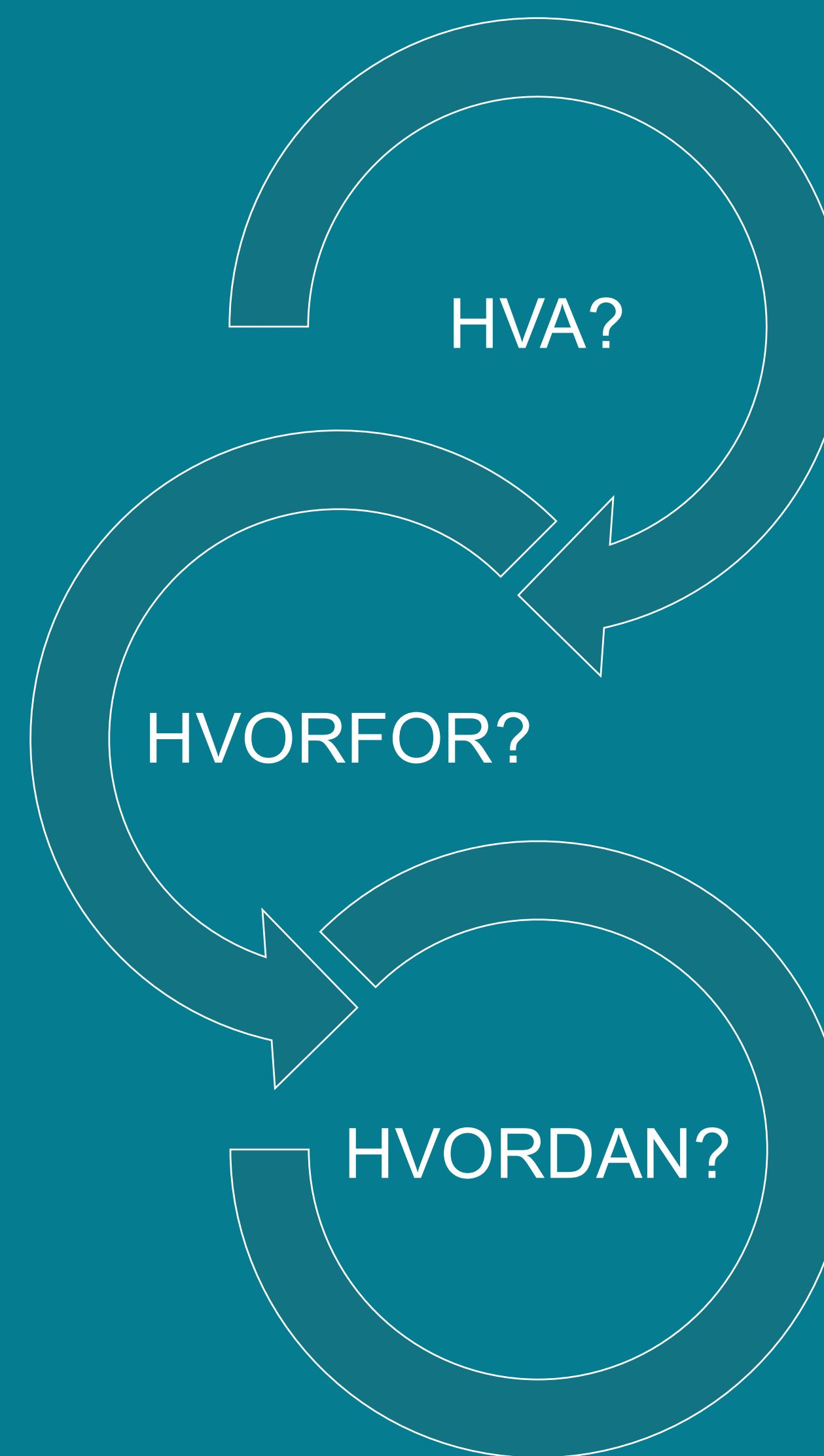




INTERNKONTROLL I NORMEN

Normkonferansen
23. april 2026



Hva er internkontroll

Med internkontroll menes i Normen

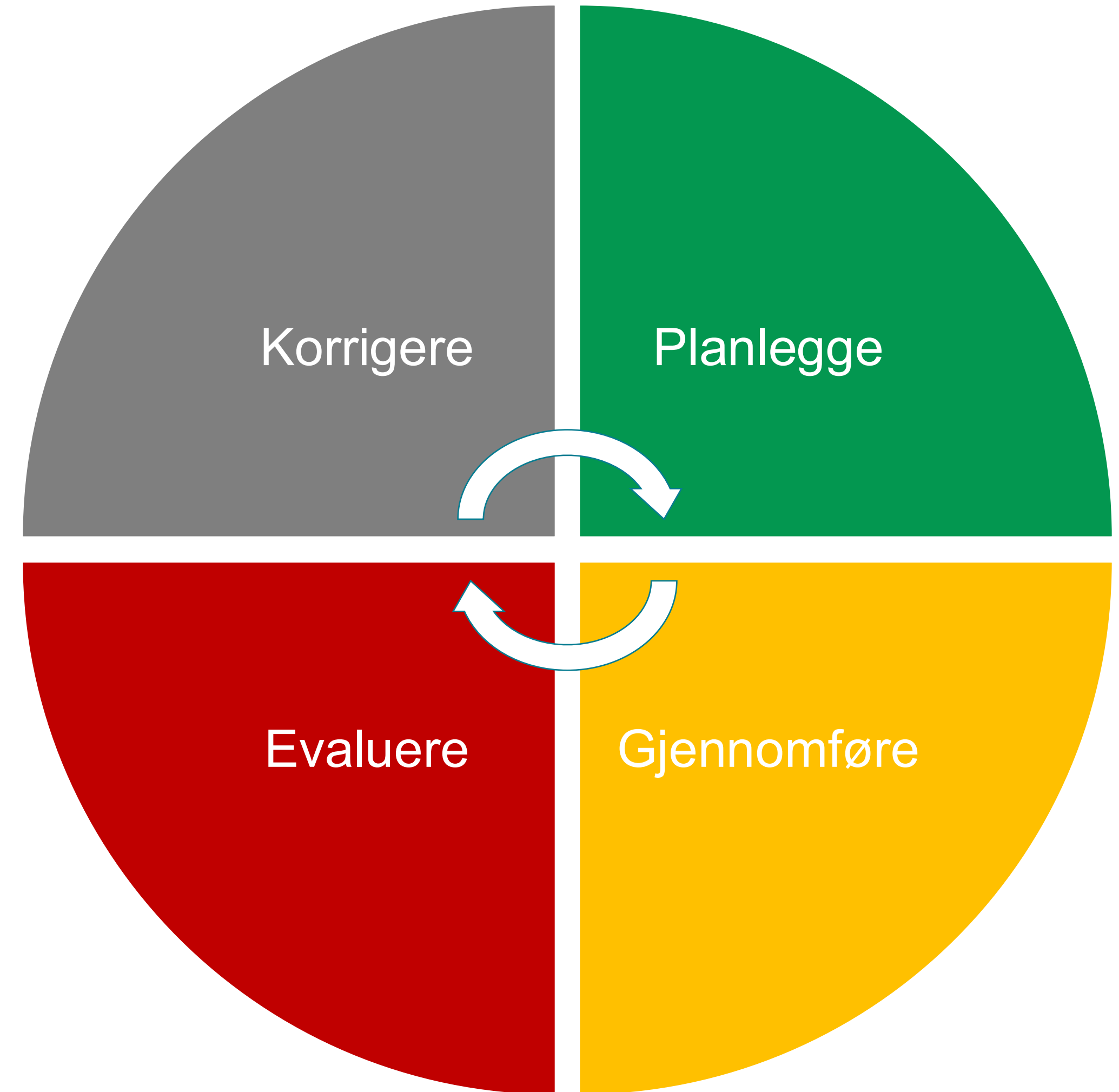
planlagte og **systematiske** tiltak som skal

sikre at virksomhetens aktiviteter

planlegges, organiseres, utføres og

vedlikeholdes i samsvar med krav fastsatt

i eller i medhold av lovgivningen.



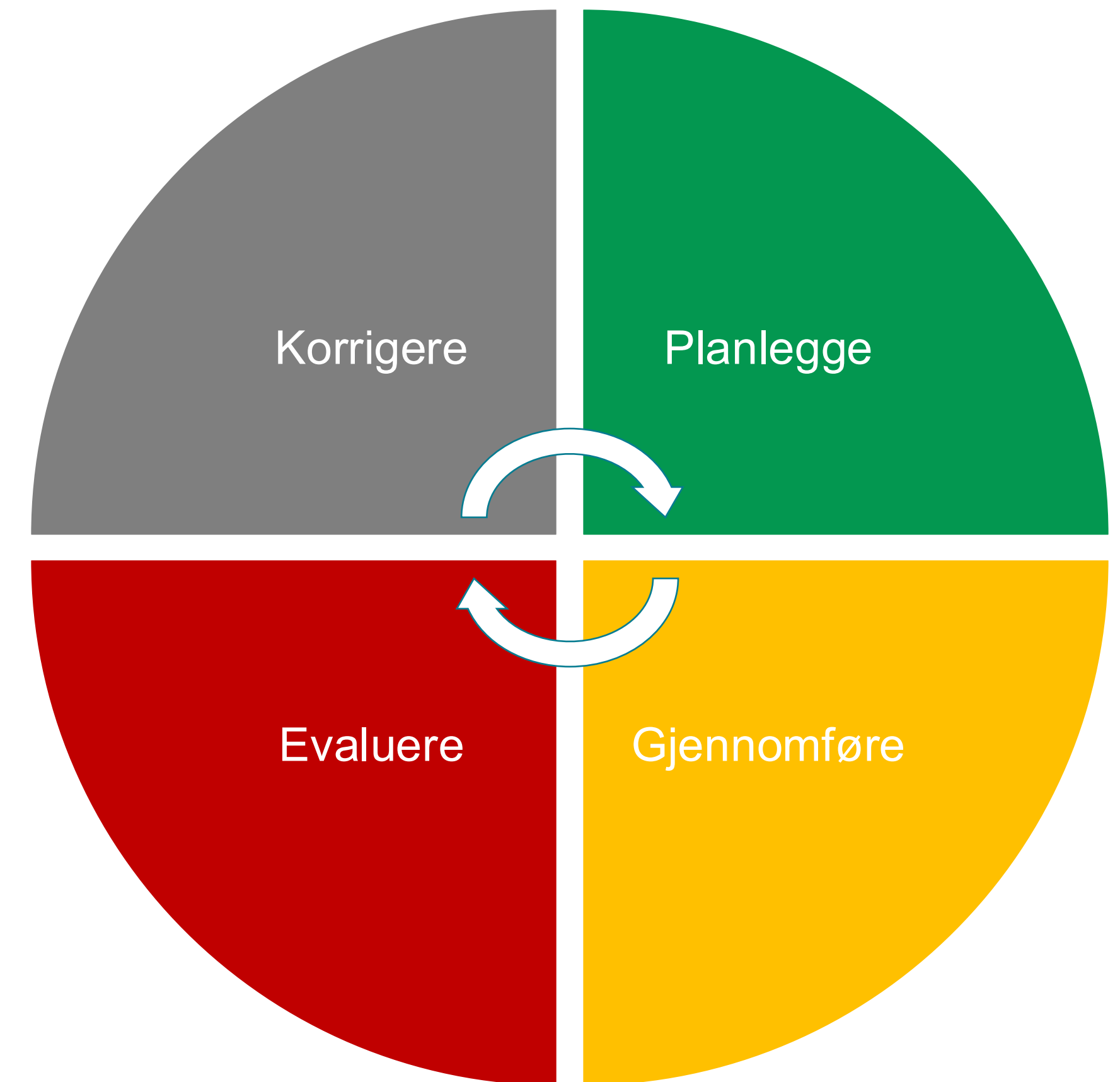
Internkontroll

Formål - bidra til

- Forsvarlige helse- og omsorgstjenester
- Pasient- og brukersikkerhet
- Øvrige krav i helse- og omsorgslovgivningen etterleves

Virksomhetsleders ansvar og plikt

- Sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter
- Plikt til å
 - Planlegge
 - Gjennomføre
 - Evaluere
 - Korrigere

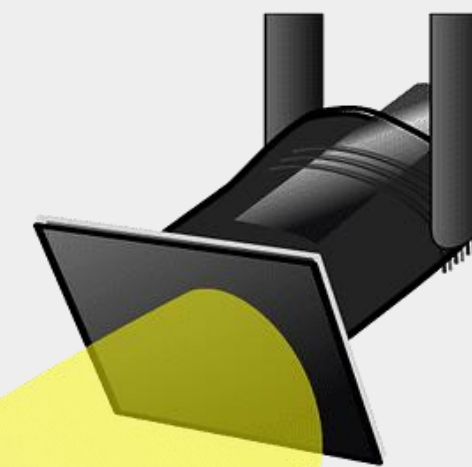


God informasjonssikkerhet er viktig for å kunne utøve forsvarlige helsetjenester, og ***internkontroll*** er et av de mest sentrale verktøyene som understøtter dette målet.

NORMEN



Personopplysningsloven



Forskrift om ledelse og
kvalitetsforbedring i helse- og
omsorgstjenesten



Personvernforordningen

« ... gjennomføre **egne tekniske og organisatoriske tiltak** for å oppnå et sikkerhetsnivå som er egnet **med hensyn til risikoen.**»

Artikkel 24. Den behandlingsansvarliges (dataansvarliges) ansvar

*«Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den **behandlingsansvarlige** gjennomføre egnede **tekniske og organisatoriske tiltak** for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.»*

Artikkel 32. Sikkerhet ved behandlingen

« ... Skal den **behandlingsansvarlige** og **databehandler** gjennomføre egnede **tekniske og organisatoriske tiltak** for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.»

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

§ 2. Virkeområde - Forskriften gjelder virksomheter som er pålagt internkontrollplikt etter

- a) Helsetilsynsloven § 5 - Plikt til å opprette internkontrollsystem og tilsyn med at det føres internkontroll
- b) Spesialisthelsetjenesteloven § 2-1a tredje ledd - De regionale helseforetakenes ansvar etter første ledd innebærer en plikt til å planlegge, gjennomføre, evaluere og korrigere virksomheten slik at tjenestenes omfang og innhold er i samsvar med krav fastsatt i lov eller forskrift.
- c) Helse- og omsorgstjenesteloven § 3-1 - Kommunens ansvar etter første ledd innebærer plikt til å planlegge, gjennomføre, evaluere og korrigere virksomheten, slik at tjenestenes omfang og innhold er i samsvar med krav fastsatt i lov eller forskrift.
- d) Tannhelsetjenesteloven § 1-3a - Fylkeskommunen skal planlegge, organisere og legge til rette for at fylkeskommunen, tannhelsetjenesten og helsepersonell kan oppfylle krav fastsatt i eller i medhold av lov eller forskrift.

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

- a) Spesialisthelsetjenesteloven § 3-4a - Enhver som yter helsetjenester etter denne lov, skal sørge for at virksomheten arbeider systematisk for kvalitetsforbedring og pasientsikkerhet.
- b) Helse- og omsorgstjenesteloven § 4-2 - Kvalitetsforbedring og pasient- og brukersikkerhet - Enhver som yter helse- og omsorgstjeneste etter loven her skal sørge for at virksomheten arbeider systematisk for kvalitetsforbedring og pasient- og brukersikkerhet.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 7.0

Vedtatt: 25. september 2025

[Hva er Normen?](#) →

Normen

- 1 Om Normen
- 2 Ledelse og ansvar
- 3 Risikostyring
- 4 Grunnleggende om behandling av helse- og personopplysninger
- 5 Informasjonssikkerhet
- 6 Vedlegg

Søk i Normen

Internkontroll

4 treff på «Internkontroll» i Normen

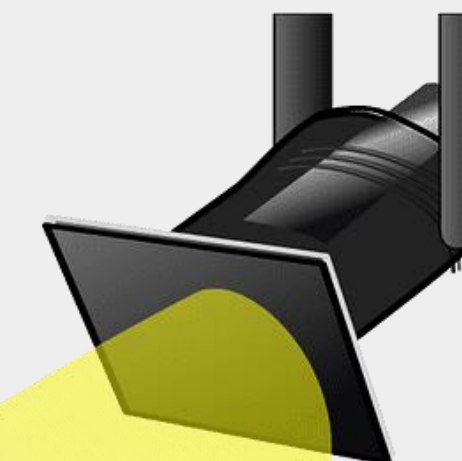
Kapitler

Oversikt over Normens krav

Styringssystem

Plikter og krav ved behandling av helse- og personopplysninger

Definisjoner



Internkontroll for informasjonssikkerhet og personvern

Veileder til Normen

Først publisert: 02. desember 2021
Siste faglige endring: 02. juni 2022



Veileder til Normen er godkjent og forvaltes av styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.



Små helsevirksomheter

Veileder til Normen

Først publisert: 14. november 2019
Siste faglige endring: 17. september 2020



Veileder til Normen er godkjent og forvaltes av styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Styringssystem for informasjonssikkerhet og personvern



Alle virksomheter i helse- og omsorgstjenesten skal etablere styringssystem

- Formålet er å:
 - sikre tilstrekkelig styring og kontroll
 - sikre og påvise etterlevelse av lover og regler
 - sikre at arbeidet ivaretas på en systematisk måte
 - være et verktøy for sikre at nødvendige sikkerhetstiltak etableres

Styringssystem

- **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.
- Styringssystemet skal **tilpasses** virksomhetens størrelse, egenart, aktiviteter og ha en **risikobasert tilnærming**. For mindre virksomheter betyr det at de ikke trenger et like omfattende styringssystem som store virksomheter.
- Viktig å ha et system som er **tilpasset virksomheten** og som en greier å følge opp og bruke aktivt

Styringssystem



Benevnes ofte som ...

- Internkontroll
- Styringssystem for informasjonssikkerhet (SSIS)
- Kvalitetssystem
- Ledelsessystem
- Information Security management system (ISMS) (ISO/IEC 27001)

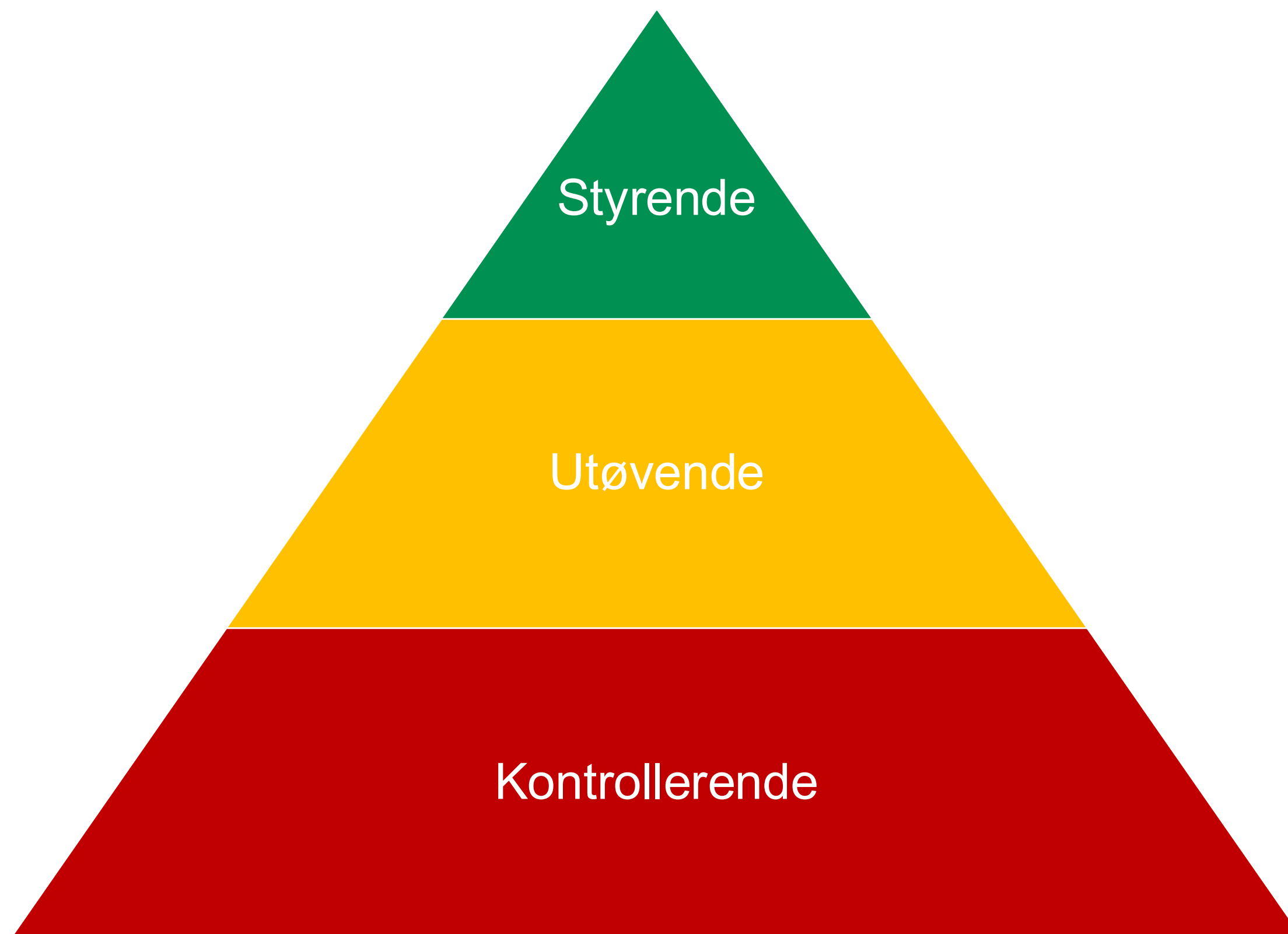
Hovedprinsipp:

Ett system - ett vedlikeholdspunkt

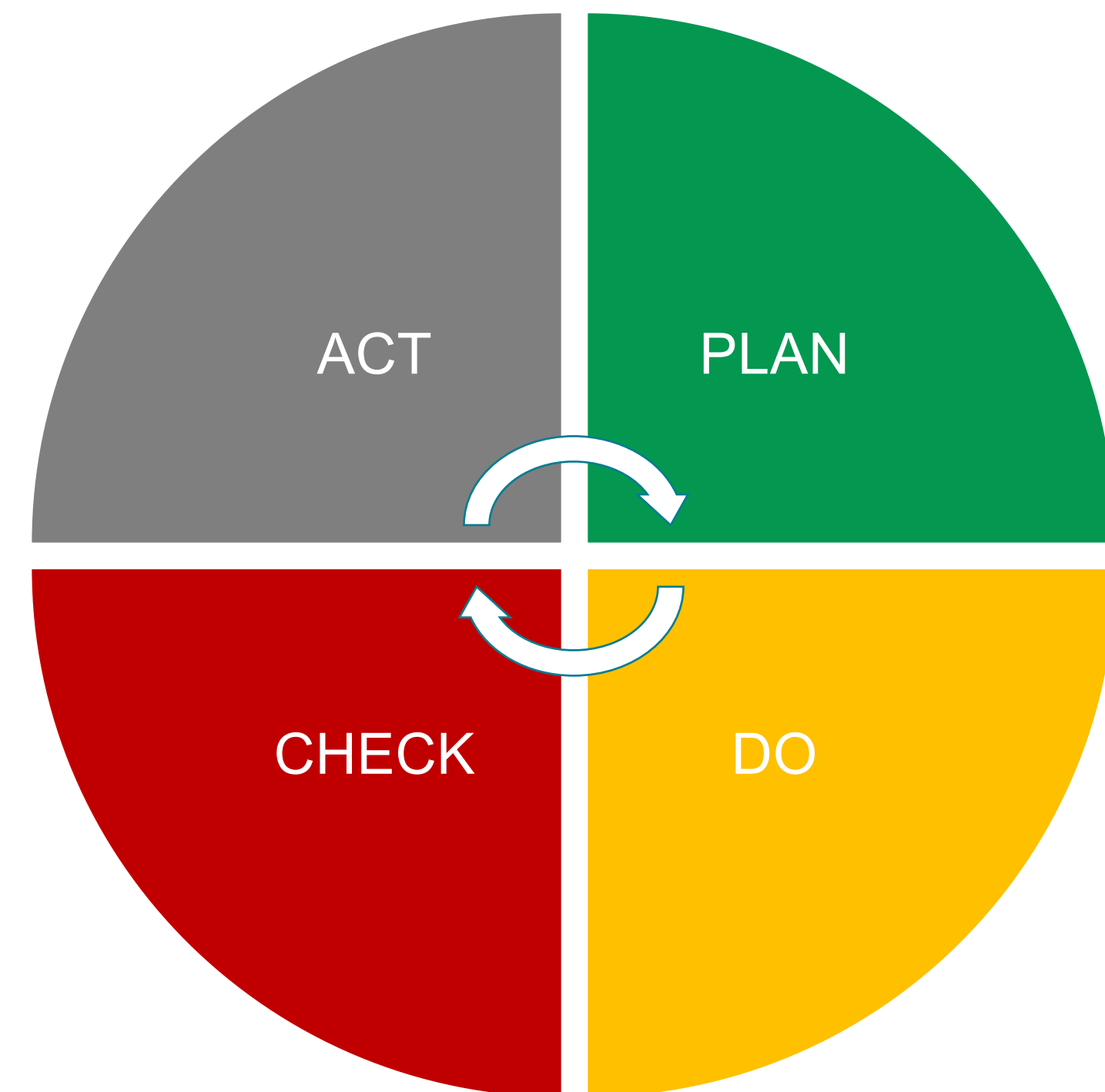


Ulike fremstillinger av styringssystemet

Hierarkisk modell



Sirkulær modell – PDCA



Roller og ansvar

- 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
- Virksomhetene i helse- og omsorgssektoren er dataansvarlig for all behandling av helse- og personopplysning som skjer i eller på vegne av virksomheten. Dataansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten.
- Videre har virksomhetens øverste ledelse et ansvar for å sikre at kravene til informasjonssikkerhet og personvern etterleves på **alle** nivåer i virksomheten, samt sørge for at styringssystemet kommuniseres og tilgjengeliggjøres for **samtlige** ansatte i virksomheten.
- 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.

Rolle	Beskrivelse
Virksomhetens leder	Den som har det overordnede ansvaret for virksomheten, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll). Informasjonssikkerhet og personvern bør inngå som en integrert del av den totale internkontrollen i virksomheten. <i>Oppgavene kan delegeres, men ikke ansvaret! All delegering skal gjøres skriftlig.</i>
(Linje-)leder	Følge opp virksomhetsleders ansvar i egen avdeling - delegert • Følge opp og kontrollere informasjonssikkerheten • Prioritere og gjennomføre tiltak
Fagansvarlig informasjonssikkerhet	Koordinere arbeidet med informasjonssikkerheten i virksomheten, på tvers av enheter Rådgiver til ledelsen og virksomheten for øvrig på informasjonssikkerhetsområdet
Fagansvarlig personvern	Koordinere arbeidet med personvern i virksomheten, på tvers av enheter Rådgiver til ledelsen og virksomheten for øvrig på personvernområdet
Fagansvarlig IKT	Sørge for at informasjonssystemet driftes og sikres iht. fastsatte krav Etablere nødvendig beredskap og sikre at beredskap øves
Alle medarbeidere	Følge virksomhetens prosedyrer og være bevisst på informasjonssikkerhet og personvern i egne arbeidsoppgaver.

Oversikt

- Skaff deg oversikt over hvilke digitale systemer virksomheten bruker og hvilke data som er lagret hvor
- Hvem har og bør ha tilgang til hvilke systemer?
- Hvilke leverandører har vi og hvilke tilganger har de?
- Har vi beskrivelser av alle arbeidsoppgaver vi skal utføre?
- Bruk gjerne behandlingsprotokollen som en start.

Ledelsens gjennomgang

HVA

- Endringer i
 - eksterne krav
 - infrastruktur og informasjonssystemer
 - behandling av helse- og personopplysninger
- Resultater fra interne vurderinger, målinger og evalueringer
 - Tester og øvelser
 - Deltakere på kompetansetiltak
- Tiltaksplan(er)

HVEM

- Øverste ledelse
- Ledere og fagpersoner
 - Informasjonssikkerhet
 - Personvern

I Normen er det beskrevet at virksomhetens ledelse selv skal gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året

HVORDAN

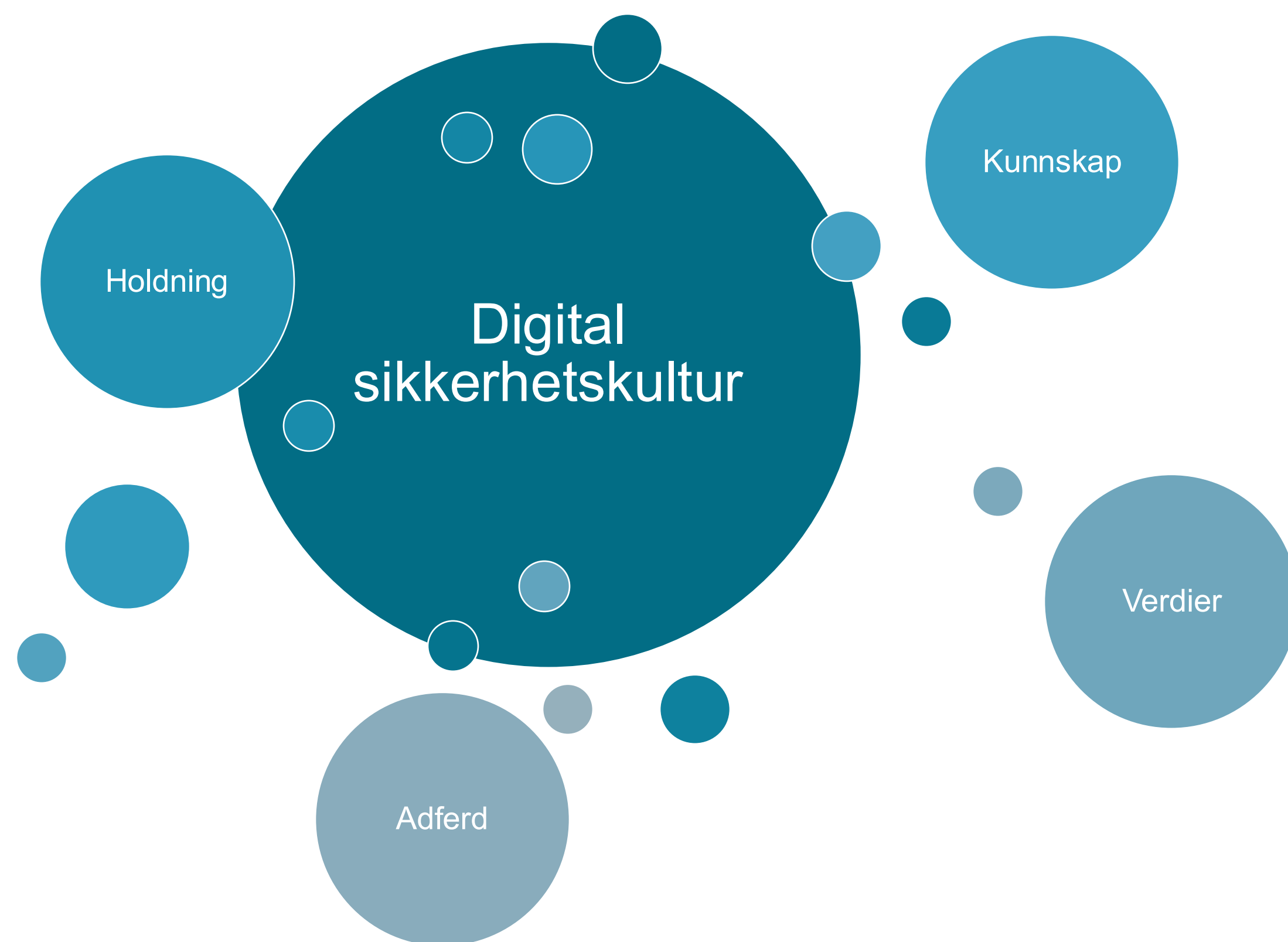
- Minst en gang i året
 - Eget møte?
 - Ledersamling(er)?
- Alt i en og samme prosess?
 - Helhetsbildet
 - Organisatoriske sammenhenger
 - Faglige sammenhenger
 - Mønster i avvik
 - Mønster i kultur
- **Dokumenter gjennomgangen med beslutninger og tiltaksplan**

Avvik – uønskede hendelser - sikkerhetsbrudd

- Som en del av sikkerhetsarbeidet (og arbeidet med en god sikkerhetskultur) er det viktig å etablere et godt system for å melde om og følge opp avvik
- Gjør det enkelt å melde avvik
- Ikke fokuser på enkeltpersoner, men se på hva som kan endres av systemer eller organisatoriske tiltak for at avviket ikke skal skje igjen.
- Formål:
 - Håndtere uønskede hendelser på systematisk måte
 - Gjenopprette normaltilstanden
 - Vurder endringer i sikkerhetsarbeidet for å hindre uønskede hendelser
- Husk at noen avvik også skal meldes eksternt

Medarbeidere, kompetanse og holdningsskapende arbeid (1)

Sikkerhetskultur er **summen av verdier, holdninger, kunnskap og normer** knyttet til sikkerhet blant ansatte i en organisasjon, og hvordan dette påvirker deres atferd og arbeidsprosesser



Overordnede krav

- Kontinuerlig lære opp medarbeidere i krav om ivaretagelse av taushetsplikten, informasjonssikkerheten og personvernet
- Etablere tiltak som sørger for at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte

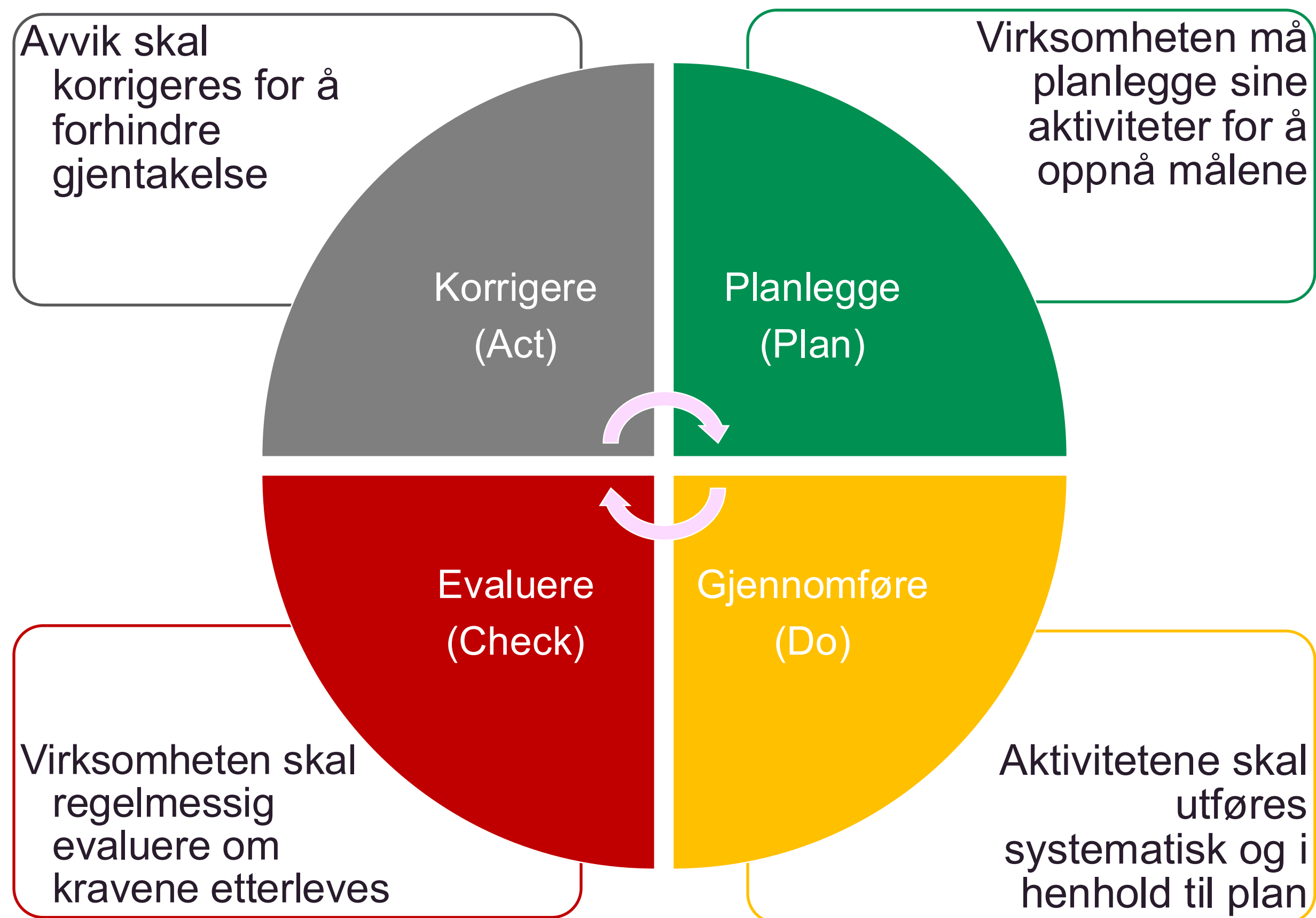
Medarbeidere, kompetanse og holdningsskapende arbeid (2)

- Jobb systematisk med å gi alle i organisasjonen kunnskap og ferdigheter de trenger for å utføre sitt arbeid på en god og trygg måte
- Etabler gjerne et årshjul for kompetanseheving
- Tilpass opplæringen til målgruppen (virksomhetens størrelse, arbeidsoppg., mv.)
- For å bygge en god sikkerhetskultur er det viktig å få med hele organisasjonen og da særlig få ledelsen til å gå foran som gode eksempler
- Etabler, bruk og vedlikehold opplæringsprogram for ledere og medarbeidere

Utdanningsdirektoratet:

«Kompetanse er å kunne tilegne seg og anvende kunnskaper og ferdigheter til å mestre utfordringer og løse oppgaver i kjente og ukjente sammenhenger og situasjoner. Kompetanse innebærer forståelse og evne til refleksjon og kritisk tenkning.»

Kontinuerlig forbedring



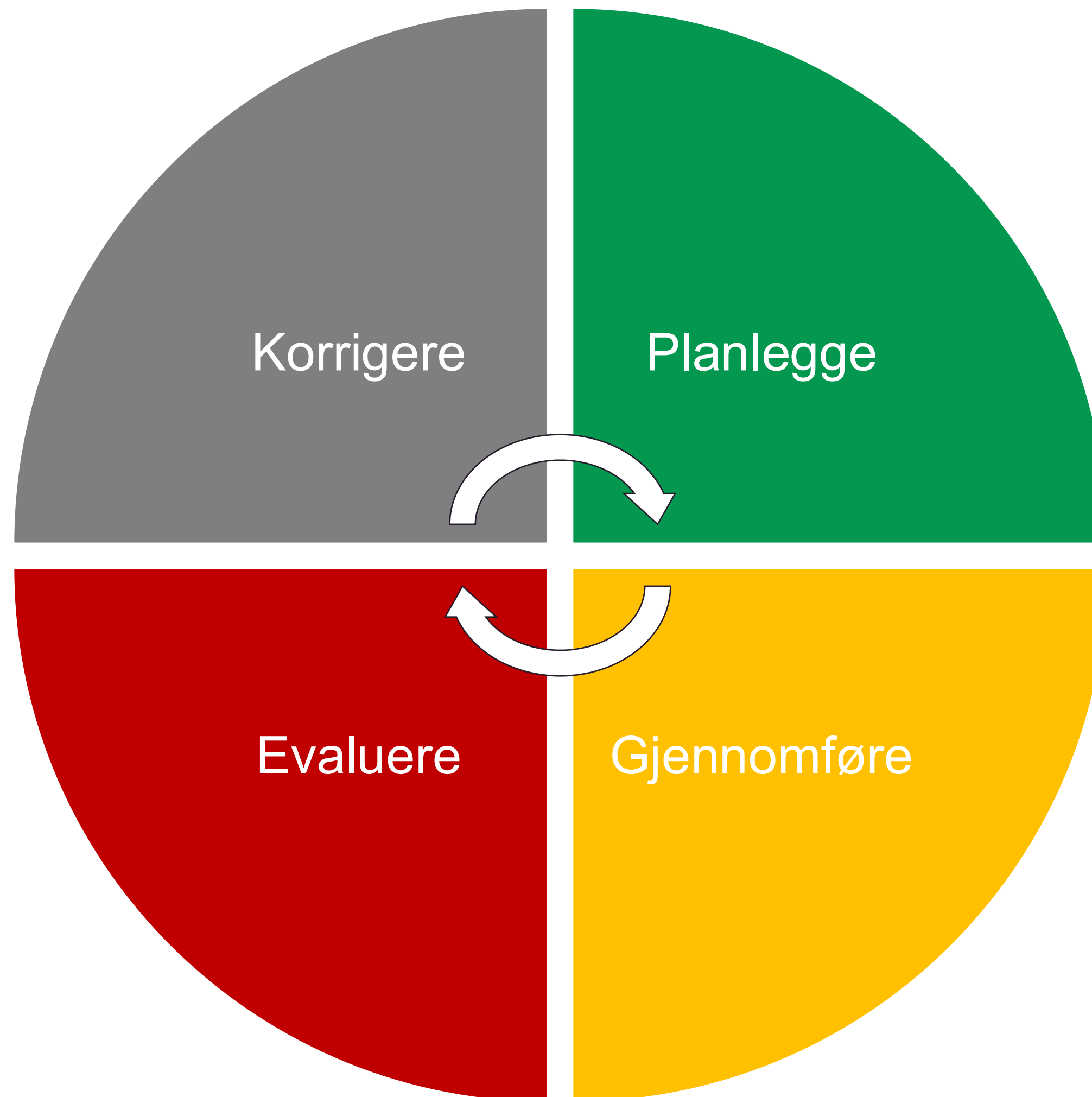
Kontinuerlig forbedring

- «... også der informasjonen brukes «sekundært» ...»

Krav til dokumentasjon

- styringssystemet skal dokumenteres, og at
- dokumentene skal holdes **løpende oppdatert**
- eldre versjoner skal arkiveres

Husk at arbeidet med internkontroll er en kontinuerlig prosess og ikke en «papierøvelse»



Jobb kontinuerlig og systematisk
Skaff oversikt
Dokumenter
Forbedre og lære
Gjenta

Sikkert.no

- [Sikkert.no](#) er en nasjonal portal med informasjon, råd og veiledning om digital sikkerhet.
- Du finner råd og anbefalinger digital sikkerhet i praksis
- Se veiledningen om arbeid med internkontroll
[Styring av informasjonssikkerhet og personopplysningsvern](#)
- Den supplerer den veiledningen du finner i Normen på en god måte
- Felles sikkerhet i forvaltningen (FSIF) er et samarbeid som skal bidra til et nasjonalt løft for informasjonssikkerhet og personopplysningsvern i offentlige virksomheter

sikkert.no

InnbyggerBedriftOffentligOm oss

Nasjonal portal for digital sikkerhet

Digital trygghet, fra hverdag til nasjonal beredskap, er et felles ansvar og angår både innbyggere, bedrifter og offentlig forvaltning i Norge.

Sikkert.no driftes av myndighetene i Norge, og er en nasjonal portal med informasjon, råd og veiledning om digital sikkerhet.

Anbefalinger om styring av informasjonssikkerhet og personopplysningsvern

Utarbeidet av Digdir, Datatilsynet, NSM, KS, DFØ og Helsedirektoratet i programmet Felles sikkerhet i forvaltningen.

Innhold

Introduksjon.....3

Sammenheng med tilgjengelig veiledning3

LS - Ledelsens styring og oppfølging.....5

LS-1Gi føringer.....5

LS-2Sørge for budsjett til arbeidet.....6

LS-3Kommunisere viktighet.....6

LS-4Løfte og håndtere problemstillinger gjennom linjen6

LS-5Virksomhetsledelsens gjennomgang7

OP – Ha oversikt og prioritere8

OP-1Oversikt over ansvarsområde8

OP-2Kartlegge eksterne krav9

OP-3Vurdere behov for risikovurderinger.....9

OP-4Oppdatert oversikt over risikovurderinger9

RV - Vurdering av risiko11

RV-1Planlegge risikovurdering.....11

RV-2Vurdere personvernkonsekvensvurdering (DPIA)12

RV-3Gjennomføre risikovurdering13

NORMEN

Side 22



SPØRSMÅL?



Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 7.0

Normen

Først publisert: 28. juni 2006
Siste faglige endring: 25. september 2025



Normen er godkjent og forvaltes av styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.



Internkontroll for informasjonssikkerhet og personvern

Veileder til Normen

Først publisert: 02. desember 2021
Siste faglige endring: 02. juni 2022



Veileder til Normen er godkjent og forvaltes av styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

- 1 Innledning
- 2 Internkontroll i helse- og omsorgssektoren
- 3 Vedlegg
 - 3.1 Eksempler på sikkerhetsansvar, -roller og oppgaver
 - 3.2 Eksempel på styringssystemets innhold
 - 3.3 Forslag til opplæringsprogram
 - 3.4 Tips og råd til daglig informasjonssikkerhet
 - 3.5 Instruks for bruk av informasjonsteknologi



Små helsevirksomheter

Veileder til Normen

Først publisert: 14. november 2019
Siste faglige endring: 17. september 2020



Veileder til Normen er godkjent og forvaltes av styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.