Oslo

Grunnkurs i styringssystem for informasjonssikkerhet og personvern

Teamskurs 21. januar 2021

Jeanne H. Espedalen ISI
Tommy Nysveen ISI

Foto: Benjamin Pham

Velkommen og kjøreregler

- Introduksjon Tommy og Jeanne
- Mange deltagere i dag, skru av lyden underveis og rekk opp hånda eller skriv spørsmål eller kommentarer i chatten.
- Vi vil stoppe noen ganger underveis for å svare på spørsmål.
- 10 minutter pause ca. kl. 12.50
- Vi forsøker å sette av god tid til å svare på spørsmål på slutten

Hva skal det handle om i dag?

- Hvorfor må alle virksomhetene ha styringssystem for personvern og informasjonssikkerhet?
- Hva er det overordnede styringssystemet for Oslo kommune?
- Grunnprinsipper - Hva er et styringssystem for informasjonssikkerhet og personvern?
- Hvilke elementer må vi ha på plass?
- Hvordan kan du lære mer om dette og finne mer informasjon?

Hvorfor må vi ha styringssystem?

Fra fellesføringer i tildelingsbrevet til alle virksomheter for 2020:

«Tilstrekkelig styring og kontroll av informasjonssikkerheten, herunder rutiner for systematiske risikovurderinger og hendelses- og avvikshåndtering, er vesentlig. I løpet av 2020 skal virksomhetene ha etablert internkontroll i tråd med krav i eforvaltningsforskriften og personopplysningsregelverket, også omtalt som et styringssystem eller ledelsessystem for informasjonssikkerhet.»

- Det handler om **tilstrekkelig styring og kontroll**
- Det er et **lederansvar** å skape og ivareta en organisasjon med tilstrekkelig styring og kontroll. Kalles også internkontroll eller ledelsessystem
- Styringssystem for informasjonssikkerhet og personvern er et **verktøy** for å sikre tilstrekkelig styring og kontroll på området

Virksomhetens behov

- Et styringssystem skal sikre virksomheten intern styring og kontroll og skal fungere som virksomhetens egenkontroll.
  - Kvalitetssikring som sikrer at virksomheten har systemer og rutiner som fungerer, og som fanger opp problemer og utfordringer i tide.
- Formålet er at ledere på alle nivå skal få tilstrekkelig (eller rimelig) sikkerhet om at man når virksomhetens samlede mål;

  - At man når mål- og resultatkrav
  - At arbeidsprosesser er effektive
  - At man etterlever lover og regler

Hvilke risikoer har vi?

HACKET: Østre Toten kommune. Foto: Geir Olsen

Angrepet av hackere – hele kommunen rammet

OPPSUMMERT

Natt til lørdag 9. januar ble Østre Toten kommune utsatt for et dataangrep. Alle sikkerhetskopier er slettet og alle data kryptert. Mens ingen av de 1300 ansatte i kommunen får brukt noen av datasystemene, kreves kommunen for løsepenger.

- Store konsekvenser for kommunens drift;
  - Tjenester er ikke tilgjengelige
  - Sosialhjelpsmottagere må søke på nytt
  - Sykehjemsbeboer fikk utdelt bjeller for å ringe i
  - Risiko for at personsensitive data kan være på avveie

- Fremover:
  - Gjenoppretting – er noe tapt permanent?
  - Tap av tillitt og omdømme
  - Bot/gebyr
  - ?

Kunne noe tilsvarende ha skjedd i din virksomhet?

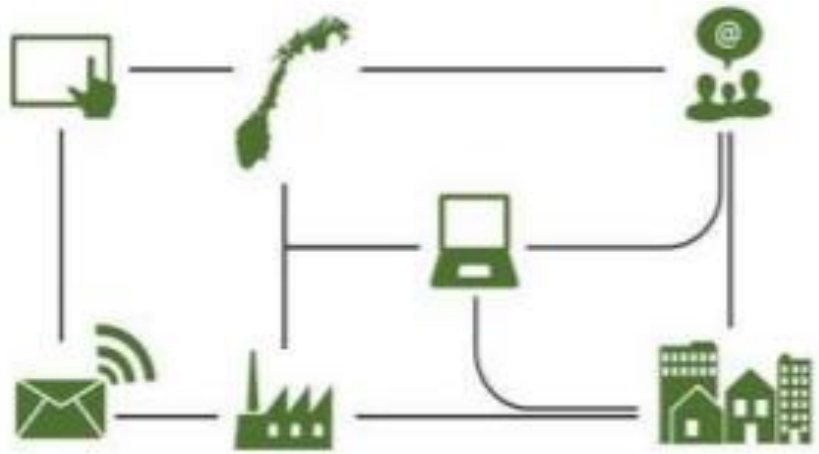
Vet vi hva vi skal beskytte?
Hvordan kan vi forebygge og forbedre/forberede?
Øver vi på å håndtere hendelser?
Lærer vi når det skjer noe?..

Det handler om informasjonsverdier og risikostyring

- **Risikoer** må **identifiseres, vurderes og håndteres** både jevnlig og når uønskede hendelser inntreffer.
- **Tiltak** må tilpasses **akseptabelt risikonivå**
- Det krever en **helhetlig systematikk** for å ha (tilstrekkelig) kontroll på risikoene

Personopplysninger er en stor og viktig gruppe av informasjonsverdier i Oslo kommune
(men også mye annet)

Myndighetenes behov



Risikoer øker i en digital verden uten internkontroll

Internkontroll sikrer effektiv bruk av offentlige midler

Når farten i digitaliseringen øker er det viktig å beholde styringen!

En lønnsom investering

- Et velfungerende styringssystem gir:
  - god intern styring og kontroll
  - tilstrekkelig sikkerhet for at virksomheten når sine samlede mål
  - grunnlag for å ta riktige beslutninger
  - bevisstgjøring internt i virksomheten og bedre kontroll på risikoene
  - målrettet og effektiv bruk av offentlige midler
  - redusert sannsynlighet for ineffektivt arbeid og lovbrudd
  - redusert sannsynlighet for omdømmetap og økonomiske tap for innbyggere, næringsliv og virksomheten selv
  - minimert sannsynlighet for hendelser som kan bety fare for liv og helse
- Etablering av internkontroll kan kreve investering i tid og penger, spesielt den første tiden. Men det vil være lønnsomt!

Hvilke krav gjelder for virksomheter i Oslo kommune?

Kommunens regelverk

- Reglement for IKT og informasjonssikkerhet
- Instruks for virksomhetsstyring
- Instruks for informasjonssikkerhet

Lovverk og bransjestandarder

- Kommuneloven
- E-forvaltningsforskriften
- Personopplysningsloven
- Norm for informasjonssikkerhet i helsesektoren
- Offentleglova
- Forvaltningsloven
- Arkivloven
- Sikkerhetsloven med forskrifter
- ..

§

Krav til **at** virksomhetene skal ha styringssystemer/internkontroll

Spesifikke krav til **innholdet** i styringssystemene

Instruks for informasjonssikkerhet

- Forankring av «Ledelsens gjennomgang» og «Virksomhetsleders egenerklæring»
- Krav til sikkerhetsarbeidet
  - Roller og ansvar
  - Dokumentasjon og rapportering
  - Oppfølging kontroll og revisjon
- Krav til kartlegging og oversikt
  - Forpliktelser og rettslige krav
  - Informasjonsverdier
- Krav til sikring av informasjon
  - Den enkeltes ansvar
  - Fysisk sikring
  - Tilgangskontroll
  - Anskaffelser, utvikling og vedlikehold av systemer
  - Drift av systemer og IKT-infrastruktur
  - Hendelseshåndtering og kontinuitetsplanlegging

Instruks for virksomhetsstyring

- Roller og ansvar - internt i virksomheten og overfor databehandlere, intern leverandør og eventuelle andre som ivaretar informasjonssikkerhetsoppgaver for virksomheten
- Risikostyring; Risikovurderinger skal utgjøre en sentral del av grunnlaget for å velge ut relevante sikkerhetstiltak
- Oppfølging, intern kontroll og revisjon av tiltak, rutiner osv. for å sikre etterlevelse.
  - Årlig ledelsens gjennomgang

Hva sier lovene?

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

§ 15. *Internkontroll på informasjonssikkerhetsområdet*

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.

Styringssystemer på mange områder

Bruk	Forankring/metodikk/veiledning
Virksomhetsstyring/ Økonomistyring	COSO-rammeverket /Økonomiregelverket (++)
Kvalitetsstyring	ISO 9001
IT-styring	COBIT, TOGAF, ITIL, ISO ...
HMS	Internk.forskr./OHSAS 18001
Miljøstyring	ISO 14001, Miljøfyrtårn...
Informasjonssikkerhet og personvern	**ISO 27001/27701**,NIST, ISACA, Personopplysningsloven/GDPR
Samfunnssikkerhet	ISO 223x, ...
Rikets sikkerhet	Sikkerhetsloven, NSM grunnprinsipper

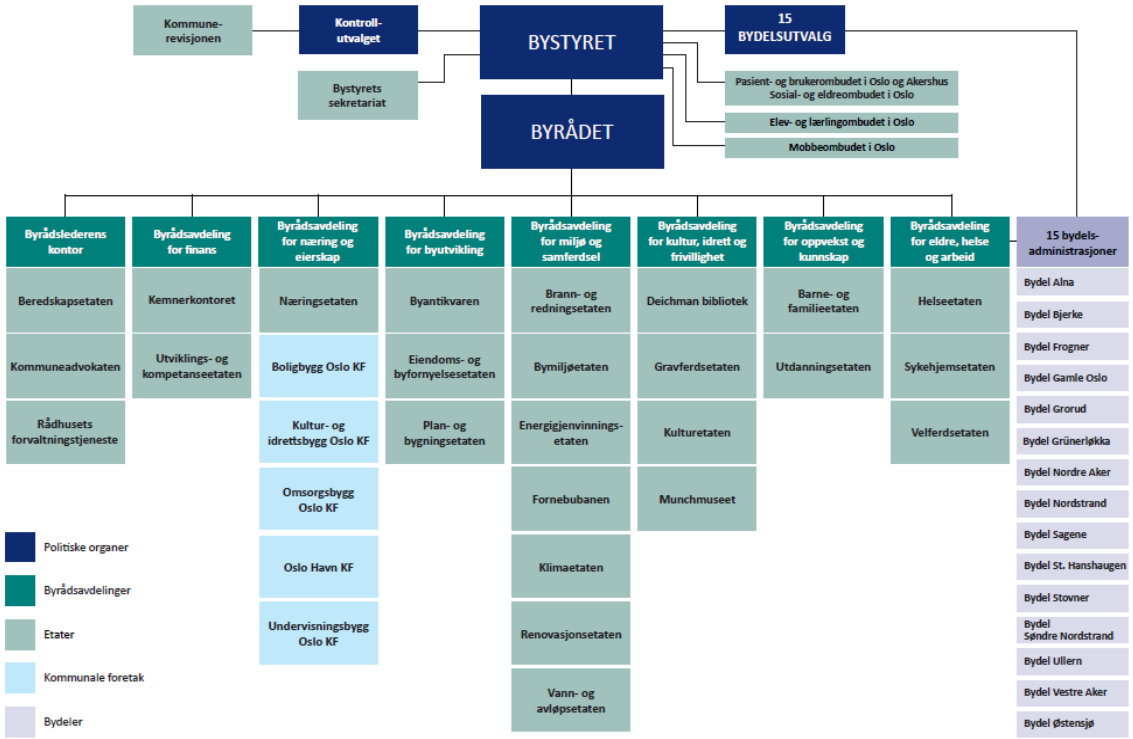
Det vil ofte være hensiktsmessig å oppfylle kravene til **Informasjonssikkerhet og personvern** innenfor rammene av et eksisterende styringssystem

?

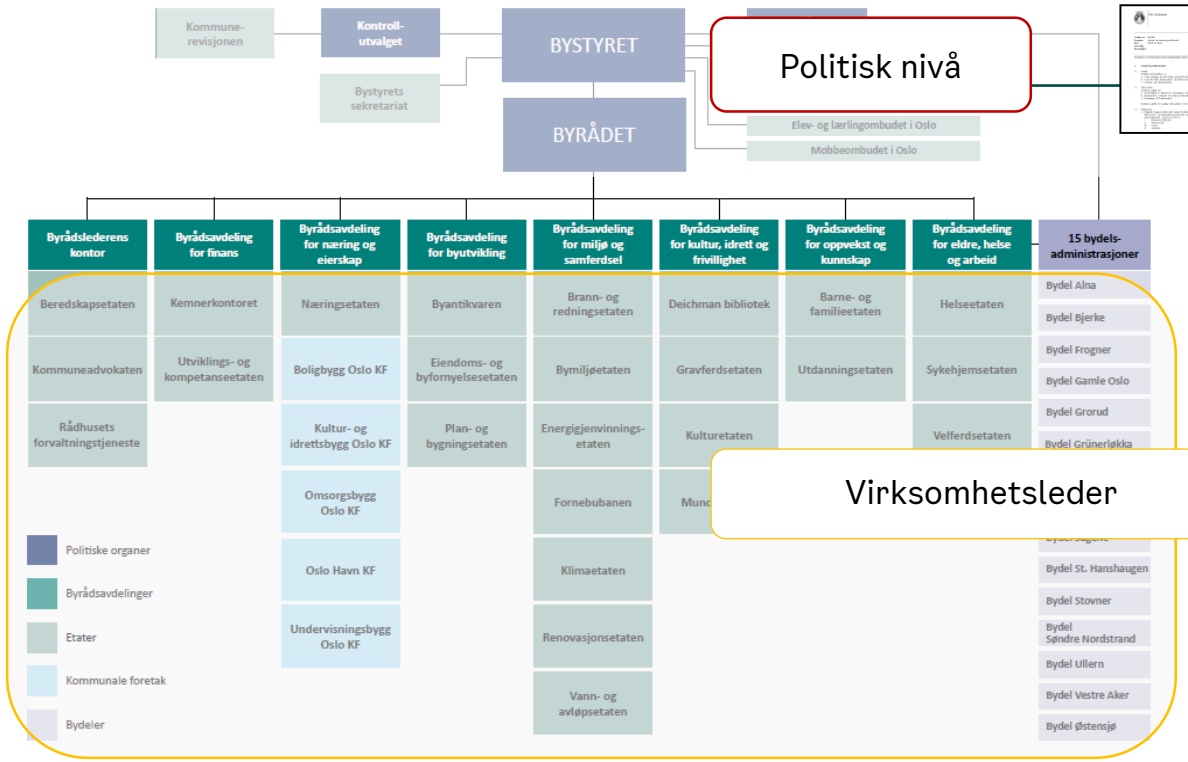
Styring og kontroll på informasjonssikkerhet Oslo kommune

- En overordnet forklaring – gjennomgående i hele kommunen

Styring og kontroll informasjonssikkerhet Oslo Kommune



Styring og kontroll informasjonssikkerhet Oslo Kommune



Politisk nivå

vedtar

NIVÅ 1

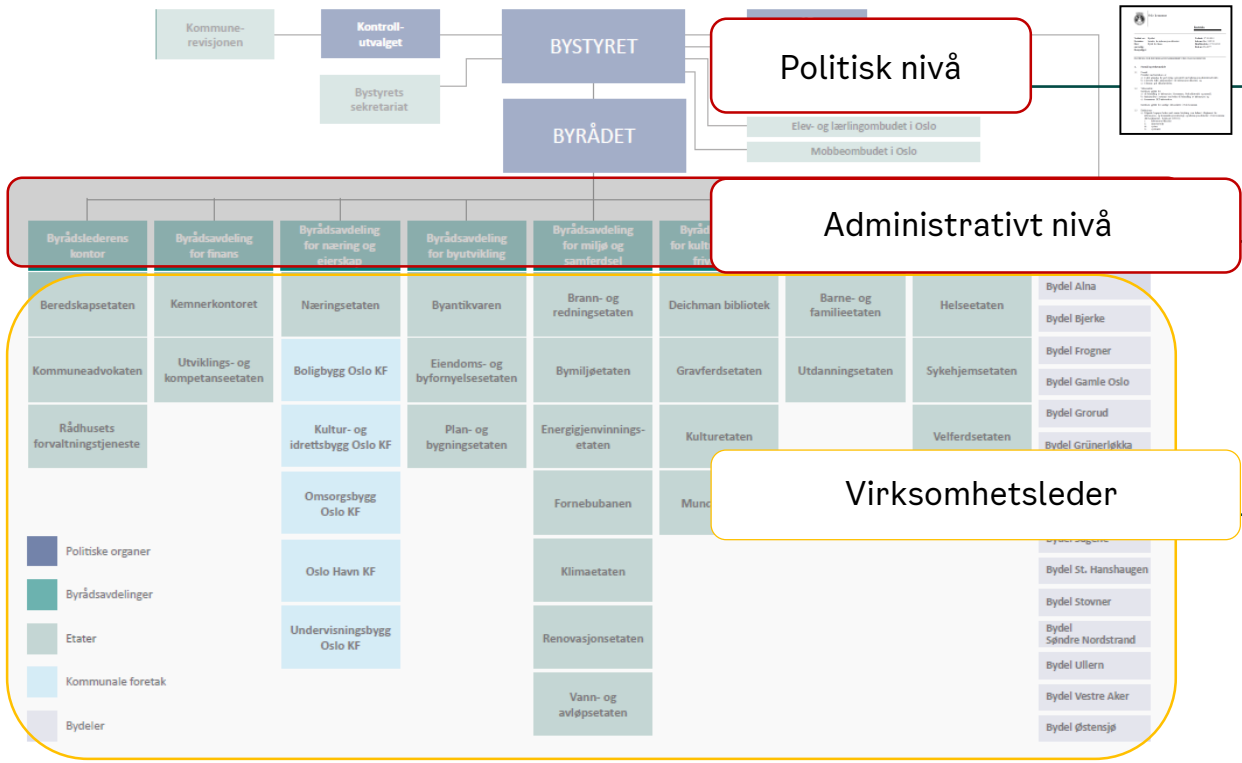
Instrukser og reglement

Virksomhetsleder

NIVÅ 3

Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Styring og kontroll informasjonssikkerhet Oslo Kommune



Politisk nivå

vedtar

Administrativt nivå

vedtar

Virksomhetsleder

NIVÅ 1

Instrukser og reglement

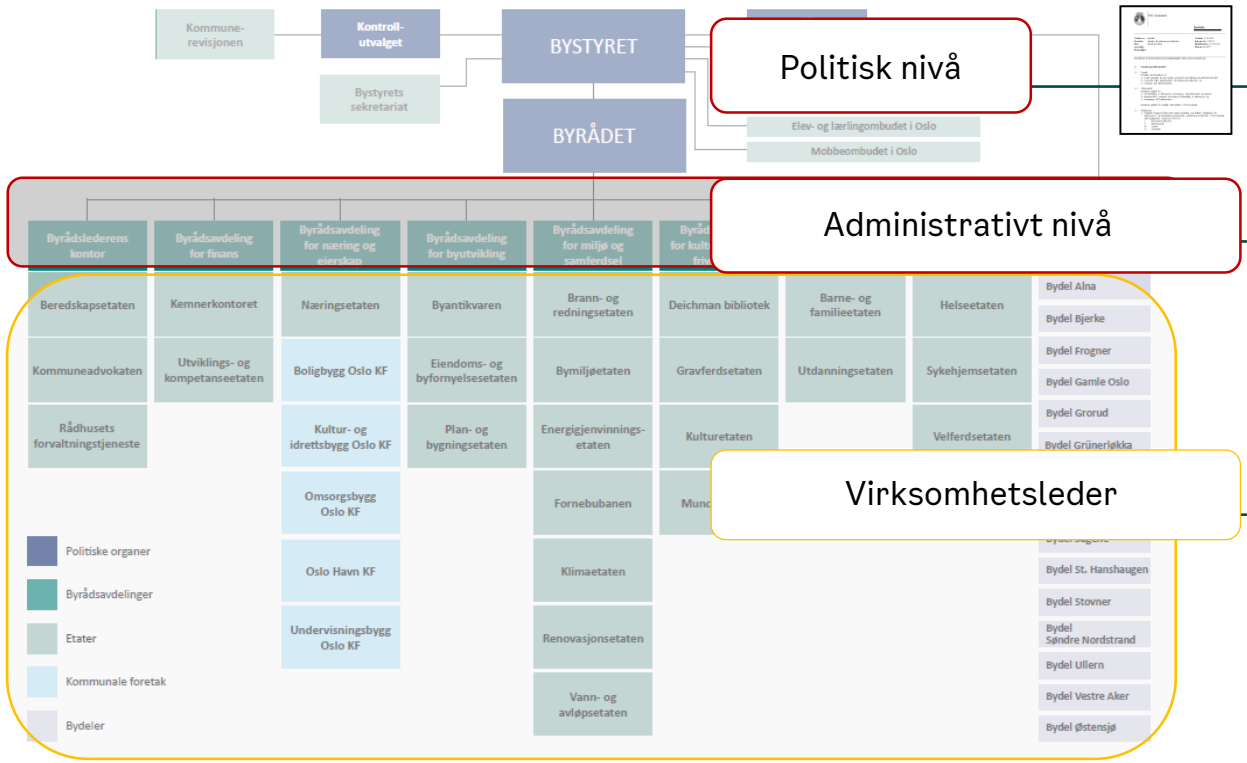
NIVÅ 2

Standarder
(skal gjelde for alle virksomheter i Oslo kommune)

NIVÅ 3

Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Styring og kontroll informasjonssikkerhet Oslo Kommune



Politisk nivå

Administrativt nivå

Virksomhetsleder

vedtar

vedtar

NIVÅ 1

Instrukser og reglement

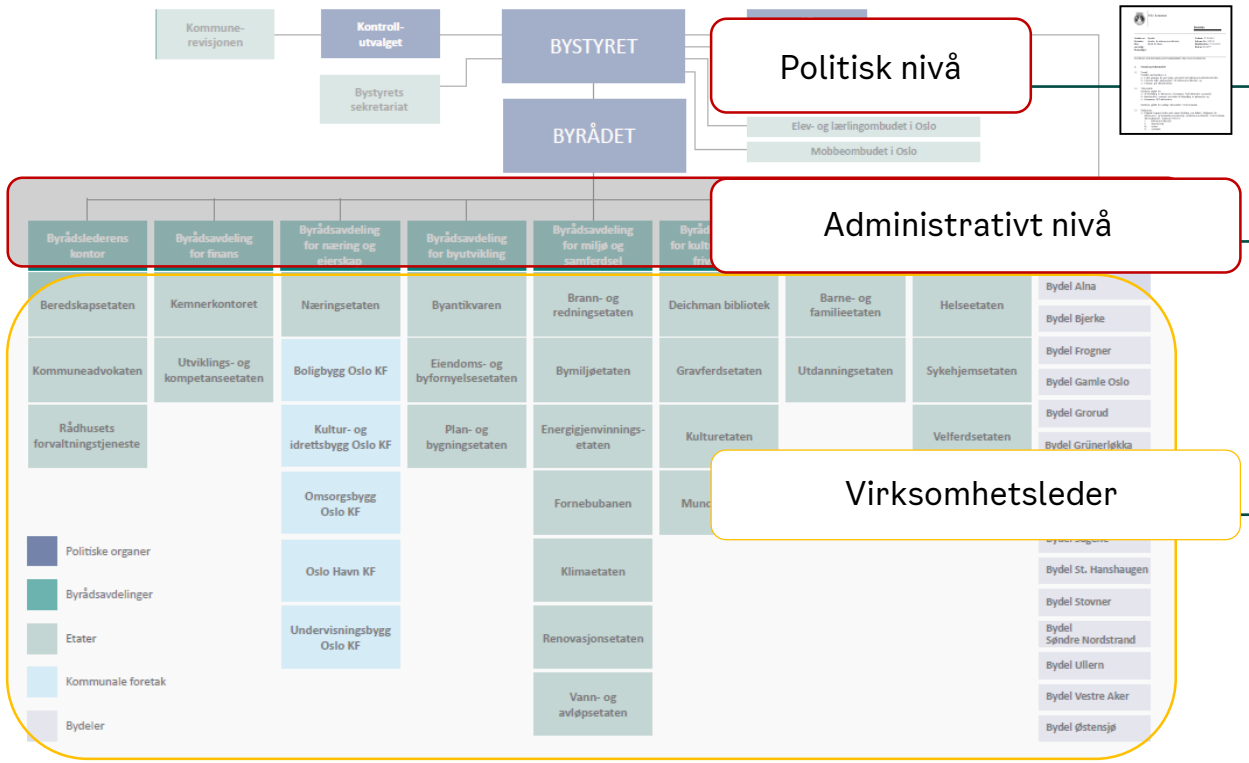
Standarder
(skal gjelde for alle virksomheter i Oslo kommune)

NIVÅ 3

Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Styring og kontroll informasjonssikkerhet Oslo Kommune

Utgjør det overordnede styringssystemet



Politisk nivå

Administrativt nivå

Virksomhetsleder

vedtar

vedtar

NIVÅ 1

Instrukser og reglement

Standarder
(skal gjelde for alle virksomheter i Oslo kommune)

NIVÅ 3

Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Overordnet styringssystem for informasjonssikkerhet i Oslo Kommune

- Hvorfor videreutvikler vi det ?
- Hva skal det bidra til ?
- Hva er det ?

Overordnet styringssystem for informasjonssikkerhet i Oslo Kommune

- Skal bidra til bedre styring og kontroll på informasjonssikkerhet i virksomhetene gjennom, og vi ønsker fremover
  - Tydeliggjøring av de overordnede krav og føringene
  - Bidra til å minske avstand mellom overordnede krav og føringer og operasjonalisering i den enkelte virksomhet gjennom utarbeidelse av styringssystemer for informasjonssikkerhet
- Bidra til bedre forutsigbarhet for virksomhetsledere og fagpersoner
  - Ved at de bl.a får bedre trygghet for at de klarer å se risikoen og de blir bedre rustet til å kunne beslutte gode og relevante tiltak
- Bidra til at sentrale risikoområder ivaretas i alle sektorer

Rammebetingelser for videreutvikling av det overordnede styringssystemet

- Styrende dokumentene for informasjonssikkerhet
- Lover, forskrift og regler
- Se hen til erfaringer fra andre fagområder, som f.eks anskaffelser
- Tett involvering av byrådsavdelingene og virksomhetene

Informasjonssikkerhet

Det er vedtatt flere styrende dokumenter for informasjonssikkerhet i Oslo kommune. Disse gjelder for alle virksomhetene. Dokumentene angir rollefordeling i kommunen, ansvar for ulike rolle, krav til sikkerhetsarbeidet i kommunen, omtale av hendelseshåndtering mv.

IKT-reglement for Oslo kommune

IKT-reglement for Oslo kommune (byrådssak 1099/10)

Instruks for informasjonssikkerhet

Instruks for informasjonssikkerhet for Oslo kommune (byrådssak 1105/13)

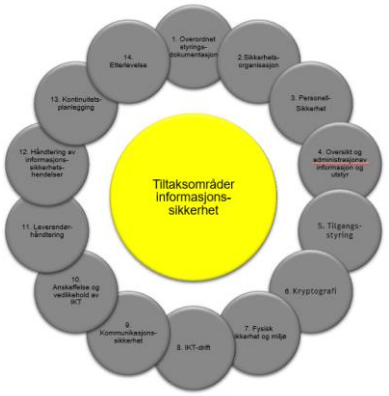
Instruks for virksomhetsstyring

Instruks for virksomhetsstyring i Oslo kommune (byrådssak 1070/15, endret i sak 1107/16, sist i sak 1104/17)

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

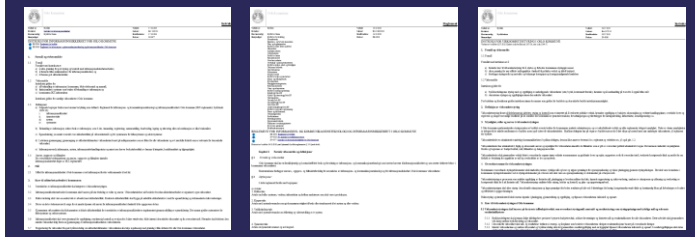
Dato	FOR-2004-06-25-988
Departement	Kommunal- og moderniseringsdepartementet
Publisert	I 2004 hefte 10
Ikrafttredelse	01.07.2004
Sist endret	FOR-2014-02-07-102 fra 01.07.2014
Gjelder for	Norge
Hjemmel	LOV-1967-02-10-§15a, LOV-2001-06-15-81-§5, LOV-1992-12-04-126-§12, jf LOV-2018-06-15-44-§10
Kunngjort	29.06.2004
Rettet	05.08.2014 (§ 3 annet ledd)
Korttittel	eForvaltningsforskriften

Risikoområder som typisk dekkes i et styringssystem for informasjonssikkerhet



Nivå 1

Retningslinjer og instrukser



Nivå 2

Eksempel – tydeliggjøring av krav til hendelseshåndtering

Instruks for informasjonssikkerhet for Oslo kommune

5.6 Hendelseshåndtering

a) Varsling og håndtering av hendelser (avvik, feilsituasjoner eller fare for slike) skal skje så nær hendelsen som mulig, og i henhold til dokumenterte rutiner for varsling og håndtering.
b) Det skal være enhetlige rutiner for etterfølgende rapportering av hendelser.
c) Rutiner for varsling og håndtering av hendelser knyttet til forvaltning eller drift av systemer må foreligge fra systemeier for så vidt gjelder fellessystemer, sektorsystemer og tverrsektorielle systemer.

Instrukser og reglement på informasjonssikkerhetsområdet (politisk nivå)

Informasjonssikkerhets-standarder (administrativt nivå)

Utdypes mer gjennom følgende temaer innenfor hendelseshåndtering:

Opplæring
Varsling
Håndtering
Rapportering
Evaluering
Læring
Internkontroll

Status for overordnet styringssystem for informasjonssikkerhet for Oslo Kommune

- Videreutvikles av byrådsavdeling for Finans
- Utvidelser forankres i alle sektorer
- Publiseres og kommuniseres til sektorer og virksomheter

Informasjonssikkerhet

God håndtering av informasjonssikkerhet handler om:

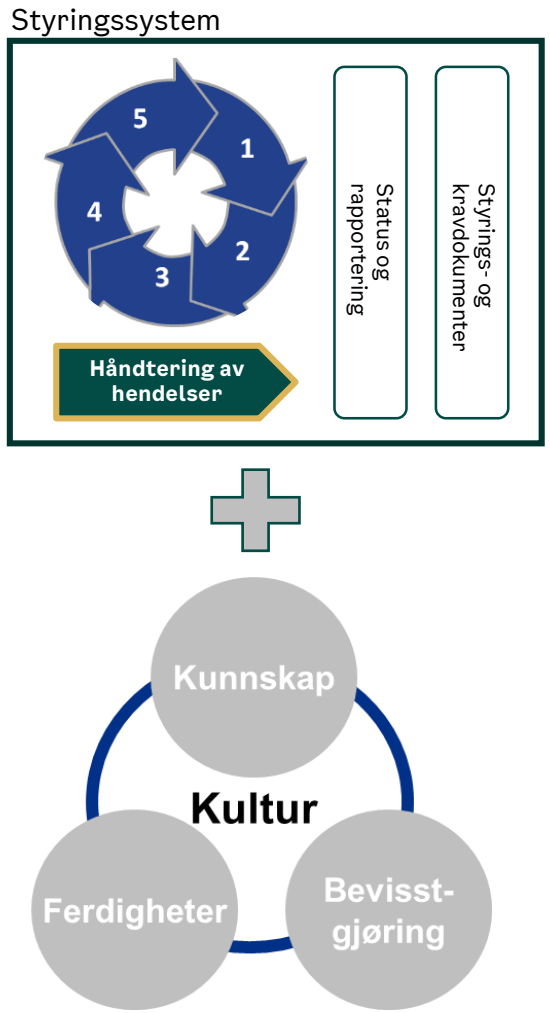
Identifisere og forstå risiko knyttet til informasjonsverdier

Styrt tilnærming til å håndtere risiko

+

Evne til å fange opp og håndtere det vi ikke klarer å forutse

Den systematiske tilnærmingen gjelder teknologi, prosesser og mennesker:



Informasjonssikkerhet

God håndtering av informasjonssikkerhet handler om:

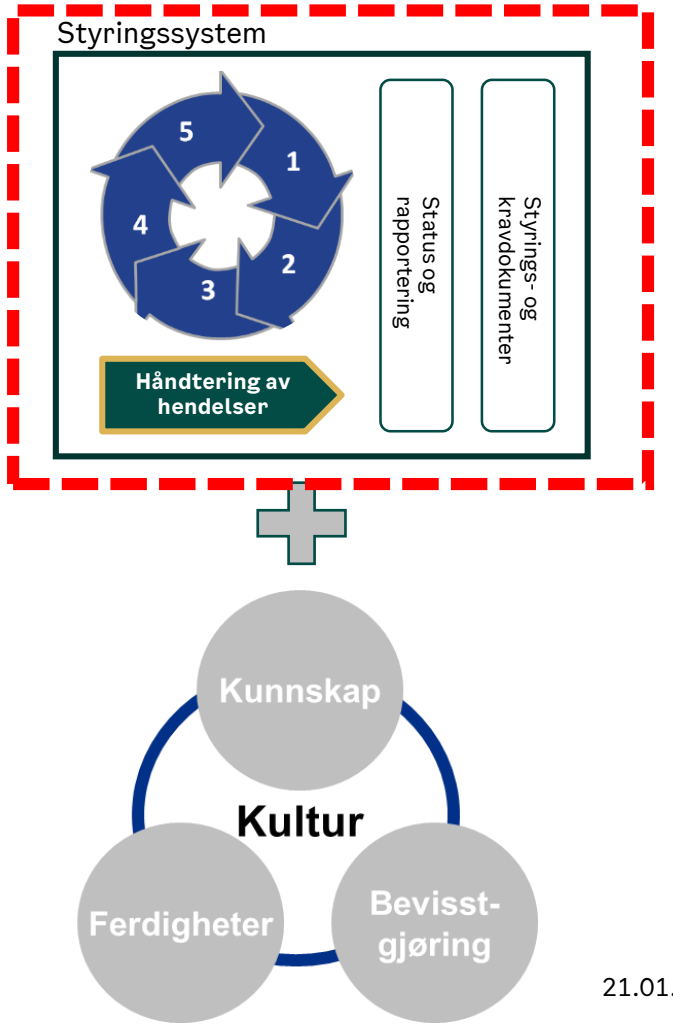
Identifisere og forstå risiko knyttet til informasjonsverdier

Styrt tilnærming til å håndtere risiko

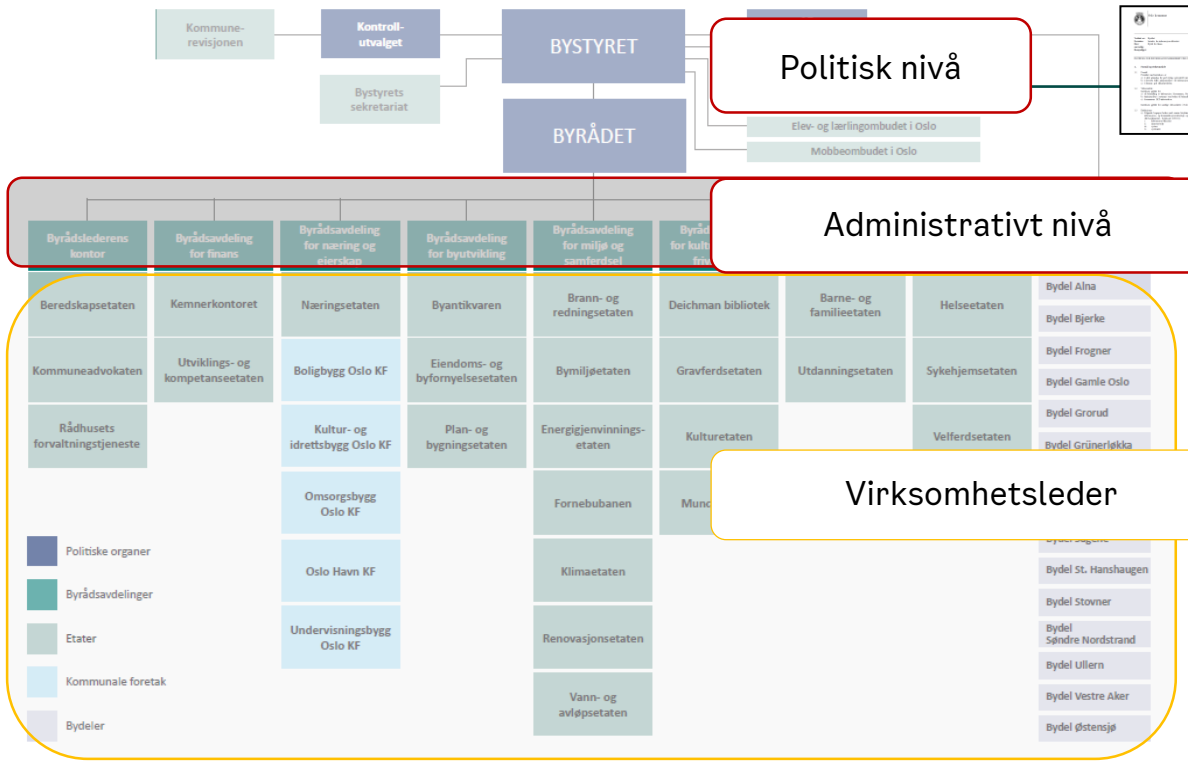
+

Evne til å fange opp og håndtere det vi ikke klarer å forutse

Den systematiske tilnærmingen gjelder teknologi, prosesser og mennesker:



Styring og kontroll informasjonssikkerhet
Virksomheter i Oslo Kommune



Politisk nivå

Administrativt nivå

Virksomhetsleder

vedtar

vedtar

NIVÅ 1

NIVÅ 2

NIVÅ 3

Instrukser og reglement

Standarder
(skal gjelde for alle virksomheter i Oslo kommune)

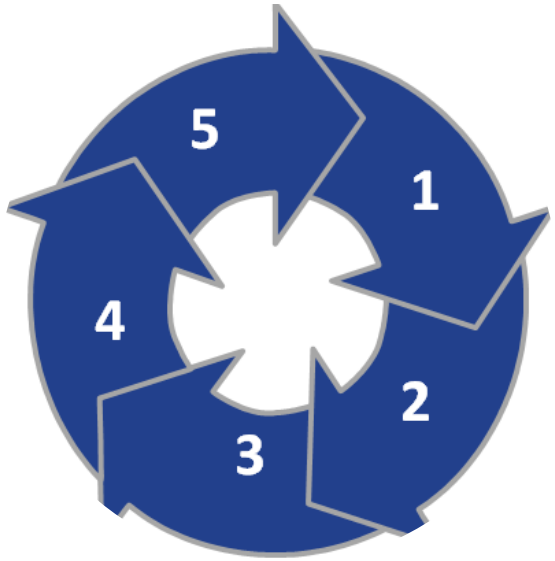
Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1. Oversikt
2. Vurdere viktighet - KIT
3. Risiko
4. Beslutte tilnærming
5. Følge opp tilnærming



Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

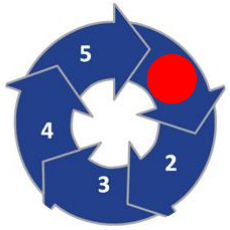
Hendelseshåndtering

Status og rapportering

Styrings- og kravdokumenter og prosesser

Oslo

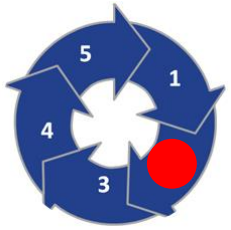
Steg 1:
Oversikt - Kartlegge og vedlikeholde verdier



- I etablering av et styringssystem for informasjonssikkerhet i en virksomhet vil alle informasjonsverdier bli kartlagt.
- Oversikt over alt som finnes av informasjonsverdier, uavhengig av eierskap, tilhørighet og verdi

En informasjonsverdi inkluderer både informasjon, IKT-system, digitale tjenester, datautstyr etc.

Steg 2:
Gjennomføre og oppdatere verdivurdering av informasjonsverdier - KIT



- Alle informasjonsverdier må verdivurderes og klassifiseres i henhold til en konsekvensskala

- «Konsekvensskala» - Et verktøy for å klassifisere hvor alvorlige konsekvensene ved brudd på henholdsvis tilgjengelighet, integritet og konfidensialitet vil kunne bli

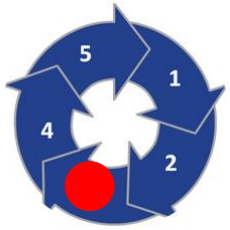
- I en verdivurdering kartlegges hvilken informasjon og hvilke informasjonssystemer som må beskyttes (informasjonsverdier)

- Verdivurderingen vil identifisere om det er behov for å gjøre en risikoanalyse av informasjonsverdien

- Ved vesentlig endring i informasjonsverdien eller i bruk av informasjonsverdien skal verdivurderingen bli oppdatert

Alt er ikke like viktig.....

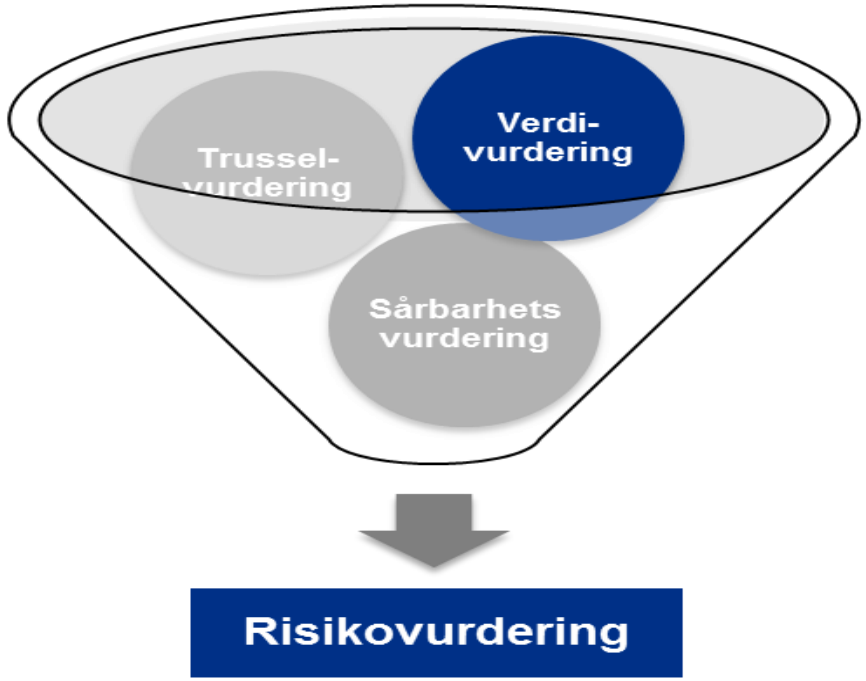
Steg 3:
Gjennomføre risikovurdering



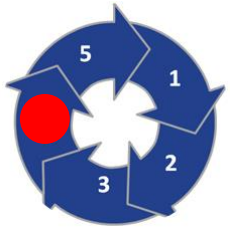
- Ved behov gjennomføres risikovurdering basert på de relevante faktorer:
  - Verdivurdering
  - Trussel/farevurdering
  - Sårbarhetsvurdering

- De tre faktorene sammenstilles til en risikovurdering

- Ved ikke behov for risikovurdering, må ansvarlig eier sørge for at minimum krav for informasjonssikkerhet er møtt

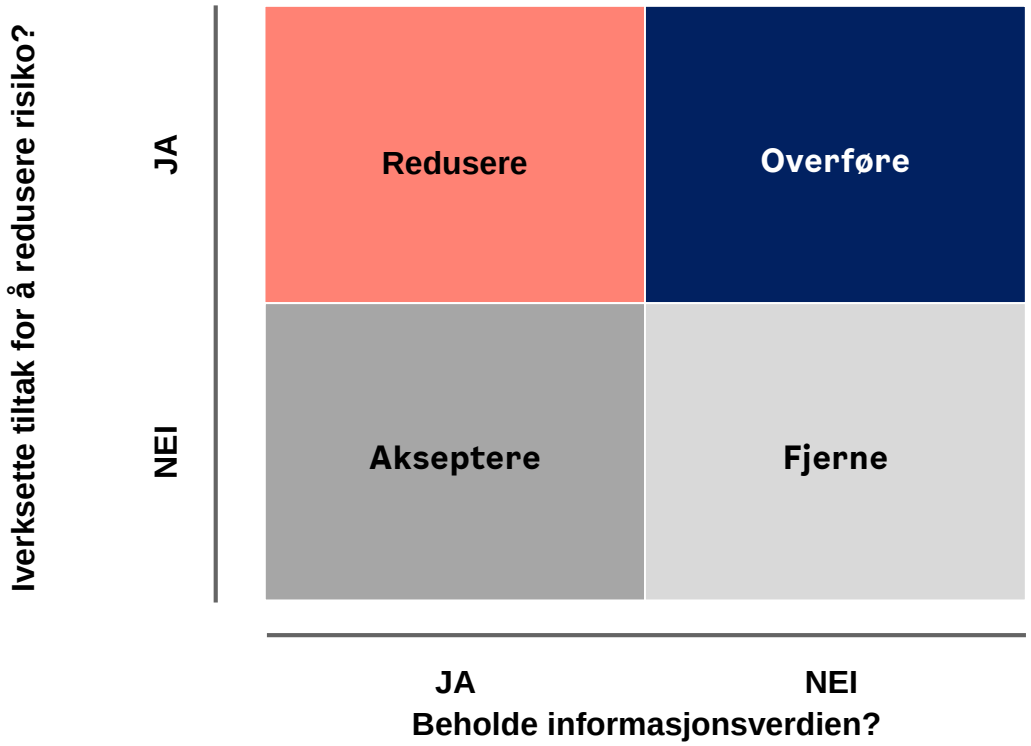


Steg 4: (1 av 2)
Beslutte overordnet risikotilnærming

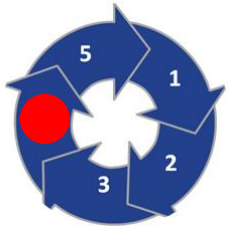


- En risikotilnærming må besluttes for en informasjonsverdi som får en risikovurdering

- De fire mulige tilnærmingene er å
  - overføre
  - beholde/akseptere
  - redusere, eller
  - fjerne risikoen

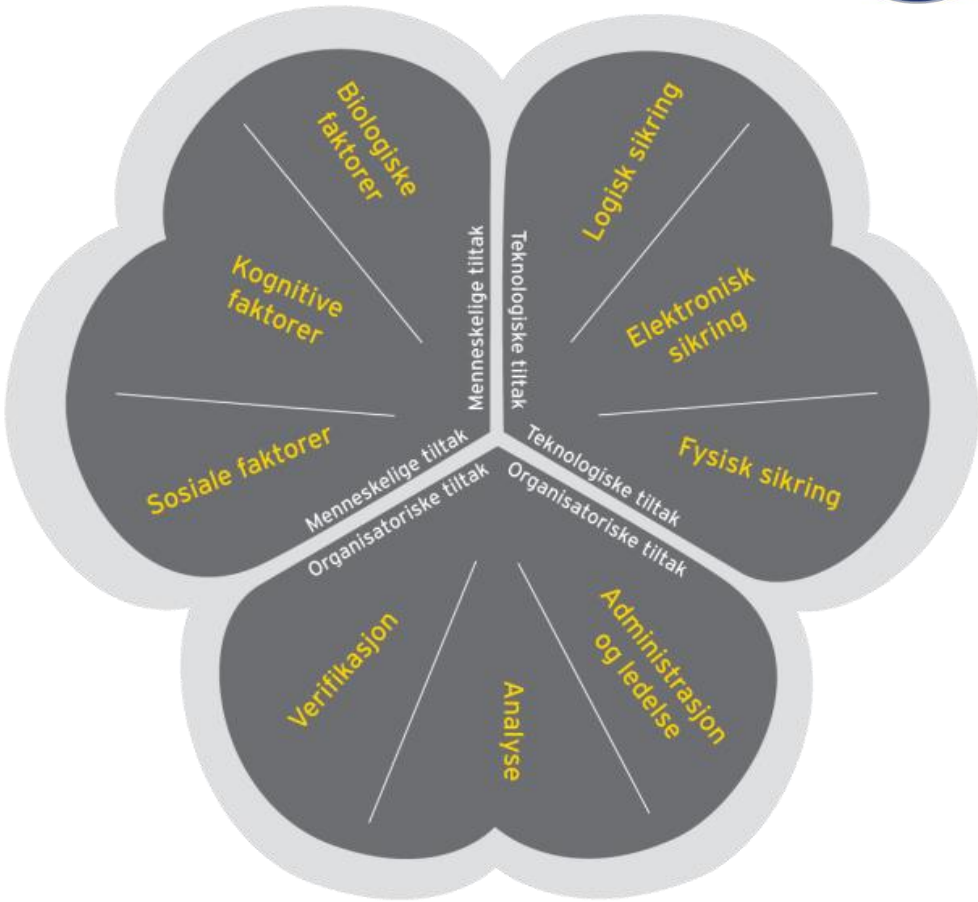


Steg 4: (2 av 2)
Etablere tiltak og plan i henhold til risikotilnærming



- En plan og tiltak må etableres i henhold til risikotilnærmingen

- Disse kan inkludere menneskelige, teknologiske eller organisatoriske tiltak for å overføre, beholde, redusere eller fjerne risikoen



Steg 5:
Følge opp plan for risikotilnærming

- Sørge for at besluttet tilnærming har ønsket effekt og at tiltak fungerer etter hensikten

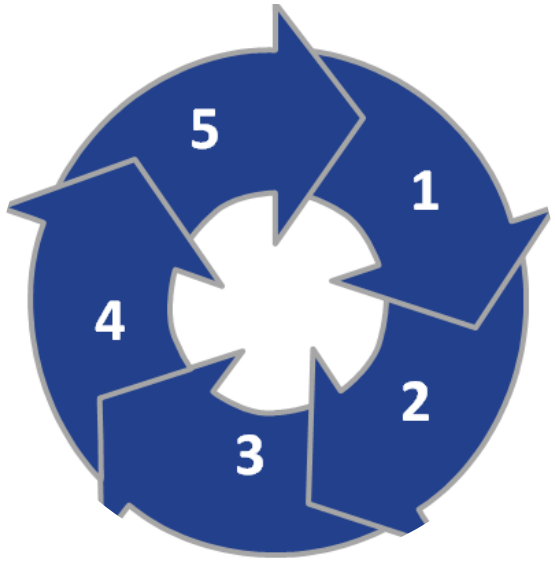
- Kontinuerlig forbedring

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1. Oversikt
2. Vurdere viktighet - KIT
3. Risiko
4. Beslutte tilnærming
5. Følge opp tilnærming



Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

Hendelseshåndtering

Status og rapportering

Styrings- og kravdokumenter og prosesser

Oslo

Tiltaksområder informasjonssikkerhet

Oslo

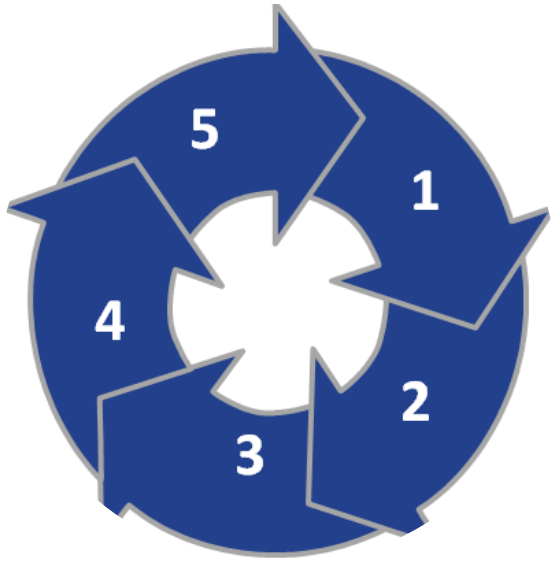
Kilde: ISO 27002

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1. Oversikt
2. Vurdere viktighet - KIT
3. Risiko
4. Beslutte tilnærming
5. Følge opp tilnærming



Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

Hendelseshåndtering

Status og rapportering

Styrings- og kravdokumenter og prosesser

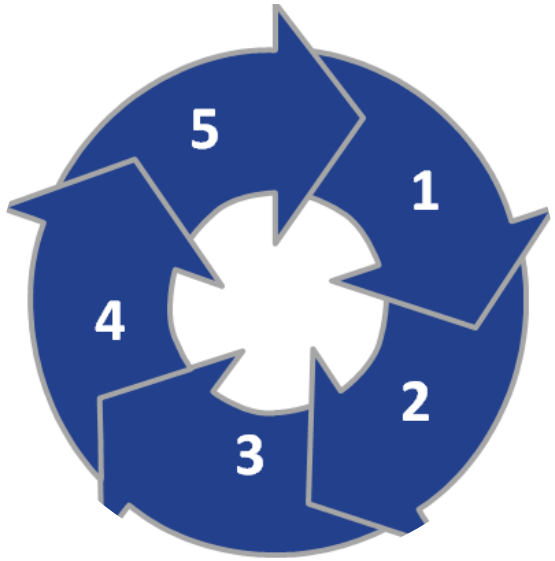
Oslo

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1. Oversikt
2. Vurdere viktighet - KIT
3. Risiko
4. Beslutte tilnærming
5. Følge opp tilnærming



Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

Hendelseshåndtering

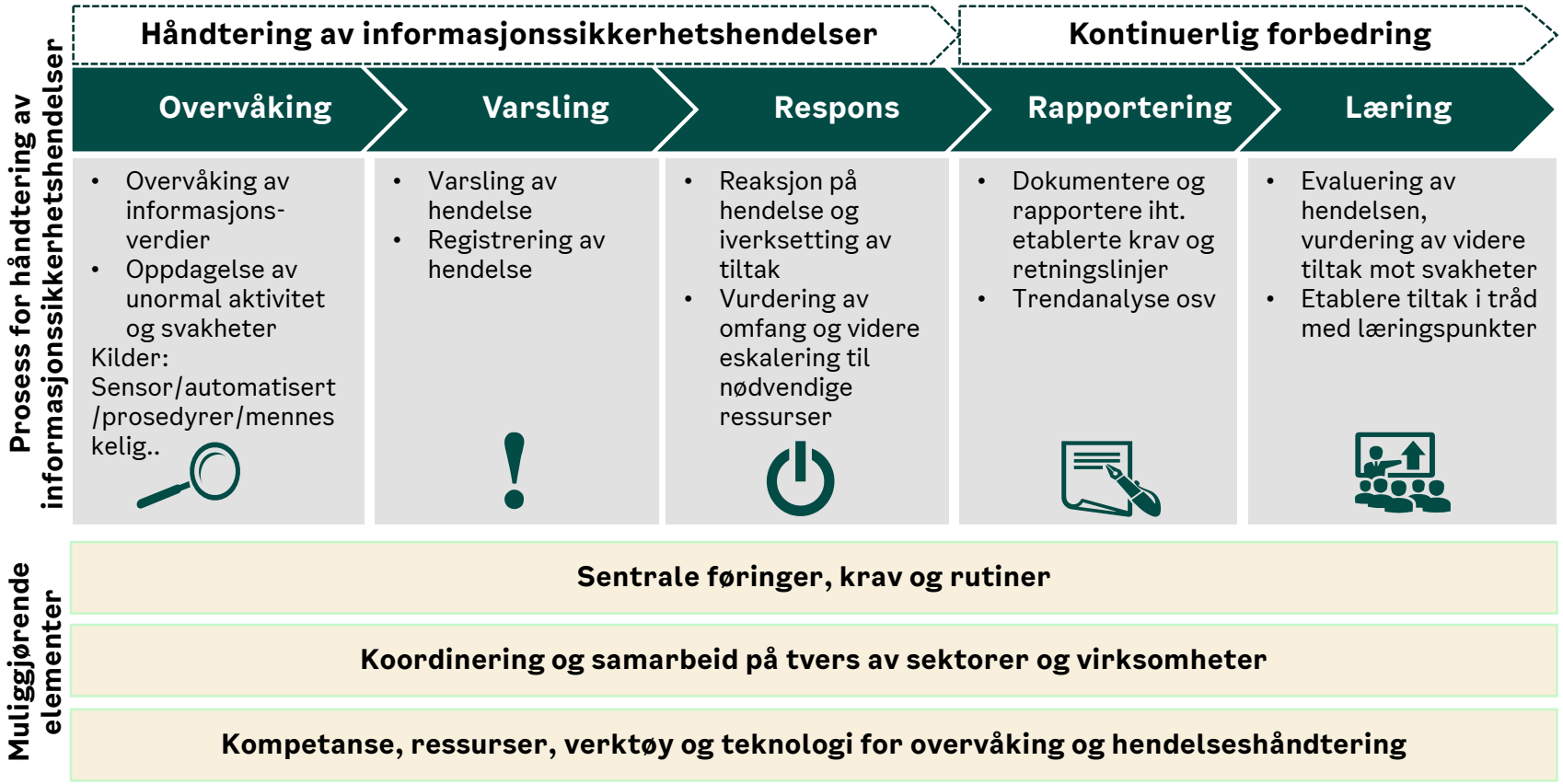
Status og rapportering

Styrings- og kravdokumenter og prosesser

Oslo

Overvåking og Hendelseshåndtering

Håndtering av informasjonssikkerhetshendelser skal gjøres gjennom en standardisert prosess med et omfang som er tilpasset Oslo kommunes behov



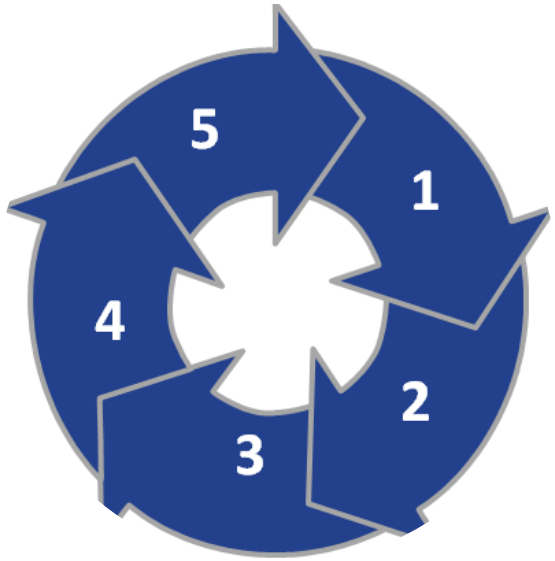
Oslo

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1. Oversikt
2. Vurdere viktighet - KIT
3. Risiko
4. Beslutte tilnærming
5. Følge opp tilnærming



Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

Hendelseshåndtering

Status og rapportering

Styrings- og kravdokumenter og prosesser

Oslo

Styring og kontroll på informasjonssikkerheten

Styringssystem

Forebyggende

1 Oversikt

2 Vurdering av risiko - IT

3 Risiko

4 Beslutte tiltak

5 Følge opp tiltak

Reagerende

Overvåking og Hendelseshåndtering: Oppfølging av feil, innbrudd og lekkasjer fra informasjonsverdier

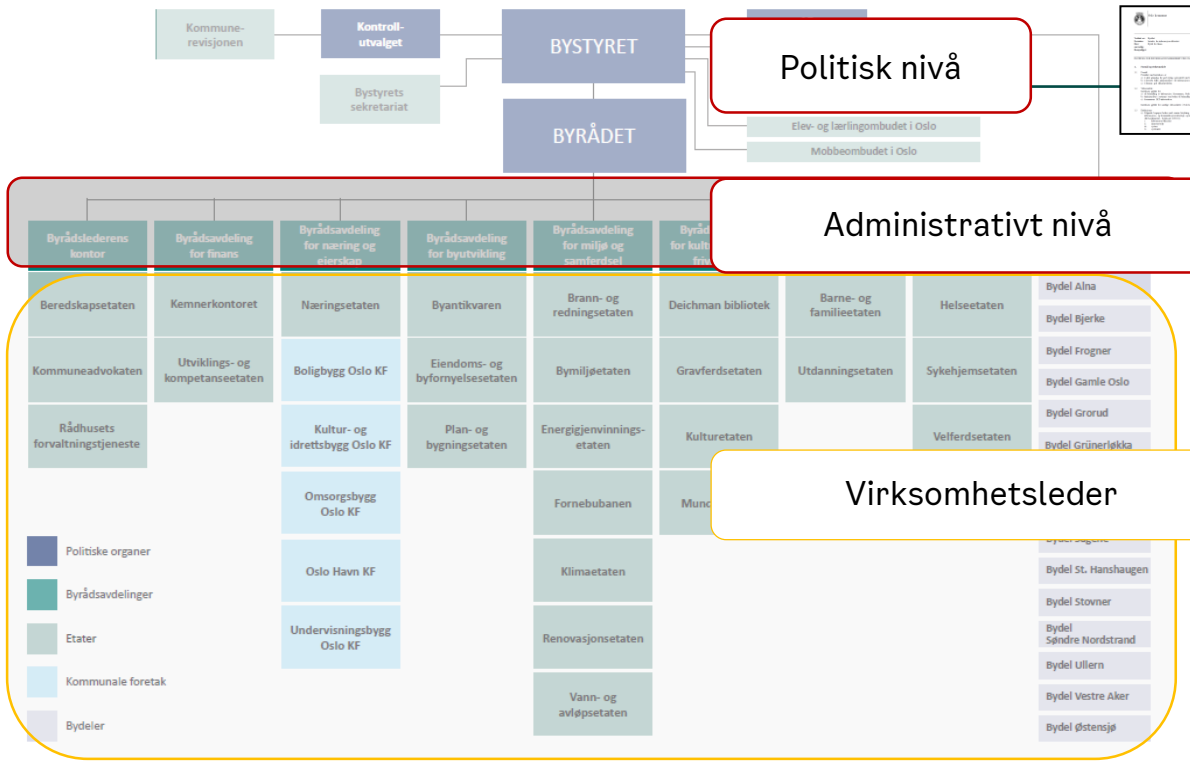
Hendelseshåndtering

Status og rapportering

Styrings- og kravdokumenter og prosesser

Beskrivelse av helheten til styringssystemet

Styring og kontroll informasjonssikkerhet
Virksomheter i Oslo Kommune



Politisk nivå

Administrativt nivå

Virksomhetsleder

vedtar

vedtar

NIVÅ 1

NIVÅ 2

NIVÅ 3

Instrukser og reglement

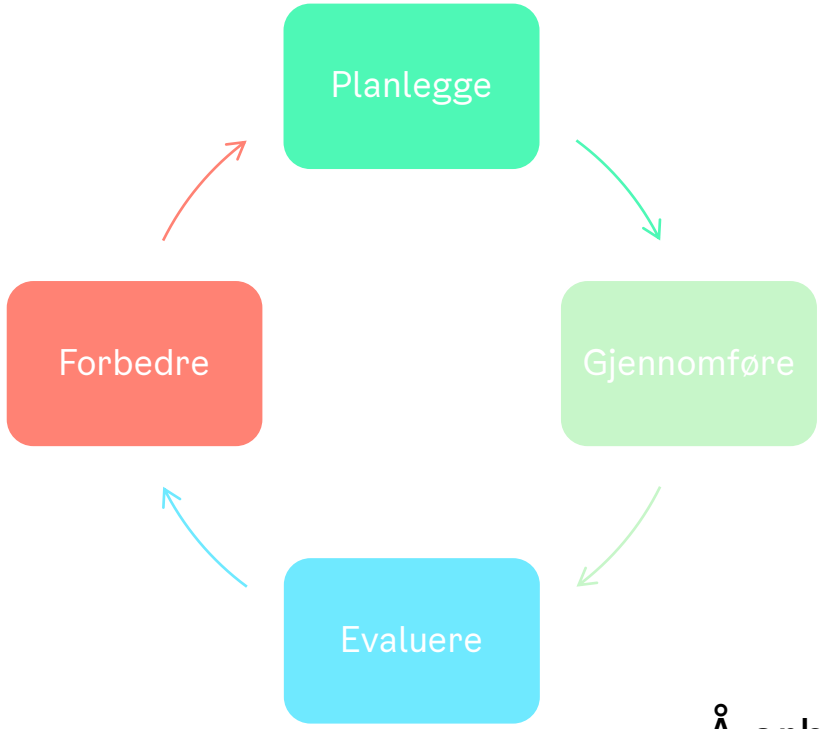
Standarder
(skal gjelde for alle virksomheter i Oslo kommune)

Virksomhetene beslutter egen operasjonalisering gjennom sine respektive styringssystemer for informasjonssikkerhet

Hvilke prosesser må på plass

- Og hvordan går vi i gang nå..?

Styringssystemet skal sikre systematisk og kontinuerlig arbeid



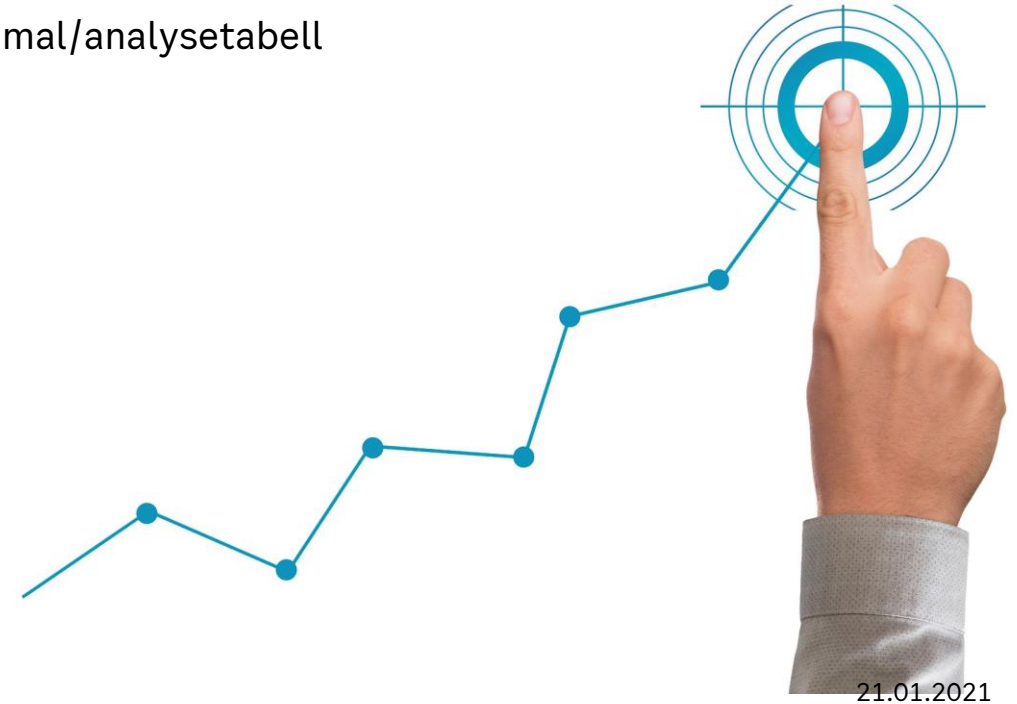
MÅL

- ✓ at vi har gode prosesser og arbeider effektivt
- ✓ at vi får bedre sikkerhet og kvalitet
- ✓ at vi etterlever lover og regler

Å arbeide med styringssystemer er også kontinuerlig og systematisk arbeid - erfaring øker modenhet

Etablering - få oversikt

- Hvor er vi i dag?
  - De fleste virksomheter har et internkontrollsystem, men er omfang og kvalitet god nok?
    - Analyser status!
      - LG sier noe om status
      - Veiledere på digdir.no/informasjonssikkerhet – blant annet en mal/analysetabell
    - Organisere arbeidet og pek ut nøkkelpersoner!
    - Lag en plan!



Få oversikt – hvor har vi mangler?

- Mange har internkontrollsystemer, men mangler for eksempel:
  - kartlegging og vurdering av informasjonsverdier (behandlingsoversikter)
  - systematikk for risikovurderinger og risikohåndtering (risikostyring på alle nivåer)
  - etablert og kommunisert nivå for akseptabel risiko - risikoforståelse
  - avvikshåndtering og kontinuerlig forbedring
  - kontinuitetsplanlegging og jevnlige øvinger
  - jevnlige revisjoner
  - riktig kompetanse
  - ledelsesforankring

Ansvar og involvering

- Ledelsesforankring!!
  - Aller viktigst er forankring i toppledelsen fra start til slutt.
    Ledelsen må ikke bare komme inn for å godkjenne
  - Ledelsesforankring gir fart og retning
  - Topplederen må **ønske** gjennomføringen og gå foran som drivkraft for å få suksess

  - Innspill til hvordan man kan ansvarliggjøre ledelsen?
- Koordinatorrollen (ISK, PVO)
  - Viktig koordinator og utfører-rolle i etablering og driftsfase

Bruk ressurser i virksomheten

- Involver og ansvarliggjør de ansatte
  - nødvendig for bevisstgjøring om mål, akseptabel risiko, informasjonsverdier, risikovurderinger og sikringstiltak
  - avgjørende for en god sikkerhetskultur
  - avgjørende for kvaliteten på styringssystemet
  - avgjørende for etterlevelsesevne og handlingskompetanse

Etablering – kom i gang

- Beskriv omfang – teknologi, prosesser og mennesker
- Hvilke interessenter og avhengigheter finnes?
  - Brukere og registrerte
  - Andre virksomheter
    - Verdikjeder – går ofte på tvers
    - Tiltaksleverandører
  - Myndigheter

- Mål, oppgaver og organisering i virksomheten
- Hvilke roller er etablert? Er ansvar tydelig?

Etablering – kom i gang

- Kartlegg lovkrav og relevant regelverk
- Kartlegg risikoområder
  - Kartlegg informasjonsverdier
  - Hvilke personopplysninger behandler dere?
  - Finnes det relevante revisjonsfunn, avvik etc?
- Hva er virksomhetens nivå for akseptabel risiko – «risiko-apetitt»?
- Kartlegg kompetansebehov og gjennomfør grunnleggende opplæring

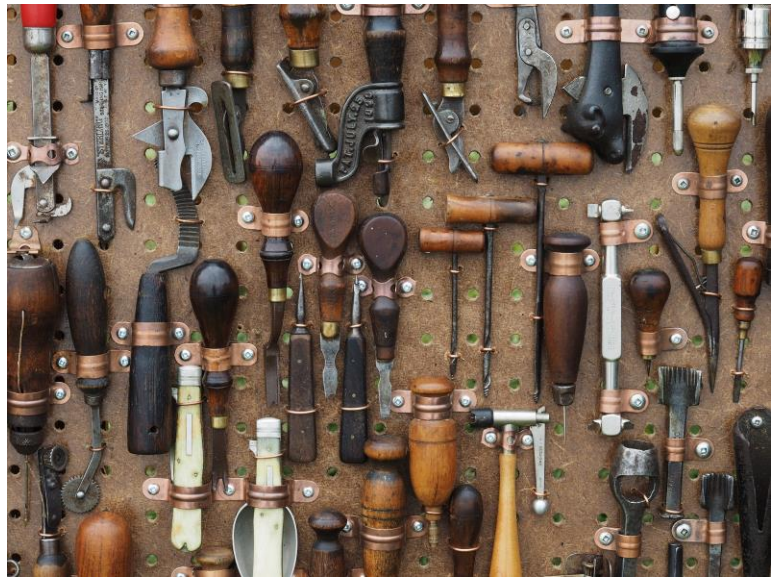
Dokumentasjon

- Et styringssystem er et sett av aktiviteter og prosesser, og **ikke** kun en perm, nettside eller et datasystem
- Noe dokumentasjon må på plass
  - Noe er pålagt (for alle)
  - Noe er nødvendig for din virksomhet
  - For noen dokumenter kreves dokumentstyring (versjonskontroll, tilgangsstyring etc)

Styrende dokumentasjon

- Beskrivelse av styringssystemet som inneholder mål og strategi, identifiserte krav og plikter, intern organisering, ansvar og myndighet.
- Styrende dokumentasjon er overordnet i sin form og er spesielt ledelsesorientert.
- Eksempler
  - Sikkerhetsmål og sikkerhetsstrategi
  - Krav til ledelsens gjennomgang og rapportering

Utførende dokumentasjon



- Beskriver organisatoriske og tekniske tiltak som er nødvendige for å opprettholde akseptabelt risiko og tilstrekkelig *informasjonssikkerhet*
- Rutiner og prosedyrer
- Arbeidsinstrukser

Eksempler:

- Rutiner for behandling av personopplysninger
- Risikovurdering - rutine
- Beskrivelse av informasjonssystem
- Sikkerhetstiltak, for eksempel *tilgangskontroll*, logging, informasjonshåndteringsrutine
- Fysisk sikring
- Driftsrutiner
- Beredskapsplan
- Sikkerhetsinstrukser for brukere, ledere og sikkerhetsansvarlig

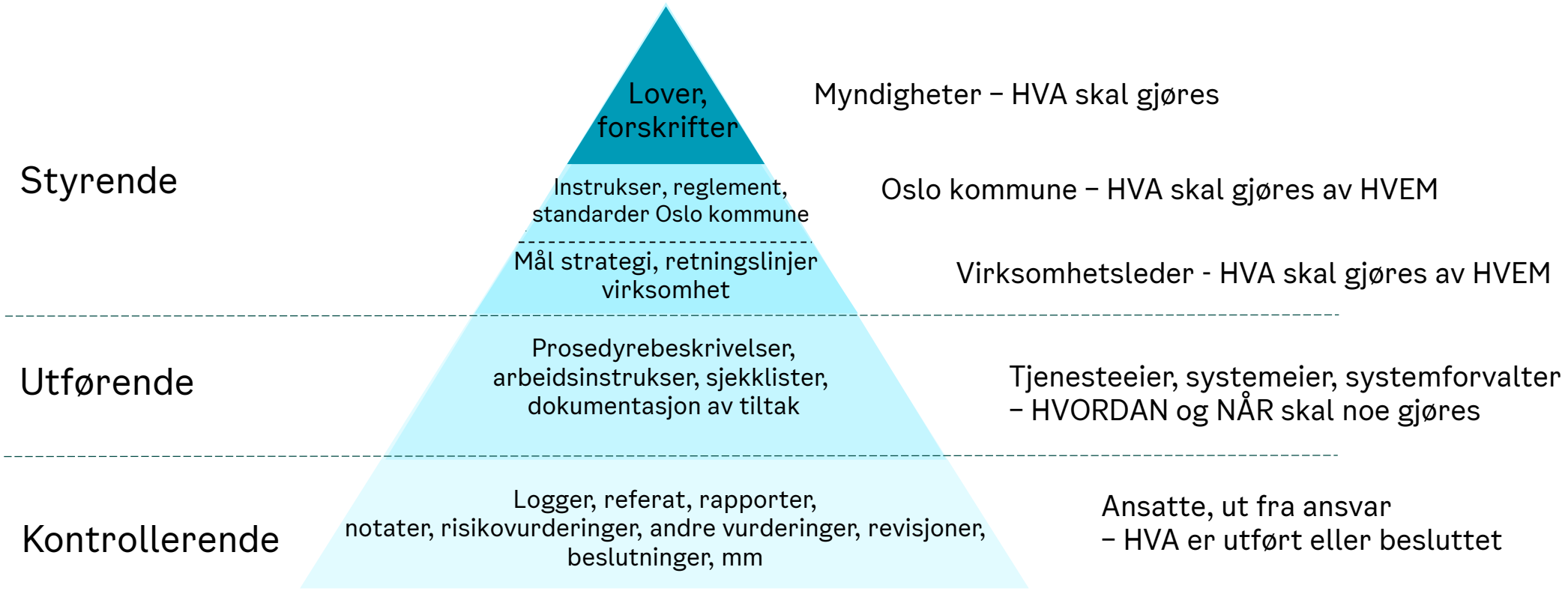
Kontrollerende dokumentasjon

- Har til formål å verifisere at aktivitetene har foregått i samsvar med fastsatte rutiner og instrukser.
- Kan betraktes som et «sikkerhetsnett» som bidrar til at styringsdokumentene følges og at eventuelle *avvik* lettere oppdages.
- Dokumentene skal ikke være statiske, men endre seg i tråd med virksomhetens utvikling og den rettslige utvikling.

Eksempler på dokumentasjon

- Ledelsens gjennomgang (rapporten)
- Dokumentasjon relatert til håndtering av avvik og hendelser
- Egenkontroll, logger, referater
- Risikovurderinger, sikkerhetstesting, revisjonsrapport
- Databehandleravtaler og oppfølging av databehandlere

Dokumentasjon



Her finner du mer informasjon om arbeid med styringssystem

- **Digitaliseringsdirektoratet** har en veileder som er basert på ISO27001.
  - Den finner du her: https://www.digdir.no/informasjonssikkerhet/veilederen-internkontroll-i-praksis-informasjonssikkerhet-er-oppdatert/1743
- **Datatilsynet** skriver om internkontroll for informasjonssikkerhet på sine nettsider:
  - https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/
- ISO27001 standarden er tilgjengelig på standard.no
  - ISO 27003 – relatert standard for implementering av styringssystem
  - NB: Man må ha medlemskap eller betale for å få tilgang på standardene.
- Følg også med på felles intranett for kurs, maler og lignende:
  - https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/

Vil du ta kurs i ISO27001?

Våren og høsten 2020 har byrådsavdeling for finans tilbudt fem dagers kurs i ISO27001-standarden, dette har vi mulighet for også våren og høsten 2021 dersom det er interesse.

Fordeler:

- Du får en grundig innføring i standarden
- Du deltar med andre deltaker fra Oslo kommune
- Du får muligheten til å ta eksamen og gjennomføre en sertifisering
- Kurset koster 15 500,- (markedspris er 25 000,-)

Kurset krever forkunnskaper i informasjonssikkerhet.

Er du interessert i dette ta kontakt med maylen.pedersen@byr.oslo.kommune.no.

?