Europeiska unionens råd

Bryssel den 18 juli 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	14 juli 2022
till:	Rådets generalsekretariat
Komm. dok. nr:	C(2022) 4882 final - ANNEX
Ärende:	BILAGA till KOMMISSIONENS DELEGERADE FÖRORDNING om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014

För delegationerna bifogas dokument – C(2022) 4882 final - ANNEX.

Bilaga: C(2022) 4882 final - ANNEX

EUROPEISKA
KOMMISSIONEN

Bryssel den 14.7.2022
C(2022) 4882 final

ANNEX

BILAGA

till

KOMMISSIONENS DELEGERADE FÖRORDNING

om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2018/1139 vad gäller krav för hantering av informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten för organisationer som omfattas av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014, och om ändring av kommissionens förordningar (EU) nr 748/2012 och nr 139/2014

BILAGA

INFORMATIONSSÄKERHET – ORGANISATIONSKRAV

[DEL-IS.D.OR]

IS.D.OR.100 Tillämpningsområde

I denna del fastställs de krav som ska uppfyllas av de organisationer som avses i artikel 2 i denna förordning.

IS.D.OR.200 System för hantering av informationssäkerhet (ISMS)

a) För att uppnå de mål som anges i artikel 1 ska organisationen inrätta, genomföra och upprätthålla ett system för hantering av informationssäkerhet (ISMS) som säkerställer att organisationen

1) inrättar en policy för informationssäkerhet som fastställer organisationens övergripande principer med avseende på informationssäkerhetsriskernas potentiella inverkan på flygsäkerheten,

2) identifierar och ser över informationssäkerhetsrisker i enlighet med punkt IS.D.OR.205,

3) definierar och genomför åtgärder för hantering av informationssäkerhetsrisker i enlighet med punkt IS.D.OR.210,

4) genomför ett internt rapporteringssystem för informationssäkerhet i enlighet med punkt IS.D.OR.215,

5) definierar och genomför, i enlighet med punkt IS.D.OR.220, de åtgärder som krävs för att upptäcka informationssäkerhetshändelser, identifierar de händelser som anses vara incidenter med en potentiell inverkan på flygsäkerheten med undantag för vad som är tillåtet enligt punkt IS.D.OR.205 e samt hanterar och sköter återställning efter sådana informationssäkerhetsincidenter,

6) genomför de åtgärder som har anmälts av den behöriga myndigheten som en omedelbar reaktion på en informationssäkerhetsincident eller sårbarhet med en inverkan på flygsäkerheten,

7) vidtar lämpliga åtgärder, i enlighet med punkt IS.D.OR.225, för att hantera brister som anmälts av den behöriga myndigheten,

8) genomför ett externt rapporteringssystem i enlighet med punkt IS.D.OR.230 för att den behöriga myndigheten ska kunna vidta lämpliga åtgärder,

9) uppfyller kraven i punkt IS.D.OR.235 när den utkontrakterar någon del av den verksamhet som avses i punkt IS.D.OR.200 till andra organisationer,

10) uppfyller de personalkrav som fastställs i punkt IS.D.OR.240,

11) uppfyller de dokumentationskrav som fastställs i punkt IS.D.OR.245,

12) övervakar att organisationen uppfyller kraven i denna förordning och ger återkoppling om brister till den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, till chefen för konstruktionsorganisationen, för att säkerställa ett effektivt genomförande av korrigerande åtgärder,

13) utan att det påverkar tillämpliga krav på incidentrapportering, skyddar konfidentialiteten för all information som organisationen kan ha mottagit från andra organisationer, i enlighet med informationens känslighetsnivå.

b) För att kontinuerligt uppfylla de krav som avses i artikel 1 ska organisationen genomföra en kontinuerlig förbättringsprocess i enlighet med punkt IS.D.OR.260.

c) Organisationen ska i enlighet med punkt IS.D.OR.250 dokumentera alla centrala processer, förfaranden, roller och ansvarsområden som krävs för att uppfylla kraven i punkt IS.D.OR.200 a och inrätta en process för att ändra denna dokumentation. Ändringar av dessa processer, förfaranden, roller och ansvarsområden ska hanteras i enlighet med punkt IS.D.OR.255.

d) De processer, förfaranden, roller och ansvarsområden som organisationen inrättat för att uppfylla kraven i punkt IS.D.OR.200 a ska motsvara verksamhetens art och komplexitet, på grundval av en bedömning av de informationssäkerhetsrisker som är

förknippade med denna verksamhet, och får integreras i andra befintliga ledningssystem som organisationen redan infört.

e) Utan att det påverkar skyldigheten att uppfylla rapporteringskraven i förordning (EU) nr 376/2014[1] och kraven i punkt IS.D.OR.200 a.13, får den behöriga myndigheten ge organisationen godkännande att inte genomföra de krav som avses i punkterna a–d och de relaterade kraven i punkterna IS.D.OR.205 till IS.D.OR.260 om organisationen på ett för myndigheten tillfredsställande sätt kan visa att dess verksamhet, anläggningar och resurser, liksom de tjänster som den driver, tillhandahåller, tar emot och upprätthåller, inte utgör några informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten, vare sig för sig själv eller för andra organisationer. Godkännandet ska baseras på en dokumenterad bedömning av informationssäkerhetsrisker som utförts av organisationen eller en tredje part i enlighet med punkt IS.D.OR.205 och granskats och godkänts av dess behöriga myndighet.

Godkännandets fortsatta giltighet kommer att ses över av den behöriga myndigheten efter den tillämpliga tillsynscykeln och närhelst ändringar genomförs i organisationens arbetsområde.

IS.D.OR.205 Bedömning av informationssäkerhetsrisker

a) Organisationen ska identifiera alla sina delar som skulle kunna utsättas för informationssäkerhetsrisker. Detta ska omfatta

1) organisationens verksamhet, anläggningar och resurser, liksom de tjänster som organisationen driver, tillhandahåller, tar emot eller upprätthåller,

2) den utrustning och information och de system och data som bidrar till att de delar som anges i punkt 1 fungerar.

b) Organisationen ska identifiera de gränssnitt som den har med andra organisationer och som kan leda till ömsesidig exponering för informationssäkerhetsrisker.

c) När det gäller de delar och gränssnitt som avses i punkterna a och b ska organisationen identifiera de informationssäkerhetsrisker som kan ha en potentiell inverkan på flygsäkerheten. För varje identifierad risk ska organisationen

1) tilldela en risknivå enligt en fördefinierad klassificering som fastställts av organisationen,

2) associera varje risk och dess nivå med motsvarande del eller gränssnitt som identifierats i enlighet med punkterna a och b.

Den fördefinierade klassificering som avses i punkt 1 ska ta hänsyn till risken för att hotscenariot inträffar och hur allvarliga konsekvenser det skulle få för säkerheten. På

([1]) Europaparlamentets och rådets förordning (EU) nr 376/2014 av den 3 april 2014 om rapportering, analys och uppföljning av händelser inom civil luftfart om ändring av Europaparlamentets och rådets förordning (EU) nr 996/2010 och om upphävande av Europaparlamentets och rådets direktiv 2003/42/EG, kommissionens förordningar (EG) nr 1321/2007 och (EG) nr 1330/2007 (EUT L 122, 24.4.2014, s. 18).

grundval av denna klassificering, och med beaktande av huruvida organisationen har en strukturerad och repeterbar riskhanteringsprocess för verksamheten, ska organisationen kunna fastställa om risken är acceptabel eller behöver hanteras i enlighet med punkt IS.D.OR.210.

För att underlätta riskbedömningarnas ömsesidiga jämförbarhet ska tilldelningen av risknivå enligt punkt 1 ta hänsyn till relevant information som erhållits i samordning med de organisationer som avses i punkt b.

d) Organisationen ska se över och uppdatera den riskbedömning som utförts i enlighet med punkterna a, b och c i någon av följande situationer:

1) Det sker en förändring i de delar som omfattas av informationssäkerhetsrisker.

2) Det sker en förändring i gränssnitten mellan organisationen och andra organisationer, eller i de risker som meddelats av de andra organisationerna.

3) Det sker en förändring i den information eller kunskap som används för att identifiera, analysera och klassificera risker.

4) Lärdom dras av analysen av informationssäkerhetsincidenter.

IS.D.OR.210 Hantering av informationssäkerhetsrisker

a) Organisationen ska utarbeta åtgärder för att hantera oacceptabla risker som identifierats i enlighet med punkt IS.D.OR.205, genomföra dem i rätt tid och kontrollera att de fortfarande är effektiva. Dessa åtgärder ska göra det möjligt för organisationen att

1) kontrollera de omständigheter som bidrar till att hotscenariot faktiskt inträffar,

2) minska konsekvenserna för flygsäkerheten i samband med att hotscenariot förverkligas,

3) undvika riskerna.

Dessa åtgärder får inte medföra några nya potentiella oacceptabla risker för flygsäkerheten.

b) Den person som avses i punkt IS.D.OR.240 a och b och annan berörd personal inom organisationen ska informeras om resultatet av den riskbedömning som utförts i enlighet med punkt IS.D.OR.205, motsvarande hotscenarier och de åtgärder som ska vidtas.

Organisationen ska också informera organisationer med vilka den har ett gränssnitt i enlighet med punkt IS.D.OR.205 b om eventuella risker som är gemensamma för de båda organisationerna.

IS.D.OR.215 Internt rapporteringssystem för informationssäkerhet

a) Organisationen ska inrätta ett internt rapporteringssystem för att möjliggöra insamling och utvärdering av informationssäkerhetshändelser, bland annat de som ska rapporteras enligt punkt IS.D.OR.230.

b) Detta system och den process som avses i punkt IS.D.OR.220 ska göra det möjligt för organisationen att

1) identifiera vilka av de händelser som rapporterats i enlighet med punkt a som anses vara informationssäkerhetsincidenter eller sårbarheter med potentiell inverkan på flygsäkerheten,

2) identifiera orsakerna och bidragande faktorer till de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt 1 och ta itu med dem som en del av riskhanteringsprocessen för informationssäkerhet i enlighet med punkterna IS.D.OR.205 och IS.D.OR.220,

3) säkerställa en utvärdering av all känd och relevant information om de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt 1,

4) säkerställa genomförandet av en metod för att internt distribuera informationen vid behov.

c) Eventuella underleverantörer som kan utsätta organisationen för informationssäkerhetsrisker med en potentiell inverkan på flygsäkerheten ska vara skyldiga att rapportera informationssäkerhetshändelser till organisationen. Dessa rapporter ska lämnas in enligt de förfaranden som fastställs i de särskilda avtalsarrangemangen och ska utvärderas i enlighet med punkt b.

d) Organisationen ska vid utredningar samarbeta med alla andra organisationer som på ett betydande sätt bidrar till informationssäkerheten för den egna verksamheten.

e) Organisationen får integrera detta rapporteringssystem med andra rapporteringssystem som den redan har infört.

IS.D.OR.220 Informationssäkerhetsincidenter – upptäckt, hantering och återställning

a) På grundval av resultatet av den riskbedömning som utförts i enlighet med punkt IS.D.OR.205 och resultatet av den riskhantering som utförts i enlighet med punkt IS.D.OR.210 ska organisationen vidta åtgärder för att upptäcka incidenter och sårbarheter som visar att oacceptabla risker potentiellt kan förverkligas och som kan ha en potentiell inverkan på flygsäkerheten. Dessa upptäcktsåtgärder ska göra det möjligt för organisationen att

1) identifiera avvikelser från fördefinierade utgångsvärden för funktionsprestanda,

2) utlösa varningar för att aktivera lämpliga reaktionsåtgärder, vid eventuella avvikelser.

b) Organisationen ska vidta åtgärder för att reagera på alla händelseförhållanden som

identifierats i enlighet med punkt a och som kan utvecklas eller har utvecklats till en informationssäkerhetsincident. Dessa reaktionsåtgärder ska göra det möjligt för organisationen att

1) inleda reaktionen på de varningar som avses i punkt a.2 genom att aktivera fördefinierade resurser och åtgärder,

2) begränsa spridningen av en attack och undvika att ett hotscenario förverkligas fullt ut,

3) kontrollera felläget för de berörda delar som anges i punkt IS.D.OR.205 a.

c) Organisationen ska vidta åtgärder som syftar till återställning efter informationssäkerhetsincidenter, inbegripet nödåtgärder om så behövs. Dessa återställningsåtgärder ska göra det möjligt för organisationen att

1) eliminera det förhållande som orsakade incidenten eller begränsa det till en acceptabel nivå,

2) uppnå ett säkert tillstånd för de berörda delar som anges i punkt IS.D.OR.205 a inom en återställningstid som tidigare fastställts av organisationen.

IS.D.OR.225 Hantering av brister som anmälts av den behöriga myndigheten

a) Efter att ha mottagit anmälan av brister från den behöriga myndigheten ska organisationen

1) identifiera grundorsaken eller grundorsakerna, samt bidragande faktorer, till den bristande kravuppfyllelsen,

2) utarbeta en plan för korrigerande åtgärder,

3) påvisa att den bristande kravuppfyllelsen har korrigerats på ett för den behöriga myndigheten tillfredsställande sätt.

b) De åtgärder som avses i punkt a ska genomföras inom den tidsfrist som överenskommits med den behöriga myndigheten.

IS.D.OR.230 Externt rapporteringssystem för informationssäkerhet

a) Organisationen ska införa ett rapporteringssystem för informationssäkerhet som uppfyller kraven i förordning (EU) nr 376/2014 och dess delegerade akter och genomförandeakter om den förordningen är tillämplig på organisationen.

b) Utan att det påverkar skyldigheterna enligt förordning (EU) nr 376/2014 ska organisationen säkerställa att alla informationssäkerhetsincidenter eller sårbarheter som kan utgöra en betydande risk för flygsäkerheten rapporteras till dess behöriga myndighet. Dessutom gäller följande:

1) Om en sådan incident eller sårbarhet påverkar ett luftfartyg eller tillhörande system eller komponent ska organisationen också rapportera den till innehavaren av konstruktionsgodkännandet.

2) Om en sådan incident eller sårbarhet påverkar ett system eller en komponent som används av organisationen, ska organisationen rapportera den till den organisation som ansvarar för konstruktionen av systemet eller komponenten.

c) Organisationen ska rapportera de omständigheter som avses i punkt b enligt följande:

1) En anmälan ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som organisationen får kännedom om omständigheterna.

2) En rapport ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som möjligt men senast 72 timmar efter det att organisationen får kännedom om omständigheterna, såvida inte exceptionella omständigheter förhindrar detta.

Rapporten ska göras i den form som fastställs av den behöriga myndigheten och innehålla all relevant information som organisationen känner till om omständigheten.

3) En uppföljningsrapport ska lämnas in till den behöriga myndigheten och, i tillämpliga fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, med uppgifter om de åtgärder som organisationen har vidtagit eller avser att vidta för återställning efter incidenten och de åtgärder den avser att vidta för att förhindra liknande informationssäkerhetsincidenter i framtiden.

Uppföljningsrapporten ska lämnas in så snart dessa åtgärder har identifierats och ska utarbetas i den form som fastställs av den behöriga myndigheten.

IS.D.OR.235 Utkontraktering av verksamhet som rör hantering av informationssäkerhet

a) Vid utkontraktering av någon del av den verksamhet som avses i punkt IS.D.OR.200 till andra organisationer ska organisationen säkerställa att den utkontrakterade verksamheten uppfyller kraven i denna förordning och att underleverantören arbetar under dess tillsyn. Organisationen ska säkerställa att de risker som är förenade med den utkontrakterade verksamheten hanteras på lämpligt sätt.

b) Organisationen ska säkerställa att den behöriga myndigheten på begäran kan få tillgång till underleverantören för att fastställa att de tillämpliga kraven i denna förordning fortfarande är uppfyllda.

IS.D.OR.240 Personalkrav

a) Den verksamhetsansvariga chefen för organisationen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen, som utsetts i enlighet med förordning (EU) nr 748/2012 och förordning (EU) nr 139/2014 och som avses i artikel 2.1 a och b i den här förordningen, ska ha organisationens bemyndigande att säkerställa att all verksamhet som krävs enligt den här förordningen kan finansieras och genomföras. Denna person ska

   1) säkerställa att alla nödvändiga resurser finns tillgängliga för att uppfylla kraven i denna förordning,

   2) fastställa och främja den informationssäkerhetspolicy som avses i punkt IS.D.OR.200 a.1,

   3) uppvisa en grundläggande förståelse av denna förordning.

b) Den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen ska utse en person eller en grupp av personer som ska säkerställa att organisationen uppfyller kraven i denna förordning och ska fastställa omfattningen av deras befogenheter. Denna person eller grupp av personer ska rapportera direkt till den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen och ska ha lämplig kunskap, bakgrund och erfarenhet för att kunna fullgöra sitt ansvar. I förfarandena ska det fastställas vem som vikarierar för en viss person om den personen är frånvarande under längre tid.

c) Den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen ska utse en person eller en grupp av personer som har ansvaret för att hantera den funktion för övervakning av kravuppfyllelse som avses i punkt IS.D.OR.200 a.12.

d) Om organisationen delar organisatoriska strukturer, policyer, processer och förfaranden för informationssäkerhet med andra organisationer eller med delar av den egna organisationen som inte omfattas av godkännandet eller försäkran, får den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen delegera verksamheten till en gemensam ansvarig person.

   I sådana fall ska samordningsåtgärder fastställas mellan organisationens verksamhetsansvariga chef eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen och den gemensamma ansvariga personen för att säkerställa att hanteringen av informationssäkerhet integreras på lämpligt sätt inom organisationen.

e) Den verksamhetsansvariga chefen eller chefen för konstruktionsorganisationen, eller den gemensamma ansvariga person som avses i punkt d, ska ha organisationens bemyndigande att upprätta och upprätthålla de organisatoriska strukturer, policyer, processer och förfaranden som krävs för att genomföra punkt IS.D.OR.200.

f) Organisationen ska ha en process för att säkerställa att den har tillräckligt med personal i tjänst för att kunna utföra den verksamhet som omfattas av denna bilaga.

g) Organisationen ska ha en process för att säkerställa att den personal som avses i punkt f har den kompetens som krävs för att utföra uppgifterna.

h) Organisationen ska ha en process för att säkerställa att personalen är medveten om det ansvar som är förenat med de tilldelade rollerna och uppgifterna.

i) Organisationen ska säkerställa att identiteten på och tillförlitligheten hos den personal som har åtkomst till informationssystem och data som omfattas av kraven i denna förordning fastställs på lämpligt sätt.

IS.D.OR.245 Dokumentation

a) Organisationen ska dokumentera sin verksamhet för hantering av informationssäkerhet.

1) Organisationen ska säkerställa att följande dokumentation arkiveras och kan spåras:

i) Alla godkännanden som mottagits och eventuella tillhörande bedömningar av informationssäkerhetsrisker i enlighet med punkt IS.D.OR.200 e.

ii) Kontrakt för verksamhet som avses i punkt IS.D.OR.200 a.9.

iii) Dokumentation av de centrala processer som avses i punkt IS.D.OR.200 d.

iv) Dokumentation av de risker som identifierats i den riskbedömning som avses i punkt IS.D.OR.205 tillsammans med de tillhörande riskhanteringsåtgärder som avses i punkt IS.D.OR.210.

v) Dokumentation av informationssäkerhetsincidenter och sårbarheter som rapporterats i enlighet med de rapporteringssystem som avses i punkterna IS.D.OR.215 och IS.D.OR.230.

vi) Dokumentation av de informationssäkerhetshändelser som kan behöva omprövas för att avslöja oupptäckta informationssäkerhetsincidenter eller sårbarheter.

2) Den dokumentation som avses i punkt 1 i ska bevaras i minst fem år efter det att godkännandet inte längre än giltigt.

3) Den dokumentation som avses i punkt 1 ii ska bevaras i minst fem år efter det att kontraktet har ändrats eller sagts upp.

4) Den dokumentation som avses i punkt 1 iii, iv och v ska bevaras i minst fem år.

5) Den dokumentation som avses i punkt 1 vi ska bevaras till dess att dessa informationssäkerhetshändelser har omprövats i enlighet med en periodicitet som anges i ett förfarande som fastställts av organisationen.

b) Organisationen ska ha dokumentation över kvalifikationer och erfarenhet när det gäller den egna personalen som arbetar med hantering av informationssäkerhet.

1) Dokumentationen av personalens kvalifikationer och erfarenhet ska bevaras så länge personen arbetar för organisationen och i minst tre år efter det att personen har lämnat organisationen.

2) Anställda ska på egen begäran få tillgång till den dokumentation som gäller dem. På deras begäran ska organisationen också ge dem en kopia av den dokumentation som gäller dem när de lämnar organisationen.

c) Formatet för dokumentationen ska anges i organisationens förfaranden.

d) Dokumentationen ska lagras på ett sätt som säkerställer skydd från skada, ändring och stöld, vid behov med uppgift om informationens säkerhetsskyddsklassificeringsnivå. Organisationen ska säkerställa att dokumentationen lagras på ett sätt som säkerställer integritet, autenticitet och behörig åtkomst.

IS.D.OR.250 Handbok för hantering av informationssäkerhet (ISMM)

a) Organisationen ska förse den behöriga myndigheten med en handbok för hantering av informationssäkerhet (ISMM) och, i tillämpliga fall, eventuella tillhörande manualer och förfaranden, med följande uppgifter:

1) En förklaring undertecknad av den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen, vilken bekräftar att organisationen alltid kommer att arbeta i enlighet med denna bilaga och med ISMM. Om den verksamhetsansvariga chefen eller, när det gäller konstruktionsorganisationer, chefen för konstruktionsorganisationen inte är organisationens verkställande direktör, ska den verkställande direktören kontrasignera förklaringen.

2) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för den eller de personer som avses i punkt IS.D.OR.240 b och c.

3) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för den gemensamma ansvariga person som avses i punkt IS.D.OR.240 d, i tillämpliga fall.

4) Organisationens informationssäkerhetspolicy som avses i punkt IS.D.OR.200 a.1.

5) En allmän beskrivning av antalet anställda och personalkategorierna samt det system som finns för att planera personalens tillgänglighet i enlighet med punkt IS.D.OR.240.

6) Titlar, namn, arbetsuppgifter, skyldigheter, ansvar och befogenheter för de centrala personer som ansvarar för genomförandet av punkt IS.D.OR.200, inbegripet den eller de personer som ansvarar för övervakning av kravuppfyllelse enligt punkt IS.D.OR.200 a.12.

7) Ett organisationsschema som visar tillhörande kedjor av ansvarsskyldighet och ansvar för de personer som avses i punkterna 2 och 6.

8) Beskrivningen av det interna rapporteringssystem som avses i punkt IS.D.OR.215.

9) De förfaranden som specificerar hur organisationen säkerställer efterlevnad av denna del, särskilt

i) punkt IS.D.OR.200 c om dokumentation,

ii) de förfaranden som definierar hur organisationen kontrollerar eventuell utkontrakterad verksamhet som avses i punkt IS.D.OR.200 a.9,

iii) det förfarande för ISMM-ändring som avses i punkt c.

10) Uppgifter om de för närvarande godkända alternativa sätten att uppfylla kraven.

b) Det första utfärdandet av ISMM ska godkännas och en kopia ska behållas av den behöriga myndigheten. ISMM ska vid behov ändras så att den förblir en aktuell beskrivning av organisationens ISMS. En kopia av eventuella ändringar av ISMM ska lämnas till den behöriga myndigheten.

c) Ändringar av ISMM ska hanteras enligt ett förfarande som fastställs av organisationen. Ändringar som inte omfattas av detta förfarande och eventuella ändringar som rör de ändringar som avses i punkt IS.D.OR.255 b ska godkännas av den behöriga myndigheten.

d) Organisationen får integrera ISMM med sina andra ledningshandböcker eller handledningar, förutsatt att det finns en tydlig korshänvisning som anger vilka delar av ledningshandboken eller handledningen som motsvarar de olika kraven i denna bilaga.

IS.D.OR.255 Ändringar av systemet för hantering av informationssäkerhet

a) Ändringar av ISMS får hanteras och anmälas till den behöriga myndigheten genom ett förfarande som utarbetats av organisationen. Detta förfarande ska godkännas av den behöriga myndigheten.

b) När det gäller ändringar av ISMS som inte omfattas av det förfarande som avses i punkt a ska organisationen ansöka om och erhålla ett godkännande från den behöriga myndigheten.

För dessa ändringar gäller följande:

1) Ansökan ska lämnas in innan någon ändring äger rum för att den behöriga myndigheten ska kunna fastställa fortsatt efterlevnad av denna förordning samt vid behov ändra organisationens certifikat och de villkor för godkännande som bifogas certifikatet.

2) Organisationen ska ge den behöriga myndigheten tillgång till all information den begär för att kunna utvärdera ändringen.

3) Ändringen ska genomföras först efter att ett formellt godkännande har mottagits från den behöriga myndigheten.

4) Vid genomförandet av sådana ändringar ska organisationen agera enligt de villkor som föreskrivs av den behöriga myndigheten.

IS.D.OR.260 Löpande förbättring

a) Organisationen ska med hjälp av lämpliga resultatindikatorer bedöma ISMS effektivitet och mognadsgrad. Bedömningen ska utföras enligt en tidsplan som fastställts på förhand av organisationen eller till följd av en informationssäkerhetsincident.

b) Om brister upptäcks till följd av den bedömning som utförts i enlighet med punkt a ska organisationen vidta nödvändiga förbättringsåtgärder för att säkerställa att ISMS fortsätter att uppfylla de tillämpliga kraven och upprätthåller en acceptabel nivå för informationssäkerhetsriskerna. Dessutom ska organisationen göra en ny bedömning av de delar av ISMS som påverkas av de antagna åtgärderna.