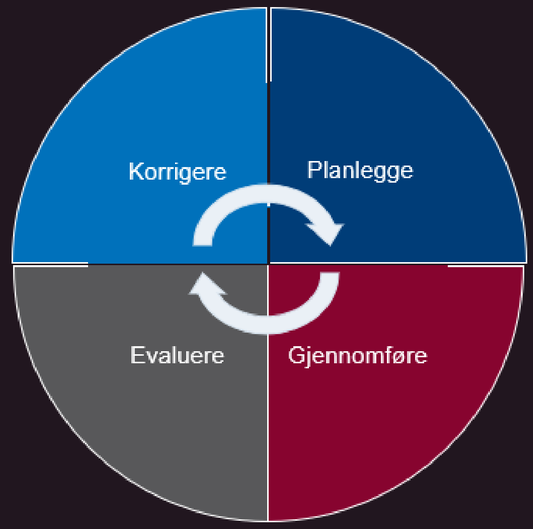
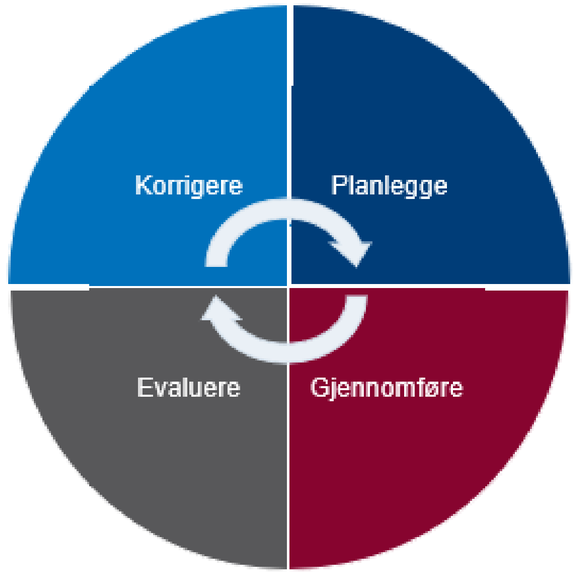
NORMEN



Internkontroll

Hva er internkontroll

Internkontroll innebærer **et systematisk arbeid for å sikre at virksomheten planlegger, organiserer, utfører og vedlikeholder sine aktiviteter i samsvar med gjeldene lover og forskrifter**. Systemet skal sikre at problemer oppdages og tas hånd om i tide.



Krav til internkontroll - Myndighetskrav
Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

- Med formål om å bidra til forsvarlige helse- og omsorgstjenester, pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves

- Den med det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter
  - Plikt til å planlegge
  - Plikt til å gjennomføre
  - Plikt til å evaluere
  - Plikt til å korrigere

§ 2.Virkeområde

Forskriften gjelder virksomheter som er pålagt internkontrollplikt etter

a) helsetilsynsloven § 5

b) spesialisthelsetjenesteloven § 2-1a tredje ledd

c) helse- og omsorgstjenesteloven § 3-1 tredje ledd eller

d) tannhelsetjenesteloven § 1-3a.

Forskriften gjelder også virksomheter som er pålagt plikt til å arbeide systematisk for kvalitetsforbedring og pasient- og brukersikkerhet etter

a) spesialisthelsetjenesteloven § 3-4a eller

b) helse- og omsorgstjenesteloven § 4-2.

NORMEN

Krav til internkontroll - Myndighetskrav
Personvernforordningen

Behandlingsansvarlig og databehandler sitt ansvar.

Gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen

Artikkel 24:
Den behandlingsansvarliges (dataansvarliges) ansvar

Artikkel 32 :
Sikkerhet ved behandlingen

NORMEN

Norm for informasjonssikkerhet

Bransjenorm for informasjonssikkerhet – og fra 2018 også for personvern.

Hva kjennetegner sektoren

I helse- og omsorgssektoren behandles det store mengder opplysninger som grunnlag for gode helse- og omsorgstjenester, helseregistre, forskning og innovasjon

Avgrensning

Normen og veilederen om internkontroll er avgrenset til internkontroll innenfor **Normens temaområder i helse- og omsorgssektoren, informasjonssikkerhet og personvern.**

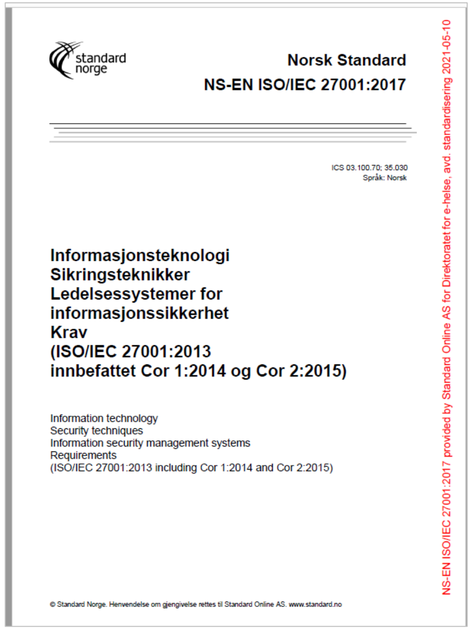
Kommuner og andre komplekse virksomheter må være oppmerksom på denne avgrensningen!

Styringssystem

- Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.
- Informasjonssikkerhet og personvern bør inngå som en **del av det totale** styringssystemet i virksomheten
- Styringssystemet skal **dokumenteres**
- Alle **offentlige virksomheter** skal beskrive mål og etablere strategi for informasjonssikkerhet. Dette skal danne grunnlaget for styringssystemet.

Internkontroll / Styringssystem / Ledelsessystem
Kjært barn har mange navn

- Internkontroll for informasjonssikkerhet
- Styringssystem for informasjonssikkerhet (SSIS)
- Kvalitetssystem for informasjonssikkerhet
- Ledelsessystem for informasjonssikkerhet
- Information Security management system (ISMS)


standard norge

Norsk Standard

NS-EN ISO/IEC 27001:2017

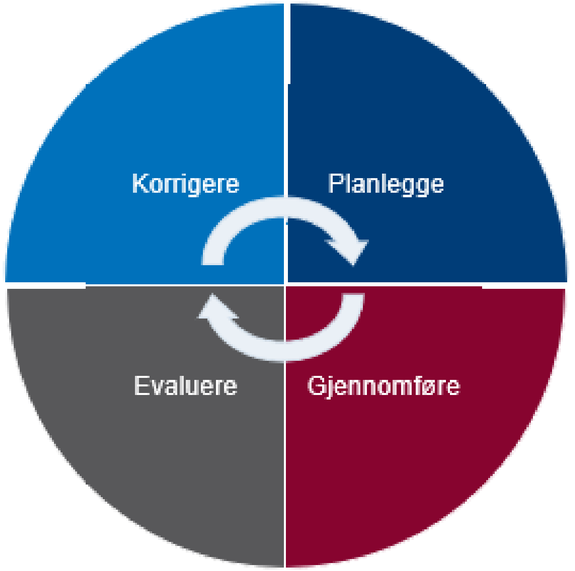
ICS 03.100.70; 35.030
Språk: Norsk

Informasjonsteknologi
Sikringsteknikker
Ledelsessystemer for informasjonssikkerhet
Krav
(ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015)

Information technology
Security techniques
Information security management systems
Requirements
(ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

- **ISO/IEC 27001** er den mest **anerkjente** standarden for informasjonssikkerhet i verden.

- PDCA hjulet



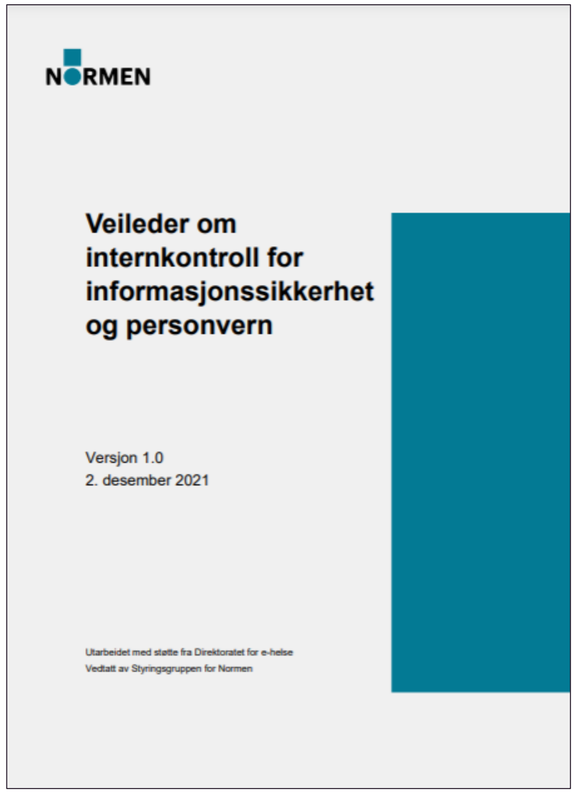
NORMEN

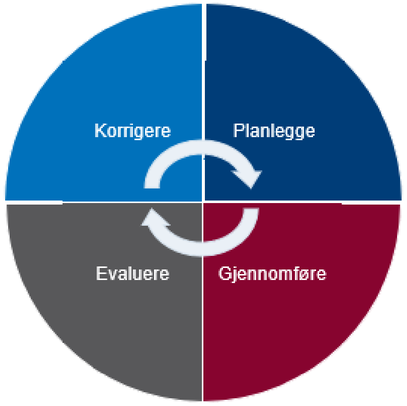
Hvordan operasjonalisere et styringssystem? PDCA - metode for kontinuerlig forbedring

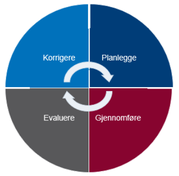
- Plan (Planlegg). Etableres styringssystemet. identifisere og vurdere risiko og er et viktig grunnlag for videre planlegging.
- Do (Gjennomføre). Implementere og vedlikeholdet styringssystem og evt. endringer.
- Check (Evaluere). Overvåke og evaluere
- Act (Korriger). Vedlikeholde og forbedre.

PDCA hjulet er mer enn bare metode – dette er et konsept av kontinuerlig forbedringsprosesser innebygd i organisasjonens kultur.

Det viktigste aspektet av PDCA-prinsippet ligger i Act-fasen – når arbeidet er fulført og syklusen starter på nytt for gjennomføring av ytterligere forbedringer







ISO 27001:2017

PLANLEGGE | **GJENNOMFØRE** | **EVALUERE** | **KORRIGERE**

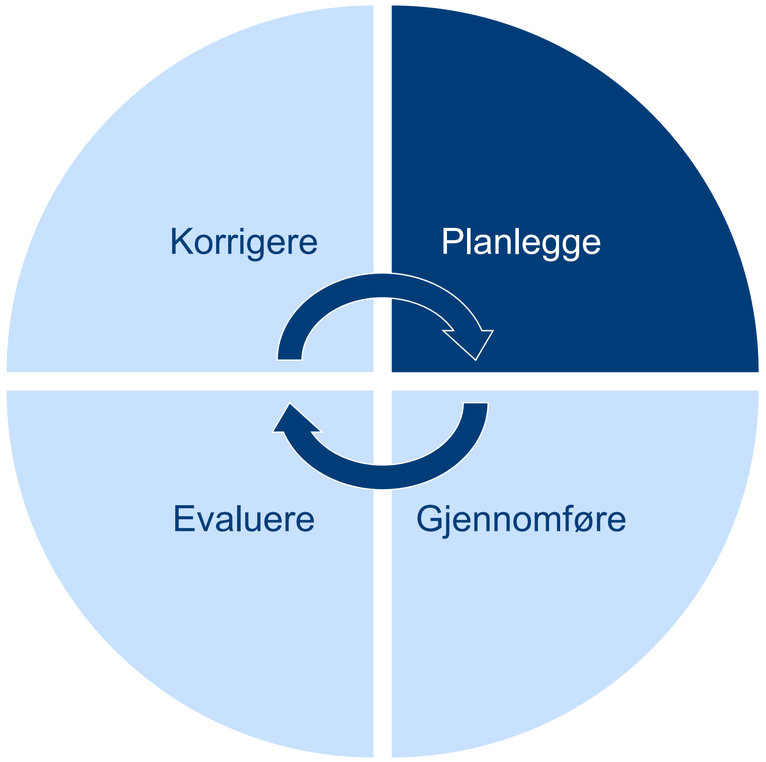
4. Organisasjonens kontekst → 5. Lederskap → 6. Planlegging → 7. Støttefunksjoner → 8. Drift → 9. Evaluering → 10. Forbedring

4. Organisasjonens kontekst	5. Lederskap	6. Planlegging	7. Støttefunksjoner	8. Drift	9. Evaluering	10. Forbedring
4.1. Forstå organisasjonen og dens kontekst	5.1 Lederskap og forpliktelse	6.1 Tiltak for å håndtere risikoer og muligheter	7.1 Ressurser	8.1 Driftsplanlegging og kontroll	9.1 Overvåking, måling, analyse og evaluering	10.1 Avvik og korrigerende tiltak
4.2 Forstå interesseparters behov og forventninger	5.2 Policy	6.1.1 Generelt	7.2 Kompetanse	8.2 Risikovurdering av informasjonssikkerheten	9.2 Intern revisjon	10.2 Kontinuerlig forbedring
4.3 Bestemme omfanget av ledelsessystemet for informasjonssikkerhet	5.3 Organisasjonens roller, ansvar og myndighet	6.1.2 Risikovurdering av informasjonss-ikkerheten	7.3 Bevisstgjøring	8.3 Håndtering av informasjonssikkerhetsrisikoene	9.3 Ledelsens gjennomgang	
4.4 Ledelsessystem for informasjons-sikkerhet		6.1.3 Håndtering av informasjons-sikkerhetsrisikoene	7.4 Kommunikasjon			
		6.2 Informasjonssikkerhets mål og planlegging for å oppnå dem	7.5 Dokumentert informasjon			

Normens krav er mappet til ISO 27001

NORMEN

Normens krav til ledelse, ansvar, planlegging og risikovurdering



Kontekst

Styringssystemet skal være tilpasset virksomhetens størrelse, risiko, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i.

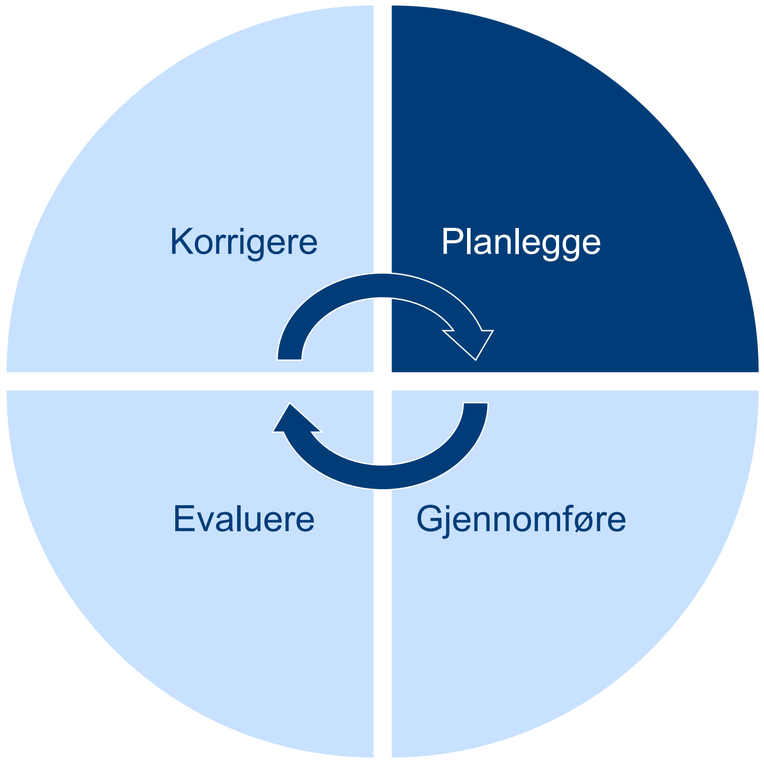
Dokumentasjon

Virksomheten skal dokumentere alle tiltak

Normens krav til ledelse, ansvar, planlegging og risikovurdering

Ledelse og ansvar

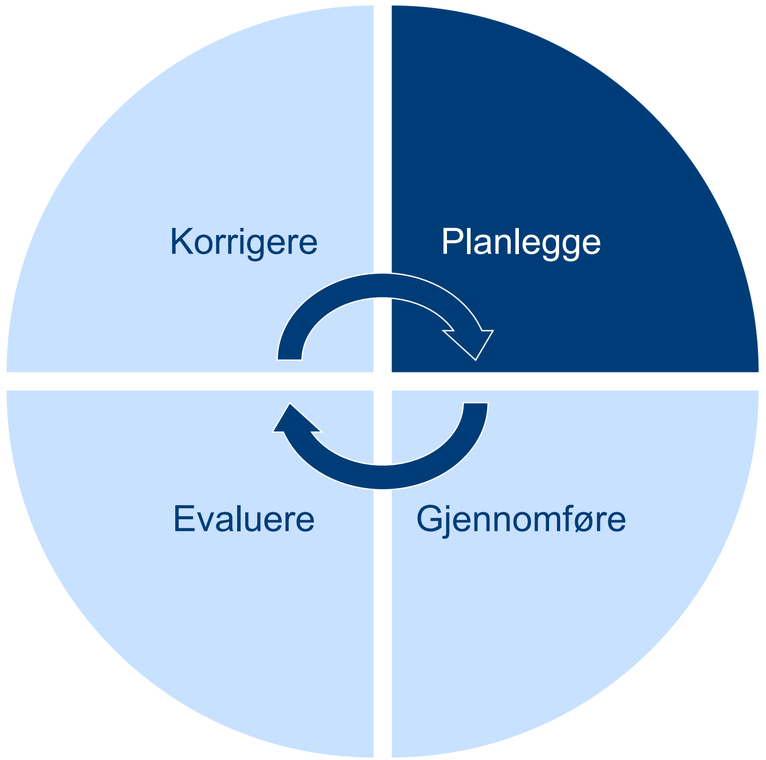
- Virksomhetenes øverste ledelse har ansvar for at virksomheten følger gjeldende krav etter Normen og lovgivning



- Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver
  - Virksomheten beslutter hvilke roller og funksjoner for informasjonssikkerhet og personvern som er nødvendig
    - PVO
    - Informasjonssikkerhetsleder
    - …
  - Alle skal være kjent med hvilke oppgaver de har

NORMEN

Normens krav til ledelse, ansvar, planlegging og risikovurdering

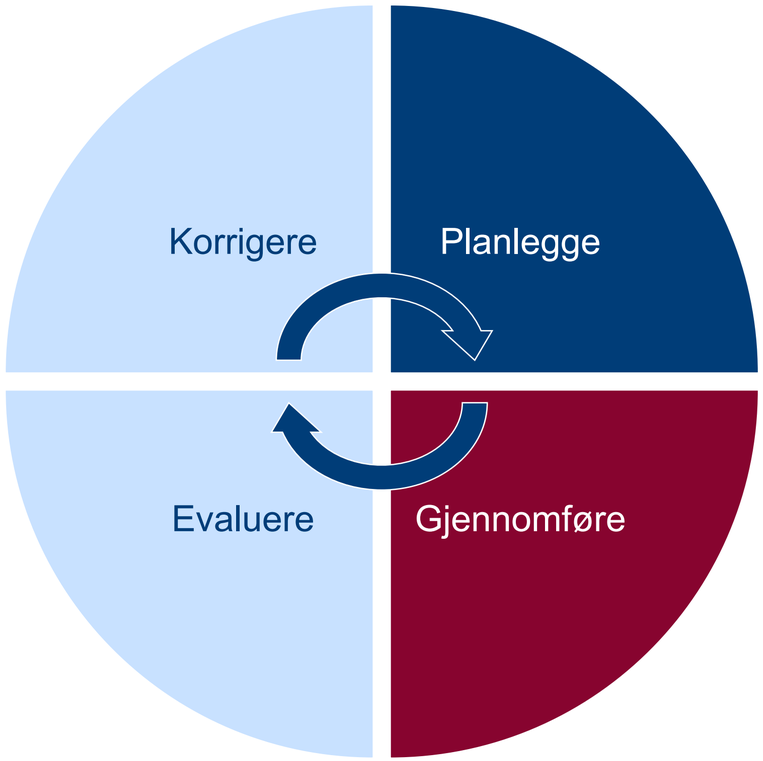


Planlegging og risikovurdering

- Virksomheten skal ha utarbeidet **protokoll** over behandlinger av helse- og personopplysninger.
- Virksomheten skal ha **oversikt** over IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, mv.
- Det skal tas avgjørende hensyn **til konsekvenser for pasient/ bruker** og forsvarlig helsehjelp i risikovurderingene.
- Planen for tiltakene skal forankres hos virksomhetens **ledelse**.
- Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering (**DPIA**).
- Virksomheten skal legge til rette for **tekniske og organisatoriske tiltak** slik at den registrerte kan få innfridd sine rettigheter.
- Virksomheten skal sørge for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med **taushetsplikten**.

NORMEN

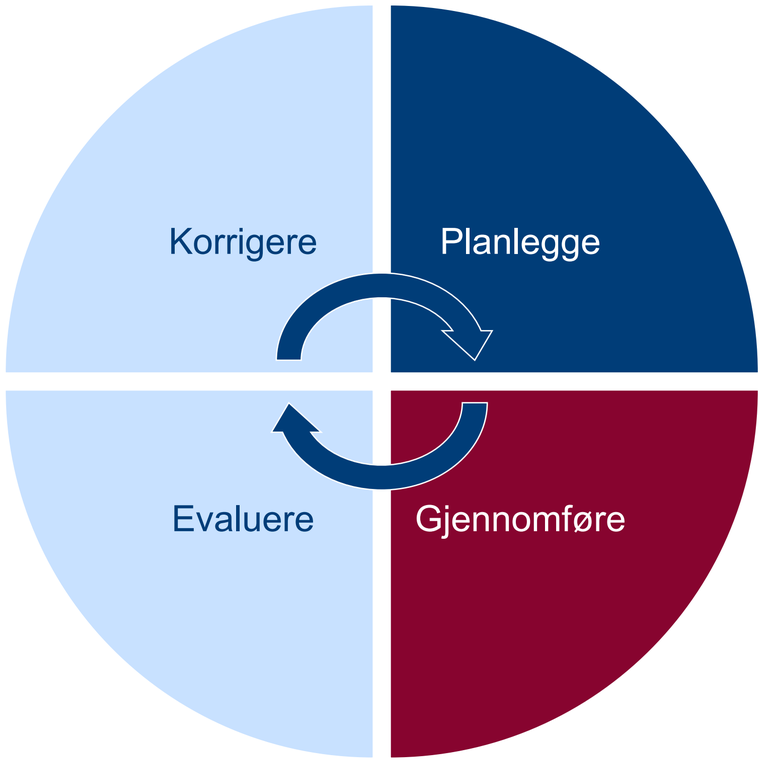
Normens krav til å implementere og vedlikeholdet styringssystem



- Virksomhetens øverste ledelse skal **gi tilstrekkelige økonomiske rammer og ressurser** for gjennomføring av nødvendige aktiviteter.
- Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med **tilstrekkelige ressurser og kompetanse** til å gjennomføre nødvendige oppgaver for å ivareta ansvaret.
- Sikkerhetstiltak skal være egnede og de skal være valgt på grunnlag av risikovurderinger. Kapittel 5 i Normen - Informasjonssikkerhet
- Øverste ledelse **skal ha gjort styringssystemet kjent i virksomheten.**

NORMEN

Normens krav til å implementere og vedlikeholdet styringssystem

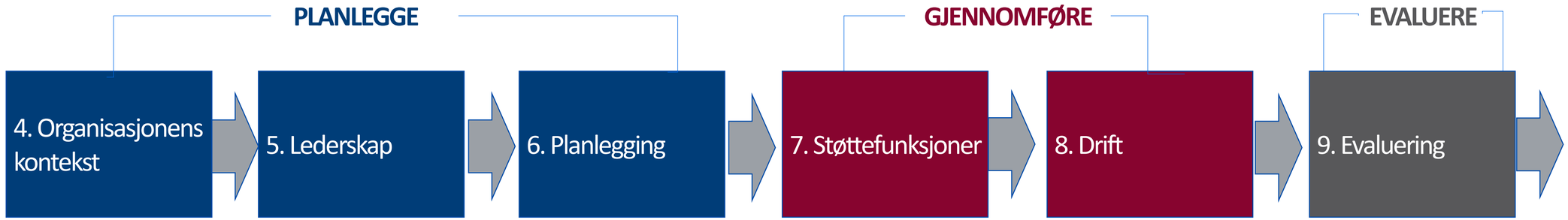


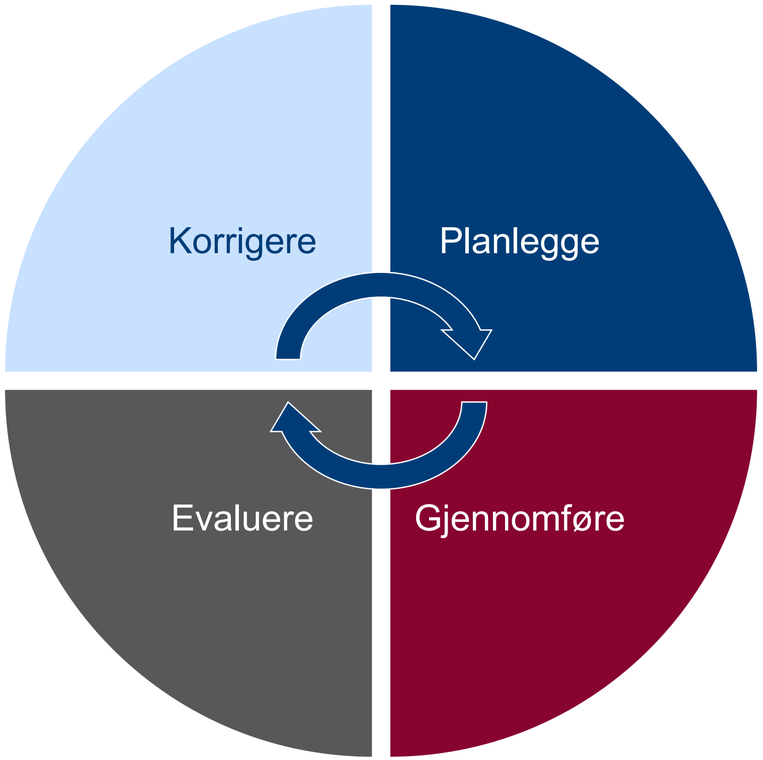
Blant annet:

- Rutine for opplæring
- Rutiner for plan, gjennomføring og oppfølging av risikovurderinger
- Oversikt over databehandlere og leverandører
- Rutine for oppretting og vedlikehold av autorisasjonsregister
- Rutine for sikkerhetskopiering
- Fysisk sikring av lokaler og områder
- Rutine for innsyn, informasjon, retting og sletting
- Rutine for tilgang til helseopplysninger
- Rutine for utlevering av helseopplysninger til kvalitetssikring
- Autentisering ved tilgang til helseopplysninger

NORMEN

Normens krav til å evaluere styringssystemet





Sikkerhetsrevisjon

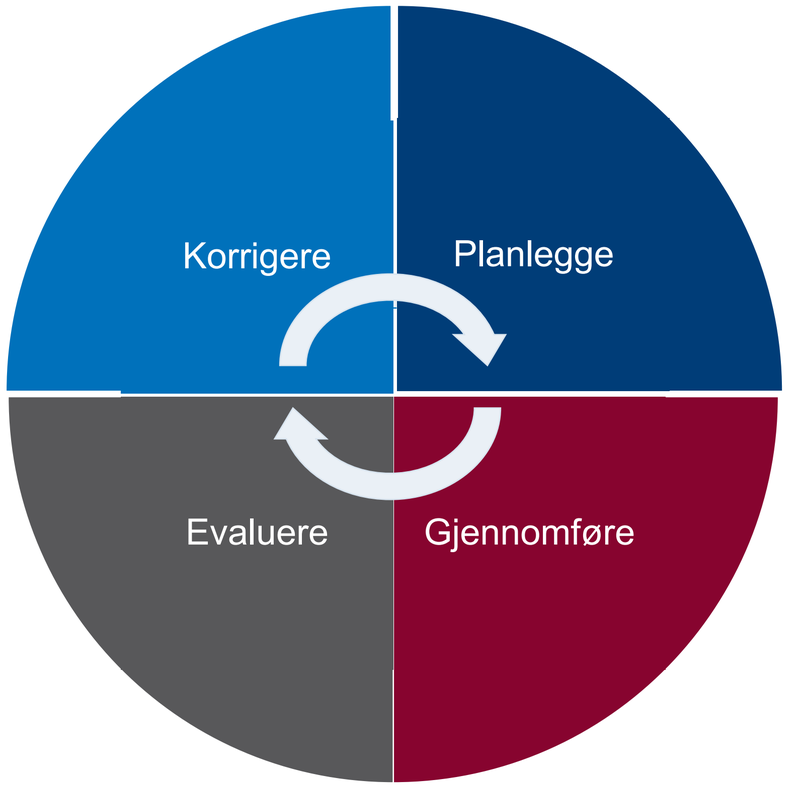
- Det skal foreligger en godkjent plan for sikkerhetsrevisjoner.
- Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner.

Ledelsens gjennomgang

- Øverste ledelse skal selv gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året.
- Dersom gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt, skal det vedtas tiltaksplaner med tiltaksfrister og plassering av ansvar.
- Ledelsens gjennomgang skal dokumenteres.

NORMEN

Normens krav til kontinuerlig forbedring



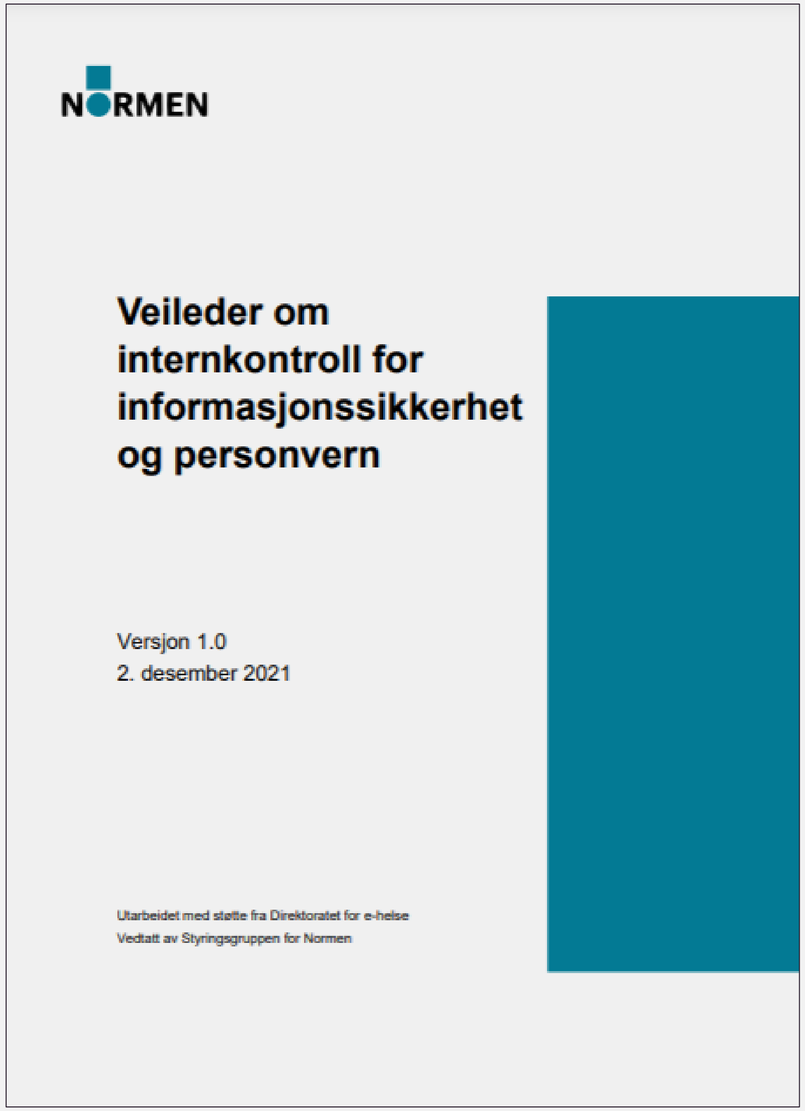
Avvikshåndtering (Håndtering av informasjonssikkerhetsbrudd)

- Virksomheten skal ha rutiner for å oppdage og håndtere avvik.
- Avvik skal behandles for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.
- Virksomheten skal samle inn fakta om hendelsesforløpet for etablering av korrigerende tiltak.

Kontinuerlig forbedring

- Ved alvorlige eller gjentatte avvik skal det gjennomføres ny risikovurdering.

NORMEN



SPØRSMÅL?

Plan for dagen

Klokkeslett	Tema
• 09:00	Intro om kurset og om Normen
• 09:45	Internkontroll
• 10:30	Pause
• 10:45	Risikostyring
• 11:30	Lunsj
• 12:15	Utvalgt personvern
• 13:00	Pause
• 13:15	Krav til informasjonssikkerhet
• 14:00	Pause
• 14:10	Normens krav i anskaffelser
• 14:40	Spørsmål og avslutning