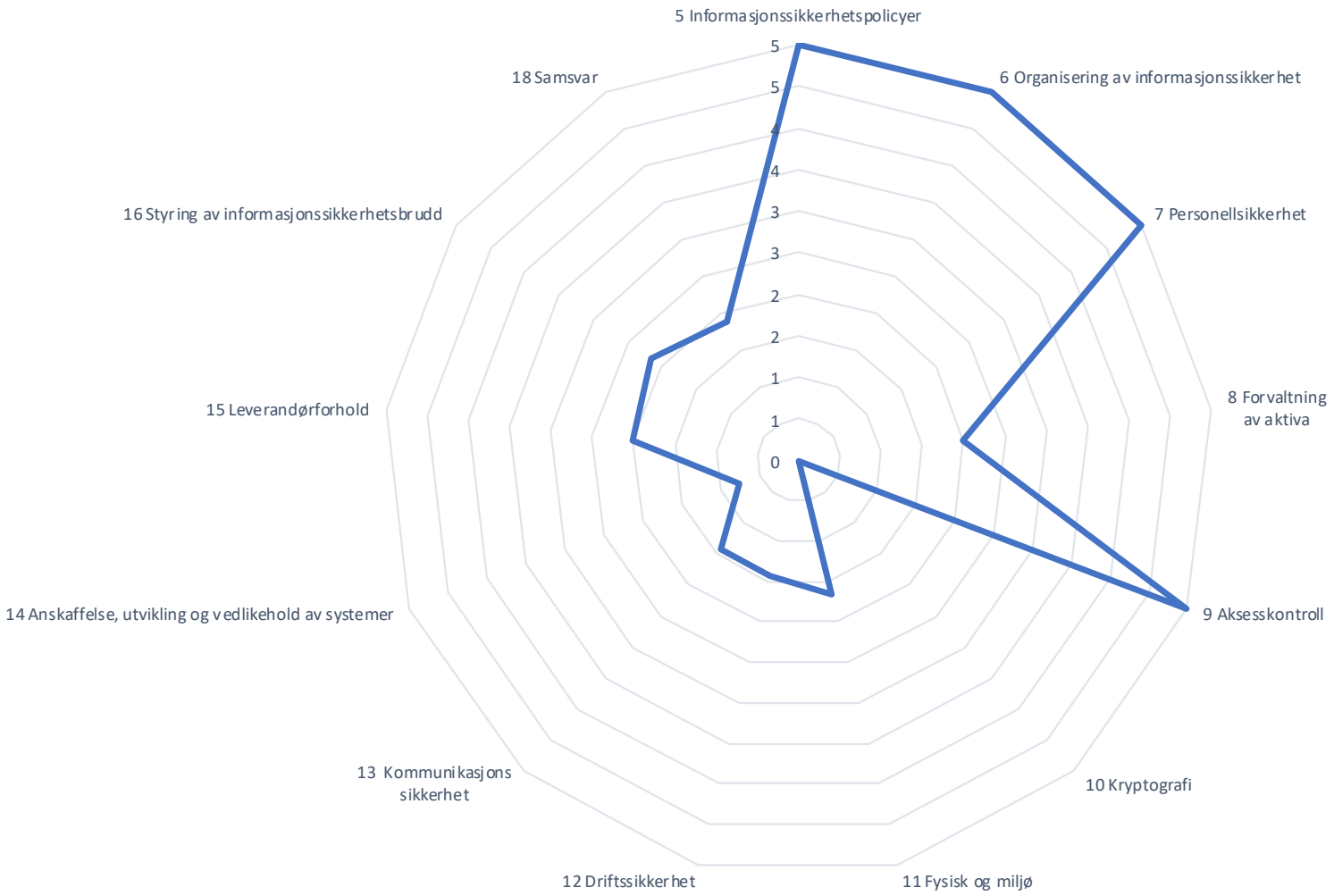
Annex A referanse	Tittel på kontroll	Beskrivelse av kontroll	Valgt? (J/N)	Begrunnelse for valg*)				Begrunnelse for utelatelse	Dokumentreferanse
				LK	KK	ISO	RA		
5 Informasjonssikkerhetspolicyer									
5.1	**Ledelsens føringer for informasjonssikkerhet**								
5.1.1	Policyer for informasjonssikkerhet	Et sett med policyer for informasjonssikkerhet bør defineres, godkjennes av ledelsen, publiseres og kommuniseres til ansatte og relevante eksterne parter.	-Velg-						
5.1.2	Gjennomgang av policyene for informasjonssikkerhet	Policyene for informasjonssikkerhet bør gjennomgås med planlagte intervaller. Dersom betydelige endringer skjer, bør det sikres at de fortsatt er egnet, tilstrekkelige og virkningsfulle.	-Velg-						
6 Organisering av informasjonssikkerhet									
6.1	**Intern organisering**								
6.1.1	Roller og ansvar for informasjonssikkerhet	Alt ansvar for informasjonssikkerhet bør være definert og tilordnet.	-Velg-						
6.1.2	Arbeidsdeling	Oppgaver og ansvar innenfor ulike områder bør være segregert for å redusere mulighetene for uautorisert eller utilsiktet modifisering eller misbruk av organisasjonens aktiva.	-Velg-						
6.1.3	Kontakt med myndigheter	Hensiktsmessig kontakt med relevante myndigheter bør opprettholdes.	-Velg-						
6.1.4	Kontakt med spesielle interessegrupper	Hensiktsmessig kontakt med spesielle interessegrupper eller andre spesialiserte sikkerhetsfora og profesjonelle foreninger skal opprettholdes.	-Velg-						
6.1.5	Informasjonssikkerhet i prosjektledelse	Informasjonssikkerhet bør håndteres som en del av prosjektledelsen, uavhengig av type prosjekt.	-Velg-						
6.2	**Mobilt utstyr og fjernarbeid**								
6.2.1	Policy for mobilt utstyr	En policy med underliggende sikringstiltak bør være innført for å håndtere risiko forbundet med bruk av mobilt utstyr.	-Velg-						
6.2.2	Fjernarbeid	En policy med underliggende sikringstiltak bør implementeres for å beskytte tilgang til, behandling av og lagring av informasjon der fjernarbeid utføres.	-Velg-						

ISO 27001 Anvendelighetserklæring

LK=Krav i lov eller forskrift.
KK= Kontraktuelle krav.
ISO: Obligatoriske krav i ISO 27001
RA: Etter etter risikoanalyse.

Annex A referanse	Tittel på kontroll	Beskrivelse av kontroll	Valgt? (J/N)	Begrunnelse for valg*)				Begrunnelse for utelatelse	Dokumentreferanse
				LK	KK	ISO	RA		
5 Informasjonssikkerhetspolicyer			**5**						
5.1	**Ledelsens føringer for informasjonssikkerhet**		**5**						
5.1.1	Policyer for informasjonssikkerhet	Et sett med policyer for informasjonssikkerhet bør defineres, godkjennes av ledelsen, publiseres og kommuniseres til ansatte og relevante eksterne parter.	j			x	x		
5.1.2	Gjennomgang av policyene for informasjonssikkerhet	Policyene for informasjonssikkerhet bør gjennomgås med planlagte intervaller. Dersom betydelige endringer skjer, bør det sikres at de fortsatt er egnet, tilstrekkelige og virkningsfulle.	j			x	x		
6 Organisering av informasjonssikkerhet			**5**						
6.1	**Intern organisering**		**4**						
6.1.1	Roller og ansvar for informasjonssikkerhet	Alt ansvar for informasjonssikkerhet bør være definert og tilordnet.	j			x			
6.1.2	Arbeidsdeling	Oppgaver og ansvar innenfor ulike områder bør være segregert for å redusere mulighetene for uautorisert eller utilsiktet modifisering eller misbruk av organisasjonens aktiva.	j			x			
6.1.3	Kontakt med myndigheter	Hensiktsmessig kontakt med relevante myndigheter bør opprettholdes.	j		x	x			
6.1.4	Kontakt med spesielle interessegrupper	Hensiktsmessig kontakt med spesielle interessegrupper eller andre spesialiserte sikkerhetsfora og profesjonelle foreninger skal opprettholdes.	j			x			
6.1.5	Informasjonssikkerhet i prosjektledelse	Informasjonssikkerhet bør håndteres som en del av prosjektledelsen, uavhengig av type prosjekt.	j			x			
6.2	**Mobilt utstyr og fjernarbeid**		**1**						
6.2.1	Policy for mobilt utstyr	En policy med underliggende sikringstiltak bør være innført for å håndtere risiko forbundet med bruk av mobilt utstyr.	j		x	x	x		
6.2.2	Fjernarbeid	En policy med underliggende sikringstiltak bør implementeres for å beskytte tilgang til, behandling av og lagring av informasjon der fjernarbeid utføres.	j			x			

GAP analyse

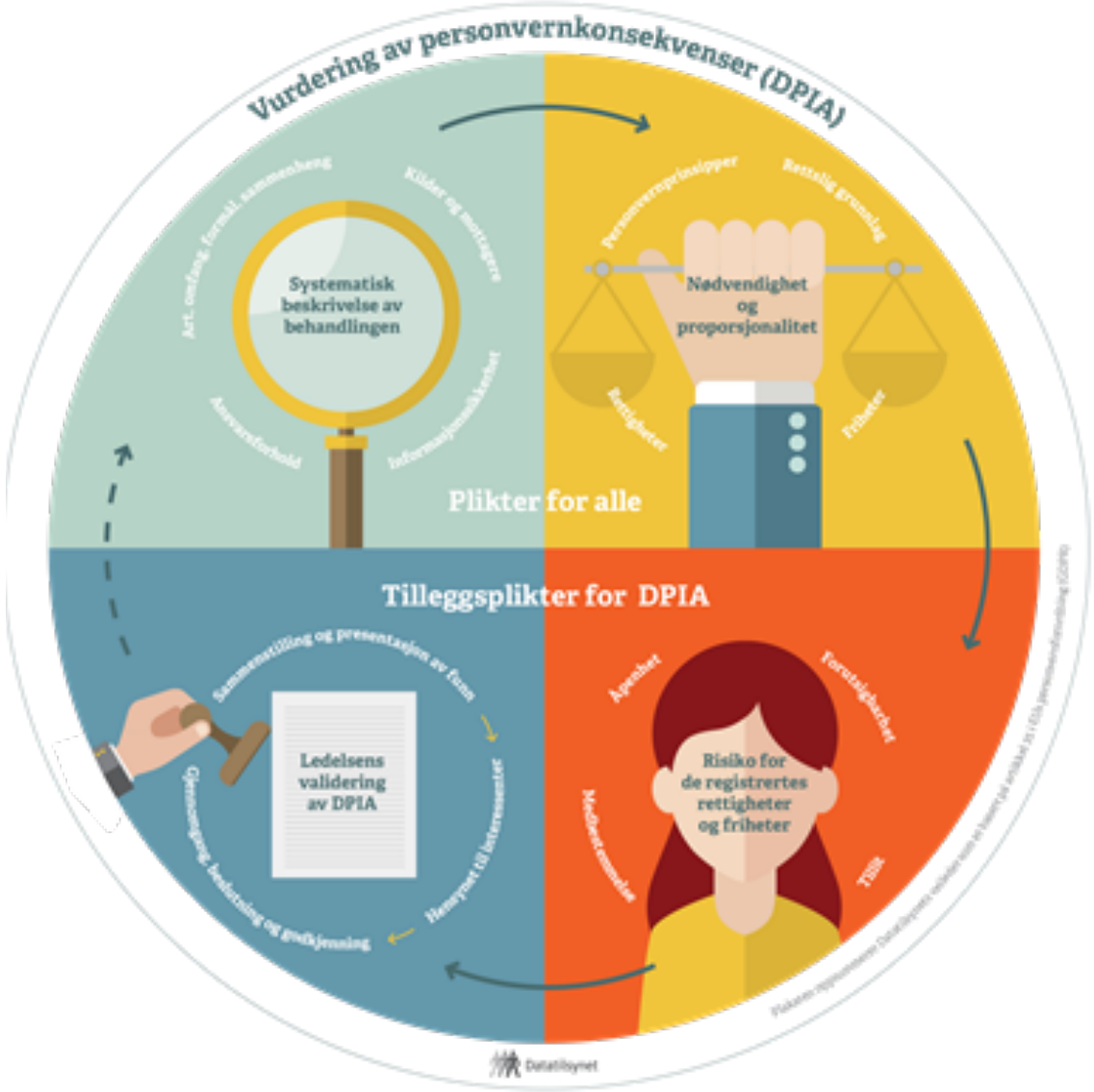

5 Informasjonssikkerhetspolicyer
6 Organisering av informasjonssikkerhet
7 Personellsikkerhet
8 Forvaltning av aktiva
9 Aksesskontroll
10 Kryptografi
11 Fysisk og miljø
12 Driftssikkerhet
13 Kommunikasjons sikkerhet
14 Anskaffelse, utvikling og vedlikehold av systemer
15 Leverandørforhold
16 Styring av informasjonssikkerhetsbrudd
18 Samsvar
5
5
4
4
3
3
2
2
1
1
0

Vi kan ikke velge bort IT-sikkerhet

- DPIA - vurdering av personvernkonsekvenser – artikkel 35
  - Bærum Kommune har laget en svært god mal for å gjennomføre DPIA

    https://kins.no/mal-for-gjennomforing-av-dpia/

- Krav til systematisk helse-, miljø og sikkerhetsarbeid – Arbeidsmiljøloven §3-1
- Straffeansvar (Aksjeloven § 19)
  - Et medlem av styret, som forsettlig eller uaktsomt overtrer bestemmelsene gitt i eller i medhold av aksjeloven, straffes med:
    Bøter eller under skjerpede forhold med fengsel inntil 1 år.
    Det er samme strafferamme ved grov uforstand.
    Medvirkning straffes på samme måte.
    Det er samme strafferamme for stifter, medlem av bedriftsforsamling, daglig leder og revisor



Ønsker du å lære mer?
Kontakt meg gjerne om du ønsker en uforpliktende prat

Roger Ison-Haug

48 01 89 14

roger.ison-haug@pedab.com