Digdir

digdir.no

Stifinneren

1 Hvor er vi, hvor skal vi?

2 Hvordan skal ting fungere hos oss?

3 Prøve ut og justere

4 Bygge et godt grunnlag

Hovedsaken 5

6 Hvordan går det?

7 Forbedre og justere

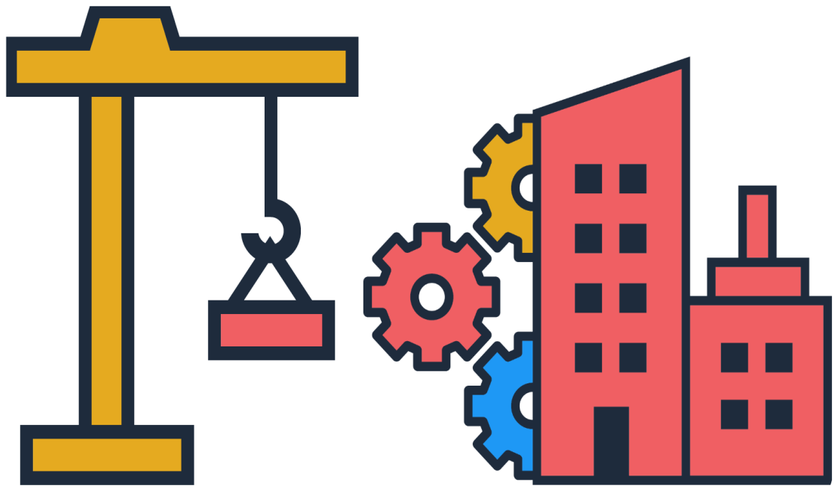
Frokostmøte, 19.10.21
Katrine Aam Svendsen

https://www.digdir.no/informasjonssikkerhet/stifinneren/2620

Dagens tema

- Hva er Stifinneren?
- Hvem kan bruke Stifinneren?
- En reise i flere etapper, med start og slutt
- Tid til spørsmål

Hva er Stifinneren?



Hjelp til hvordan etableringsaktiviteter benyttes for å forbedre styring av informasjonssikkerhet

Etableringsaktiviteter i sammenheng med styringsaktiviteter som etter hvert kommer på plass

Hva består Stifinneren av?

Hva består Internkontroll i praksis - informasjonssikkerhet av?

- Styringsaktiviterer:
  - 7 hovedaktiviteter
  - Delaktiviteter til hver hovedaktivitet
- Etableringsaktiviteter
- Praktiske fremgangsmåter / metoder

https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601

Hva består Stifinneren av?

- 7 etapper, med flere steg i hver etappe
- Hvert steg peker til en eller flere delaktiviteter – eller en del av en delaktivitet.
- Ender i en «loop» – starten på kontinuerlig forbedring

Hva er IKKE Stifinneren?

- Full beskrivelse av hva man skal gjøre for å etablere god styring av informasjonssikkerhet.

Hvem kan bruke Stifinneren?

Nybegynner

- Ved å følge Stifinneren vil du
  - kunne ta ting etappe for etappe og ende på et bra sted
  - forstå hvorfor *Internkontroll i praksis - Informasjonssikkerhet* er utformet slik som den er
  - bli i stand til å se skogen, ikke bare trærne

Erfaren person

- Ved å sette deg inn i Stifinneren vil du
  - få inspirasjon til å finne en god sti i det terrenget du befinner deg i
  - oppdage hva som ligger til grunn for utformingen av *Internkontroll i praksis – Informasjonssikkerhet*, og forstå hensikten med struktur og innhold

«Virksomhetsledelsens gjennomgang» i Stifinneren

- Behovet for virksomhetsledelsens gjennomgang varierer.
- Virksomhetsledelsens gjennomgang går igjen i flere etapper, men med ulikt omfang og innhold.
- I en etableringsprosess er det større behov for tett kontakt med ledelsen.
- Man vil over tid komme inn i en fast rutine og frekvens for virksomhetsledelsens gjennomgang.

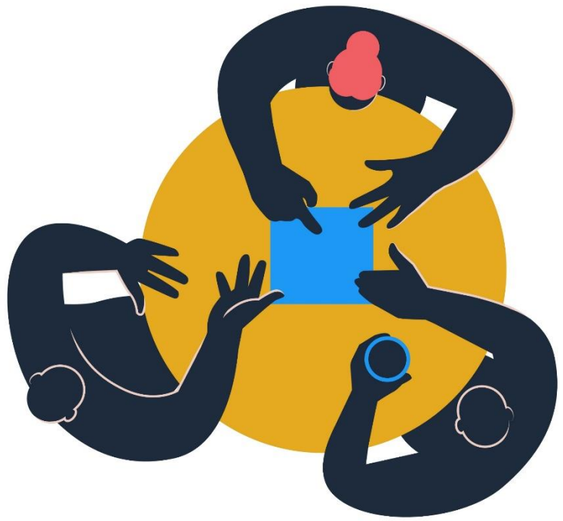
En reise i flere etapper

- Etappe 1 – Hvor er vi, hvor skal vi?
- Etappe 2 – Hvordan skal ting fungere hos oss?
- Etappe 3 – Prøve ut og justere
- Etappe 4 – Bygge et godt grunnlag
- Etappe 5 – Hovedsaken
- Etappe 6 – Hvordan går det?
- Etappe 7 – Forbedre og justere

Digdir

Start

- Etabler en arbeidsgruppe – mer enn én person
- Sørg for god forståelse av hva man skal jobbe mot



Tips på veien

Samarbeid med
andre virksomheter

Etableringsaktiviteter
og styringsaktiviteter

Kommunikasjon!

Begrepsforståelse

Arbeid langs to spor

Skap engasjement

Koordiner med
virksomhetsstyringen

Oversikt over virksomhetens rammebetingelser

- Nyttig for å tilpasse omfang, struktur og ressursinnsats på informasjonssikkerhetsarbeidet til virksomheten
- Oversikt over rammevilkårene for det dere gjør
- Kunnskap om omgivelsene dere befinner dere i
- Kan for eksempel dokumenteres i et notat

Digdir

Etappe 1

Hvor er vi, hvor skal vi?

- Hvordan står det til hos oss?
- Ønsker vi å gjøre noe for å endre noe?
- Hvordan skal vi gå frem?

Digdir

Etappe 1

Hvor er vi, hvor skal vi? Steg (1)

- Analysere status
  - vurdere status opp mot gjeldende anbefalinger om struktur og innhold på styringsaktiviteter
  - se styringsaktivitetene i sammenheng med hva man allerede har på andre områder i virksomheten
  - danner grunnlaget for beslutning om veien videre
- Plan
  - benytte analysen av status til å vurdere og prioritere behov i forbindelse med etablering av det anbefalte settet med styringsaktiviteter
  - lage en overordnet plan for etablering eller forbedring av styring av informasjonssikkerhet

Digdir

Etappe 1

Hvor er vi, hvor skal vi? Steg (2)

- Virksomhetsledelsens gjennomgang
  - gå gjennom analysen av status og forslaget til plan sammen med toppleder og virksomhetsledelsen
  - Virksomhetsledelsen skal ta beslutning om veien videre, og sørge for tilstrekkelig finansiering av arbeidet
- Dialog med styrende organ
  - dersom det er relevant å rapportere styringsinformasjon til overordnet organ

Digdir

Etappe 1 – Sjekkliste (utdrag)

- Vi har sammenliknet våre styringsaktiviteter med gjeldende anbefalinger.
- Vi har overordnet oversikt over hva vi bør gjøre for å etablere eller forbedre styring av informasjonssikkerhet.
- Toppleder og virksomhetsledelsen forstår sitt ansvar og virksomhetens behov. De har tatt beslutning om en overordnet plan for videre arbeid.
- Vi har ressurser til å gjennomføre første del av planen.

Digdir

Etappe 2

Hvordan skal ting fungere hos oss?

- Dere har analysert status og etablert en plan
- Nå skal dere finne ut hvordan ting skal fungere hos dere

Digdir

Etappe 2

Hvordan skal ting fungere hos oss? Steg (1)

- Føringer
  - Beskrive struktur og innhold i styringsaktivitetene
  - Finne ut hvem som skal gjøre hva
  - Skrive ned føringer for hvordan det skal gjøres
- Virksomhetsledelsens gjennomgang
  - Presentere en oppsummering av arbeidet så langt
  - Skissere veien videre
  - Virksomhetsledelsen må beslutte at føringene er gode nok til å testes ut

Digdir

Etappe 2

Hvordan skal ting fungere hos oss? Steg (2)

- Få på plass fagansvarlig informasjonssikkerhet
  - skal gi faglig støtte til virksomhetsledelsen i arbeidet med å etablere styringsaktivitetene, og i det videre arbeidet med styring av informasjonssikkerhet.

https://www.digdir.no/informasjonssikkerhet/rolle-fagansvarlig-informasjonssikkerhet/2104

Digdir

Etappe 2

Hvordan skal ting fungere hos oss? Steg (2)

- Få på plass fagansvarlig informasjonssikkerhet
  - skal gi faglig støtte til virksomhetsledelsen i arbeidet med å etablere styringsaktivitetene, og i det videre arbeidet med styring av informasjonssikkerhet.
- Etablere rammeverk for dokumentasjon
  - gjør at nødvendig dokumentasjon har en fornuftig struktur og er lett tilgjengelig for de som har behov for den

Digdir

Etappe 2 – sjekkliste (utdrag)

- Vi har en god beskrivelse av hvordan styring av informasjonssikkerhet skal fungere hos oss.
- Ansvaret for å styre risiko (på informasjonssikkerhetsområdet) er delegert i ordinær linje, til de som har ansvaret for våre oppgaver og tjenester.
- Toppleder / virksomhetsledelsen har besluttet å prøve ut hvordan det vil fungere i praksis.
- Ledelsen får støtte i det videre arbeidet av en fagansvarlig informasjonssikkerhet (eller tilsvarende rolle).

Digdir

Etappe 3

Prøve ut og justere

- Nå skal det som ble utformet i forrige etappe prøves ut
  - Bør noe gjøres annerledes?
  - Er det klart for dem med ansvar for gjennomføring hva de skal gjøre?
- Prøv ut noen av aktivitetene som skal gjennomføres i deler av virksomheten

Digdir

Etappe 3

Prøve ut og justere
Steg (1)

- Kommunisere viktighet
  - Toppleder kommuniserer sine forventninger til organisasjonen – hva er viktig og hva er prioritert
  - Behovet vil være avhengig av omfang av utprøving
  - Benytt eksisterende kanaler
- Grunnopplæring
  - utarbeid og gjennomfør opplæring til de som skal ha sentrale roller i styringsaktivitetene.

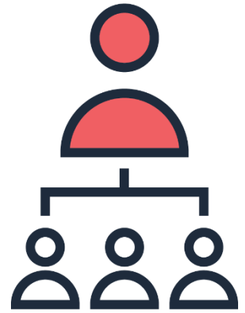
Digdir

Fire historier om styring av informasjonssikkerhet

Styringsaktivitetene Digitaliseringsdirektoratet beskriver i denne veilederen er våre offisielle råd til forvaltningen om hvordan man bør arbeide med styring og kontroll av informasjonssikkerhet. Men hvorfor bør man gjøre det på denne måten? Hvilke behov dekker den systematikken vi anbefaler?

https://www.digdir.no/2647

Turid Topplеder



Linus Linjeleder

Fridtjof Fagansvarlig

Trine Tiltaksleverandør

Digdir

Etappe 3

Prøve ut og justere
Steg (2)

- Vurdere risiko del 1 – Oversikt og prioritering
  - På områdene der dere prøver ut føringene
  - Mål: Skaffe tilstrekkelig oversikt over oppgaver og tjenester, informasjonsbehandlingen i disse, og hvor store konsekvensene kan bli ved informasjonssikkerhetsbrudd
  - Tips: Vær tydelig på formålet med å gjøre dette, og hvilke fordeler det vil gi på sikt

Digdir

Etappe 3

Prøve ut og justere
Steg (3)

- Vurdere risiko del 2 – Planlegge og gjennomføre risikovurdering
  - Gjennomfør risikovurdering for minst en av virksomhetens oppgaver
- Håndtere risiko
  - I forlengelsen av vurderingen dere nettopp har gjennomført
  - Her handler det i hovedsak om å ta beslutninger om hvordan risiko skal håndteres, ikke om detaljene i sikkerhetstiltak

Digdir

Etappe 3

Prøve ut og justere
Steg (4)

- Evaluering
  - Hvordan gikk utprøvingen? Er det noe dere bør endre på eller forbedre?
  - Beskriv forslag til endringer i hvordan ting skal fungere hos dere
- Virksomhetsledelsens gjennomgang
  - Evalueringen presenteres for toppledelsen
  - Toppleder tar beslutning om at føringene skal gjelde i virksomheten

Digdir

Etappe 3 - Sjekkliste

- De som skal prøve ut styring av risiko (…) har god forståelse for hva dette handler om og hvilket ansvar de har.
- Vi har prøvd ut det å skaffe seg tilstrekkelig oversikt over et ansvarsområde, prioritere videre arbeid, og det å vurdere og håndtere risiko.
- Vi har evaluert utprøvingen av hvordan ting skal fungere hos oss.
- Toppleder har tatt beslutning om at føringene skal gjelde i virksomheten.

Digdir

Etappe 4

Bygge et godt grunnlag

- Før dere kan rulle ut i hele virksomheten må dere begynne å etablere en del ting dere vil ha behov for
- Dette gjør det lettere å få styringsaktivitetene gjennomført rundt omkring i virksomheten
- Få på plass grunnleggende ting som er nødvendig for å ha god informasjonssikkerhet

Digdir

Etappe 4

Bygge et godt grunnlag Steg (1)

- Grunnopplæring
  - Den grunnopplæringen dere testet ut i forrige etappe skal nå forbedres, tilpasses og gjennomføres i hele virksomheten.
- Etablere fellessikring
  - Et felles grunnleggende nivå på tvers av virksomhetens enheter og ansvarsområder.

Digdir

Etappe 4

Bygge et godt grunnlag
Steg (2)

- Etablere system for hendelses- og avvikshåndtering
  - sørge for at dere har et sted å registrere, følge opp og dokumentere hendelser og avvik
- Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen
  - etablering av funksjoner og grupper, og utpeking av hvilke personer som skal dekke funksjonene eller inngå i gruppene

Digdir

Etappe 4 – Sjekkliste

- Risikoeiere og andre som skal være i stand til å styre risiko (…) har god forståelse for hva dette handler om og hvilket ansvar de har.
- Tiltaksleverandører og forskjellige fagpersoner har god forståelse for sine roller.
- Vi har startet arbeidet med å etablere fellessikring.
- Vi har etablert systematikk for hendelses- og avvikshåndtering.
- Vi har startet arbeidet med å etablere tilstrekkelige fellesfunksjoner, støttefunksjoner og samarbeidsgrupper.

Digdir

Etappe 5

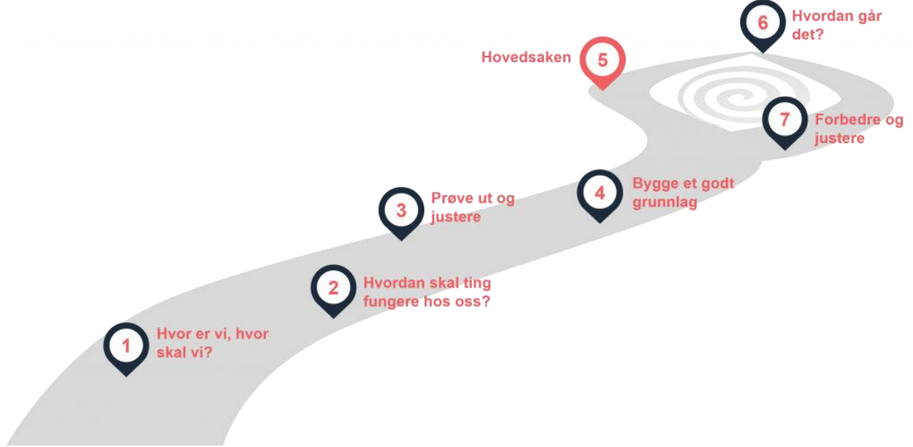
Hovedsaken

- Gjennomføre noen av de viktigste styringsaktivitetene rundt omkring i hele virksomheten
- Første tur gjennom aktiviteter som etter hvert vil bli en del av det regelmessige arbeidet
- Det er viktig at risikoeiere har god støtte i gjennomføringen

Digdir

Etappe 5

Hovedsaken
Steg (1)

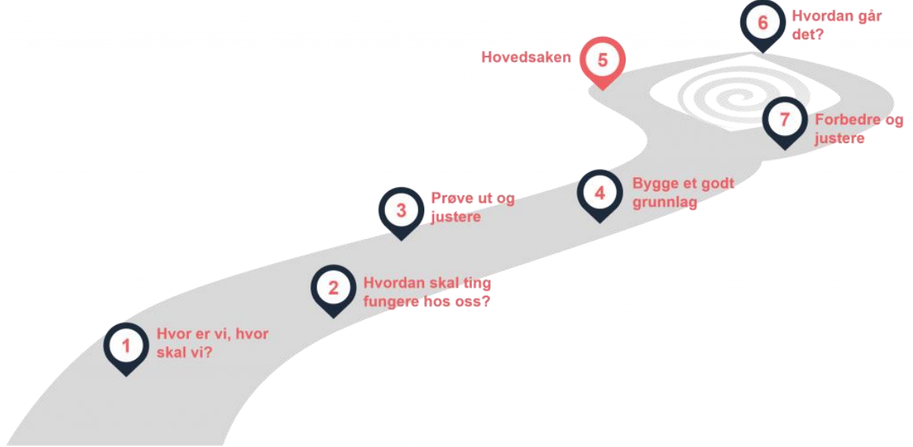


- Kommunisere viktighet
  - toppleder kommuniserer sine forventninger til organisasjonen, og er tydelig på hva som er viktig og hva som er prioritert
  - Som minimum: benytt de kanalene ledelsen ellers benytter til å kommunisere prioriteringer og få ting til å skje i organisasjonen
  - Spesielt viktig: toppleder er tydelig i sine forventninger til de som rapporterer direkte til vedkommende

Digdir

Etappe 5

Hovedsaken
Steg (2)

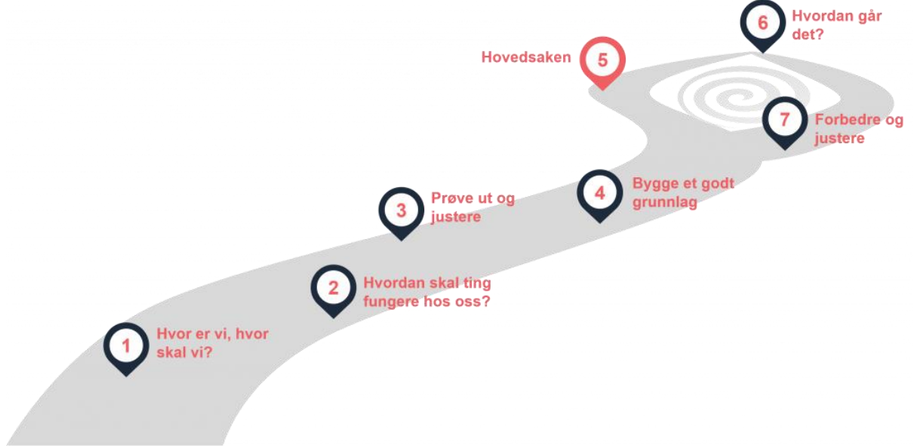


- Vurdere risiko del 1 – Oversikt og prioritering
  - Risikoeiere skal skaffe seg, og vedlikeholde, oversikt over sitt ansvarsområde:
    - hvor store kan konsekvensene bli ved informasjonssikkerhetsbrudd?
    - hvilke trusler, farer og sårbarheter de må være spesielt oppmerksomme på
  - Dette gjør risikoeiere i stand til å
    - gruppere eller dele opp ansvarsområdet sitt i hensiktsmessige deler
    - bestemme hvordan arbeidet med informasjonssikkerhet skal prioriteres
  - Dette vil være aktiviteter som gjentas jevnlig

Digdir

Etappe 5

Hovedsaken
Steg (3)



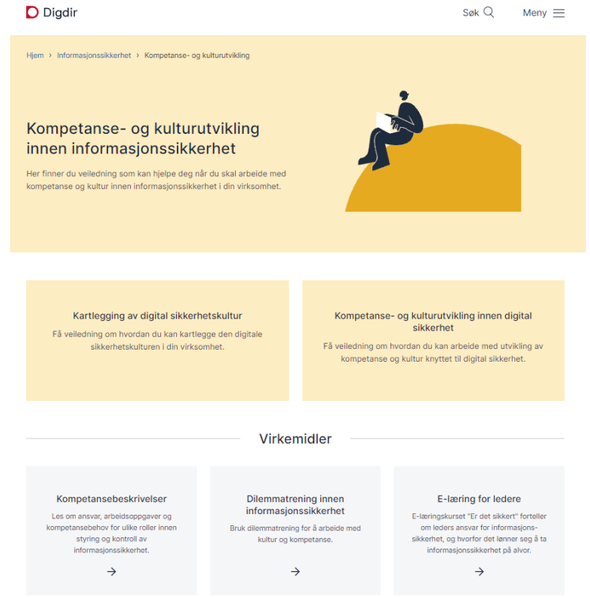
- Vurdere risiko del 2 – Planlegge og gjennomføre risikovurdering
  - Der det er identifisert størst behov
  - Det er viktig at personer som kjenner fagområdet og de aktuelle oppgavene og tjenestene godt deltar
  - Det kan etableres en arbeidsgruppe for gjennomføringen. Det er allikevel viktig at risikoeier er involvert.
- Håndtere risiko
  - Arbeidet med å iverksette beslutningene om å håndtere risiko kan pågå over lengre tid, parallelt med de andre etappene

Digdir

Etappe 5

Hovedsaken
Steg (4)

- Kompetanse- og kulturutvikling
  - Grunnopplæringen må vedlikeholdes og følges opp
  - Det må også jobbes med kompetanse- og kulturutvikling i resten av organisasjonen



https://www.digdir.no/informasjonssikkerhet/kompetanse-og-kulturutvikling-innen-informasjonssikkerhet/2187

Digdir

Etappe 5 – Sjekkliste (utdrag)

- Alle risikoeiere i alle enheter i virksomheten har oversikt over sine ansvarsområder og er i stand til å prioritere ressursinnsatsen.
- Det er planlagt og gjennomført vurdering og håndtering av risiko i alle enheter.
- Vi har god oversikt over behovet for sikkerhetstiltak og ser det i sammenheng med innholdet i fellessikringen.
- Vi har startet arbeid med kompetanse- og kulturutvikling for ulike roller i virksomheten, og opplæring er tilpasset de oppgavene de har eller tjenestene de leverer.

Digdir

Etappe 6

Hvordan går det?

- Evaluere hvordan ting har fungert, og legge til rette for å få ting til å fungere enda bedre
- Ta en pust i bakken og vurder:
  - hvordan har det gått til nå?
  - hva fungerer godt og mindre godt?
  - er det behov for å endre kursen litt?

Digdir

Etappe 6

Hvordan går det?

- Vurdere status på eget ansvarsområde
  - Gjøres av ledere og andre som har et eget ansvarsområde
  - Det kan være behov for grundigere undersøkelser
- Evaluering
  - Hvordan har det gått med
    - gjennomføringen av styringsaktivitetene på forrige etappe?
    - vurderingene av status på eget ansvarsområde på denne etappen?
  - Evaluer helheten, og beskriv forslag til forbedringer. Dette inngår i beslutningsgrunnlag til virksomhetsledelsen på neste etappe.

Digdir

Etappe 6 – Sjekkliste

- Risikoeiere og tiltaksleverandører har vurdert status på sine ansvarsområder i alle enheter i hele virksomheten.
- Vi har evaluert hvor godt styring av informasjonssikkerhet fungerer og foreslått forbedringer.

Digdir

Etappe 7

Forbedre og justere

- Følg opp vurderingene fra evalueringen
- Stak ut kursen videre

Digdir

Etappe 7

Forbedre og justere Steg (1)

- Oppdatere plan
  - Basert på evalueringen
  - Må noe gjennomføres på nytt?
  - Kan mer nå planlegges i detalj?
- Virksomhetsledelsens gjennomgang
  - Vurdere resultatet fra evalueringen, og forbedringer og endringer som er foreslått
  - Ta beslutning om veien videre

Digdir

Etappe 7

Forbedre og justere
Steg (2)

- Kommunisere viktighet
  - Toppleder kommuniserer resultatene fra evalueringen til organisasjonen.
    - hva som fungerte godt
    - hva som fungerte mindre godt
    - hva ledelsen gjør for å sørge for kontinuerlig forbedring
- Dialog med styrende organ
  - dersom det er relevant å rapportere styringsinformasjon til overordnet organ

Digdir

Etappe 7 – Sjekkliste (utdrag)

- Vi har oppdatert planen for etablering eller forbedring av styring av informasjonssikkerhet.
- Toppleder og virksomhetsledelsen forstår sitt ansvar og har besluttet en plan for videre arbeid.
- Det er tilstrekkelig med ressurser til arbeidet med informasjonssikkerhet.
- Toppleder har tydelige forventninger til de som rapporterer direkte til seg.

Slutt

- Grunnlag for effektiv styring av informasjonssikkerhet
- Virksomhetsledelsens gjennomgang og oppfølging endrer seg
- En evig loop – kontinuerlig forbedring
- Det er nå det begynner!

Spør dere selv disse spørsmålene

- Synes virksomhetsledelsen at de har tilstrekkelig oversikt over risiko, ressursbruk, hvilken betydning informasjonssikkerhet har for oppgavene og tjenestene, og om styringen fungerer bra?
- Synes risikoeiere at de har god oversikt over hva de har ansvaret for, og er i stand til å ta gode beslutninger?
- Klarer vi å gjennomføre styringsaktivitetene, spesielt vurdering og håndtering av risiko, med mindre ressursinnsats enn før?
- Har vi god oversikt over sikkerhetstiltakene våre, hvem som er ansvarlig for forvaltning av dem, og om de fungerer etter hensikten?

Digdir

Spørsmål?

infosikkerhet@digdir.no

https://www.digdir.no/infosikkerhet

Digdir

infosikkerhet@digdir.no

https://www.digdir.no/infosikkerhet