INTRODUKTION TIL SIKKERHEDSSTANDARDEN ISO 27002

- De nye attributter og overlap til andre sikkerhedskrav

Rådet for Digital Sikkerhed

INDHOLD

1. Introduktion til sikkerhedsstandarden – 27002

Danmark står over for et væsentlig skærpet trusselsbillede, og vi skal derfor kunne håndtere trusler som cyberangreb[1]. Det fremgår af en ny analyse udarbejdet af regeringens sikkerhedspolitiske analysegruppe. Det er derfor vigtigt, at danske virksomheder og myndigheder ruster sig til at imødegå truslen, og her er brug af informationssikkerhedsstandarder et godt værktøj til at få styr på organisationens risikobillede og relevante foranstaltninger, der bør iværksættes. ISO/IEC 27002 er en vejledende standard, som knytter sig til den internationale ledelsesstandard for informationssikkerhed, ISO/IEC 27001, med udgangspunkt i de nye versioner og de implementerede ændringer i disse.

Nærværende papir gennemgår:

1. Kravstandarden - ISO 27001
2. Implementeringsvejledningen - ISO 27002 – herunder nye attributter
3. Overlap til andre sikkerhedskrav og standarder
4. 4 trin til hvordan kommer man i gang

Målgruppen for vejledningen er sikkerhedsansvarlige i små og mellemstore virksomheder.

1.1 Hvorfor er brug af sikkerhedsstandarder en god ide?

De sidste år er der kommet flere EU-reguleringer vedr. informationssikkerhed, som sætter krav til øverste ledelse. Denne udvikling forventes at fortsætte, grundet kommende reguleringer.

Der er derfor en række gode grunde til at bruge standarder, når man skal have styr på organisationens informationssikkerhed og compliance, til at understøtte de kommende reguleringer. For det første baserer standarderne sig på international årelang erfaring på tværs af sektorer, interesser og kulturer, hvorfor standarder giver et solidt forslag til "den bedste måde at gøre ting på", ofte beskrevet i et fælles sprog og en fælles tilgang, som finder anvendelse på tværs af faglige grupper – f.eks. jurister og teknikere.

For det andet sikrer standarder, at man kommer hele vejen rundt om problemstillingen og ikke står tilbage med noget, der mangler, som man ikke selv har tænkt på.

For det tredje er standarder ofte noget, der er kendt på tværs af lande, organisationer og brancher. Standarder kan derfor være et let genkendeligt signal til omverdenen om, at man arbejder med sikkerhed ud fra en anerkendt metode baseret på best-practice, og dermed kan der bygges tillid på baggrund af standarder. Brug af standarden vil også gøre det nemmere at finde certificerede personer med viden om standarden. Ligeledes kan brug af en kendt standard muliggøre kortlægning til andre kendte standarder. Endelig er mange standarder indrettet således, at man let kan auditere efter dem og dermed rapportere fremskridt eller udfordringer til ledelsen.

Der er altså mange gode grunde til at bruge standarder i sit arbejde med informationssikkerhed og databeskyttelse. Nogle af de mest gængse standarder er netop blevet opdateret og kan anbefales af Rådet.

2. Kravstandarden - ISO 27001

ISO 27001[1] beskriver et såkaldt ledelsessystem, der sætter rammerne for, hvorledes man styrer og organiserer arbejdet med informationssikkerhed, på samme måde som ISO 9000 sætter rammerne for god kvalitetsledelse. ISO27001 standarden er en kravstandard indeholdende følgende hovedområder[2]:

- Etablering af forståelse for organisationen og dens kontekst
- Etablering af ledelsessystem og forventninger til ledelsen
- Roller og ansvar
- Risikostyring
- Planlægning, ressourcestyring og uddannelse
- Drift af ledelsessystemet
- Løbende evaluering og forbedring

Idet ISO 27001 er en kravstandard, vil en organisation kunne blive certificeret i henhold til overholdelse af standarden ved, at en uvildig part auditerer implementeringen af ledelsessystemet. Derved opnår organisationen en blåstempling af implementeringen af ledelsessystemet, som vil kunne bruges til at dokumentere et struktureret arbejde med informationssikkerhed og databeskyttelse[3].

Anneks A i ISO 27001 oplister en række forskellige foranstaltninger, som alle på forskellig vis vil kunne fastholde eller mitigere det risikobillede, som er blevet afdækket i den risikovurdering og efterfølgende risikostyring, som er etableret i forbindelse med etablering af selve ledelsessystemet.

Annekset over foranstaltninger er udarbejdet af forskellige eksperter, og udgør best-practices for, hvordan en organisation kan imødekomme informationssikkerhedsmæssige risici ud fra forskellige perspektiver og fokusområder.

Annekset understøtter selve ledelsessystemet, men vil også kunne stå alene og, som tidligere nævnt, bruges som:

- Checkliste i forhold til hvad der giver en god baseline informationssikkerhed
- Referenceramme på tværs af brancher og organisationer, der kan skabe tillid i forhold til informationssikkerhedsniveauet
- Fælles sprog på tværs af afdelinger og fagområder

[1] https://sikkerdigital.dk/myndighed/iso-27001-implementering
[2] ISO27000 serien undergår i løbet af 2022 og første halvår af 2023, en væsentlig opdatering, og den nyeste version "2022", findes pt. kun på engelsk. Overskrifterne herunder er fra 2017 versionen, men forventes at kunne genfindes i 2022 versionen, når den foreligger på dansk i starten af 2023.
[3] I forbindelse med modtagelse og vurdering af certificeringer, skal man som modtager altid forholde sig kritisk til det certificerede Scope, og dermed vurdere hvor meget værdi man i praksis vil kunne tillægge certificeringen.

3. Implementeringsvejledningen - ISO 27002

Anneks A i ISO 27001 indeholder som nævnt en liste af best-practices, der beskriver ***Hvad*** organisationen kan gøre, for at imødekomme forskellige risici, men annekset beskriver ikke ***Hvordan*** en given foranstaltning er tænkt eller kan implementeres i praksis.

ISO 27002 er ikke en kravstandard, og man kan derfor ikke certificeres efter denne, men den underbygger Anneks A i ISO 27001 ved at komme med en *implementeringsvejledning* til, hvordan en given foranstaltning med fordel vil kunne implementeres, herunder yderligere detaljer omkring hvad man bør overveje i forbindelse med implementeringen. Den følger i struktur Anneks A fra ISO 27001.

Historisk set har Anneks A og dermed også ISO 27002 haft en opdeling, der har været emneopdelt og fokuseret på f.eks. *Politikker, Roller- og ansvar, Aktivstyring, Adgangsstyring, IT-drift, Leverandørstyring, Beredskabsstyring, Compliance etc.* ISO 27002:2017 bestod derfor tidligere af en beskrivelse på 114 forskellige foranstaltninger fordelt på 14 forskellige kapitler.

I forbindelse med den nye ISO 27002, hvor den engelske version udkom februar 2022 (noteret ISO 27002:2022), har man valgt at gå bort fra emneopdelingen og overgå til en temabaseret opdeling med følgende temaer:

- Organisatorisk
- Menneskeligt/adfærdsmæssigt
- Fysisk
- Teknisk

Foranstaltningerne er i denne forbindelse reduceret fra 114 kontrol-foranstaltninger til 93. Det skyldes, at man har fokuseret på at anskue foranstaltningerne i deres livscyklus og slå en række af de foranstaltninger sammen, som var en del af samme livscyklus. Et eksempel på dette er, at de tidligere foranstaltninger i *5.1.1* og *5.1.2*, som fokuserede på dels udarbejdelse og offentliggørelse af sikkerhedspolitikker (*5.1.1)* og dels periodisk review *(5.1.2),* fremover er at finde i foranstaltningen under 5.1, der dækker hele livscyklussen for sikkerhedspolitikker.

I forbindelse med sammenlægningerne er indholdet også blevet opdateret, så dette er blevet mere tidssvarende. F.eks. har der tidligere været fokus på ”bærbare” enheder som værende noget helt særligt. Disse er nu i højere grad blevet indarbejdet i alle sikringstiltag, som den naturlige del mobile enheder er i en moderne organisation.

Endelig er der også tilføjet en række nye sikringstiltag, som enten ikke har været til stede i 2017 udgaven, eller som har været ”gemt”/indarbejdet i nogle mere generelle sikringstiltag.

Eksempler på dette er:

- ***5.7 Threat intelligence***

  Et mere fokuseret og konkretiseret sikringstiltag på løbende at indhente oplysninger omkring det aktuelle trusselsbillede, som en organisation står over for og sikre, at dette håndteres og indarbejdes i den generelle risikostyring og understøttende processer. Dette synes implementeret grundet det stigende fokus, der er på korrekt risikoidentifikation og håndtering, som alle organisationer står overfor. Det ligger også godt i tråd med de forøgede krav, der ses fra lovgivers side, f.eks. i forbindelse med NIS2 og DORA.

- ***5.23 Information security for use of cloud services***

  Som forventet indeholder den nye standard forøget fokus på en opblødning af det klassiske perimeterforsvar. Et eksempel på dette er det forøgede fokus i forhold til Cloud Services, som har fået sit eget sikringstiltag, der fokuserer på håndtering af de forskellige sikringsaspekter, der er i forbindelse med anvendelse af Cloud Services - herunder governance, risikostyring, hændelseshåndtering og kontrol.

- **7.4 *Physical security monitoring***

  Fokuserer på at overvåge og alarmere, såfremt der sker uautoriseret fysisk adgang.

- ***8.10 → 8.12 Information deletion, data masking og leakage prevention***

  Der er generelt kommet et større og mere konkretiseret fokus på data og datas livscyklus. Dette skyldes nok dels både det forøgede fokus, som der har været på personhenførbare informationer over de seneste år (GDPR), men også ud fra et generelt perspektiv om beskyttelse af virksomheders data, som for mange organisationer er deres eksistensgrundlag i højere grad end tidligere.

For alle sikringstiltagene generelt, synes ISO 27002:2022 at være langt mere detaljeret og yder langt større støtte i forbindelse med selve implementeringsarbejdet.

3.1 Tematisering

Med en tematisering på kun 4 områder og 93 sikringstiltag i alt, så indeholder de to største temaer hhv. 34 og 37 sikringstiltag. For blandt andet at kunne strukturere disse yderligere, så introducerer den nye ISO 27002 såkaldte attributter.

Attributterne er "tags"/"områder", som for hvert sikringstiltag beskriver en eller flere egenskaber, som kan bruges til at anskue både det enkelte sikringstiltag, men også alle sikringstiltag indenfor et specifikt område.

De nye attributter er:

1. **Type af foranstaltning**
   Forebyggende, Opdagende, Korrigerende
2. **Egenskaber for informationssikkerhed**
   Fortrolighed, Integritet, Tilgængelighed
3. **Cybersikkerhedskoncept (fra NIST-rammeværkerne)**
   Identify, Protect, Detect, Respond, Recover
4. **Operationelle ressourcer**
   Denne attribut indeholder mange under-attributter, og beskriver det operationelle område, som sikringstiltaget normalt ville blive varetaget af, og minder mest om strukturen fra ISO27002:2017
5. **Sikkerhedsdomæne (fra ENISAs rammeværker)**
   Governance and Ecosystem, Protection, Defense, Resilience

Attributterne kan anvendes til at besvare spørgsmål som:

- *Hvordan er min fordeling af implementerede sikringstiltag i forhold til at være forebyggende, opdagende eller korrigerende?*
- *Hvordan relaterer mine implementerede sikringstiltag sig i forhold til forslag fra f.eks. NIST.?*
- *Hvorledes passer organisationens sikkerhedsdomæner til ENISAs vejledning og guidelines?*

Ydermere åbner standarden op for, at man kan tilføje egne attributter og dermed filtrere og vurdere tiltagene, f.eks. ud fra forretningsområder, trusler, selskabskonstruktioner, kritiske leverancer ol.

4. Overlap til andre standarder

Som det ses af ovenstående attributkatalog, så åbner den nye ISO 27002 i højere grad op for direkte at kortlægge og relatere til andre standardiserede rammer, som f.eks. NISTs, NIS2, DORA samt ENISAs rammeværk. Blandt andet introduceres koncepter som trusselsinformation og øget monitorering som nye kontroldomæner i linje med krav i ny EU-regulering. Dette sker nok af forskellige årsager, men understøtter den generelle trend med, at informationssikkerhedsområdet bliver mere og mere vitalt for virksomheder og samfundet som helhed, og der derfor løbende skabes mere og mere lovgivningsmæssig regulering og standardisering for at sikre et så højt informationssikkerhedsniveau som muligt.

Hvilken standard man skal/bør vælge at evt. at læne sig op ad, afhænger i meget høj grad af ens fokusområde. Det ses dog i højere og højere grad, at organisationer ikke alene fokuserer på en enkelt standard, men tænker i *Multidimensional Compliance,* og indarbejder alle de nødvendige eksterne rammer i et fælles compliance model/overblik. Den nye ISO 27002 er komplementeret af standarden ISO 27014, som dækker governance og øverste ledelse. ISO-serierne repræsenterer således et komplet sæt af standarder, som kan dække flere reguleringskrav.

Uagtet om en organisation går efter en certificering (og dermed også fokuserer på ISO27001), eller blot ønsker at efterleve en række best-practices, så vil ISO 27002 i mange organisationer fungere som en rigtig god ”rygrad” for implementering af et godt niveau af informationssikkerhed, hvis struktur og niveau kan genkendes på tværs af lande (især europæiske), brancher og organisationer (f.eks. leverandører og kunder). Dette understøttes også af, at fra de danske myndigheders side er krav om, at statslige myndigheder følger denne standard.

Ved at vælge ISO27002 som ”rygrad”, og dermed det holistiske perspektiv som denne har omkring ledelse af informationssikkerhed, vil det fremadrettet blive nemmere at udbygge med yderligere rammeværk (NIST, CIS18, ENISA vejledning og andre mere målrettede ISO-standarder). Desuden vil det blive nemmere at efterleve nuværende og fremadrettet lovgivning/regulering, der har informationssikkerhed som en fundamental parameter. Eksisterende såvel som kommende lovgivningskrav, såsom, GDPR, NIS, NIS2, DORA, CRA, NSIS, e-Privacy o.a., vil kunne understøttes - enten helt eller delvist - af ISO 27002 .

5. Konvertering – hvordan kommer man i gang

Alt efter organisationens egne behov og evt. omverdenens forventninger, er der som udgangspunkt god tid til at overveje en transition fra den gamle til den nye ISO 27002 standard. En stor del af alle sikringstiltagene er med stor sandsynlighed allerede implementeret i ens organisation, men skal evt. "restruktureres" til at følge den nye standard. De nye tiltag følger desuden i meget høj grad best-practices, og dermed er der også her en sandsynlighed for, at disse er implementeret i organisationen - måske dog uden at være en del af organisationens politik eller øvrige beskrevne informationssikkerhed.

For dels at skabe overblik over de nye sikringstiltag og dels give et overblik over ændringerne fra 2017 -> 2022 versionen, så indeholder ISO27002:2022 Anneks B oversigter over, hvor sikringstiltagene fra ISO27002:2017 er placeret i ISO27002:2022, og hvad de enkelte afsnit i ISO27002:2022 indeholder fra den gamle standard.

Hvis man er certificeret, så vil man kunne vedligeholde ens certificering i 3 år på den gamle, men her vil det være en god idé at tage en dialog med ens certificeringspartner og få skabt en god og solid tidsplan for en transition.

For organisationer, der bruger ISO27002:2017 som inspiration, er der som udgangspunkt ingen fast bagkant i forhold til at skifte. Men eftersom både brancher, eventuelle kunder og leverandører vil skifte, så vil organisationen løbende blive presset til at skifte version, og begynde i højere grad at implementere den nye ISO27002. Og efterhånden som lovgiver også implementerer lovgivning, der i højere grad relaterer til sikringstiltagene i den nye ISO 27002, vil presset også forøges.

For statslige myndigheder, der skal efterleve ISO27001 og 2, må det forventes, at der fra myndighedernes side vil komme en deadline for, hvornår myndighederne skal følge den nye, og det må også forventes, at der vil blive udarbejdet nogle nye/opdaterede hjælpeværktøjer (skabeloner, eksempler etc.), der vil kunne hjælpe transitionen.

Fælles for dem alle er dog, at man allerede nu godt kan begynde at forberede sig på transitionen igennem følgende 4 skridt:

1. **Skab overblik over ændringerne i den nye ISO27002 som vil påvirke din organisation**
   Brug evt. strukturen fra et SoA[4] dokument til at fastlægge den nuværende implementering, set i forhold til de nye og ændrede krav som den nye ISO27002 introducerer

2. **Fastlæg roller og ansvar**
   Få fastlagt roller og ansvar både for selve planlægningen og styringen af transformationen, men også for hvem der skal implementere og/eller dokumentere nye sikringstiltag

3. **Vurder eksterne afhængigheder**
   Vurder om der er nogle tidsmæssige afhængigheder, f.eks. i forhold til ny lovgivning som organisationen skal følge. F.eks. vil en forestående NIS2 implementering med meget stor sandsynlighed fordre, at organisationen samtidigt skifter til den nye IS27002 for at være sikker på at ramme det ønskede informationssikkerhedsniveau i forhold til implementering af kravene i NIS2.

4. **Tænk forankring**
   Som nævnt introducerer den nye ISO 27002 en række nye foranstaltninger. Hvor disse skal implementeres fra bunden, så husk at involvere teknikere, procesejer, afdelingsledere ol., for at sikre, at sikringstiltagene bliver implementeret og forankret bedst muligt i organisationen. Til trods for at ISO27002 angiver en række best-practices, så er det essentielt, at disse oversættes til den lokale kontekst og implementeres på en måde, som organisationen kan arbejde med i det daglige og dermed giver værdi, så det ikke kun bliver en compliance-øvelse på et stykke papir.

[4] Statement of applicability (SoA) eller efterlevelsesdokument er en struktureret model, der pr. krav i ISO standarden beskriver, hvad der er implementeret af sikringstiltag og evt. hvor modne disse er. Hvis man allerede følger ISO 27001 i dag, vil det gamle SoA dokument skulle opdateres til den nye struktur.

Dokumentet er blevet til i samarbejde med:

- Tue Jagtfelt, Director, RA, Cyber Strategy, Deloitte
- Jesper B. Hansen, Chief Technical Officer, Siscon

Rådet for Digital Sikkerhed arbejder for at fremme et trygt og frit digitalt samfund for alle. Et samfund med god balance mellem effektiv brug af moderne teknologi, beskyttelse mod digitale trusler og den enkeltes ret til privatliv.

Danmark skal være et af de mest trygge digitale samfund i verden med konstant fokus på datas fortrolighed, tilgængelighed, integritet og høj grad af dataansvarlighed.

LÆS MERE OM OS PÅ DIGITALSIKKERHED.DK