Informasjonssikkerhet: Teori og praksis
Audun Jøsang
2. utgave 2023
Universitetsforlaget

Sammendrag av ISO/IEC 27001

Audun Jøsang, UiO

Bakgrunn: JTC 1, SC 27, WG 1

ISO (International Organization for Standardization) og IEC (International Electrotechnical Commission) opprettet i 1987 et samarbeidsorgan kalt JTC 1 (Joint Technical Committee nr.1) med formål å drive standardisering av "Information technology". Vær oppmerksom på at JTC 2 ikke fins, ingen andre JTC-er ble opprettet.
Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_JTC_1

Det fins ca. 40 underkomiteer (SC: subcommittees) under JTC 1 som jobber med standardisering innen ulike IT-områder. SC 27 fokuserer på informasjonssikkerhet.
Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_JTC_1/SC_27

Det fins 5 arbeidsgrupper (WG: working groups) under SC 27 som jobber med standardisering av informasjonssikkerhet innen ulike IT-sikkerhetsområder. WG 1 fokuserer på styring og ledelse av informasjonssikkerhet.
Wikipedia: https://en.wikipedia.org/wiki/Information_security_management

Standarder som vedlikeholdes av WG 1 er bl.a.
ISO/IEC 27000: Overview and vocabulary (Oversikt og ordliste)
ISO/IEC 27001: Requirements for Information Security Management System (ISMS)
(Krav til ledelsessystem for informasjonssikkerhet)
ISO/IEC 27002: Information Security Controls (Tiltak for informasjonssikkerhet)

ISO/IEC 27001 er en standard for et såkalt «styringssystem» eller «ledelsessystem». Eksempler på standarder for styrings-/ledelsessystemer er:

- ISO 9001 Quality Management (Kvalitetsledelse)
- ISO/IEC 20000 Service Management (Tjenesteledelse)
- ISO 22300 Security and Resilience (Samfunnssikkerhet)
- ISO/IEC 27001(ISMS: Information security management System) (Ledelsessystem for informasjonssikkerhet)
- ISO 31000 Risk management (Risikostyring)
- ISO 39001 Road Safety Management System (Styringssystem for trafikksikkerhet)
- ISO 22000 Food Safety Management System (Ledelsessystem for næringsmiddeltrygghet)

De ulike standardene for ledelses-/styringssystemer har en felles struktur.

Strukturen av ISO/IEC 27001

Tabellen nedenfor viser avsnittene og strukturen i ISO/IEC 27001: 2022.

1. Scope (formål og anvendelsesområde)			
2. Normgivende referanser			
3. Begreper og definisjoner			
4. Kontekstuelle krav			
4.1. Forstå kontekst for virksomheten	4.2. Forstå forventninger fra berørte parter	4.3. Spesifiser omfang av ISMS	4.4. Initiativ om å opprette ISMS
5. Ledelseskrav			
5.1. Ledelsesforankring til forvaltning av ISMS	5.2. Opprett adekvate policyer for informasjonssikkerhet	5.3. Tilordne ansvar for forvaltning av ISMS	
6. Planleggingskrav			
6.1. Beskriv tilnærminger for å styre sikkerhetsrisiko og utnytte muligheter	6.2. Beskriv målsettinger for info-sikkerhet og planer for å oppnå disse		
7. Krav til ressurser og støttefunksjoner			
7.1. Ressurser for ISMS	7.2. Kompetanse	7.3. Oppmerksomhet på ansvar	7.4. kommunikasjon	7.5. Dokumentasjon
8. Krav til drift			
8.1. Utfør planer og foreta styring av prosesser	8.2. Utfør risikovurdering for informasjonssikkerhet	8.3. Håndtere informasjonssikkerhetsrisiko	
9. Krav til evaluering			
9.1. Monitorere, måle, analysere og evaluere ISMS	9.2. Internrevisjon av ISMS	9.3. Ledelsens gjennomgang av evalueringer og revisjon	
10. Krav til kontinuerlig forbedring			
10.1. Kontinuerlig forbedring	10.2. Identifiser avvik og innfør tiltak		
Annex A			

Avsnitt 4-10 i ISO/IEC 27001 som omhandler krav, er kort beskrevet nedenfor.

Avsnitt 4: Kontekstuelle krav

Et helhetlig krav er at organisasjonen skal etablere, implementere, vedlikeholde og kontinuerlig forbedre et ISMS, som inkluderer de nødvendige prosessene og deres interaksjoner, i samsvar med alle kravene i standarden.

Organisasjonen skal identifisere eksterne og interne aspekter betingelser som er relevante for dens formål og som berører informasjonssikkerhet. For eksempel er regulatoriske etterlevelseskrav og bransjenormer viktige eksterne betingelser. Videre må organisasjonen forstå informasjonssikkerhetsbehov og -forventninger til relevante tredjeparter som virksomheten kommer i kontakt med og må forholde seg til.

Omfanget av organisasjonens ISMS skal bestemmes ut ifra behov og organisasjonens størrelse.

Avsnitt 5: Ledelseskrav

Toppledelsen skal vise lederskap bl.a. ved å sørge for at policyer og målsettinger for informasjonssikkerhet er etablert og er kompatible med organisasjonens helhetlige strategi, sørge for tilstrekkelige ressurser til arbeidet med informasjonssikkerhet, og kommunisere viktigheten av informasjonssikkerhet til hele organisasjonen, og sjekke at ISMS oppnår de forventede resultater.

Toppledelsen skal sørge for at ansvar og myndighet for roller som er relevante for informasjonssikkerhet er tildelt og kommunisert internt i organisasjonen.

Avsnitt 6: Planleggingskrav

Organisasjonen skal planlegge for risikostyring ved å velge metode for risikovurdering, definere kriterier for risikoaksept. Videre skal organisasjonen etablere en prosess for å håndtere identifiserte risikoer.

Ved valg av sikkerhetstiltak for å redusere risiko til et akseptabelt nivå, eller for å tilfredsstille regulatoriske krav, skal organisasjonen ta i betraktning listen over sikkerhetstiltak i Annex A (og som er beskrevet i detalj i ISO/IEC 27002). I tillegg kan andre sikkerhetstiltak vurderes.

SoA (Statement of Applicability) er et dokument som lister opp alle sikkerhetstiltakene i Annex A, og som for hvert tiltak kort forklarer om, og hvorfor, tiltaket er implementert eller ikke. Når en risikovurdering utføres (som del av avsnitt 8 Drift nedenfor) og det velges måter å håndtere risikoene, skal det utarbeides en SoA som minst skal inneholde:

- nødvendige informasjonssikkerhetstiltak
- begrunnelse for deres inkludering;
- om de nødvendige sikkerhetstiltak er implementert eller ikke; og
- begrunnelsen for å ekskludere noen av sikkerhetstiltakene i Annex A.

Organisasjonen skal etablere målsettinger for informasjonssikkerhet for relevante domener, funksjoner og forretningsprosesser, som betyr å spesifisere behov for konfidensialitet, integritet og tilgjengelighet (KIT). Hvis praktisk mulig skal det måles og dokumenteres om målsettingene oppnås.

Avsnitt 7: Krav til ressurser og støttefunksjoner

Organisasjonen skal tildele tilstrekkelige ressursene som trengs for arbeidet med ISMS. Organisasjonen skal kartlegge behov for kompetansen og sørge for relevante medarbeidere faktisk har den kompetansen.

Organisasjonen skal sørge for at ansatte har bevissthet rundt sikkerhetspolicyer, viktigheten av å følge policyer, og konsekvenser av å ikke følge policyer. Organisasjonen skal ha en plan for kommunikasjon vedrørende informasjonssikkerhet, både internt og med ulike eksterne parter.

Dokumentasjon er et grunnleggende krav. Organisasjonens ISMS skal innbefatte dokumentert informasjon som eksplisitt kreves av standarden, og dokumentert informasjon som er nødvendig for effektiviteten i hele ISMS, bl.a. om de ulike prosessene som inngår. Omfanget av dokumentasjon kan variere fra ut ifra størrelsen på organisasjonen og dens type aktiviteter, prosesser, produkter og tjenester, kompleksiteten til prosesser og deres interaksjoner, og kompetansen til personer.

Avsnitt 8: Krav til forvaltning.

Organisasjonen skal planlegge, implementere og forvalte prosesser og sikkerhetstiltak som er nødvendige for å oppfylle kravene i ISMS, og for å drifte aktivitetene relatert til håndtering av risiko og forvaltning av sikkerhetstiltak beskrevet under avsnitt 6: Planlegging.

Organisasjonen skal peke ut relevante domener, funksjoner og forretningsprosesser for vurdering av informasjonssikkerhetsrisiko. Vurdering av risikoer skal bestå av å kartlegge verdier, identifisere trusler og sårbarheter, estimere sannsynlighet og alvorlighetsgrad for de ulike risikoene, som til slutt danner grunnlag for å beregne risikonivåer.

Ut ifra risikovurderingen og kriterier for risikoaksept, samt regulatoriske etterlevelseskrav, skal organisasjonen bestemme og sette i verk håndtering av de ulike risikoene, som kan være å redusere risiko ved å implementere sikkerhetstiltak, overføre risiko f.eks. ved å kjøpe cyberforsikring, akseptere risiko ut ifra nivået for risikoaksept, eller unngå risiko ved å stanse forretningsprosessen som medfører risiko.

Organisasjonen skal oppbevare dokumentert informasjon om risikovurderinger og hvordan risikoene er håndtert.

Avsnitt 9: Krav til evaluering

For overvåking, måling, analyse og evaluering av ISMS skal organisasjonen skal bestemme hva som må overvåkes og måles, samt metoder for dette. Metodene som velges bør gi sammenlignbare og reproduserbare resultater for å anses som gyldige.

Organisasjonen skal gjennomføre internrevisjoner med planlagte intervaller for å gi informasjon om hvorvidt ISMS fungerer som planlagt.
Toppledelsen skal gjennomgå organisasjonens ISMS med planlagte intervaller for å sikre kontinuerlig egnethet, tilstrekkelighet og effektivitet.

Ledelsesgjennomgangen skal omfatte bl.a. vurdering av status for aksjonspunkter fra tidligere ledelsesgjennomganger, endringer i eksterne og interne forhold som er relevante for informasjonssikkerhet, trussel- og risikovurderinger, og hvordan risiko er håndtert.

Resultatene av ledelsesgjennomgangen skal omfatte beslutninger knyttet til kontinuerlige forbedringsmuligheter og eventuelle behov for endringer i ISMS. Ledelsesgjennomgangen skal dokumenteres.

Avsnitt 10: Krav til kontinuerlig forbedring.

Organisasjonen skal kontinuerlig forbedre egnetheten, tilstrekkeligheten og effektiviteten til ISMS.

Når identifiseres svakheter eller avvik i ISMS skal organisasjonen iverksette tiltak for å korrigere det, håndtere mulige konsekvenser, og vurdere behovet for tiltak for å eliminere årsakene til avvik, slik at det ikke gjentar seg eller oppstår andre steder.

Annex A: Referanser for sikkerhetstiltak

Dette tillegget inneholder en tabell med kortfattet beskrivelse av de 93 sikkerhetstiltakene som er beskrevet i detalj i ISO/IEC 27002.

Sikkerhetstiltakene i denne tabellen skal brukes i sammenheng med kravene i avsnitt 6.1. Ved utførelse av en relevanserklæring (SoA – Statement of Applicability) skal hvert sikkerhetstiltak nevnes, typisk som en tabell med ett tiltak på hver rad. Utarbeidelse av en relevanserklæring gjøres typisk i sammenheng med en revisjon av virksomhetens ISMS.