DIGITALISERINGSSTYRELSEN

Guide til SoA-dokumentet – Statement of Applicability

Marts 2013

Indhold

1. Introduktion til SoA

I arbejdet med ISO27001 er SoA-dokumentet centralt og værdifuldt. SoA står for Statement of Applicability, hvilket frit oversat kan forstås som en erklæring af, hvilket sikkerhedsniveau organisationen aktiv har besluttet sig for og hvorfor.

SoA-dokumentet underbygger således, hvorfor en organisation har gjort ét på et område og noget andet på et andet. Alt sammen begrundet i organisationens risikovurdering og risikoprofil. SoA-dokumentet kan ses som en statusopgørelse for organisationens arbejde med informationssikkerhed og som beslutningsdokumentation for dens til- og fravalg af sikkerhedsmæssige indsatser.

Denne vejledning gennemgår de centrale elementer i SoA-dokumentet (begrundelse for til- og fravalg, implementeringsniveau, risikohåndtering) og forklarer, hvordan man kan gå til opgaven med at udfylde dokumentet.

Digitaliseringsstyrelsen har udviklet et regnearksværktøj, der kan lette gennemgangen af de enkelte punkter i SoA-dokumentet. Indholdet i værktøjet bygger på ISO 27002, dvs. det afspejler kontrolområderne i Annex A i den gældende version af ISO 27001. Når man har udfyldt regnearket, bliver der genereret en rapport, som kan udgøre selve SoA-dokumentet. Værktøj og vejledning kan downloades fra Digitaliseringsstyrelsens hjemmeside.

2. Indhold og krav til SoA

SoA-dokumentet er et krav i sikkerhedsstandarden og er desuden angivet som en af forudsætningerne for at kunne implementere et fungerende ledelsessystem for informationssikkerhed (ISMS).

I standarden anbefales det, at organisationen som minimum forholder sig til sikringsforanstaltningerne i standardens anneks A, når den udarbejder SoA-dokumentet.

Annex A er inddelt i de områder, der fremgår af figuren nedenfor.

Områder i ISO27001, Anneks A, som SoA-dokumentet skal forholde sig til

ISO 27001 Anneks A
Styringsmål og foranstaltninger
Statement of Applicability (SoA)

Informationssikkerhedspolit k
Organisering af informationssikkerhed
Styring af aktiver
Medarbejders kkerhed
Fysisk og mi jømæssig s kkerhed
Styring af kommunikation og drift
Adgangsstyring
Anskaffelse, udvikling og vedligeholdelse af informationssystemer
Styring af informationss kkerhedshændelser
Beredskabsstyring
Overensstemmelse/compliance

Annex A er tænkt som en inspirationsliste med eksempler på sikringsforanstaltninger og kontroller. Hvis det giver mening, kan den enkelte organisation tilføje andre relevante sikringsforanstaltninger og kontroller.

I SoA-dokumentet skal det anføres og begrundes, om sikringsforanstaltninger på et givent område er relevante for organisationen eller ej, og hvor langt organisationen er i implementeringen af sikkerhedsstyringen. SoA-dokumentet giver således både et overblik over arbejdet med informationssikkerhed og input til den fortsatte proces.

SoA-dokumentet er et nøgledokument i arbejdet med informationssikkerhed og indgår allerede i planlægningsfasen, hvor alle nødvendige sikkerhedsforanstaltninger til behandling af risici stilles op, uanset om de er implementeret eller ej. SoA-dokumentet bliver således udgangspunkt for

aktiviteterne i de efterfølgende faser. SoA-dokumentet skal opfattes som et dynamisk dokument, som løbende opdateres, så det viser status på det aktuelle arbejde med styring af informationssikkerheden. Opdateringen bør ske enten årligt, eller når der er registreret ændringer i risikobilledet eller i organisationens ønskede sikkerhedsniveau.

Udarbejdelsen af SoA-dokumentet giver endvidere et overblik over den aktuelle modenhed i organisationens styring af informationssikkerhed.

Organisationen kan bruge SoA-dokumentet til at:

- Gennemføre en Gap-analyse i forhold til Best Practice
- Gennemføre en Gap-analyse i forhold til organisationens besluttede sikkerhedsniveau
- Tage beslutninger om fremtidige sikkerhedsmæssige initiativer
- Fravælge sikringsforanstaltninger på et kvalificeret grundlag
- Hjælpe med at effektivisere revisionsgennemgange.

SoA-dokumentet skal udarbejdes med udgangspunkt i en it-risikovurdering. Man vælger sikringsforanstaltninger med afsæt i den seneste risikovurdering og de identificerede og vurderede risici. Hertil kommer lovkrav, aftalemæssige forpligtelser i forhold til eksterne interessenter (borgere og samarbejdspartnere), ledelsesmæssige ønsker eller best practice. På tilsvarende måde fravælger man foranstaltninger, hvis de ikke er relevante eller aktuelle.

I praksis bør der være sammenhæng mellem valget af sikringsforanstaltninger og de indsatsområder og målsætninger, der er beskrevet i informationssikkerhedspolitikken. SoA- dokumentet vil ideelt kunne ses som en læsevejledning og guide til organisationens ledelsessystem.

Der er ingen specifikke formkrav til selve udfyldelsen af dokumentet. Kun krav om, at det skal indeholde alle nødvendige sikringsforanstaltninger til at kunne håndtere risici. Det er derfor op til den enkelte organisation, om gennemgangen skal rapporteres i notatform, skemaform eller noget helt tredje.

Til- og fravalget af sikringsforanstaltninger og kontroller vil kunne være forskelligt fra system til system eller fra løsning til løsning. Det afhænger naturligvis af kritikaliteten af data og den konkrete risikoprofil.

3. Roller og proces

Når SoA-dokumentet skal skrives, er det vigtigt at holde styr på processens roller. Rollerne er *ikke* sammenfaldende med roller og ansvar i forhold til sikringsforanstaltningerne.

3.1 Dokumentejer og beslutningstager

Sikkerhedskoordinatoren har som regel det største overblik over de eksisterende sikkerhedsmæssige forhold og er naturligt også den person, der har ejerskabet til SoA-dokumentet. Alternativt kan opgaven uddelegeres til en person med tilsvarende indsigt.

Dokumentejeren har ansvaret for, at SoA-dokumentet bliver skrevet, og at de enkelte vurderinger foretages og opdateres periodisk.

3.2 Inputgivere

Ofte vil it-chefen, sikkerhedskoordinatoren og/eller medarbejdere fra it-afdelingen være i stand til at bidrage med de fleste oplysninger som inputgivere til dokumentet. Men også repræsentanter fra HR, systemejere, dataejere, leverandører mv. kan være relevante at få input fra til de områder af SoA-dokumentet, der direkte berører deres arbejdsområder.

3.3 Godkender

Når selve dokumentet er skrevet, skal det godkendes af organisationens øverste ledelse eller informationssikkerhedsudvalg. Særlig opmærksomhed rettes mod de beslutninger, der er taget i forhold til de enkelte sikringsforanstaltninger. Om kommunikationsformen se nedenfor.

Processen med at udfylde SoA-dokumentet kan med fordel faciliteres af en ekstern part som fx en it-sikkerhedskoordinator fra en anden organisation eller en anden person end dokumentejeren.

En ekstern facilitator vil kunne forbedre både spørgsmål og dokumenterede begrundelsers kvalitet. Facilitatoren vil ikke være påvirket af forudindtagede holdninger eller indforståede forhold, som kan hindre vigtige pointer eller sikringsforanstaltninger i at blive taget med. Det er vigtigt, at facilitatoren er dedikeret til opgaven og sætter tid af til at forberede og gennemføre den.

Input til dokumentet kan fx ske via individuelle eller fælles møder, interviews, workshops mv., alt efter den aktuelle organisations kultur og temperament.

4. Valg af sikringsforanstaltninger

De enkelte sikringsforanstaltninger og kontroller kan tilvælges med en af følgende begrundelser:

- Kontrolområdet skal være implementeret af hensyn til overholdelse af lovmæssige forpligtelser (forkortes LOV i bilag 1 - SoA-skema)
- Kontrolområdet skal være implementeret af hensyn til overholdelse af aftalemæssige forpligtelser (forkortes AFT i bilag 1 - SoA-skema)
- Kontrolområdet skal være implementeret for at overholde Best Practice i henhold til ledelsens beslutning (forkortes BP i bilag 1 - SoA-skema)
- Kontrolområdet skal være implementeret for at mitigere risici, der er afdækket i seneste risikoanalyse (forkortes RV i bilag 1 - SoA-skema)

Der kan selvfølgelig være andre begrundelser, fx strategiske eller politiske tiltag, der tilsiger, at sikkerheden styrkes på bestemte områder. Disse begrundelser skal tilføjes i bemærkningsfeltet.

Husk at Annex A ikke er udtømmende; der kan være andre sikringsforanstaltninger og kontroller, som er relevante at få med i SoA-dokumentet.

4.1 Tilvalgte sikringsforanstaltninger

De valgte sikringsforanstaltninger kan være implementeret på tre forskellige niveauer, hvilket ofte er et udtryk for organisationens modenhed eller ressourceanvendelsen på området i lyset af det aktuelle risikobillede.

De tre implementeringsniveauer er:

- Foranstaltningen er beskrevet
  Hvis sikringsforanstaltningen er beskrevet, har organisationen aktivt taget stilling til designet i den pågældende foranstaltning. Foranstaltningen er dokumenteret i form af skriftlige politikker, retningslinjer eller procedurer.

- Foranstaltningen er kontrolleret
  Hvis sikringsforanstaltningen er kontrolleret, er det kontrolleret/testet minimum én gang, at den beskrevne politik/ retningslinje/procedure udføres i praksis - og er relevant for at opfylde kontrolmålet.

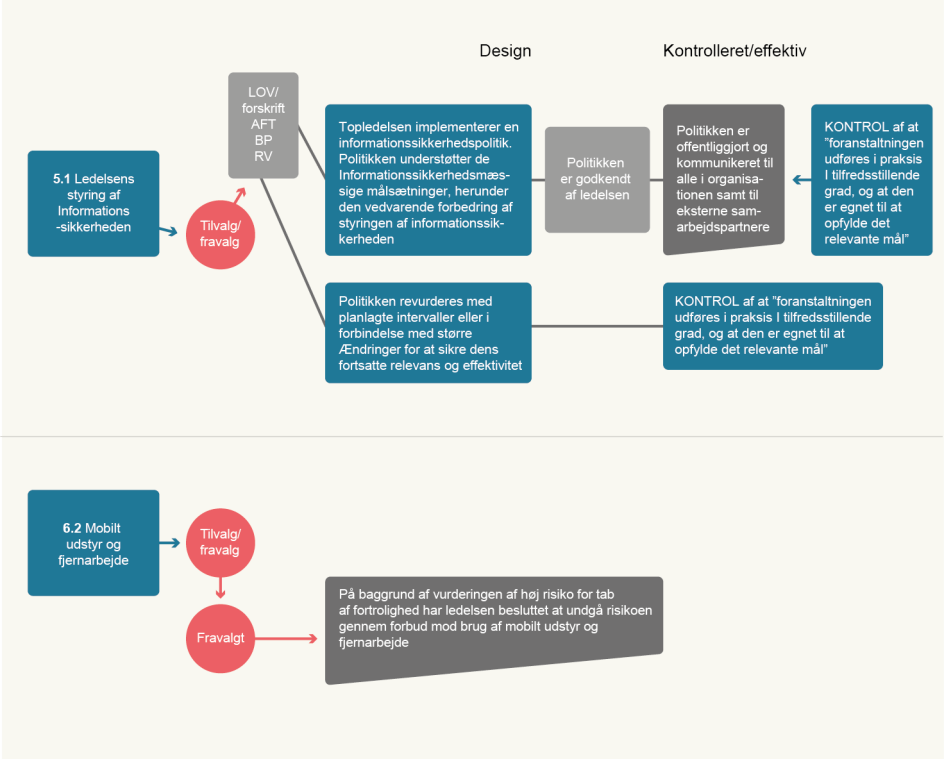
- Foranstaltningen er effektiv
  Hvis foranstaltningen er effektiv, er det regelmæssigt testet/kontrolleret, at

foranstaltningen udføres i praksis i tilfredsstillende grad, og at den er egnet til at opfylde det relevante mål. Resultatet af kontrollen rapporteres til ledelsen.

Hvis implementeringsgraden af foranstaltningerne ikke vurderes som tilstrækkelig, skal initiativer til at opnå et acceptabelt sikkerhedsniveau på det givne område noteres i bemærkningsfeltet for foranstaltningen.

Nedenfor vises en grafisk oversigt over beslutninger for et kontrolområde. Oversigten kan bruges i kommunikationen med de relevante personer i organisationen.

Kontrolområder og kontroller - informationssikkerhedspolitik



4.2 Fravalgte sikringsforanstaltninger

Organisationen kan vælge ikke at bruge en sikringsforanstaltning ud fra den begrundelse, at den ikke er relevant, eller at risikoen accepteres, modificeres, undgås eller overføres til en tredje part. Et fravalg skal begrundes i SoA-dokumentet, så sikkerhedsudvalget og ledelsen kan kommentere, modsætte sig eller godkende de enkelte fravalg. SoA-dokumentet bør i givet fald indeholde en angivelse af, hvordan risikoen – som følge af fravalget - ønskes håndteret.

Nogle af sikringsforanstaltningerne er rettet mod nært beslægtede risici, og der kan derfor være tilfælde, hvor organisationen vælger et forholdsvist lavt implementeringsniveau på et område. Det kan fx begrundes i en vurdering af, at risi-

koen er tilstrækkeligt kontrolleret med allerede implementerede sikringsforanstaltninger.

Foranstaltningen om *automatisk lukning af programmer* (punkt A.11.5.5 i SoA-dokumentet) kan fx fravælges med den begrundelse, at der er implementeret kompenserende foranstaltninger, såsom skærmlås og/eller der bruges lukkede netværk, som vurderes at minimere risikoen tilstrækkeligt.

Nogle sikringsforanstaltninger er muligvis slet ikke relevante for de aktiviteter, som organisationen beskæftiger sig med. Hvis den pågældende myndighed fx ikke driver *online handels- virksomhed*, vil det ikke være relevant at implementere standardens foranstaltninger vedr. e- handelssystemer og deres anvendelse. (punkt A.10.9 i SoA-dokumentet).

digst.dk