Rådet for
Den Europæiske Union

Bruxelles, den 18. juli 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	14. juli 2022
til:	Generalsekretariatet for Rådet
Komm. dok. nr.:	C(2022) 4882 final - ANNEX
Vedr.:	BILAG til KOMMISSIONENS DELEGEREDE FORORDNING om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2018/1139 for så vidt angår krav til styring af informationssikkerhedsrisici med potentiel indvirkning på luftfartssikkerheden gældende for de organisationer, der er omfattet af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014, og om ændring af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014

Hermed følger til delegationerne dokument C(2022) 4882 final - ANNEX.

Bilag: C(2022) 4882 final - ANNEX

EUROPA-
KOMMISSIONEN

Bruxelles, den 14.7.2022
C(2022) 4882 final

ANNEX

BILAG

til

KOMMISSIONENS DELEGEREDE FORORDNING

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2018/1139 for så vidt angår krav til styring af informationssikkerhedsrisici med potentiel indvirkning på luftfartssikkerheden gældende for de organisationer, der er omfattet af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014, og om ændring af Kommissionens forordning (EU) nr. 748/2012 og (EU) nr. 139/2014

BILAG

INFORMATIONSSIKKERHED — ORGANISATIONSKRAV

[DEL-IS.D.OR]

IS.D.OR.100 Anvendelsesområde

I denne del fastsættes de krav, som de organisationer, der er omhandlet i artikel 2 i denne forordning, skal opfylde.

IS.D.OR.200 System til styring af informationssikkerhed (ISMS)

a) For at nå de mål, der er fastsat i artikel 1, skal organisationen oprette, gennemføre og opretholde et system til styring af informationssikkerhed (ISMS), som sikrer, at organisationen:

   1) fastlægger en politik for informationssikkerhed og fastlægger organisationens overordnede principper med hensyn til informationssikkerhedsrisicis potentielle indvirkning på luftfartssikkerheden

   2) indkredser og gennemgår informationssikkerhedsrisici i overensstemmelse med

punkt IS.D.OR.205

3) udarbejder og gennemfører foranstaltninger til håndtering af informationssikkerhedsrisici i overensstemmelse med punkt IS.D.OR.210

4) indfører en intern indberetningsordning for informationssikkerhed i overensstemmelse med punkt IS.D.OR.215

5) udarbejder og gennemfører, i overensstemmelse med punkt IS.D.OR.220, de foranstaltninger, der er nødvendige for at opdage informationssikkerhedsbegivenheder, identificerer de begivenheder, der betragtes som hændelser med en potentiel indvirkning på luftfartssikkerheden, bortset fra når det er tilladt i henhold til punkt IS.D.OR.205, litra e), og sørge for reaktion på og genopretning efter disse informationssikkerhedshændelser

6) gennemfører de foranstaltninger, som den kompetente myndighed har givet meddelelse om, som en omgående reaktion på en informationssikkerhedshændelse eller sårbarhed med indvirkning på luftfartssikkerheden

7) træffer passende foranstaltninger i overensstemmelse med punkt IS.D.OR.225 for at følge op på de anmærkninger, som den kompetente myndighed har meddelt

8) indfører en ekstern indberetningsordning i overensstemmelse med punkt IS.D.OR.230 med henblik på at sætte den kompetente myndighed i stand til at træffe passende foranstaltninger

9) opfylder kravene i punkt IS.D.OR.235, når der indgås kontrakter med andre organisationer om en hvilken som helst del af de aktiviteter, der er omhandlet i punkt IS.D.OR.200

10) opfylder personalekravene i punkt IS.D.OR.240

11) opfylder registreringskravene i punkt IS.D.OR.245

12) overvåger organisationens opfyldelse af kravene i denne forordning og giver feedback om resultaterne til den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, til lederen af konstruktionsorganisationen for at sikre effektiv gennemførelse af korrigerende foranstaltninger

13) beskytter, uden at dette berører gældende krav om indberetning af hændelser, fortroligheden af alle oplysninger, som organisationen måtte have modtaget fra andre organisationer, i henhold til deres følsomhedsgrad.

b) For kontinuerligt at opfylde kravene i artikel 1 skal organisationen gennemføre en løbende forbedringsproces i overensstemmelse med punkt IS.D.OR.260.

c) Organisationen skal i overensstemmelse med punkt IS.D.OR.250 dokumentere alle centrale processer, procedurer, roller og ansvarsområder, der er nødvendige for at overholde punkt IS.D.OR.200, litra a), og fastlægge en procedure for ændring af denne

dokumentation. Ændringer af disse processer, procedurer, roller og ansvarsområder skal forvaltes i overensstemmelse med punkt IS.D.OR.255.

d) De processer, procedurer, roller og ansvarsområder, som organisationen har fastlagt med henblik på at overholde punkt IS.D.OR.200, litra a), skal stemme overens med karakteren og kompleksiteten af organisationens aktiviteter på grundlag af en vurdering af de informationssikkerhedsrisici, der er forbundet med disse aktiviteter, og kan integreres i andre eksisterende administrationssystemer, som organisationen allerede har indført.

e) Uden at det berører forpligtelsen til at opfylde indberetningskravene i forordning (EU) nr. 376/2014([1]) og kravene i punkt IS.D.OR.200, litra a), nr. 13), kan organisationen få tilladelse af den kompetente myndighed til ikke at gennemføre de krav, der er omhandlet i litra a) -d), og de relaterede krav i punkt IS.D.OR.205 til IS.D.OR.260, hvis den over for myndigheden godtgør, at dens aktiviteter, faciliteter og ressourcer samt de tjenester, den udøver, yder, modtager og vedligeholder, ikke udgør nogen informationssikkerhedsrisiko med potentiel indvirkning på luftfartssikkerheden, hverken for sig selv eller for andre organisationer. Godkendelsen skal baseres på en dokumenteret vurdering af informationssikkerhedsrisici, der er udført af organisationen eller en tredjepart i overensstemmelse med punkt IS.D.OR.205 og gennemgået og godkendt af dens kompetente myndighed.

Godkendelsens fortsatte gyldighed vil blive gennemgået af den kompetente myndighed efter den gældende cyklus for evaluering af tilsynet, og når der gennemføres ændringer i organisationens arbejdsområde.

IS.D.OR.205 Vurdering af informationssikkerhedsrisici

a) Organisationen skal identificere alle dens elementer, som kan være udsat for informationssikkerhedsrisici. Dette skal omfatte:

1) organisationens aktiviteter, faciliteter og ressourcer samt de tjenester, som organisationen udøver, yder, modtager eller vedligeholder

2) det udstyr og de systemer, de oplysninger og den information, som bidrager til funktionen af de elementer, der er nævnt i punkt 1).

b) Organisationen skal identificere de grænseflader, den har med andre organisationer, og som kan medføre gensidig eksponering for informationssikkerhedsrisici.

c) Med hensyn til de elementer og grænseflader, der er omhandlet i litra a) og b), skal organisationen identificere de informationssikkerhedsrisici, som kan have en potentiel indvirkning på luftfartssikkerheden. For hver identificeret risiko skal organisationen:

([1]) Europa-Parlamentets og Rådets forordning (EU) nr. 376/2014 af 3. april 2014 om indberetning og analyse af samt opfølgning på begivenheder inden for civil luftfart, ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 996/2010 og ophævelse af Europa-Parlamentets og Rådets direktiv 2003/42/EF, Kommissionens forordning (EF) nr. 1321/2007 og Kommissionens forordning (EF) nr. 1330/2007 (EUT L 122 af 24.4.2014, s. 18).

1) tildele et risikoniveau i henhold til en foruddefineret klassifikation fastsat af organisationen

2) knytte hver risiko og dens niveau til det tilsvarende element eller den tilsvarende grænseflade, der er identificeret i overensstemmelse med litra a) og b).

Der skal i forbindelse med den foruddefinerede klassificering, der er omhandlet i punkt 1), tages hensyn til trusselsscenariets potentielle opståen og alvoren af de sikkerhedsmæssige konsekvenser heraf. På grundlag af denne klassificering og under hensyntagen til, hvorvidt organisationen har en struktureret og repeterbar risikostyringsprocedure for operationer, skal organisationen kunne fastslå, hvorvidt risikoen er acceptabel eller skal behandles i overensstemmelse med punkt IS.D.OR.210.

For at lette den gensidige sammenlignelighed af risikovurderinger skal der ved tildelingen af risikoniveauet i henhold til punkt 1) tages hensyn til relevante oplysninger, der er indhentet i samarbejde med de organisationer, der er omhandlet i litra b).

d) Organisationen skal gennemgå og ajourføre den risikovurdering, der udføres i overensstemmelse med litra a), b) og c), i følgende situationer:

1) der er sket en ændring i de elementer, der er genstand for informationssikkerhedsrisici

2) der er sket en ændring i grænsefladerne mellem organisationen og andre organisationer eller i de risici, der meddeles af andre organisationer

3) der er sket en ændring i den information eller viden, der bruges til identifikation, analyse og klassificering af risici

4) der er høstet erfaring fra analysen af informationssikkerhedshændelser.

IS.D.OR.210 Håndtering af informationssikkerhedsrisici

a) Organisationen skal udvikle foranstaltninger til håndtering af de uacceptable risici, der identificeres i overensstemmelse med punkt IS.D.OR.205, gennemføre dem rettidigt og kontrollere deres fortsatte effektivitet. Disse foranstaltninger skal gøre det muligt for organisationen at:

1) udøve kontrol over de omstændigheder, der bidrager til, at trusselsscenariet rent faktisk opstår

2) mindske de konsekvenser for luftfartssikkerheden, der er forbundet med trusselsscenariets opståen

3) undgå risiciene.

Disse foranstaltninger må ikke medføre nye potentielle uacceptable risici for luftfartssikkerheden.

b) Den person, der er omhandlet i punkt IS.D.OR.240, litra a) og b), og andet berørt personale i organisationen skal orienteres om resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.D.OR.205, de tilsvarende trusselsscenarier og de foranstaltninger, der skal gennemføres.

Organisationen skal også underrette organisationer, som den har en grænseflade med, jf. punkt IS.D.OR.205, litra b), om enhver risiko, der deles af begge organisationer.

IS.D.OR.215 Intern indberetningsordning for informationssikkerhed

a) Organisationen skal etablere en intern indberetningsordning for at muliggøre indsamling og evaluering af informationssikkerhedsbegivenheder, herunder begivenheder der skal indberettes i henhold til punkt IS.D.OR.230.

b) Denne ordning og den proces, der er omhandlet i punkt IS.D.OR.220, skal gøre det muligt for organisationen at:

1) identificere, hvilke af de begivenheder der indberettes i henhold til litra a), der anses som informationssikkerhedshændelser eller sårbarheder med en potentiel indvirkning på luftfartssikkerheden

2) afdække årsagerne til og de faktorer, der medvirker til de informationssikkerhedshændelser og sårbarheder, der identificeres i overensstemmelse med punkt 1), og håndtere dem som led i proceduren for styring af informationssikkerhedsrisici i overensstemmelse med punkt IS.D.OR.205 og IS.D.OR.220

3) sikre en evaluering af alle kendte og relevante oplysninger vedrørende de informationssikkerhedshændelser og sårbarheder, der identificeres i overensstemmelse med punkt 1)

4) sikre indførelsen af en metode til intern distribution af oplysningerne, hvis det er nødvendigt.

c) Enhver organisation, med hvilken der er indgået kontrakt, og som kan udsætte organisationen for informationssikkerhedsrisici med potentiel indvirkning på luftfartssikkerheden, skal indberette informationssikkerhedsbegivenheder til organisationen. Disse indberetninger indsendes i henhold til de procedurer, der er fastsat i de specifikke kontraktlige ordninger, og evalueres i overensstemmelse med litra b).

d) Organisationen skal arbejde sammen om undersøgelser med enhver anden organisation, der yder et væsentligt bidrag til informationssikkerheden for sine egne aktiviteter.

e) Organisationen kan integrere denne indberetningsordning med andre indberetningsordninger, som den allerede har indført.

IS.D.OR.220 Informationssikkerhedshændelser — opdagelse, reaktion og genopretning

a) Baseret på resultatet af den risikovurdering, der udføres i overensstemmelse med punkt IS.D.OR.205, og resultatet af den risikohåndtering, der udføres i overensstemmelse med punkt IS.D.OR.210, skal organisationen gennemføre foranstaltninger for at opdage hændelser og sårbarheder, der potentielt kan bevirke, at der opstår uacceptable risici, og som kan have en potentiel indvirkning på luftfartssikkerheden. Disse opdagelsesforanstaltninger skal gøre det muligt for organisationen at:

1) opdage afvigelser fra forudbestemte funktionelle præstationsreferencescenarier

2) udløse advarsler for at aktivere passende reaktionsforanstaltninger i tilfælde af afvigelser.

b) Organisationen skal gennemføre foranstaltninger som reaktion på enhver omstændighed i forbindelse med en begivenhed i overensstemmelse med litra a), som kan udvikle sig eller har udviklet sig til en informationssikkerhedshændelse. Disse reaktionsforanstaltninger skal gøre det muligt for organisationen at:

1) indlede en reaktionen på de advarsler, der er omhandlet i litra a), nr. 2), ved at aktivere foruddefinerede ressourcer og fremgangsmåder

2) begrænse spredningen af et angreb og undgå, at et trusselsscenarie bliver til virkelighed

3) kontrollere svigttilstanden for de berørte elementer, der er omhandlet i punkt IS.D.OR.205, litra a).

c) Organisationen skal gennemføre foranstaltninger med henblik på genopretning efter informationssikkerhedshændelser, herunder om nødvendigt nødforanstaltninger. Disse genopretningsforanstaltninger skal gøre det muligt for organisationen at:

1) fjerne den omstændighed, der forårsagede hændelsen, eller begrænse den til et acceptabelt niveau

2) opnå en sikker tilstand for de berørte elementer, der er omhandlet i punkt IS.D.OR.205, litra a), inden for en genopretningstid, der i forvejen er fastlagt af organisationen.

IS.D.OR.225 Reaktion på anmærkninger meddelt af den kompetente myndighed

a) Efter modtagelsen af meddelelsen om anmærkninger, som den kompetente myndighed har forelagt, skal organisationen:

1) påvise den eller de bagvedliggende årsager til samt medvirkende faktorer, som ligger til grund for den manglende overensstemmelse

2) fastlægge en plan for afhjælpende foranstaltninger

3) påvise, at den manglende overensstemmelse er afhjulpet til den kompetente myndigheds tilfredshed.

b) Foranstaltningerne som omhandlet i litra a) skal træffes inden for den frist, der er aftalt med den pågældende kompetente myndighed.

IS.D.OR.230 Ekstern indberetningsordning for informationssikkerhed

a) Organisationen skal indføre et indberetningssystem for informationssikkerhed, der opfylder kravene i forordning (EU) nr. 376/2014 og i dennes delegerede retsakter og gennemførelsesretsakter, hvis nævnte forordning finder anvendelse på organisationen.

b) Uden at det berører forpligtelserne i henhold til forordning (EU) nr. 376/2014, skal organisationen sikre, at enhver informationssikkerhedshændelse eller sårbarhed, der kan udgøre en væsentlig risiko for luftfartssikkerheden, indberettes til dens kompetente myndighed. Derudover:

1) hvor en sådan hændelse eller sårbarhed påvirker et luftfartøj eller et dermed forbundet system eller en dermed forbundet komponent, skal organisationen også indberette hændelsen eller sårbarheden til indehaveren af konstruktionsgodkendelsen

2) hvor en sådan hændelse eller sårbarhed påvirker et system eller dele heraf, der anvendes af organisationen, skal organisationen indberette hændelsen eller sårbarheden til den organisation, der er ansvarlig for konstruktionen af systemet eller dets dele.

c) Organisationen skal indberette de omstændigheder, der er omhandlet i litra b), som følger:

1) der skal foretages en underretning til den kompetente myndighed og, hvis det er relevant, til indehaveren af konstruktionsgodkendelsen eller til den organisation, der er ansvarlig for systemets eller komponentens konstruktion, så snart organisationen har fået kendskab til omstændigheden

2) der skal forelægges en rapport for den kompetente myndighed og, hvis det er relevant, for indehaveren af konstruktionsgodkendelsen eller for den organisation, der er ansvarlig for systemets eller komponentens konstruktion, hurtigst muligt, men ikke senere end 72 timer fra det tidspunkt, hvor organisationen har fået kendskab til omstændigheden, medmindre særlige omstændigheder forhindrer dette.

Rapporten skal udarbejdes i den form, der er fastlagt af den kompetente myndighed, og skal indeholde alle de relevante oplysninger om den omstændighed, som organisationen er bekendt med

3) der skal forelægges en opfølgningsrapport for den kompetente myndighed og, hvis det er relevant, for indehaveren af konstruktionsgodkendelsen eller for den organisation, der er ansvarlig for systemets eller komponentens konstruktion, med oplysninger om de foranstaltninger, som organisationen har truffet eller agter at træffe for at forebygge lignende informationssikkerhedshændelser i fremtiden.

Den opfølgende rapport skal forelægges, så snart disse foranstaltninger er identificeret, og skal udarbejdes i den form, der er fastlagt af den kompetente myndighed.

IS.D.OR.235 Indgåelse af kontrakter om aktiviteter i forbindelse med styring af informationssikkerhed

a) Organisationen skal sikre at, når der er indgået kontrakt om enhver del af aktiviteterne i punkt IS.D.OR.200 med andre organisationer, opfylder disse aktiviteter kravene i denne forordning, og den organisation, med hvilken der er indgået kontrakt, arbejder under organisationens tilsyn. Organisationen skal sikre, at de risici, der er forbundet med de udliciterede aktiviteter, håndteres hensigtsmæssigt.

b) Organisationen skal sikre, at den kompetente myndighed efter anmodning kan få adgang til den organisation, med hvilken der er indgået kontrakt, for at fastlægge, om de gældende krav i denne forordning fortsat er opfyldt.

IS.D.OR.240 Personalekrav

a) Den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen, som er udpeget i overensstemmelse med forordning (EU) nr. 748/2012 og forordning (EU) nr. 139/2014, jf. artikel 2, nr. 1, litra a) og b), i denne forordning, skal have organisationens bemyndigelse til at sikre, at alle de aktiviteter, der kræves i henhold til denne forordning, kan finansieres og udføres. Denne person skal:

1) sikre, at alle nødvendige ressourcer er til rådighed for at opfylde kravene i denne forordning

2) fastlægge og fremme den informationssikkerhedspolitik, der er angivet i punkt IS.D.OR.200, litra a), nr. 1)

3) udvise en grundlæggende forståelse af denne forordning.

b) Den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen skal udpege en person eller en gruppe af personer for at sikre, at organisationen opfylder kravene i denne forordning, og skal definere omfanget af deres beføjelser. Denne person eller gruppe af personer skal rapportere direkte til den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, til lederen af konstruktionsorganisationen og skal have den nødvendige viden, baggrund og erfaring til at varetage sit ansvar. Det skal fastlægges i procedurerne, hvem der er stedfortræder for en given person i tilfælde af, at denne person er fraværende i længere tid.

c) Den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen skal udpege en person eller en gruppe af personer med ansvar for at forvalte den overvågningsfunktion, der er angivet i punkt IS.D.OR.200, litra a), nr. 12).

d) Når organisationen deler organisationsstrukturer, politikker, processer og procedurer for informationssikkerhed med andre organisationer eller med områder af deres egen organisation, som ikke er omfattet af godkendelsen eller erklæringen, kan den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen uddelegere sine aktiviteter til en fælles ansvarlig person.

I et sådant tilfælde skal der træffes koordineringsforanstaltninger mellem organisationens teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen og den fælles ansvarlige person for at sikre tilstrækkelig integration af styringen af informationssikkerheden i organisationen.

e) Den teknisk/økonomisk ansvarlige personeller lederen af konstruktionsorganisationen eller den fælles ansvarlige person, der er omhandlet i litra d), skal have organisationens bemyndigelse til at etablere og vedligeholde de organisationsstrukturer, politikker, processer og procedurer, der er nødvendige for at gennemføre punkt IS.D.OR.200.

f) Organisationen skal indføre en procedure for at sikre, at den har tilstrækkeligt personale i tjeneste til at udføre de aktiviteter, der er omfattet af dette bilag.

g) Organisationen skal indføre en procedure for at sikre, at det personale, der er omhandlet i litra f), har de nødvendige kompetencer til at udføre deres opgaver.

h) Organisationen skal indføre en procedure for at sikre, at personalet anerkender det ansvar, der er forbundet med de tildelte roller og opgaver.

i) Organisationen skal sikre, at identiteten og troværdigheden af det personale, som har adgang til informationssystemer og data, der er omfattet af kravene i denne forordning, er behørigt fastlagt.

IS.D.OR.245 Registrering

a) Organisationen skal føre dokumentation for sine aktiviteter inden for styring af informationssikkerhed

1) Organisationen skal sikre, at følgende dokumentation arkiveres og kan spores:

i) enhver godkendelse, der er modtaget, og enhver tilknyttet vurdering af informationssikkerhedsrisici i overensstemmelse med punkt IS.D.OR.200, litra e)

ii) kontrakter for aktiviteter, jf. punkt IS.D.OR.200, litra a), nr. 9)

iii) dokumentation for centrale procedurer, jf. punkt IS.D.OR.200, litra d)

iv) dokumentation for de risici, der er identificeret i risikovurderingen, jf. punkt IS.D.OR.205, sammen med de tilknyttede foranstaltninger til håndtering af risiciene, jf. punkt IS.D.OR.210

v) dokumentation for informationssikkerhedshændelser og sårbarheder, der er indberettet i overensstemmelse med indberetningsordningerne, jf. punkt IS.D.OR.215 og IS.D.OR.230

vi) dokumentation for de informationssikkerhedsbegivenheder, der eventuelt skal revurderes for at afsløre uopdagede informationssikkerhedshændelser eller sårbarheder.

2) Dokumentationen i punkt 1), nr. i), skal opbevares i mindst fem år efter udløbet af godkendelsens gyldighedsperiode.

3) Dokumentationen i punkt 1), nr. ii), skal opbevares i mindst fem år efter, at kontrakten er blevet ændret eller afsluttet.

4) Dokumentationen i punkt 1), nr. iii), iv) og v), skal opbevares i mindst fem år.

5) Dokumentationen i punkt 1), nr. vi), skal opbevares, indtil disse informationssikkerhedsbegivenheder er blevet revurderet i med den hyppighed, der er defineret i en procedure, som organisationen har fastsat.

b) Organisationen skal føre dokumentation for kvalifikationer og erfaring hos sit eget personale, der er involveret i aktiviteter inden for styring af informationssikkerhed

1) Dokumentationen for personalets kvalifikationer og erfaring opbevares, så længe personen arbejder for organisationen og i mindst tre år efter, at personen har fratrådt organisationen.

2) De ansatte skal på deres anmodning have adgang til deres personlige oplysninger. Endvidere skal organisationen efter anmodning forsyne personalet med en udskrift af deres personlige oplysninger, når de fratræder organisationen.

c) Formatet for dokumentationen specificeres i organisationens procedurer.

d) Dokumentationen skal lagres på en måde, der sikrer beskyttelse mod skade, forandringer og tyveri, idet oplysningerne identificeres, når det er nødvendigt, i henhold til deres sikkerhedsklassificeringsniveau. Organisationen skal sikre, at dokumentationen lagres på en måde, der sikrer integritet, ægthed og autoriseret adgang.

IS.D.OR.250 Håndbog til styring af informationssikkerhed (ISMS)

a) Organisationen skal stille en håndbog til styring af informationssikkerhed (ISMS) til rådighed for den kompetente myndighed og, hvis det er relevant, alle dertil knyttede håndbøger og procedurer, der indeholder:

1) en erklæring underskrevet af den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, af lederen af konstruktionsorganisationen, der bekræfter, at organisationen til enhver tid vil arbejde i overensstemmelse med dette bilag og med ISMM. Hvis den teknisk/økonomisk ansvarlige person eller, hvis der er tale om konstruktionsorganisationer, lederen af konstruktionsorganisationen ikke er organisationens administrerende direktør, skal en sådan administrerende direktør kontrasignere erklæringen

2) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelser for den eller de personer, der er omhandlet i punkt IS.D.OR.240, litra b) og c)

3) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelser for den fælles ansvarlige person, jf. punkt IS.D.OR.240, litra d), hvis det er relevant

4) organisationens informationssikkerhedspolitik som omhandlet i punkt IS.D.OR.200, litra a), nr. 1)

5) en generel beskrivelse af antallet af personalemedlemmer og disses kategorier og af det system, der er indført for at planlægge disponibiliteten af det personale, der kræves i henhold til punkt IS.D.OR.240

6) stillingsbetegnelse, navn, opgaver, ansvarlighed, ansvarsområder og bemyndigelser for de centrale personer, der har ansvaret for gennemførelsen af punkt IS.D.OR.200, herunder den eller de personer, der har ansvaret for overvågningsfunktionen, jf. punkt IS.D.OR.200, litra a), nr. 12)

7) en organisationsplan, der viser de tilknyttede ansvarligheds- og ansvarskæder for de personer, der er omhandlet i nr. 2) og 6)

8) beskrivelsen af den interne indberetningsordning, jf. punkt IS.D.OR.215

9) procedurerne for, hvordan organisationen sikrer overensstemmelse med denne del og især:

   i) dokumentationen i IS.D.OR.200, litra c)

   ii) de procedurer, der definerer, hvordan organisationen skal kontrollere udliciterede aktiviteter som omhandlet i punkt IS.D.OR.200, litra a), nr. 9)

   iii) ISMM-ændringsproceduren som defineret i litra c)

10) oplysningerne om de på nuværende tidspunkt godkendte alternative måder for overensstemmelse.

b) Den kompetente myndighed godkender og opbevarer en kopi af den første udstedelse af den pågældende ISMM. ISMM skal ændres i det nødvendige omfang for at forblive en ajourført beskrivelse af organisationens ISMS. En kopi af alle ændringer af ISMM'en skal sendes til den kompetente myndighed.

c) Ændringer af ISMM skal forvaltes efter en procedure, der fastlægges af organisationen. Ændringer, der ikke er omfattet af denne procedure, og ændringer i forbindelse med de ændringer, der er omhandlet i punkt IS.D.OR.255, litra b), skal godkendes af den kompetente myndighed.

d) Organisationen kan integrere ISMM'en i andre redegørelser eller håndbøger, den er i besiddelse af, forudsat at der er en klar krydshenvisning, der angiver, hvilke dele af redegørelsen eller håndbogen der svarer til de forskellige krav i dette bilag.

IS.D.OR.255 Ændring af systemet til styring af informationssikkerhed

a) Ændringer af ISMS kan håndteres og formidles til den kompetente myndighed efter en procedure, der er udviklet af organisationen. Denne procedure skal godkendes af den kompetente myndighed.

b) For ændringer af ISMS, der ikke er omfattet af proceduren i litra a), skal organisationen ansøge om og opnå en godkendelse udstedt af den kompetente myndighed.

Hvad angår disse ændringer:

1) ansøgningen skal indgives, før en sådan ændring foretages, for at gøre det muligt for den kompetente myndighed at fastslå den fortsatte overensstemmelse med denne forordning og om nødvendigt ændre organisationens certifikat og de betingelser for godkendelse, som er knyttet til det

2) organisationen skal stille alle oplysninger til rådighed for den kompetente myndighed, som denne ønsker for at evaluere ændringen

3) ændringen må først gennemføres efter, at den kompetente myndigheds formelle godkendelse er modtaget

4) Organisationen skal drives i overensstemmelse med de betingelser, som den kompetente myndighed foreskriver, under gennemførelsen af sådanne ændringer.

IS.D.OR.260 Vedvarende forbedring

a) Organisationen skal ved hjælp af passende resultatindikatorer vurdere effektiviteten og modenheden af ISMS. Denne vurdering skal foretages med en hyppighed, som organisationen på forhånd har fastsat, eller efter en informationssikkerhedshændelse.

b) Hvis der konstateres mangler efter den vurdering, der foretages i henhold til litra a), skal organisationen træffe de nødvendige udbedrende foranstaltninger for at sikre, at ISMS fortsat opfylder de gældende krav og bevarer informationssikkerhedsrisiciene på et acceptabelt niveau. Desuden skal organisationen revurdere de elementer i ISMS, som påvirkes af de vedtagne foranstaltninger.