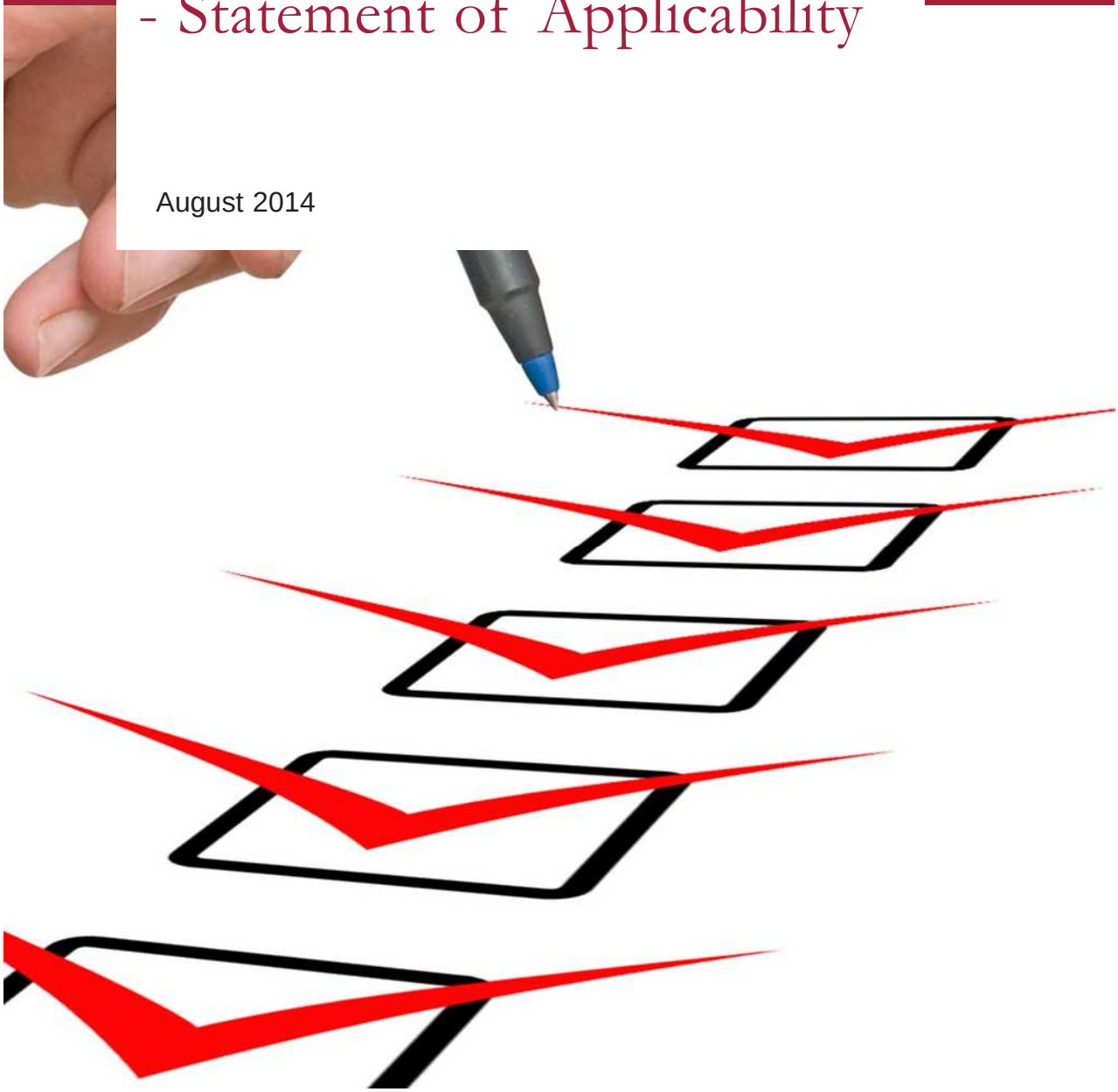
DIGITALISERINGSSTYRELSEN

Guide til SoA-dokumentet - Statement of Applicability

August 2014



Guide til SoA-dokumentet - Statement of Applicability

Udgivet august 2014

Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen
kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox

Elektronisk publikation
ISBN 978-87-93073-08-1

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. 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 og forklarer, hvordan man kan gå til opgaven med at udfylde dokumentet.

Digitaliseringsstyrelsen har udviklet et regnearksværktøj, der kan lette gennemgangen af kontrollerne i Anneks A, der er en del af ISO27001. Kontrollerne i Anneks A er afledt direkte fra kontrollerne i ISO27002, der skal anvendes som reference og vejledning ved fravalg og tilvalg af kontroller.

Når man har udfyldt regnearket (SoA-skemaet), kan dette udgøre selve SoA-dokumentet.

2. Indhold og krav til SoA

SoA-dokumentet er et krav i ISO27001 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.

Kontrollerne i Anneks A er baseret på indholdet i ISO27002, der i alt indeholder 14 punkter om sikkerhedskontroller, der tilsammen omfatter 35 sikkerhedskategorier og 114 kontroller.

I ISO27002 indledes hver kontrol med en beskrivelse af et kontrolmål (formål), der angiver, hvad der skal opnås ved kontrollen. Der gives ligeledes en implementeringsvejledning samt anden relevant info, som vedrører den givne kontrol. Standarden kan dermed bruges både som reference i arbejdet med SoA-skemaet, og i det videre arbejde med implementering af kontrollerne.

3. Valg af kontroller

SoA-dokumentet skal udarbejdes med udgangspunkt i en it-risikovurdering. Man vælger kontroller med afsæt i den seneste risikovurdering og de identificerede og vurderede risici. SoA-dokumentet bliver således udgangspunkt for aktiviteterne i de efterfølgende faser.

Det er vigtigt, at en organisation identificerer sine sikkerhedskrav. Der er tre hovedkilder til sikkerhedskrav, som kan give anledning til at etablere kontroller:

a) Vurdering af risici i organisationen, idet der tages højde for organisationens overordnede forretningsstrategi og målsætninger (markeres med RV i SoA-skemaet).

b) Lov-, myndigheds- og kontraktkrav, som en organisation, dens handelspartnere, leverandører og serviceudbydere skal opfylde (markeres med LOV i SoA-skemaet).

c) Best Practice - Sæt af principper, målsætninger og forretningskrav til informationshåndtering, -behandling, -lagring, -kommunikation og -arkivering, som en organisation har udviklet for at understøtte driften (markeres med BP i SoA-skemaet).

Husk, at Anneks A ikke er udtømmende; der kan være andre sikringsforanstaltninger og kontroller, som er relevante at få med i SoA-dokumentet. Valg af kontroller afhænger også af den måde, hvorpå kontrollerne supplerer hinanden og derved samlet udgør et solidt værn til beskyttelse af organisationens informationssikkerhed. Kontroller der er implementeret i organisationen, som ikke fremgår af Anneks A, kan tilføjes i bunden af SoA-skemaet.

Det eneste krav til udfyldelsen af SoA er, at det skal indeholde alle nødvendige kontroller til at håndtere risici.

3.1 Fravalgte sikringsforanstaltninger

Organisationen kan fravælge en kontrol ud fra den begrundelse, at den ikke er relevant, eller at risikoen ved at fravælge den accepteres, undgås eller overføres til en tredje part. Et fravalg skal begrundes i SoA-dokumentet, og godkendes af topledelsen.

4. Proces for udarbejdelse

Når SoA-dokumentet skal udarbejdes, er det vigtigt at holde styr på proces og interessenter.

Dokumentejer
Sikkerhedskoordinatoren har som regel det største overblik over de eksisterende sikkerhedsmæssige forhold, og er naturligt også den person, der har ejerskabet af 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.

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.

Godkender
Når selve dokumentet er skrevet, skal det godkendes af organisationens topledelse. Særlig opmærksomhed rettes mod de valg, der er taget i forhold til de enkelte kontroller.

5. Status på kontroller

I ISO27001 specificeres kravene til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for informationssikkerhed (ISMS).

Kontrollernes effektivitet til at håndtere informationsrisici sikres ved at de gennemgår et tilsvarende forløb. Med dette udgangspunkt angives status af hver kontrol i SoA-skemaet som:

- Planlægning
- Drift
- Evaluering og forbedring

Status af kontrollerne kan altså afspejle modenhed på sikkerhedsområdet i organisationen eller ressourceanvendelsen på et område i lyset af det aktuelle risikobillede.

1. Planlægning (markeres med PL i SoA-skemaet)
Dette vil være status på helt nye kontroller.

For kontroller med planlægningsstatus fastlægges og dokumenteres i en handlingsplan:

1. Hvad der skal gøres
2. Hvilke ressourcer der skal bruges
3. Hvem der skal være ansvarlige
4. Hvornår det vil blive færdiggjort
5. Hvordan resultaterne skal evalueres

Hertil bør det overvejes, om der vil være behov for at rapportere et øget risikoniveau til topledelsen indtil kontrollerne er i drift.

2. Drift (markeres med DR i SoA-skemaet)
I denne fase gennemføres de handlinger som er fastlagt i planlægningsfasen indtil kontrollen er implementeret og kan siges at have status af at være i drift. Kontrollen er ligeledes dokumenteret med relevante politikker, retningslinjer og procedurer som understøtter, eller er en del af kontrollen.

3. Evaluering og forbedring (markeres med EV i SoA-skemaet)
Når kontrollen kan siges af have status af drift, påbegynder evalueringsfasen. Til brug i denne fase fastlægges hvordan resultaterne skal evalueres:

1. Hvad der skal overvåges og måles
2. Hvilke metoder der skal anvendes til overvågning, måling, analyse og evaluering, for at sikre valide (sammenlignelige og reproducerbare) resultater
3. Hvornår overvågningen og målingen skal udføres
4. Hvem der skal overvåge og måle
5. Hvornår resultaterne fra overvågningen og målingen skal analyseres
6. Hvem der skal analysere og evaluere disse resultater

Organisationen skal opbevare dokumenteret information som bevis for resultaterne af overvågningen og målingen.

6. Om SoA-skemaet

Digitaliseringsstyrelsen har udarbejdet et SoA-skema i et regnearks, der kan downloades fra styrelsens hjemmeside, www.digst.dk. Regnearket indeholder alle kontrollerne fra ISO27001:2013, og skemaet vil i udfyldt stand kunne udgøre organisationens SoA-dokument.

Opbygning og navigering
Simpelt regneark udviklet i Excel 2010, som derfor nemt kan tilpasses organisationens behov.

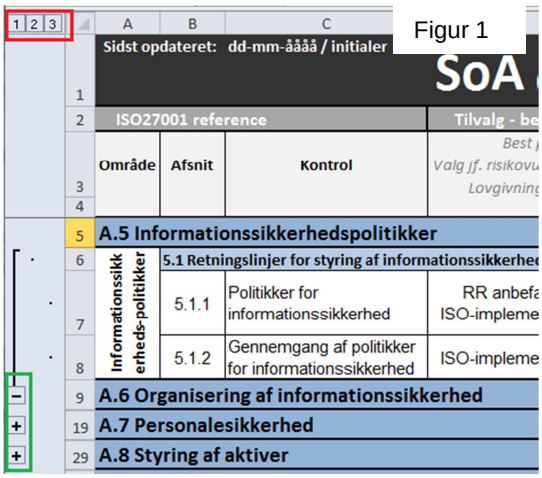
Indholdet er opdelt i tre niveauer:

1. Et overordnet *kontrolområde* fra Anneks A i ISO 27001 – fx **A.5**
2. *Afsnit* inden for kontrolområdet – fx **A.5.1**
3. De enkelte *kontroller* inden for afsnittet – fx **A.5.1.1**

Visning af de tre niveauer (Figur 1)
De tre niveauer vises ved at trykke på tallene (hhv. 1,2 og 3) i arkets øverste venstre hjørne (markeret med rødt). Vil man fx se alle 114 kontroller, skal man trykke på 3.

Man kan også folde det enkelte kontrolområde eller afsnit ud og ind, ved at trykke på hhv. +/- tegn i arkets yderste venstre del (markeret med grønt). På figur 1 er der trykket på + ud for **A.5**.

Figur 1



Sortering af indhold (Figur 2).
Ved at trykke på den lille pil (markeret med rødt), kan man sortere i indholdet.

Ved at trykke på den markerede pil i figur 2, får man fx mulighed for at vælge hvilke sikkerhedskrav man ønsker at se.

Der kan sorteres i indholdet ved at trykke på tilsvarende pile i kolonne E-H.

Figur 2