advisense

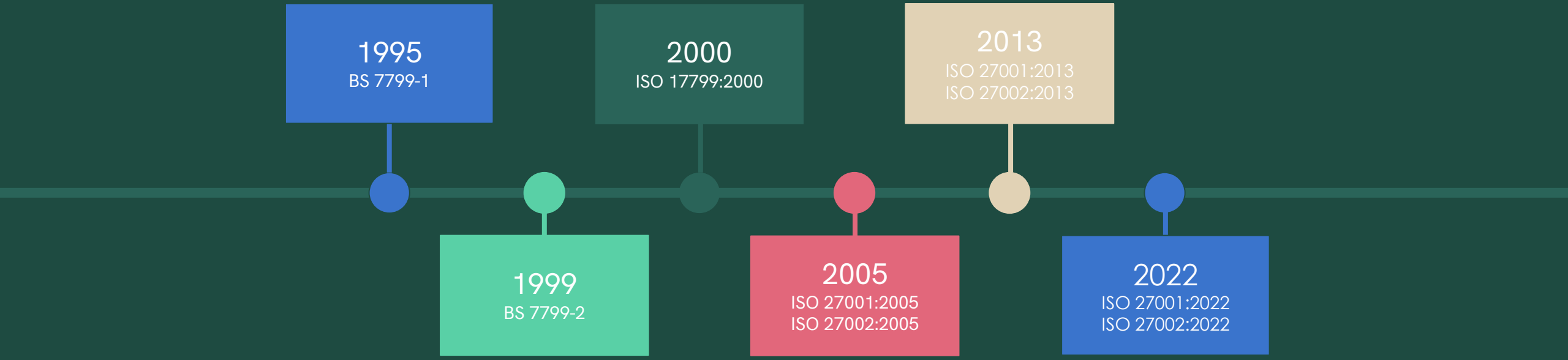
NS-EN ISO/IEC 27001 og NS-EN ISO/IEC 27002

Standard Morgen - Tilpasning til det digitale landskapet

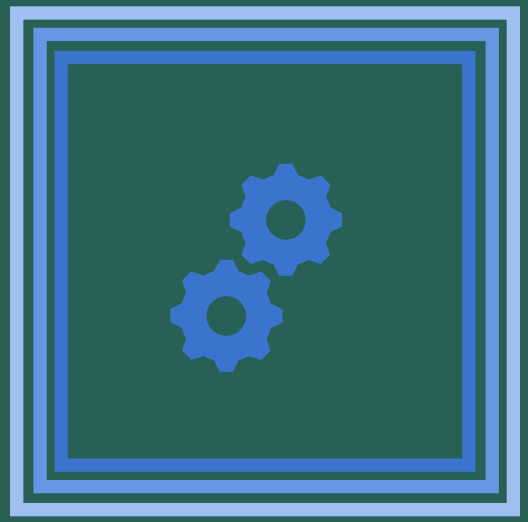
Eli Sofie Finnøy Amdam

2023-10-30

Historikk

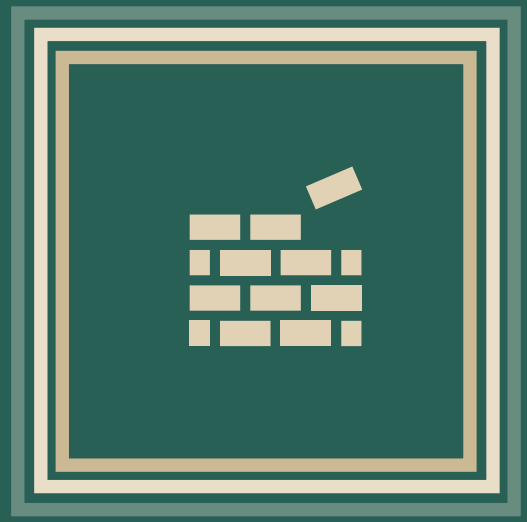

1995
BS 7799-1
1999
BS 7799-2
2000
ISO 17799:2000
2005
ISO 27001:2005
ISO 27002:2005
2013
ISO 27001:2013
ISO 27002:2013
2022
ISO 27001:2022
ISO 27002:2022

ISO 27001og 27002



ISO 27001
Ledelsessystem for informasjonssikkerhet

Hvordan bygge et ISMS i en organisasjon, stiller krav til etablering, implementering, vedlikehold og kontinuerlig forbedring.



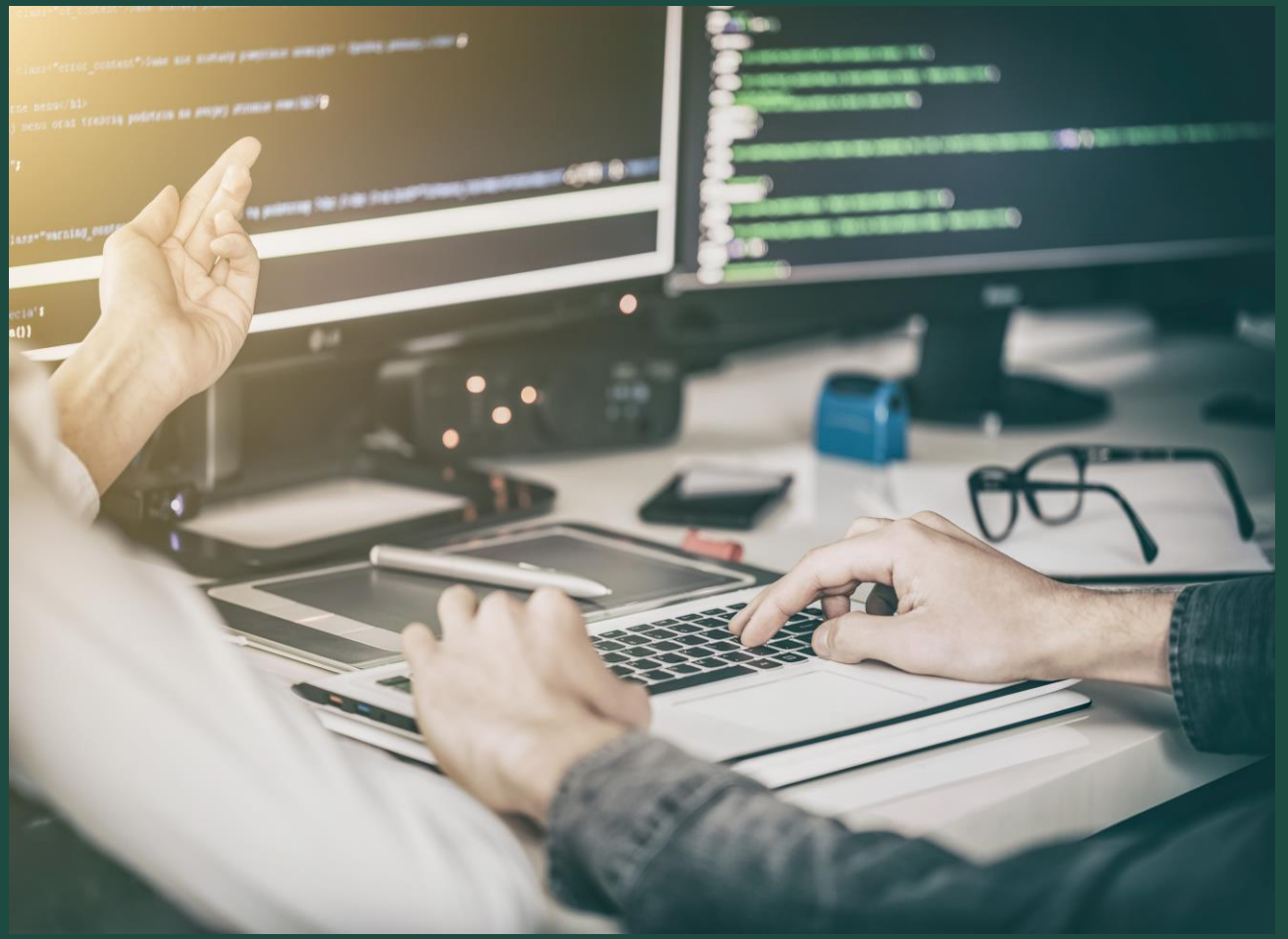
ISO 27002
Sikkerhetstiltak

Sett med retningslinjer og teknikker for å implementere sikkerhetstiltak. Gir god praksis for hva en bør gjøre, hva en bør vurdere og hva en bør ha på plass.

Hva er et ledelsessystem for informasjonssikkerhet?

Et rammeverk for å systematisk jobbe med informasjonssikkerhet

- Levende rammeverk integrert i daglig drift.
- Oppdateres jevnlig med nye risikoer, teknologi og forretningsbehov.
- Systematiserer risikohåndteringen og implementerer sikkerhetstiltak og -verktøy.
- Sikrer juridisk etterlevelse og andre forpliktelser.
- Muliggjør rask respons på sikkerhetshendelser.



Ledelsessystem for informasjonssikkerhet

Hvorfor er ISMS så viktig?

Unngå Ad Hoc Sikkerhet: Jobber systematisks og strukturert for å forhindrer sporadisk tilnærming og unngå hull i sikkerheten

Helhetlig sikkerhet: Integrerer organisatoriske, fysiske, tekniske, og juridiske aspekter.

Beskytt informasjon: Sikrer kundedata, forretningshemmeligheter og immaterielle rettigheter.

Støtter Etterlevelse: Reduserer risiko for bøter og skade på omdømme.

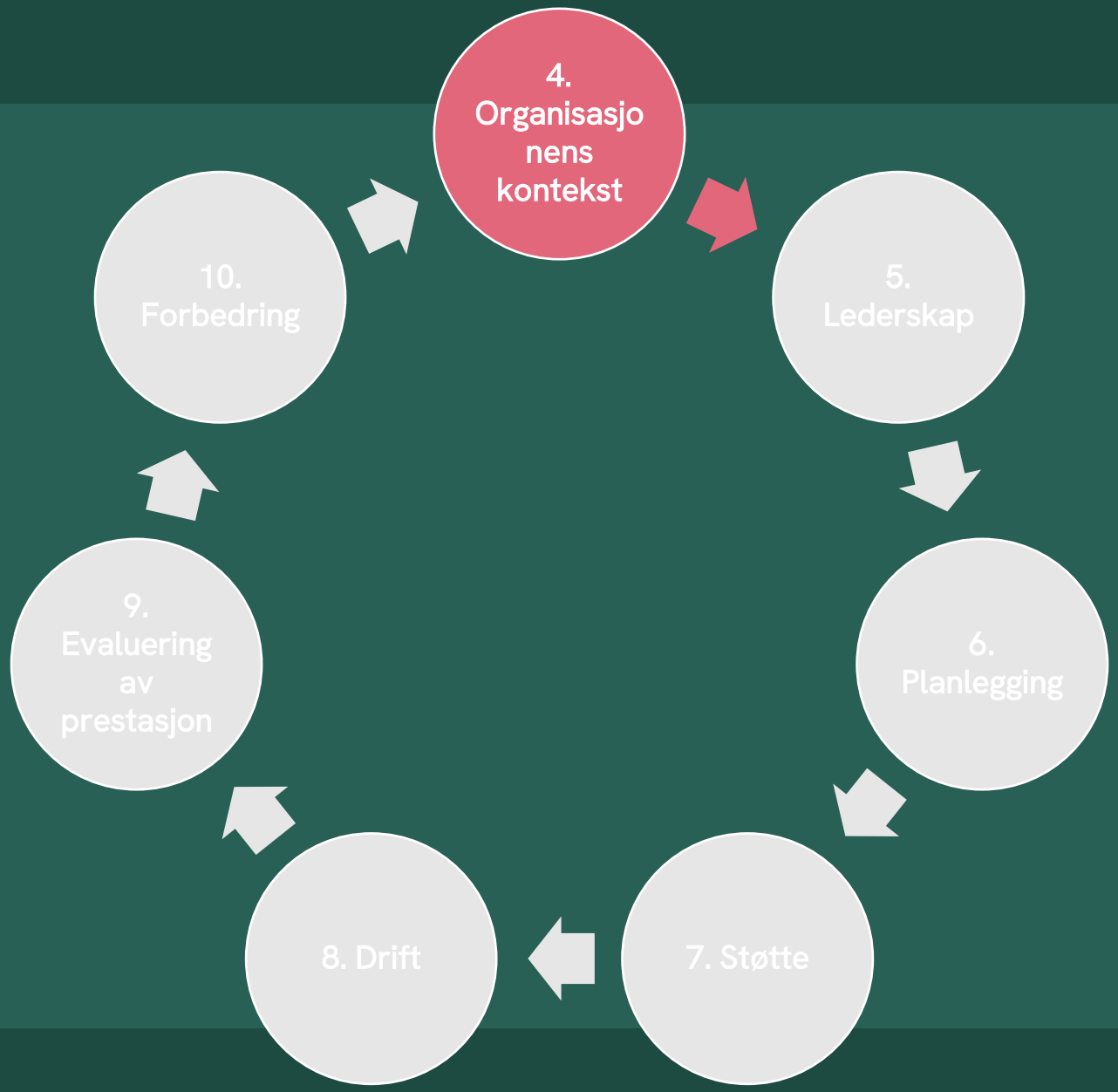
Forsterker Forretningskontinuitet: Begrenser og gjenoppretter fra sikkerhetshendelser.

Bygger Tillit: Forpliktelse til sikkerhet og personvern for kunder og partnere.

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

Nytt i 4 – Organisasjonens kontekst

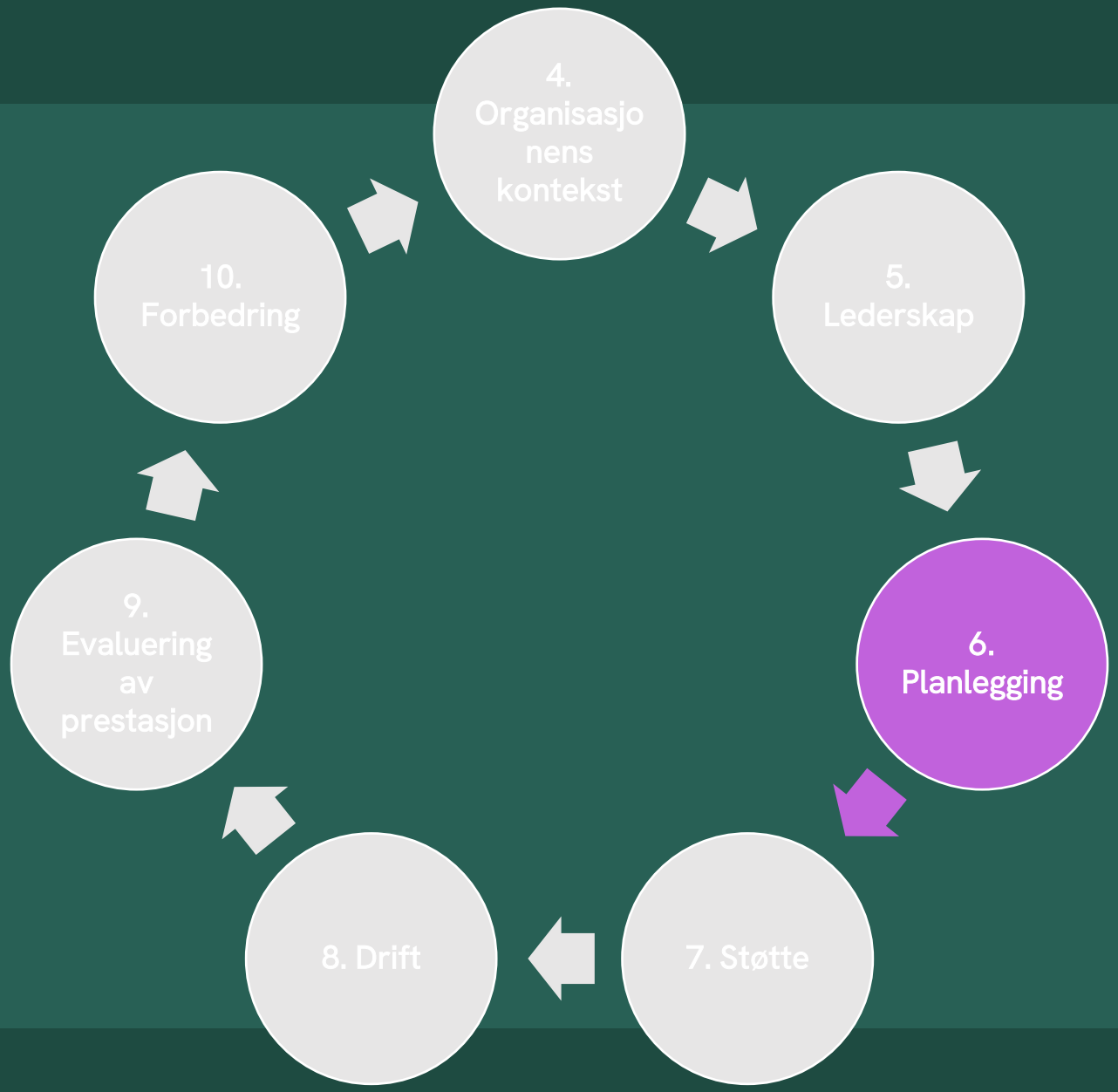
Forstå interessentenes behov og forventninger (4.2)

- I tillegg til å finne ut hvem interessentene er og hva de krever, er det nå et nytt krav (4.2 c) om å klargjøre hvilke av deres krav som er tatt hensyn til i ISMS-et, og hvilke som ikke er det.

Ledelsessystem for informasjonssikkerhet (4.4)

- Økt fokus på prosesser og deres interaksjoner i styring, implementering, og forbedring av ISMS-et.

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

Nytt i 6 – Planlegging

Behandling av informasjonssikkerhetsrisiko (6.1.3)

- Annex A beskrives nå som et sett med mulige tiltak, ikke et helhetlig sett.
- ISO 27001 tillater utforming av tiltak etter behov eller valg fra andre kilder. Ved sertifisering er mapping mot Annex A fortsatt nødvendig.

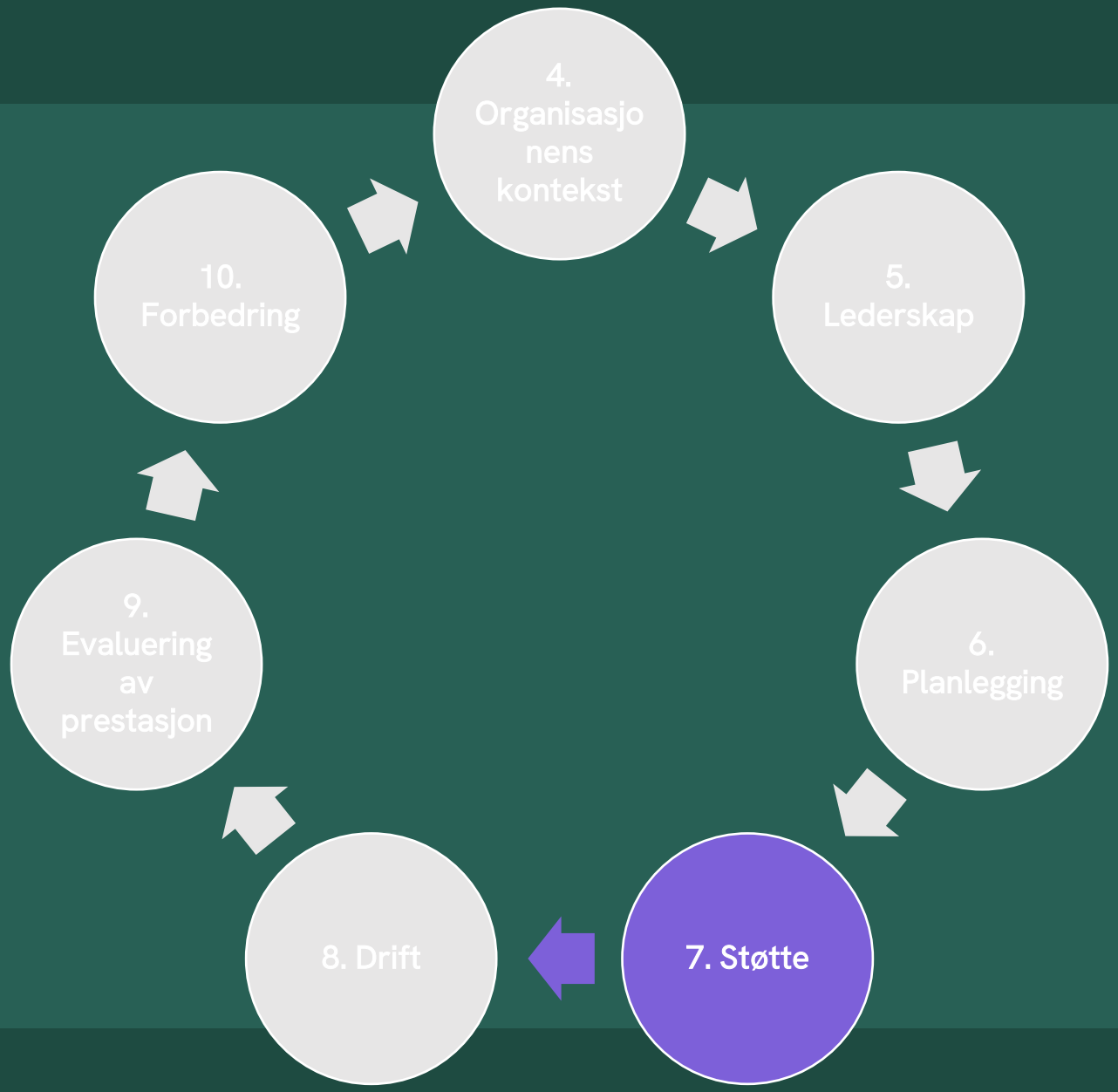
Informasjonssikkerhetsmål og planlegging for å oppnå dem (6.2)

- Kravet sier at organisasjonen skal fastsette informasjonssikkerhetsmål for relevante funksjoner og nivåer.
- To nye krav er lagt til. Informasjonssikkerhetsmål skal:
  - overvåkes (6.2 d)
  - være tilgjengelige som dokumentert informasjon (6.2 g)

Planlegging av endringer (6.3)

- Nytt krav om planlagte endringer i ISMS.
- Planlegg hvordan og når endringene skal gjennomføres (og dokumenter planleggingen)

ISO 27001

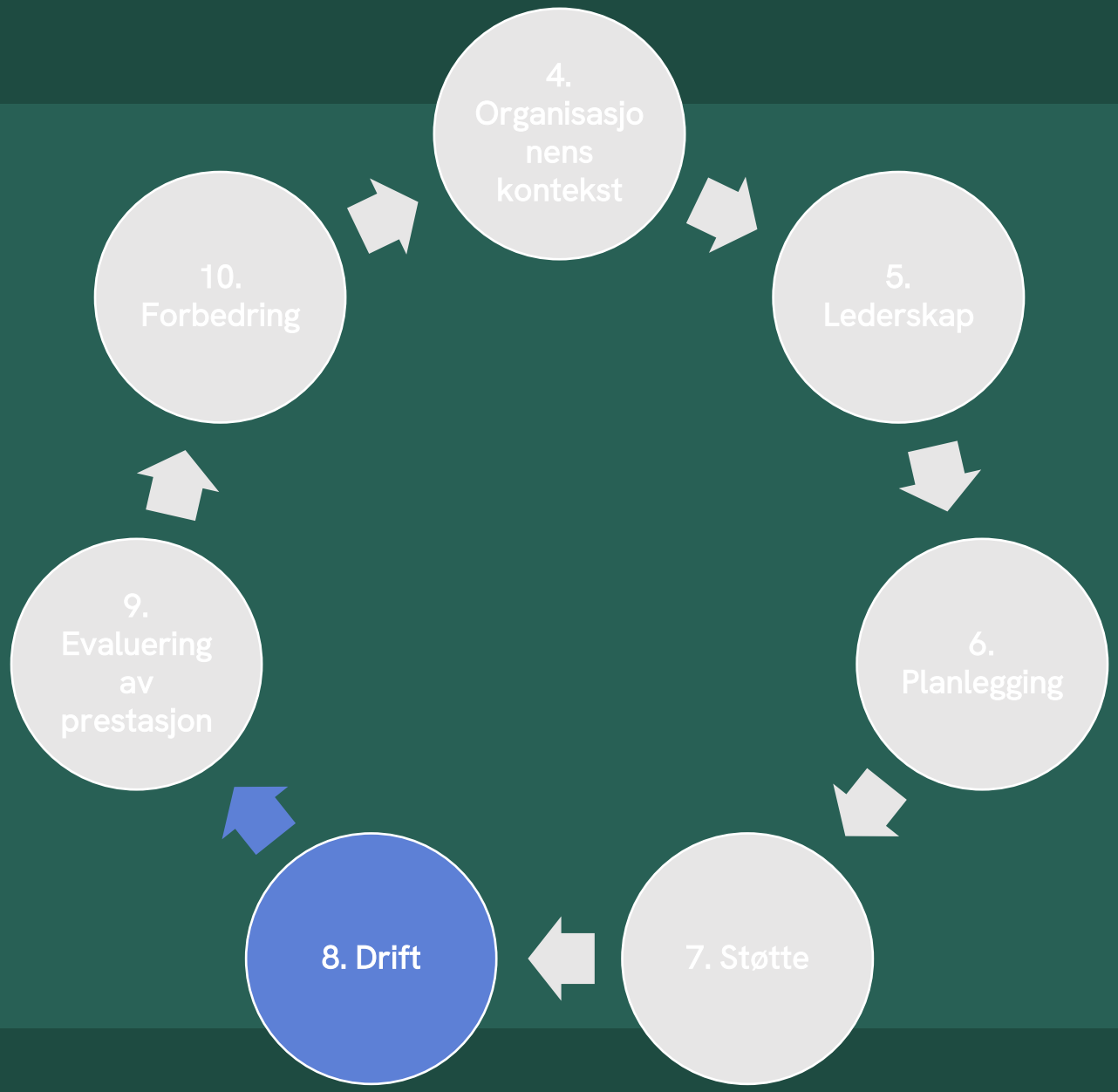

4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

Nytt i 7 – Støtte

Kommunikasjon (7.4)

- Krav 7.4 d) og e) slått sammen endret fra «hvem som skal kommunisere» og «prosessene der kommunikasjon skal gjennomføres» til «hvordan det skal kommuniseres»

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

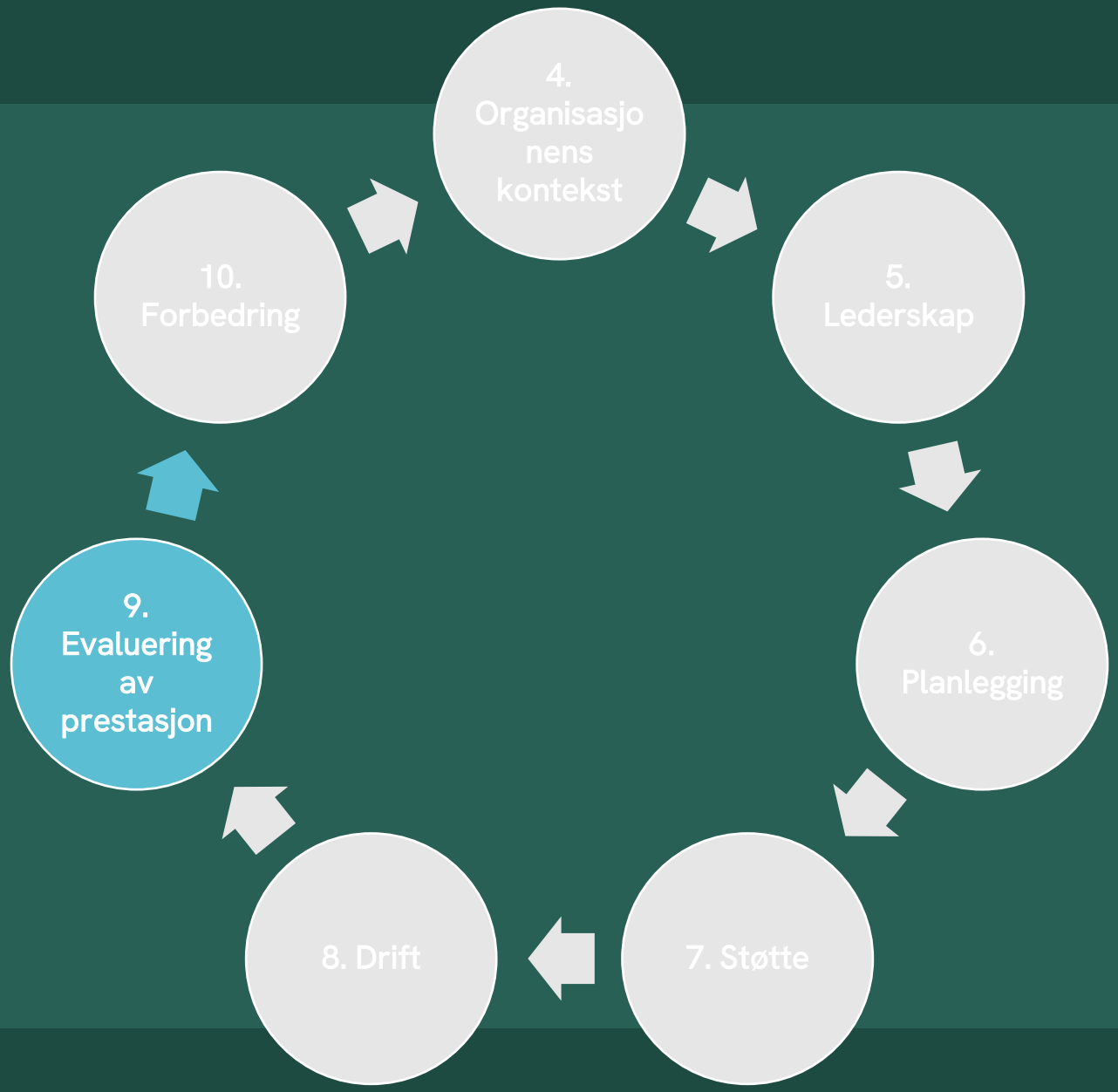
Nytt i 8 – Drift

Planlegging og styring av drift (8.1)

- Kanskje største endring i ISO 27001, bortsett fra Annex A
- 8.1 sier at man skal planlegge, implementere og styre prosessene som er nødvendige for å etterleve informasjonssikkerhetskrav og redusere risiko.
- Nytt krav om å fastsette kriterier for disse prosessene.

- Eksterne prosesser: istedenfor å skrive at man skal sikre at outsourcede prosesser er definert og kontrollert så er den utdypet til at eksternt leverte prosesser, produkter eller tjenester som er relevante for styringssystemet for informasjonssikkerhet skal kontrolleres.

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

Nytt i 9 – Evaluering av prestasjon

Overvåkning, måling, analyse og evaluering (9.1)

- Lagt til et krav om at organisasjonen skal evaluerer prestasjonen og virkningen av ISMS-et.

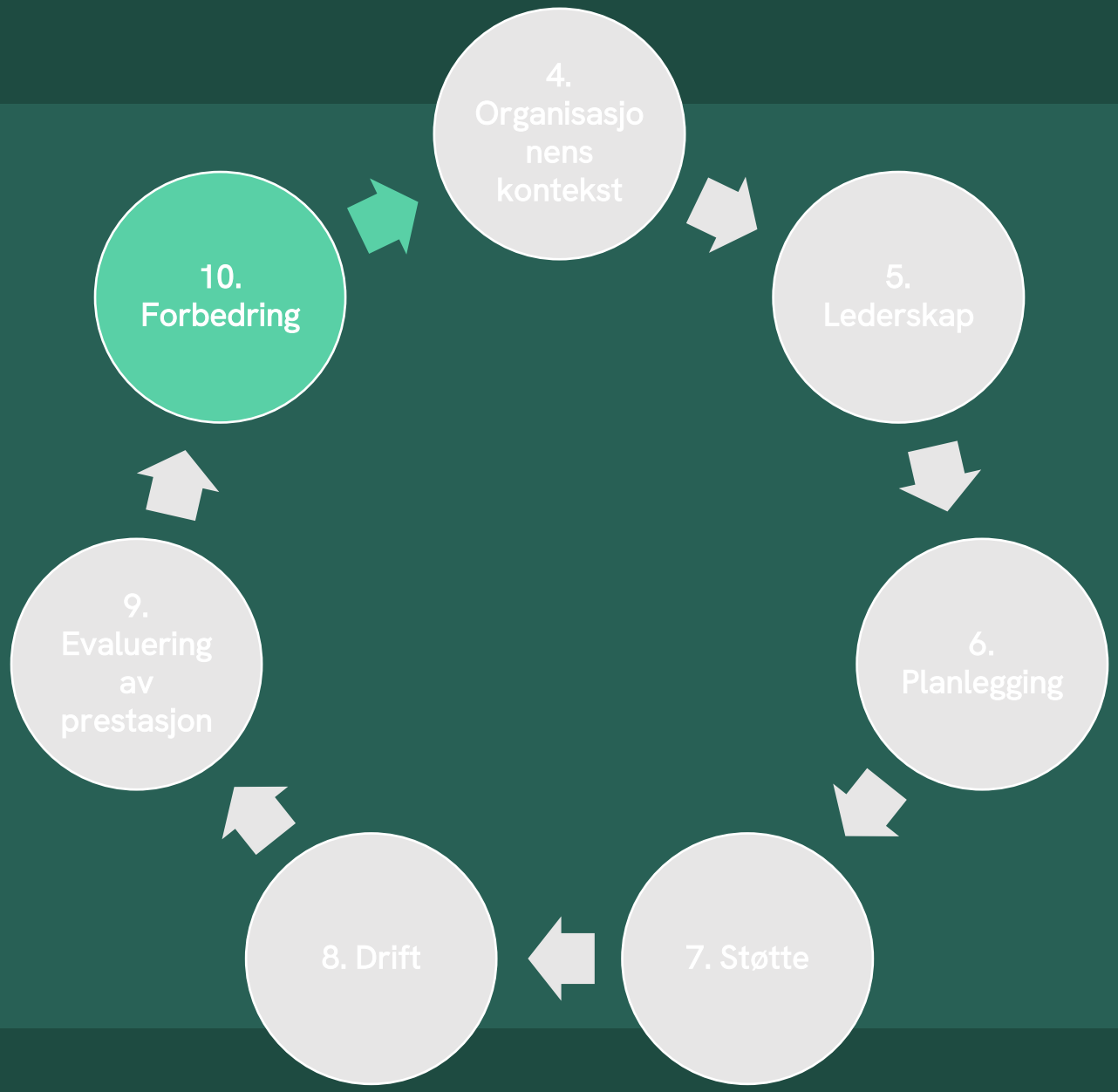
Internrevisjon (9.2)

- Ny struktur med to underkapitler for generelle krav og krav til internrevisjonsprogrammet.

Ledelsens gjennomgang (9.3)

- Ny struktur med underkapitler for generelle krav, grunnlag og resultater fra ledelsens gjennomgang.
- Nytt krav (9.3.2 c) om vurdering av endringer i interessenters behov og forventninger i ledelsens gjennomgang.

ISO 27001


4. Organisasjonens kontekst
5. Lederskap
6. Planlegging
7. Støtte
8. Drift
9. Evaluering av prestasjon
10. Forbedring

Nytt i 10 – Forbedring

10 - Forbedring

- Her er det ingen nye krav eller endringer, men det er gjort en strukturell endring hvor «Kontinuerlig forbedring» og «Avvik og korrigerende aktiviteter» har byttet rekkefølge fra tidligere versjoner.


ISO 27002

ISO 27002

- Informasjonssikkerhetspolicyer
- Organisering av informasjons-sikkerhet
- Personellsikkerhet
- Forvaltning av aktiva
- Aksesskontroll
- Kryptografi
- Fysisk og miljømessig sikkerhet
- Driftssikkerhet
- Kommunikasjons-sikkerhet
- Anskaffelse, utvikling og vedlikehold av systemer
- Leverandørforhold
- Håndtering av informasjonss-ikkerhets-hendelser
- Beredskaps- og kontinuitetsstyring
- Etterlevelse

- **Organisatoriske sikkerhetstiltak** *(37 tiltak)*
- **Personellrelaterte sikkerhetstiltak** *(8 tiltak)*
- **Fysiske sikkerhetstiltak** *(14 tiltak)*
- **Teknologiske sikkerhetstiltak** *(34 tiltak)*

Sikkerhetstiltak – eksempel

Identitets- og tilgangskontroll

ISO/IEC 27002:2022	ISO/IEC 27002:2013	Sikkerhetstiltak
5.15	9.1.1, 9.1.2	Tilgangskontroll
5.16	9.2.1	Identitetshåndtering
5.17	9.2.4, 9.3.1, 9.4.3	Autentiseringsinformasjon
5.18	9.2.2, 9.2.5, 9.2.6	Tilgangsrettigheter
8.2	9.2.3	Privilegerte tilgangsrettigheter
8.3	9.4.1	Begrensing av informasjonstilgang
8.4	9.4.5	Tilgang til kildekode
8.5	9.4.2	Sikker autentisering
8.18	9.4.4	Bruk av priviligerte hjelpeprogrammer

Nye sikkerhetstiltak

1. 5.7 Trussel-etterretning
2. 5.23 Informasjons-sikkerhet - skytjenester
3. 5.30 IKT-beredskap – virksomhets-kontinuitet
4. 7.4 Fysisk sikkerhets-overvåkning
5. 8.9 Konfigurasjons -styring
6. 8.10 Sletting av informasjon
7. 8.11 Data-maskering
8. 8.12 Forebygging av datalekkasje
9. 8.16 Overvåknings -aktiviteter
10. 8.22 Nettsteds-filtrering
11. 8.28 Sikker koding

Attributter

Type sikkerhetstiltak

#Forebyggende, #Oppdagende, #Korrigerende

Informasjonssikkerhetsegenskaper

#Konfidensialitet, #Integritet, #Tilgjengelighet

Cybersikkerhetsdomener

#Identifisere, #Beskytte, #Oppdage, #Reagere, #Gjenopprette

Operasjonell Kapasitet

#Styring, #Forvaltning_av_verdi, #Informasjonsbeskyttelse, #Personellsikkerhet, #Fysisk_sikkerhet, #System-_og_nettverkssikkerhet, #Applikasjonssikkerhet, #Sikker_konfigurasjon, #Identitets-_og_tilgangsstyring, #Håndtering_av_trusler_og_sårbarheter, #Kontinuitet, #Sikkerhet_i_leverandørforhold, #Juridisk_og_etterlevelse, #Håndtering_av_informasjonssikkerhetshendelser, #Bekreftelse_av_informasjonssikkerhet

Sikkerhetsdomener

#Styring og økosystem, #Beskyttelse, #Forsvar, #Resiliens

Eksempler

6.6 Konfidensialitets- eller taushetserklæringer:

Konfidensialitets- eller taushetserklæringer som gjenspeiler organisasjonsen behov for beskyttelse av informasjon bør identifiseres, dokumenteres, gjennomgås regelmessig og signeres av personell og andre relevante interessenter.

Type sikkerhetstiltak	Informasjons-sikkerhets-egenskaper	Cybersikkerhets-konsepter	Operasjonell kapasitet	Sikkerhetsdomener
#Forebyggende	#Konfidensialitet	#Beskytte	#Personellsikkerhet #Informasjonsbeskyttelse #Leverandørforhold	#Styring_og_økosystem

8.4 Tilgang til kildekode

Lese- og skrivetilgang til kildekode, utviklingsverktøy og programvarebiblioteker bør forvaltes på riktig mate.

Type sikkerhetstiltak	Informasjons-sikkerhets-egenskaper	Cybersikkerhets-konsepter	Operasjonell kapasitet	Sikkerhetsdomener
#Forebyggende	#Konfidensialitet #Integritet #Tilgjengelighet	#Beskytte	#Identitets_og_Tilgangsstyring #Applikasjonssikkerhet #Sikker_konfigurasjon	#Beskyttelse

Oppsummering

- Endringene kan virke store, men kan kreve minimal justering i ledelsessystemet.
- Potensielle oppdateringer i Risikohåndteringsplanen (RTP) og Relevanserklæringen (SOA).
- Risikovurdering - Utforsk nye tiltak i Annex A for å redusere risiko, om nødvendig.
- Anbefaling:
  - Utfør en gap-analyse for å sammenligne eksisterende tiltak med de nye tiltak.
  - Eksempler:
    - Sikker koding kan allerede være dekket i sikker utviklingsprosess.
    - Sikker konfigurasjon kan være integrert i change management.
- Vurder selv omfanget av nødvendige endringer i din organisasjon.

Dette er en sjanse til å forbedre og effektivisere ISMS-et i din organisasjon

advisense

Eli Sofie Amdam
Teamleder i ITGS at Transcendent Group