Veileder for virksomheter som skal gå fra ISO/IEC 27001:2005 til ISO/IEC 27001:2013

Direktoratet for forvaltning og IKT

Innhold

1. Hva er et styringssystem for informasjonssikkerhet?

Det en virksomhet samlet sett gjør for å ha styring og kontroll på informasjonssikkerheten, kalles virksomhetens styringssystem for informasjonssikkerhet. Hensikten med et slikt styringssystem er å ha en helhetlig tilnærming til informasjonssikkerhet i virksomheten.

Difi anbefaler at statlige virksomheter baserer seg på ISO/IEC 27001 ved etablering av styringssystem for informasjonssikkerhet. Denne anbefalingen gir handlingsrom for bruken av standarden ut fra virksomhetens egenart, samt risiko og vesentlighet. Dette er også i samsvar med de overordnede føringene for intern kontroll i økonomiregelverket i staten.

ISO/IEC 27001 er bygget rundt noen kjerneprinsipper:

- Ledelsesforankring – det er virksomhetens ledelse som er ansvarlig for informasjonssikkerheten, det er ledelsen som må sette styringssignalene og som er ansvarlig for hvilke sikringstiltak som iverksettes.
- Risikostyring – kjernen i arbeidet å velge sikringstiltak er risikostyring. God risikostyring innebærer å definere hva som er akseptabel risiko for virksomheten, jobbe kontinuerlig med risikovurdering, og med grunnlag i dette iverksette nødvendige sikringstiltak.
- Kontinuerlig forbedring – det er et kjerneprinsipp i styringssystemet at man evaluerer styringssystemet og de sikringstiltakene man har iverksatt, og kontinuerlig jobber med å tilpasse det virksomhetens behov.

I vedlegg A til standarden ISO/IEC 27001 defineres relevante sikringstiltak for å håndtere risiko. Disse er nærmere utdypet i ISO/IEC 27002. Forrige versjon av standardene kom i 2005 - i september 2013 ble begge disse standardene publisert i ny versjon.

Formålet med dette dokumentet er å gi informasjon om hvilke endringer som ligger inne i ny standard, og veiledning i hva en virksomhet må gjøre dersom de har et styringssystem basert på gammel versjon, og ønsker å tilpasse seg den nye.

I kapittel 3 sammenliknes 2005-versjonen med 2013-versjonen av ISO/IEC 27001. I kapittel 4 presenteres de delene av standarden som krever endringer for at styringssystemet skal være i henhold til ISO/IEC 27001:2013. Innholdsmessig er disse kapitlene basert på veilederen «Transition guide - Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013» utgitt av British Standards Institution.

2. Bakgrunn for revisjon av standarden

ISO/IECs motivasjon for å gjennomføre revisjonen har først og fremst vært praktisk bruk av standarden over flere år. Samtidig er det nå et krav fra ISO at alle nye og reviderte standarder for styringssystemer skal være like når det gjelder oppbygning og struktur.

At det tilstrebes en lik oppbygning og struktur av standardene er positivt for virksomheter som forholder seg til flere standarder for styringssystemer, slik som f. eks. ISO 9001 for kvalitet og ISO 14001 for miljø. Ordlyden blir mer lik, noe som gjør de generelle kravene gjenkjennelige på tvers av standarder. Formålet er å redusere ressursbruken ved implementering av flere standarder, og at man lettere skal kunne se styringssystemene i sammenheng.

En annen viktig årsak til endringene har vært beslutningen om å harmonisere ISO/IEC 27001 med prinsippene og retningslinjene som er gitt i ISO 31000 Risikostyring. Igjen er dette positivt for virksomheter som ønsker å implementere flere standarder for styringssystemer.

Som resultat av dette har den nye versjonen av ISO/IEC 27001 en annen oppbygning enn 2005-utgaven. Dupliserte krav er fjernet, og man har omformulert kravene slik at virksomheten står friere i forhold til hvordan disse skal implementeres. Videre er det ikke lenger nødvendig å identifisere informasjonsverdier[1], trusler og sårbarheter for å kunne identifisere risiko knyttet til informasjonssikkerhet. Det fremgår også tydeligere i den nye utgaven at sikringstiltakene i vedlegg A ikke er obligatoriske, men at man på bakgrunn av risikovurderinger velger de sikringstiltak som er best egnet til å redusere identifiserte risikoer.

[1] Tidligere norske oversettelser av ISO/IEC 27001 og ISO/IEC 27002 har benyttet «informasjonsaktiva» for det engelske «information assets». Det finnes ingen offisiell norsk oversettelse av 2013-versjonene av standardene, og vi mener det er mest formålstjenlig å benytte begrepet «informasjonsverdier» inntil annen terminologi foreligger i en eventuell norsk versjon.

3. Sammenlikning av ISO/IEC 27001:2013 med ISO/IEC 27001:2005

I det følgende presenteres de mest vesentlige endringene fra gammel til ny versjon av standarden. Sammenhengen mellom de ulike elementene i de to versjonene er også presentert i tabell 1 i vedlegg 2.

Det foreligger ikke en offisiell norsk oversettelse av standarden og vi har derfor benyttet engelsk terminologi der dette har vært ansett som mest hensiktsmessig. Vi har også benyttet forkortelsen ISMS (Information Security Management System) for å omtale styringssystem for informasjonssikkerhet.

3.1 Kapittel 0 Introduksjon (Introduction)

Introduksjonen til standarden er betydelig redusert i forhold til tidligere versjon. Spesielt gjelder dette Demings PDCA (Plan-Do-Check-Act)-modell som nå er tatt bort. Årsaken er at PDCA-modellen kun er en av mange konseptuelle modeller som illustrerer kontinuerlig forbedring (som er et krav i kapittel 10), og man står nå friere til å velge andre modeller.

3.2 Kapittel 1 Standardens omfang (Scope)

Teksten i avsnittet som omhandler standardens formål er kortet ned i forhold til 2005-utgaven. Tidligere var dette to deler; en generell del og en del som omhandlet selve anvendelsen av standarden. I ny utgave er dette slått sammen, og man har utelatt tidligere referanse til sikringstiltakene i vedlegg A.

3.3 Kapittel 2 Referanser (Normative references)

Tidligere ble det referert til ISO/IEC 17799:2005. Dette er erstattet med ISO/IEC 27000. ISO/IEC 27000 gir en overordnet beskrivelse av styringssystemer for informasjonssikkerhet, og definerer terminologien knyttet til dette. Alle standarder i ISMS-familien (ISO2700X) skal nå henvise til denne standarden for definisjoner og terminologi.

3.4 Kapittel 3 Terminologi og definisjoner (Terms and definitions)

Terminologi og definisjoner er i sin helhet tatt ut av standarden. Brukeren henvises i stedet til ISO/IEC 27000. Man skal likevel være klar over at 27000-standarden i sin nåværende form sist ble revidert i 2012. Inntil ISO/IEC 27000 kommer i ny utgave, er det viktig å være klar over at det kan forekomme noe ulik terminologi og at enkelte definisjoner kan avvike fra ISO/IEC 27001:2013. Vi mener det uansett er viktig å gjøre seg kjent med 27000-standarden.

3.5 Kapittel 4 Organisasjonskontekst (Context of the organization)

Dette er et nytt kapittel og omhandler hvilken kontekst styringssystemet skal operere innenfor. Det skal gjøres vurderinger av hvilke interne og eksterne forhold som kan påvirke virksomheten, samt hvordan disse påvirker styringssystemets innretning. Eksterne forhold er forhold som er utenfor virksomhetens kontroll. Dette kan for eksempel være forhold knyttet til lover og regelverk, eller politiske forhold virksomheten må forholde seg til.

Videre skal det gjøres vurderinger av hvem (interne og eksterne) som er relevante i forhold til styringssystemet, dvs. hvordan disse interessentenes krav og forventinger kan påvirke informasjonssikkerheten.

Som tidligere skal virksomheten definere styringssystemets omfang (scope), nå med bakgrunn i de interne og eksterne forholdene, interessenter, samt grenseflater man har mot andre virksomheter og organisasjoner.

3.6 Kapittel 5 Ledelse (Leadership)

Dette kapittelet stiller tydeligere krav til toppledelsen sammenliknet med gammel versjon. Toppledelsen er den personen eller gruppen som styrer virksomheten på øverste nivå. 2013-versjonen av standarden legger særlig vekt på ledelsesforankring på områder som tidligere var elementer organisasjonen som helhet hadde ansvar for.

Et nytt krav til ledelsen er å sørge for at kravene som vil fremgå gjennom styringssystemet, skal være integrerte mot de øvrige virksomhetsprosessene. I tillegg har det kommet inn et eget avsnitt i den nye standarden som er viet hvilke krav som gjelder ved etablering av en informasjonssikkerhets-policy. Tidligere var dette inkludert i kravene til ledelsen som ett punkt. Det er også kommet krav om at det er ledelsen som har ansvar for at styringssystemet er gjenstand for kontinuerlig forbedring.

3.7 Kapittel 6 Planlegging (Planning)

6.1.1 Generelt: Den nye versjonen av standarden introduserer i dette punktet at det i tillegg til identifisering av risiko også skal fastslås hvilke muligheter som kan håndteres for å sikre at styringssystemet for informasjonssikkerhet oppfyller de målsetningene som er satt, og at man oppnår kontinuerlig forbedring. Risiko og muligheter knyttet til styringssystemet i seg selv skal identifiseres med utgangspunkt i de interne og eksterne forhold som er identifisert i 4.1 og de krav som er identifisert i 4.2 (interessenters krav og forventninger). Virksomheten skal så planlegge hvilke tiltak som er nødvendige for å håndtere de identifiserte risikoene og mulighetene, hvordan disse skal integreres i ISMS-prosessene og hvordan effektiviteten av tiltakene skal evalueres.

6.1.2 Risikovurdering: Dette punktet omhandler spesifikt vurdering av risiko knyttet til informasjonssikkerhet (information security risk). Prinsippene er i den nye versjonen avstemt med de retningslinjer som gis i ISO 31000, ved at identifisering av verdier, trusler og sårbarheter ikke lenger er forutsetninger for å identifisere risiko. Dette medfører at virksomhetene i større grad kan velge hvilken metodikk for risikovurderinger de ønsker å benytte, og fortsatt være i samsvar med standarden.

Begrepet «asset owner» fra ISO/IEC 27001:2005 er erstattet med «risk owner» (risikoeier) i ny versjon av standarden. I punkt 6.1.3 beskrives dette som den eller de som er ansvarlige for å godkjenne tiltaksplanen («risk treatment plan»), samt akseptere gjenværende risiko.

6.1.3 Risikohåndtering: Dette punktet omhandler håndtering av informasjonssikkerhetsrisiko, og tilsvarer i stor grad den tidligere beskrivelsen i ISO/IEC 27001:2005. Det er imidlertid en endring ved at man istedenfor å velge sikringstiltak fra vedlegg A skal fastslå hvilke tiltak som er nødvendige. Valgte tiltak skal så sammenlignes med vedlegg A for å kontrollere at ingen relevante tiltak er utelatt. Virksomheten må fortsatt etablere en «Statement of Applicability» (SoA), der nødvendige sikringstiltak skal begrunnes. Det skal også begrunnes hvorfor sikringstiltak i vedlegget eventuelt er utelatt.

Som tidligere stilles det krav til at en tiltaksplan skal formuleres. Tiltaksplanen skal godkjennes av risikoeierne, og det er også de som skal gi sin aksept for gjenværende risiko. Dette ansvaret var i 2005-versjonen mer generelt plassert på ledelsen.

6.2: Mål for informasjonssikkerhet (Information security objectives): Det skal defineres informasjonssikkerhetsmål for alle relevante funksjoner og nivåer, der «funksjon» refererer til ulike funksjoner i virksomheten, mens «nivå» refererer til ledelsesnivå. Punktet er mer spesifikt enn det var i 2005-versjonen, og beskriver hvilke egenskaper virksomhetens informasjonssikkerhetsmål skal inneha. De skal blant annet være målbare, kommunisert og oppdatert.

3.8 Kapittel 7 Ressursplanlegging (Support)

Kapittelet stiller krav til at virksomheten skal avklare og gjøre tilgjengelig de ressurser som er nødvendig for etablering, implementering, vedlikehold og kontinuerlig forbedring av styringssystemet for informasjonssikkerhet.

Videre stilles det krav til kompetanse, bevisstgjøring og intern og ekstern kommunikasjon.

Punkt 7.5 omhandler «dokumentert informasjon» (documented information). Dette er et nytt begrep som erstatter 2005-versjonens referanser til «documents» og «records». Kravene omhandler opprettelse og oppdatering av dokumentert informasjon, og hvordan disse kontrolleres. Kravene har mange likhetstrekk med de krav 2005-versjonen stilte til «control of documents» og «control of records».

Dokumentasjonskravene i ISO/IEC 27001:2013 er definert i de ulike punktene der de er relevante, og ikke som i forrige versjon av standarden der dokumentasjonskravene var oppsummert i et eget punkt.

3.9 Kapittel 8 Gjennomføring (Operation)

Dette kapitlet omhandler gjennomføringen av de planer og prosesser som er beskrevet i de tidligere kapitlene.

Punkt 8.1 stiller krav til at virksomheten skal planlegge, implementere og kontrollere de prosessene som er nødvendige for å nå de kravene som stilles til informasjonssikkerhet, for å gjennomføre

tiltakene som er identifisert i punkt 6.1, og for å oppnå informasjonssikkerhetsmålene man har besluttet i 6.2.

Det stilles også spesifikt krav til at virksomheten skal ha kontroll på planlagte endringer, og evaluere konsekvensene av utilsiktede endringer. Man skal også ha kontroll med eventuelle prosesser som er satt ut til tredjepart.

Som tidligere stilles det i punkt 8.2 krav til gjennomføring av risikoanalyser med fokus på informasjonssikkerhet. Risikoanalyser skal gjennomføres regelmessig, i planlagte intervaller, eller når vesentlige endringer planlegges eller oppstår.

Punkt 8.3 stiller krav til at planen for risikohåndtering implementeres, og at resultatet av dette arbeidet dokumenteres.

3.10 Kapittel 9 Evaluering (Performance evaluation)

Punkt 9.1 omhandler overvåking, måling, analyse og evaluering. For å kunne gjennomføre måling og overvåking av informasjonssikkerheten, samt effektiviteten til styringssystemet, skal man først identifisere hvilke parametere man trenger. Deretter må man vurdere hva, når og hvordan en skal måle, samt hvem som skal gjennomføre målingene.

Punkt 9.2 Internrevisjon: Dette kravet har ikke blitt endret i særlig grad fra 2005-versjonen av standarden. Kravet om at ledelsen skal sørge for at det blir gjennomført tiltak innen rimelig tid etter at revisjoner er utført, er imidlertid fjernet. Grunnen til dette er at krav til oppfølging av avvik dekkes gjennom kravene i punkt 10.1.

Punkt 9.3 Ledelsens gjennomgang: Dette kravet er endret til å dreie seg mer om å sette krav til hvilke deler av styringssystemet som skal gjennomgås, fremfor å spesifikt si noe om hvilke faktorer som spiller inn i vurderingene og hva utfallet skal være. Videre har man tatt bort kravet om at det skal være årlige gjennomganger. Det er imidlertid ikke gjort endringer i kravet om at slike gjennomganger skal utføres med planlagte intervaller.

3.11 Kapittel 10: Forbedring (Improvement)

Kapittelet omhandler forbedring av styringssystemet. Det stilles ikke lenger krav om at virksomheten skal planlegge forebyggende tiltak mot potensielle avvik fra standarden. Dette skyldes endringen i måten det stilles krav til korrigerende tiltak på; dersom det oppdages avvik, må virksomheten først gjennomføre nødvendige endringer som skal til for å rette opp avvikene. Deretter må man vurdere om det finnes tilsvarende avvik i andre deler av styringssystemet, eller om samme avvik kan oppstå på nytt. For øvrig har det kommet inn et nytt krav om at man skal kunne dokumentere at de korrigerende tiltakene man har iverksatt, faktisk fungerer som forutsatt.

I tillegg til at kravet til kontinuerlig forbedring nå også dekker styringssystemets egnethet og tilstrekkelighet, er det fortsatt krav om å sikre styringssystemets effektivitet. Imidlertid fastsettes det ikke hvordan virksomheten skal oppnå dette, slik det ble gjort tidligere.

3.12 Vedlegg A (Annex A)

Tittelen til vedlegg A (Annex A) er nå «Reference control objectives and controls». Innledningen er betydelig forenklet, og det fremgår tydeligere enn i 2005-versjonen at kontrollmålene og sikringstiltakene i vedlegget er hentet direkte fra ISO/IEC 27002:2013. Videre presiseres det at både mål og tiltak skal sees i sammenheng med kravene i punkt 6.1.3 i standarden.

Antallet sikringstiltak i ISO/IEC 27002:2013 er redusert fra 133 til 114 i forhold til 2005-versjonen. Samtidig er antallet kapitler økt fra 11 til 14. Noen sikringstiltak er uendret eller kun marginalt endret, andre er slått sammen, noen er fjernet i sin helhet, mens noen er helt nye. En oversikt over sammenhengen mellom tiltakene i vedlegg A i 2005- og 2013-versjonene er presentert i vedlegg 2, tabell 2 og 3.

4. Overgang til ny standard

Difi anbefaler at virksomheter som skal etablere et styringssystem for informasjonssikkerhet baserer seg på ISO/IEC 27001:2013.

For virksomheter som allerede har et velfungerende styringssystem basert på ISO/IEC 27001:2005 anbefales det en gradvis overgang til ISO/IEC 27001:2013 som en del av arbeidet med kontinuerlig forbedring av styringssystemet. Dersom virksomheten har risikoer over akseptabelt nivå anbefales det imidlertid at man tidlig vurderer de oppdateringer og endringer som ligger i vedlegg A i ISO/IEC 27001:2013, og videre ISO/IEC 27002:2013, for å identifisere eventuelle nye sikringstiltak som kan bidra til å redusere risikoen.

Før virksomheten starter arbeidet med å tilpasse styringssystemet til ISO/IEC 27001:2013, bør det gjennomføres en gap-analyse for å identifisere forskjeller mellom de krav som fremgår av ny standard og det eksisterende styringssystemet. Dette bør resultere i en plan for hvilke grep virksomheten må gjennomføre for å tilfredsstille de nye eller endrede kravene.

I det følgende presenteres områdene i standarden som krever endringer for at styringssystemet skal være i henhold til ISO/IEC 27001:2013. Områdene er gruppert ut i fra hvor omfattende endringene antas å være. Imidlertid understreker vi at alle virksomheter er ulike og derfor må denne veiledningen tolkes i forhold til de ulike behovene den enkelte virksomhet har. Elementer som er relativt enkle for en virksomhet kan vise seg å være utfordrende for en annen, og omvendt. Forhåpentligvis er denne veilederen et godt utgangspunkt for de fleste virksomheter.

4.1 Nye temaer og krav som allerede kan være oppfylt

4.1.1 Interessenter og deres krav

I punkt 4.2 stilles det krav til at virksomheten skal identifisere interessenter som er relevante for styringssystemet for informasjonssikkerhet, og hvilke krav og forventninger disse interessentene har. Interessenter kan inkludere brukere og leverandører, og kravene kan være dokumentert i kontrakter, spesifikasjoner eller lignende.

Informasjon om relevante interessenter er det sannsynlig at virksomheten allerede har. Det som da må gjøres for å oppfylle kravet vil derfor være å identifisere hvor dette er dokumentert, og hvor kravene er spesifisert, og henvise til dette. Dersom denne informasjonen ikke tidligere er kartlagt, vil det være en større jobb å gjøre dette for å oppfylle kravet.

4.1.2 Integrasjon

I punkt 5.1b) stilles det krav til at ISMS-kravene skal være integrert i virksomhetens prosesser. Dersom virksomhetens prosesser er beskrevet i arbeidsflytdiagrammer eller lignende, og de aktivitetene som korresponderer med ISMS-kravene er fordelt på disse arbeidsflytene, er kravet til integrasjon sannsynligvis oppfylt.

Dersom ISMS-kravene imidlertid er representert av en enkelt arbeidsflyt/prosess som ikke består av noe annet er integrasjonskravet sannsynligvis ikke oppfylt. Det vil da være nødvendig å innarbeide

ISMS-prosessen i de øvrige prosessene i virksomheten, og dokumentere dette, for å oppfylle dette kravet.

4.1.3 Kommunikasjon

Kravene for kommunikasjon i punkt 7.4 er mer spesifikke enn de tilsvarende kravene i den tidligere versjonen av standarden. De nye kravene følger imidlertid det som ofte er etablert praksis, og dette kan medføre at kommunikasjonskravene allerede er oppfylt.

4.2 Temaer og krav som ikke bør kreve store endringer

4.2.1 Dokumentert informasjon (Documented information)

Dette er ny terminologi sammenliknet med utgående standard hvor dette refereres til som documents (dokumenter) og records (dokumentasjon). For å etterleve kravene til ny standard, må gammel terminologi byttes ut med ny der dette er nødvendig.

Hvis man ser behov for å skille mellom de to termene, må man være klar over at documents (dokumenter) pr. definisjon er et skriftstykke eller tilsvarende som har betydning for en viss sak. Records (dokumentasjon) er på sin side bevisførsel ved hjelp av dokumenter.

4.2.2 Policy

Det er et krav i ISO/IEC 27001:2005 at det skal foreligge en ISMS-policy. Dette dokumentet skal inneholde informasjonssikkerhetspolicy og risikokriterier. Kravene til policyer og retningslinjer i 2013-versjonen av standarden (punkt 5.2) omtaler kun informasjonssikkerhetspolicy, men det fremgår av punkt 6.1.2 at virksomheten skal definere nivåene for hva som er akseptabel risiko og hvilke kriterier som ligger til grunn for når og hvordan risikovurderinger relatert til informasjonssikkerhet skal gjennomføres. Dette skal holdes oppdatert med jevne mellomrom. I det samme punktet er det også krav om at virksomheten skal dokumentere selve prosessen omkring risikovurderingene.

For de virksomhetene som allerede har dokumentert risikokriteriene og informasjonssikkerhets-policyen i sin ISMS-policy, er det ikke nødvendig å lage en ny policy. Det er heller ikke nødvendig med noe navnebytte, da 2013-versjonen ikke legger opp til standardiserte navn på obligatoriske dokumenter.

4.2.3 Risikovurderinger

I 2005-versjonen av standarden er det en forutsetning at virksomheten må ha oversikt over både informasjonsverdier, trusler og sårbarheter før risikoene kan identifiseres. I den oppdaterte versjonen av standarden er det ikke lenger slik. I stedet benyttes samme terminologi og vokabular som ISO 31000. Kravene er imidlertid strukturert likt som i 2005-versjonen, ved at man skal identifisere risiko på bakgrunn av sannsynlighets- og konsekvensvurderinger. Virksomheten kan derfor benytte samme metodikk for risikovurderinger og risikohåndtering som man har benyttet tidligere. Dokumentasjonskravene er stort sett de samme, og det er heller ikke her nødvendig å gjøre store endringer i de skriftlige rutinene.

4.2.4 Krav til ledelsen

For å tilfredsstille kravene som fremgår av punkt 5.1, kan det være nødvendig å dokumentere ledelsens engasjement i noe større utstrekning enn før.

4.2.5 Roller og ansvar

For å tilfredsstille kravene som fremgår av punkt 5.3 a) og b), kan det være nødvendig å synliggjøre ytterligere hvem som har ansvar for at styringssystemet tilfredsstiller kravene i standarden, samt at ledelsen holdes informert om styringssystemets effektivitet.

4.2.6 Ledelsens gjennomgang (management review)

Det er ikke nødvendig å gjøre store endringer i rutinene for ledelsens gjennomgang av styrings-systemet. Imidlertid bør man vurdere å inkludere elementene som fremgår av punkt 9.3 a) – f).

4.2.7 Håndtering av avvik fra standarden

Eksisterende rutiner bør antakeligvis endres noe for å sikre at virksomheten har mulighet til å oppdage og håndtere avvik fra standarden.

4.2.8 Kontinuerlig forbedring

Virksomheten skal ha rutiner og prosedyrer som sikrer at styringssystemet holdes oppdatert og at det fungerer effektivt. I henhold til ny standard, ligger det i dette at disse rutinene også skal ta høyde for at styringssystemet må være tilpasset virksomhetens risiko og egenart.

4.3 Temaer og krav som kan være arbeidskrevende

4.3.1 Styringssystemets omfang (scope)

I gammel standard var kravet at virksomheten måtte definere omfanget av styringssystemet på bakgrunn av virksomhetens egenart. Videre skulle forhold omkring lokasjon, eiendeler og teknologi tas med i betraktningen. I ny standard er disse kravene ytterligere spesifisert og utvidet i punkt 4.3, eksempelvis ved at forventninger og krav fra tredjeparter skal tas hensyn til.

4.3.2 Mål for informasjonssikkerheten

Dersom informasjonssikkerhetsmålene har vært statiske og på et overordnet nivå, kan det umiddelbart fremstå som krevende å etterleve kravene som fremgår av punkt 6.2. Det kan imidlertid hende at virksomheten ikke trenger å gjøre de helt store endringene. De fleste virksomheter har sannsynligvis noen målsetninger for relevante funksjoner og nivåer i organisasjonen. Arbeidet vil bestå i å dokumentere dette.

4.3.3 Statement of Applicability (SoA)

Vedlegg A er oppdatert for å reflektere sikringstiltakene som fremgår av ISO/IEC 27002:2013. Selv om sikringstiltakene ikke er obligatoriske, skal likevel virksomheten dokumentere i SoAen hvorfor eventuelle tiltak er utelatt. Dersom virksomheten mener det er mer hensiktsmessig å implementere tiltak fra andre rammeverk, eksempelvis fra COBIT[2], så bør også dette fremgå av SoAen.

Selve formatet på SoAen trenger ikke å endres, men ettersom sikringstiltakene i seg selv har vært gjenstand for endring, må innholdet i SoAen oppdateres.

[2] COBIT er et rammeverk for IT-styring og kontroll utarbeidet av ISACA, som blant annet har som mål å koble virksomhetens forretningsmål til IT-målene. http://www.isaca.org/cobit/pages/default.aspx

4.3.4 Eksterne og interne forhold (issues)

Jf. punkt 4.1 i standarden skal interne og eksterne forhold som er relevante for virksomheten kartlegges. Det er sannsynlig at slike forhold allerede er kjent for virksomheten, men de er ikke nødvendigvis dokumentert.

4.3.5 Handlinger for å håndtere risiko og muligheter - generelt

Ettersom kravene i punktene 4.1 og 4.2 er nye og således kan påvirke risikobildet, må virksomheten foreta endringer i sine risikoanalyser slik at kravene som fremgår av punkt 6.1.1 blir ivaretatt. Det er også nytt i 2013-versjonen av standarden at virksomheter skal identifisere og håndtere både risikoer og muligheter knyttet til styringssystemet.

4.3.6 Overvåking, måling, analyse og evaluering

Kravene i punkt 9.1 er mer detaljert og nøyaktige i ny versjon av standarden sammenliknet med tidligere. Det er blant annet krav om at man skal dokumentere og måle effektiviteten av de implementerte sikringstiltakene, i tillegg til at styringssystemet i seg selv skal være gjenstand for evaluering. I denne sammenheng kan det være hensiktsmessig å støtte seg til NS-ISO/IEC 27004:2009 Styring av informasjonssikkerhet – Måling. Vi gjør imidlertid oppmerksom på at denne ennå ikke har vært gjenstand for revisjon, og således referer til 2005-versjonen av NS-ISO/IEC 27001.

Vedlegg 1 - Referanser

- «Transition guide – Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013» - British Standards Institution: http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf
- «Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013" - British Standards Institution: http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf
- "Styringssystem for informasjonssikkerhet. Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002» - Difi-rapport 2012:15
- NS-ISO/IEC 27001:2005
- NS-ISO/IEC 27001:2013

Vedlegg 2 – Speilingstabeller

Tabell 1: Tabellen viser sammenhengen mellom ISO/IEC 27001:2013 og ISO/IEC 27001:2005, og er hentet fra veilederen «Transition guide - Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013» utgitt av British Standards Institution. Dette er en forenklet tabell som hovedsakelig illustrerer forskjellene.

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
0	Introduction	**0**	Introduction
1	Scope	**1**	Scope
2	Normative references	**2**	Normative references
3	Terms and definitions	**3**	Terms and definitions
4.1	Understanding the organization and its context	**8.3**	Preventive action
4.2	Understanding the needs and expectations of interested parties	**5.2.1 c)**	Identify and address legal and regulatory requirements and contractual security obligations
4.3	Determining the scope of the information security management system	**4.2.1 a)** **4.2.3 f)**	Define scope and boundaries Ensure the scope remains adequate
4.4	Information security management system	**4.1**	General requirements
5.1	Leadership and commitment	**5.1**	Management commitment
5.2	Policy	**4.2.1 b)**	Define an ISMS policy
5.3	Organizational roles, responsibilities and authorities	**5.1 c)**	Establishing roles and responsibilities for information security
6.1.1	Actions to address risks and opportunities – general	**8.3**	Preventive action
6.1.2	Information security risk assessment	**4.2.1 c)** **4.2.1 d)** **4.2.1 e)**	Define the risk assessment approach Identify the risks Analyse and evaluate the risks
6.1.3	Information security risk treatment	**4.2.1 f)** **4.2.1 g)** **4.2.1 h)** **4.2.1 i)** **4.2.1 j)** **4.2.2 a)**	Identify and evaluate options for the treatment of risks Select control objectives and controls for the treatment of risks Obtain management approval of the proposed residual risk Obtain management authorization to implement and operate the ISMS Prepare a Statement of Applicability Formulate a risk treatment plan
6.2	Information security objectives and planning to achieve them	**5.1 b)**	Ensuring that ISMS objectives and plans are established
7.1	Resources	**4.2.2 g)** **5.2.1**	Manage resources for the ISMS Provision of resources
7.2	Competence	**5.2.2**	Training, awareness and competence
7.3	Awareness	**4.2.2 e)** **5.2.2**	Implement training and awareness programmes Training, awareness and competence
7.4	Communication	**4.2.4 c)** **5.1 d)**	Communicate the actions and improvements Communication to the organization
7.5	Documented information	**4.3**	Documentation requirements
8.1	Operational planning and control	**4.2.2 f)**	Manage operations of the ISMS
8.2	Information security risk assessment	**4.2.3 d)**	Review risk assessments at planned intervals
8.3	Information security risk treatment	**4.2.2 b)** **4.2.2 c)**	Implement the risk treatment plan Implement controls
9.1	Monitoring, measurement, analysis and evaluation	**4.2.2 d)** **4.2.3 b)** **4.2.3 c)**	Define how to measure effectiveness Undertake regular reviews of the effectiveness of the ISMS Measure the effectiveness of controls
9.2	Internal Audit	**4.2.3 e)** **6**	Conduct internal ISMS audits Internal ISMS audits
9.3	Management review	**4.2.3 f)** **7**	Undertake a management review of the ISMS Management review of the ISMS
10.1	Nonconformity and corrective action	**4.2.4** **8.2**	Maintain and improve the ISMS Corrective action
10.2	Continual improvement	**4.2.4** **8.1**	Maintain and improve the ISMS Continual improvement

Tabell 2: Tabellen viser sammenhengen mellom sikringstiltakene i Vedlegg A i ISO/IEC 27001:2013 og ISO/IEC 27001:2005, og er hentet fra veilederen «Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013» utgitt av British Standards Institution.

Vedlegg A-tiltak i ISO/IEC 27001:2013		Vedlegg A-tiltak i ISO/IEC 27001:2005
A.5.1.1	Policies for information security	**A.5.1.1**
A.5.1.2	Review of the policies for information security	**A.5.1.2**
A.6.1.1	Information security roles and responsibilities	**A.6.1.3, A.8.1.1**
A.6.1.2	Segregation of duties	**A.10.1.3**
A.6.1.3	Contact with authorities	**A.6.1.6**
A.6.1.4	Contact with special interest groups	**A.6.1.7**
A.6.1.5	Information security in project management	**NY**
A.6.2.1	Mobile device policy	**A.11.7.1**
A.6.2.2	Teleworking	**A.11.7.2**
A.7.1.1	Screening	**A.8.1.2**
A.7.1.2	Terms and conditions of employment	**A.8.1.3**
A.7.2.1	Management responsibilities	**A.8.2.1**
A.7.2.2	Information security awareness, education and training	**A.8.2.2**
A.7.2.3	Disciplinary process	**A.8.2.3**
A.7.3.1	Termination or change of employment responsibilities	**A.8.3.1**
A.8.1.1	Inventory of assets	**A.7.1.1**
A.8.1.2	Ownership of assets	**A.7.1.2**
A.8.1.3	Acceptable use of assets	**A.7.1.3**
A.8.1.4	Return of assets	**A.8.3.2**
A.8.2.1	Classification of information	**A.7.2.1**
A.8.2.2	Labelling of information	**A.7.2.2**
A.8.2.3	Handling of assets	**A.10.7.3**
A.8.3.1	Management of removable media	**A.10.7.1**
A.8.3.2	Disposal of media	**A.10.7.2**
A.8.3.3	Physical media transfer	**A.10.8.3**
A.9.1.1	Access control policy	**A.11.1.1**
A.9.1.2	Access to networks and network services	**A.11.4.1**
A.9.2.1	User registration and de-registration	**A.11.2.1, A.11.5.2**
A.9.2.2	User access provisioning	**A.11.2.1**
A.9.2.3	Privilege management	**A.11.2.2**
A.9.2.4	Management of secret authentication information of users	**A.11.2.3**
A.9.2.5	Review of user access rights	**A.11.2.4**
A.9.2.6	Removal or adjustment of access rights	**A.8.3.3**
A.9.3.1	Use of secret authentication information	**A.11.3.1**
A.9.4.1	Information access restriction	**A.11.6.1**
A.9.4.2	Secure log-on procedures	**A.11.5.1, A.11.5.5, A.11.5.6**
A.9.4.3	Password management system	**A.11.5.3**
A.9.4.4	Use of privileged utility programs	**A.11.5.4**
A.9.4.5	Access control to program source code	**A.12.4.3**
A.10.1.1	Policy on the use of cryptographic controls	**A.12.3.1**
A.10.1.2	Key management	**A.12.3.2**
A.11.1.1	Physical security perimeter	**A.9.1.1**
A.11.1.2	Physical entry controls	**A.9.1.2**
A.11.1.3	Securing office, rooms and facilities	**A.9.1.3**
A.11.1.4	Protecting against external end environmental threats	**A.9.1.4**
A.11.1.5	Working in secure areas	**A.9.1.5**
A.11.1.6	Delivery and loading areas	**A.9.1.6**
A.11.2.1	Equipment siting and protection	**A.9.2.1**
A.11.2.2	Supporting utilities	**A.9.2.2**
A.11.2.3	Cabling security	**A.9.2.3**
A.11.2.4	Equipment maintenance	**A.9.2.4**
A.11.2.5	Removal of assets	**A.9.2.7**
A.11.2.6	Security of equipment and assets off-premises	**A.9.2.5**
A.11.2.7	Security disposal or re-use of equipment	**A.9.2.6**

A.11.2.8	Unattended user equipment	**A.11.3.2**
A.11.2.9	Clear desk and clear screen policy	**A.11.3.3**
A.12.1.1	Documented operating procedures	**A.10.1.1**
A.12.1.2	Change management	**A.10.1.2**
A.12.1.3	Capacity management	**A.10.3.1**
A.12.1.4	Separation of development, test and operational environments	**A.10.1.4**
A.12.2.1	Controls against malware	**A.10.4.1, A.10.4.2**
A.12.3.1	Information backup	**A.10.5.1**
A.12.4.1	Event logging	**A.10.10.1, A.10.10.2, A.10.10.5**
A.12.4.2	Protection of log information	**A.10.10.3**
A.12.4.3	Administrator and operator logs	**A.10.10.3, A.10.10.4**
A.12.4.4	Clock synchronisation	**A.10.10.6**
A.12.5.1	Installation of software on operational systems	**A.12.4.1**
A.12.6.1	Management of technical vulnerabilities	**A.12.6.1**
A.12.6.2	Restrictions on software installation	**NY**
A.12.7.1	Information systems audit controls	**A.15.3.1**
A.13.1.1	Network controls	**A.10.6.1**
A.13.1.2	Security of network services	**A.10.6.2**
A.13.1.3	Segregation in networks	**A.11.4.5**
A.13.2.1	Information transfer policies and procedures	**A.10.8.1**
A.13.2.2	Agreements on information transfer	**A.10.8.2**
A.13.2.3	Electronic messaging	**A.10.8.4**
A.13.2.4	Confidentiality or non-disclosure agreements	**A.6.1.5**
A.14.1.1	Security requirements analysis and specification	**A.12.1.1**
A.14.1.2	Securing applications services on public networks	**A.10.9.1, A.10.9.3**
A.14.1.3	Protecting application services transactions	**A.10.9.2**
A.14.2.1	Secure development policy	**NY**
A.14.2.2	System change control procedures	**A.12.5.1**
A.14.2.3	Technical review of applications after operating platform changes	**A.12.5.2**
A.14.2.4	Restrictions on changes to software packages	**A.12.5.3**
A.14.2.5	Secure system engineering principles	**NY**
A.14.2.6	Secure development environment	**NY**
A.14.2.7	Outsourced development	**A.12.5.5**
A.14.2.8	System security testing	**NY**
A.14.2.9	System acceptance testing	**A.10.3.2**
A.14.3.1	Protection of test data	**A.12.4.2**
A.15.1.1	Information security policy for supplier relationships	**NY**
A.15.1.2	Addressing security within supplier agreements	**A.6.2.3**
A.15.1.3	Information and communication technology supply chain	**NY**
A.15.2.1	Monitoring and review of supplier services	**A.10.2.2**
A.15.2.2	Managing changes to supplier services	**A.10.2.3**
A.16.1.1	Responsibilities and procedures	**A.13.2.1**
A.16.1.2	Reporting information security events	**A.13.1.1**
A.16.1.3	Reporting information security weaknesses	**A.13.1.2**
A.16.1.4	Assessment and decision on information security events	**NY**
A.16.1.5	Response to information security incidents	**NY**
A.16.1.6	Learning from information security incidents	**A.13.2.2**
A.16.1.7	Collection of evidence	**A.13.2.3**
A.17.1.1	Planning information security continuity	**A.14.1.2**
A.17.1.2	Implementing information security continuity	**A.14.1.1, A.14.1.3, A.14.1.4**
A.17.1.3	Verify, review and evaluate information security continuity	**A.14.1.5**
A.17.2.1	Availability of information processing facilities	**NY**
A.18.1.1	Identification of applicable legislation and contractual requirements	**A.15.1.1**
A.18.1.2	Intellectual property rights (IPR)	**A.15.1.2**
A.18.1.3	Protection of records	**A.15.1.3**
A.18.1.4	Privacy and protection of personally identifiable information	**A.15.1.4**
A.18.1.5	Regulation of cryptographic controls	**A.15.1.6**
A.18.2.1	Independent review of information security	**A.6.1.8**
A.18.2.2	Compliance with security policies and standards	**A.15.2.1**
A.18.2.3	Technical compliance review	**A.15.2.2**

Tabell 3: Tabellen viser sikringstiltakene i vedlegg A i ISO/IEC 27001:2005 som er fjernet i 2013-versjonen. Tabellen er hentet fra veilederen «Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013» utgitt av British Standards Institution.

Sikringstiltak i Vedlegg A i ISO/IEC 27001:2005 som er fjernet i ISO/IEC 27001:2013	
A.6.1.1	Management commitment to information security
A.6.1.2	Information security coordination
A.6.1.4	Authorisation process for information processing facilities
A.6.2.1	Identification of risks related to external parties
A.6.2.2	Addressing security when dealing with customers
A.10.7.4	Security of system documentation
A.10.8.5	Business Information Systems
A.11.4.2	User authentication for external connections
A.11.4.3	Equipment identification in networks
A.11.4.4	Remote Diagnostic and configuration port protection
A.11.4.6	Network Connection control
A.11.4.7	Network routing control
A.11.6.2	Sensitive system isolation
A.12.2.1	Input data validation
A.12.2.2	Control of internal processing
A.12.2.3	Message integrity
A.12.2.4	Output data validation
A.12.5.4	Information leakage
A.15.1.5	Prevention of misuse of information processing facilities
A.15.3.2	Protection of information systems audit tools