0.3

**Management personnel**

Ledningspersonal måste stå i detta kapitel utöver övriga manualer. Här skall CAMO-ledningspersonal framgå med titel, förnamn, efternamn och kontaktinformation.

- AM
- Nominerade personer
- Ersättare för nominerade personer (deputies)
- Chefer (om andra än nominerade personer)

Det ska framgå vem som ersätter vem vid frånvaro upp till 30 dagar.
Vid frånvaro längre än 30 dagar ska en ansökan till TS göras.

Organisationens ledningspersonal och ersättare (deputy) presenteras i tabellform med för och efternamn.

*Exempel:*

| *Roll* | *Nominerad person* | **Ersätter (Deputy)* | *Kontaktinformation* |
|---|---|---|---|
| *AM* | *För & Efternamn* | *För & Efternamn* | *epost & telefonnummer* |
| *CAM* | | | |
| *CMM* | | | |
| *SM* | | | |
| *ISM* | | | |
| *CRP* | | | |
| *ITM* | | | |

*Deputy tillsätts vid behov och skall utvärderas att personen har rätt kompetens för sin roll.

0.3 fort.

**Duties and responsibilities**

Ansvar, befogenheter, arbetsuppgifter och kvalifikationskrav för personerna listade i CAME 0.3

- AM, Accountable Manager, ansvar enligt CAME 0.1.1,
  Safety policy and objectives, säkerhetsledningssystem, tillräckliga resurser, nominera personal, betalning av myndighetsavgifter och att tillståndet återlämnas till myndigheten vid återkallelse eller avslut av tillstånd.

- Nominerade personer, enl. CAMO.A.305

- CMM, Compliance Monitoring Manager,
- Del-IS CMM (vid behov)

- SM, Safety Manager,
- Del- IS SM (vid behov)

- ISM – Information security manager enl. CAMO.A.200A
- CRP – Common responsible person (vid behov) (enl. CAMO.A.200A)
- ITM- Information technology manager (vid behov) (enl. CAMO.A.200A)
- External auditörer

- Alla nominerade personer ska se till att efterlevnad hanteras proaktivt och att tidiga varningstecken på icke efterlevnad dokumenteras och åtgärdas

| 2A – INFORMATION SECURITY MANAGEMENT SYSTEM PROCEDURES | | |
|---|---|---|
| 2A.1 | **Information Security Risk Assessment**<br><br>(a) Procedur för att identifiera de delar av organisationen som kan vara exponerade för informationssäkerhetsrisker:<br><br>1. organisationens verksamhet, anläggningar och resurser. Samt de tjänster som organisationen driver, tillhandahåller, tar emot eller underhåller;<br><br>2. den utrustning, de system, data och information som bidrar till funktionen hos de delar som anges i punkt (1) ovan<br><br>(b) Procedur för att identifiera de gränssnitt som organisationen har med andra organisationer, och vilket som kan leda till ömsesidig exponering för informationssäkerhetsrisker.<br><br>(c) Procedur för att identifiera vilka av de informationssäkerhetsrisker som identifierats under punkterna (a) och (b) ovan som kan ha en potentiell inverkan på flygsäkerheten.<br><br>(d) En fördefinierad tabell över risknivåer<br><br>(e) Processen för att tilldela motsvarande risknivå till var och en av de informationssäkerhetsrisker som identifierats som potentiellt påverkande för flygsäkerheten enligt punkt (c) ovan, och koppla varje risk och dess nivå till motsvarande element eller gränssnitt som identifierats i punkterna (a) och (b) ovan<br><br>(f) Procedur för att granska och uppdatera riskbedömningen när någon av följande situationer inträffar:<br><br>1. det sker en förändring i de delar/system som är föremål för informationssäkerhetsrisker;<br><br>2. det sker en förändring i gränssnitten mellan organisationen och andra organisationer, eller i de risker som kommuniceras av de andra organisationerna;<br><br>3. det sker en förändring i den information eller kunskap som används för identifiering, analys och klassificering av risker;<br><br>4. det finns lärdomar från analysen av informationssäkerhetsincidenter | |

| | | |
|---|---|---|
| 2A.1 Forts. | Proceduren som beskrivs i punkt (a) ovan bör också specificera den metod som organisationen använder för att registrera de delar/system som kan utsättas för informationssäkerhetsrisker.<br><br>Den fördefinierade tabellen över risknivåer som beskrivs i punkt (d) ovan ska beakta potentialen för att ett hotscenariot inträffar (sannolikheten) och hur allvarliga dess säkerhetskonsekvenser är. Baserat på den tabellen, och med hänsyn till huruvida organisationen har en strukturerad och repeterbar riskhanteringsprocess för verksamheten. Organisationen ska kunna fastställa om risken är acceptabel eller behöver hanteras i enlighet med punkt IS.I.OR.210.<br><br>Detta kapitel ska innehålla tydliga ansvarsområden för de personer som ansvarar för att utvärdera riskerna och besluta om en risk är acceptabel eller behöver hanteras<br><br>***Typiska exempel på gränssnitt (enligt punkt (b) ovan) som Del-CAMO-organisationen kan ha med andra organisationer, och som kan resultera i ömsesidig exponering för informationssäkerhetsrisker kan vara samverkan med:***<br><br>*• CAMO som tillhandahåller arbetsordrar, instruktioner för fortsatt luftvärdighet (ICA), information om flygplanskonfiguration, lista över uppskjutna punkter, MEL-information etc. .*<br>*• OEM- och DOA-tillverkare som ger tillgång till instruktioner för fortsatt luftvärdighet (ICA), modifieringsunderlag, programvara för uppdatering av flygelektroniska system etc.*<br><br>*• Leverantörer av delar, verktyg, testutrustning (inklusive till exempel programuppdatering för testutrustning) etc.*<br><br>*• (Sub-) kontrakterade och underleverantörer (för specialiserade uppgifter, underhållsåtgärder etc.), eventuellt även tillverkarens underhållsteam.*<br><br>*• Utbildningsorganisationer för underhållspersonal.*<br><br>*• Myndigheter.* | |

| | | |
|---|---|---|
| 2A.1 Forts. | ***Typiska <u>exempel</u> på informationssäkerhetsrisker som en Del-CAMO-organisation kan möta är följande:***<br><br>*• Programvaran för underhållshantering som används av organisationen komprometteras (oavsett om det är deras egen programvara eller om åtkomst tillhandahålls via CAMO).*<br><br>*• Obehörig användning av elektroniska signaturer (t.ex. dokument för underhållsfriskrivning utfärdade av obehöriga personer eller simulering av en behörig person).*<br>*OBS: I en lägre skala kan detta också vara en risk för pappersfriskrivningar.*<br><br>*• Användning av komprometterade nycklar för att kryptera och dekryptera data som överförs mellan organisationer.*<br><br>*• Användning av komprometterade instruktioner för fortsatt luftvärdighet (ICA).*<br><br>*• Användning av komprometterade arbetsordrar.*<br><br>*• Uppladdning av komprometterad programvara (t.ex. navigationsdata) eller nedladdning av programvara från otillförlitliga källor eller användning av olämplig hårdvara för att lagra data.*<br><br>*• Användning av komprometterade kvalifikationsregister (t.ex. utbildning, erfarenhet, fysiologiska utvärderingar…), antingen digitala eller pappersbaserade, vilket resulterar i felaktig certifiering av personalbehörigheter.*<br><br>*• Förlitande på komprometterade kalibreringsregister för verktyg/utrustning*<br><br>*• Förlitande på komprometterad information i listan över godkända kompetenser, vilket resulterar i utförande av icke-auktoriserat underhåll.* | |

| | | |
|---|---|---|
| 2A.2 | **Information Security Risk Treatment**<br><br>(a) Procedur för att fastställa åtgärder för att hantera oacceptabla risker (identifierade enligt IS.I.OR.205), implementera dem i tid och kontrollera deras fortsatta effektivitet.<br><br>Dessa åtgärder ska göra det möjligt för organisationen att:<br><br>(1) kontrollera de omständigheter som bidrar till att hotscenariot faktiskt inträffar;<br>(2) minska konsekvenserna för flygsäkerheten i samband med att hotscenarion;<br>(3) undvika riskerna.<br><br>Dessa åtgärder ska inte införa några nya potentiella oacceptabla risker för flygsäkerheten.<br><br>(b) Procedur för att informera de personer som avses i punkt IS.I.OR.240(a) och (b) och annan berörd personal i organisationen om resultatet av riskbedömningen, motsvarande hotscenarier och de åtgärder som ska genomföras.<br><br>Proceduren måste inkludera behovet av att organisationen informerar de organisationer som den har ett gränssnitt med om eventuella risker som delas mellan båda organisationerna.<br><br>***Viktiga aspekter att beakta vid utveckling av rutiner för "Hantering av informationssäkerhetsrisker" är följande:***<br><br>*• ”Risköverföring” är inte en acceptabel riskhanteringsåtgärd (t.ex. att hantera risken enbart genom att teckna en försäkring som täcker ekonomiska förluster, utan att ta itu med påverkan på flygsäkerheten).*<br><br>*Möjliga acceptabla åtgärder är till exempel:*<br>- *Förebygga risken (t.ex. införa åtkomstkontrollåtgärder, såsom en lösenordspolicy)*<br>- *Minska risken (t.ex. ha en incidenthanteringsplan, säkerhetskopior av data etc.)*<br>- *Undvika risken (t.ex. undvika vissa tekniska lösningar som skapar risken och använda mer robusta sådana)*<br><br>*• De informationssäkerhetsåtgärder som vidtas ska inte introducera nya potentiella risker för flygsäkerheten.*<br><br>*• Åtgärder ska vara väl kommunicerade, förstådda och godkända av den ansvariga chefen och han/hon bör kommunicera dem effektivt inom organisationen.*<br><br>*• Andra organisationer som delar ett gränssnitt med organisationen ska informeras om de gemensamma riskerna och de åtgärder som vidtagits.*<br><br>*• Åtgärder ska genomföras på ett säkert sätt och kontrolleras för deras kontinuerliga effektivitet.* | |

| | | |
|---|---|---|
| 2A.3 | **Information Security Internal Reporting Scheme**<br><br>Detta kapitel kan integreras information med CAME kapitel 2.2<br><br>Detta kapitel bör beskriva det interna säkerhetsrapporteringssystem som organisationen har etablerat för att samla in och utvärdera informationssäkerhetshändelser, inklusive de som ska rapporteras via det externa rapporteringssystem (Ref. IS.I.OR.230).<br><br>Det interna rapporteringssystemet, tillsammans med processen som beskrivs i kapitel 3A.4, ska göra det möjligt för organisationen att:<br><br>1. identifiera vilka av de rapporterade händelserna som anses vara informationssäkerhetsincidenter eller sårbarheter med potentiell inverkan på flygsäkerheten;<br>2. identifiera orsakerna till, och bidragande faktorer till, de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt (1) ovan, och åtgärda dem som en del av den riskhanteringsprocess som beskrivs i kapitel 2A.1 och 2A.4.<br>3. säkerställa en utvärdering av all känd och relevant information om de informationssäkerhetsincidenter och sårbarheter som identifierats i enlighet med punkt (1) ovan;<br>4. säkerställa implementeringen av en metod för att internt distribuera informationen efter behov.<br><br>Det interna rapporteringssystem ska beakta att alla anlitade organisationer, som kan utsätta organisationen för informationssäkerhetsrisker med potentiell inverkan på flygsäkerheten, rapporterar informationssäkerhetshändelser till organisationen och lämnar in dessa rapporter enligt kontraktsprocedurer.<br><br>Detta kapitel bör också beskriva hur organisationen samarbetar i utredningar med andra organisationer som har ett betydande bidrag till informationssäkerheten i sin egen verksamhet.<br><br>De förfaranden som beskrivs i detta kapitel måste tydligt specificera vilka personer som är inblandade och vad deras roller och ansvarsområden är, särskilt i fråga om:<br><br>- Utvärdering av rapporterade händelser.<br>- Beslutet om vilka händelser som anses vara incidenter och/eller sårbarheter med potentiell inverkan på säkerheten. | |

| | | |
|---|---|---|
| 2A.4 | **Information Security Incidents – Detection, Response and Recovery**<br><br>Detta kapitel beskriver följande:<br><br>(a) Procedurer för att genomföra åtgärder för att upptäcka incidenter och sårbarheter som indikerar en potentiell oacceptabel risk och som kan ha en inverkan på flygsäkerheten. Dessa detekteringsåtgärder ska göra det möjligt för organisationen att:<br><br>1. identifiera avvikelser från förutbestämda funktionella prestandabaslinjer;<br><br>2. utlösa varningar för att aktivera lämpliga responsåtgärder i händelse av avvikelser.<br><br>(b) Procedurer för att genomföra åtgärder för att reagera på alla händelseförhållanden som identifierats i enlighet med punkt (a) och som kan utvecklas eller har utvecklats till en informationssäkerhetsincident.<br><br>Dessa responsåtgärder ska göra det möjligt för organisationen att:<br><br>1. initiera åtgärder på de varningar som avses i punkt (a)(2) genom att aktivera fördefinierade resurser och åtgärdsplaner;<br>2. begränsa spridningen av en attack och undvika att ett hotscenario utvecklas fullt ut;<br>3. kontrollera felläget för de berörda elementen som definieras i punkt IS.I.OR.205(a).<br><br>(c) Procedur för att genomföra åtgärder som syftar till att återhämta sig från informationssäkerhetsincidenter, inklusive nödåtgärder, om det behövs.<br><br>Dessa återställningsåtgärder ska göra det möjligt för organisationen att:<br><br>1. undanröja det tillstånd som orsakade incidenten, eller begränsa den till en acceptabel nivå;<br>2. uppnå ett säkert tillstånd för de berörda elementen som definieras i punkt IS.I.OR.205(a) inom en återställningstid som definierats av organisationen. | |

| | | |
|---|---|---|
| 2A.5 | **Information Security External Reporting Scheme**<br><br>Detta kapitel kan integrera information med CAME kapitel 2.11<br><br>Beskriv det externa rapporteringssystemet för informationssäkerhet som organisationen har implementerat för att säkerställa att alla informationssäkerhetsincidenter eller sårbarheter som kan utgöra en betydande risk för flygsäkerheten rapporteras till Transportstyrelsen.<br><br>(1) Om en sådan incident eller sårbarhet påverkar ett luftfartyg eller tillhörande system eller komponent ska organisationen också rapportera det till innehavaren av konstruktionsgodkännandet;<br><br>(2) Om en sådan incident eller sårbarhet påverkar ett system eller en komponent som används av organisationen ska organisationen rapportera det till den organisation som ansvarar för konstruktionen av systemet eller komponenten.<br><br>Detta externa rapporteringssystem ska omfatta:<br><br>(1) Inlämning av en anmälan till Transportstyrelsen och i förekommande fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som tillståndet har blivit känt för organisationen;<br><br>(2) Inlämning av en rapport till Transportstyrelsen och i förekommande fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, så snart som möjligt, men inte överstigande 72 timmar från det att tillståndet har blivit känt för organisationen, såvida inte exceptionella omständigheter förhindrar detta.<br><br>(3) Inlämning av en uppföljningsrapport till Transportstyrelsen och i förekommande fall, till innehavaren av konstruktionsgodkännandet eller till den organisation som ansvarar för konstruktionen av systemet eller komponenten, med detaljer om de åtgärder som organisationen har vidtagit eller avser att vidta för att återhämta sig från incidenten och de åtgärder den avser att vidta för att förhindra liknande informationssäkerhetsincidenter i framtiden. Denna uppföljningsrapport ska lämnas in så snart dessa åtgärder har identifierats.<br><br>Procedurer i detta kapitel måste tydligt specificera vilka personer som är inblandade och vad deras roller och ansvarsområden är, särskilt i fråga om:<br><br>- Beslutet om vilka incidenter och/eller sårbarheter som behöver rapporteras externt eftersom de kan utgöra en betydande risk för flygsäkerheten.<br><br>- Utvärderingen av dessa incidenter och sårbarheter.<br><br>- Utarbetande och godkännande av tillämpliga rapporter, samt inlämning av sådana rapporter till den behöriga myndigheten och, i förekommande fall, till innehavaren av konstruktionsgodkännandet och/eller till den organisation som ansvarar för konstruktionen av det berörda systemet eller den berörda komponenten. | |

| | | |
|---|---|---|
| 2A.5 forts. | Dessa procedurer behöver också specificera:<br><br>• De metoder som används för rapportering.<br>• Tidsfristerna för rapportering (inklusive initial anmälan, uppföljning/analys och avslutande av utredning)<br>• De sekretessåtgärder som införts för att skydda den anmälande personens och de personers identitet som nämns i rapporterna.<br>• De kategorier som införts för att definiera rapporternas status.<br>• Behovet av att rapporter innehåller relevant information och utvärdering av resultat (där sådana är kända)<br>• Rapportfält som måste fyllas i<br>• Behovet av att beakta händelser som rapporterats av underleverantörer<br>• Behovet av att uppföljningsrapporter ger information om de åtgärder som organisationen avser att vidta för att förhindra liknande händelser i framtiden så snart dessa åtgärder har identifierats.<br><br>Rapportering sker via ECCAIRS 2. Information finns på Transportstyrelsen hemsida: “Rapportera luftfartshändelse” på www.transportstyrelsen.se (Organisationer beställer egna konton) | |
| 2A.6 | **Contracting of Information Security Activities**<br><br>Lista över kontrakterade organisationer för informationssäkerhets aktiviteter, namn och kontaktuppgifter<br><br>Procedur hur organisationen säkerställer att när någon del av informationssäkerhets aktiviteterna som avses i punkt IS.I.OR.200 kontrakteras till andra organisationer.<br>Att de avtalade aktiviteterna uppfyller kraven i denna förordning och att den kontrakterade organisationen arbetar under organisationens tillstånd.<br><br>Proceduren ska säkerställa att riskerna i samband med de avtalade aktiviteterna hanteras på lämpligt sätt.<br><br>Process för att organisationen ska vidta lämpliga åtgärder för att säkerställa att Transportstyrelsen på begäran kan kontakta den avtalade organisationen för att fastställa fortsatt efterlevnad av de tillämpliga kraven i denna förordning. Detta bör specificeras i motsvarande avtal. | |

| | | |
|---|---|---|
| 2A.7 | **Personnel requirements**<br><br>Detta kapitel kan integrera information med CAME kapitel 0.3, 0.5, 2.8.6 och 2.9.<br><br>Procedurer för utvärdering av kompetens för all personal:<br><br>(a) Kvalifikationskraven som gäller för personal som är involverad i Del-IS-aktiviteter, så att organisationen kan säkerställa att de har den kompetens som krävs för att utföra sina uppgifter. OBS: Kvalifikationskraven för personal för regelefterlevnadsövervakning behandlas i kapitel 2.8.6.<br><br>(b) Den process som finns på plats för att säkerställa att personalen bekräftar det ansvar som är förknippat med de tilldelade<br>rollerna och uppgifterna.<br><br>(c) En fördefinierad klassificering av nivåer av tillförlitlighet som krävs för att personal ska få tillgång till de olika informationssystem och data som används av organisationen, beroende på hur allvarliga de säkerhetskonsekvenser som identifierats genom den tillämpliga riskbedömningen.<br><br>(d) Det förfarande som används för att verifiera identiteten och bedöma nivån av tillförlitlighet hos den personal som beskrivs i punkt (c) ovan (vägledning finns i GM1 IS.I.OR.240(i)) | |
| 2A.8 | **Record-keeping**<br><br>Detta kapitel beskriver procedurer, metod/format och åtgärder som organisationen har implementerat för att säkerställa att:<br><br>(a) Organisationen förvarar register över följande informationssäkerhetshanteringsaktiviteter under de angivna perioderna:<br><br>(1) alla godkännanden som erhållits och alla tillhörande riskbedömningar för informationssäkerhet i enlighet med punkt IS.I.OR.200(e). Dessa register ska bevaras i minst 5 år efter att godkännandet har förlorat sin giltighet;<br><br>(2) avtal för verksamheter som avses i punkt IS.I.OR.200(a)(9). Dessa avtal ska bevaras i minst 5 år efter att avtalet har ändrats eller sagts upp;<br><br>(3) register över de viktigaste processer som avses i punkt IS.I.OR.200(d). Dessa register ska bevaras i minst 5 år;<br><br>(4) register över de risker som identifierats i den riskbedömning som avses i punkt IS.I.OR.205 tillsammans med de tillhörande riskhanteringsåtgärder som avses i punkt IS.I.OR.210. Dessa register ska bevaras i minst 5 år;<br><br>(5) register över informationssäkerhetsincidenter och sårbarheter som rapporterats i enlighet med de rapporteringssystem som avses i punkterna IS.I.OR.215 och IS.I.OR.230. Dessa register ska bevaras i minst 5 år;<br><br>(6) register över de informationssäkerhetshändelser som kan behöva omprövas för att avslöja oupptäckta informationssäkerhetsincidenter eller sårbarheter. Dessa register ska bevaras åtminstone tills dessa informationssäkerhetshändelser har omprövats i enlighet med en periodicitet som definieras i ett förfarande som fastställts av organisationen. | |

| | | |
|---|---|---|
| 2A.8 Forts. | (b) Organisationen behåller register över kvalifikationer och erfarenhet för sin egen personal som är involverad i informationssäkerhetshantering under de angivna perioderna:<br><br>(1) Personalens kvalifikations- och erfarenhetsregister ska behållas så länge personen arbetar för organisationen, och i minst 3 år efter att personen har lämnat organisationen.<br>(2) Personalen ska, på begäran, ges tillgång till sina individuella register. Dessutom ska organisationen, på begäran, förse dem med en kopia av sina individuella register när de lämnar organisationen.<br><br>(c) Organisationen lagrar de ovan beskrivna registren på ett sätt som säkerställer skydd mot skador, ändringar och stöld, med information identifierad, vid behov, i enlighet med dess säkerhetsklassificeringsnivå. Organisationen ska säkerställa att registren lagras med hjälp av metoder som säkerställer integritet, äkthet och behörig åtkomst. | |
| 2A.9 | **Continuous Improvement**<br><br>Detta kapitel bör beskriva hur organisationen, med hjälp av lämpliga prestationsindikatorer, bedömer ledningssystemets effektivitet och mognad. Denna bedömning ska genomföras enligt en kalender som fördefinierats av organisationen eller efter en informationssäkerhetsincident.<br><br>Om brister upptäcks efter den bedömning som utförts i enlighet med punkt (a), ska organisationen vidta nödvändiga förbättringsåtgärder för att säkerställa att ledningssystemet fortsätter att uppfylla tillämpliga krav och upprätthåller informationssäkerhetsriskerna på en acceptabel nivå. Dessutom ska organisationen ompröva de delar av ledningssystemet som påverkas av de antagna åtgärderna.<br><br>Viktiga aspekter att ta hänsyn till vid utveckling av rutiner för "Kontinuerlig förbättring" är följande:<br><br>• Kontinuerlig förbättring är kopplad till regelefterlevnadsövervakning.<br><br>• Det måste finnas ett åtagande att åtminstone upprätthålla, och om möjligt förbättra, säkerhetsnivån, med hänsyn till att både säkerhetsmiljön och organisationen ständigt utvecklas. Det finns ett behov av att organisationen dynamiskt anpassar sig till:<br><br>- Ständigt nya sårbarheter, hotaktörer, verktyg och metoder, vilket kan minska effektiviteten hos befintliga kontroller.<br>- Förändringar i organisationens mål, arkitekturer, organisatoriska strukturer och processer, vilket kan minska efterlevnadsnivån.<br>-<br>• Det är viktigt att säkerställa att det inte sker någon försämring av prestandan. Nyckeltal (KPI:er) behöver användas för att mäta om det utförda arbetet försämras och för att bedöma ledningssystemets effektivitet och mognad. | |

| | | |
|---|---|---|
| 2A.9 Forts. | ***Typiska <u>exempel</u> på nyckeltal (KPI:er) som kan fastställas för att bedöma ledningssystemets effektivitet och mognad är följande:***<br><br>*• Angående "Riskbedömning och behandling":*<br>- *Antal identifierade risker: Spåra förändringar i antalet identifierade risker under bedömningar.*<br>- *Tid för att minska risker: Genomsnittlig tid för att implementera riskhanteringsåtgärder.*<br>-<br>*• Angående "Policyer och rutiner":*<br>- *Efterlevnadsgrad av policy: % av anställda som följer säkerhetspolicyer baserat på revisionsresultat.*<br>- *Antal avvikelser: Problem med bristande efterlevnad som identifierats under interna/externa revisioner.*<br>-<br>*• Angående "Säkerhetskontroller (åtgärder)":*<br>- *Överträdelser av åtkomstkontroll: Antal upptäckta obehöriga åtkomstförsök eller intrång. o Logggranskningstäckning: Andel av säkerhetsloggar som granskats inom en definierad tidsram.*<br>-<br>*• Angående "Incidenthantering":*<br>- *Incidentlösningstid: Genomsnittlig tid som krävs för att lösa rapporterade incidenter.*<br>- *Driftstopp på grund av säkerhetsincidenter: Totalt antal kritiska (säkerhets)system var otillgängliga.*<br>-<br>*• Angående "Utbildning och medvetenhet":*<br>- *Andel genomförda utbildningar: % av anställda som genomför säkerhetsutbildning.*<br>- *Resultat av nätfiskesimulering: Antal anställda som framgångsrikt identifierat nätfiskeförsök.* | |
| 2A.10 | **Protection of confidentiality of information received from other parties**<br><br>Detta kapitel beskriver de förfaranden som används av organisationen för att skydda sekretessen för all information som organisationen kan ha mottagit från andra organisationer, i enlighet med dess känslighetsnivå.<br><br>För detta ändamål bör organisationen upprätta ett informationsklassificeringsschema i enlighet med informationens känslighetsnivå, och bör implementera och upprätthålla informationssäkerhetskontroller som är tillräckligt robusta och effektiva för att skydda information och säkerställa principen om behov (dvs. begränsa åtkomsten till information till endast de som behöver den för att utföra sina uppgifter). Den bör skydda informationskällan i enlighet med de relevanta bestämmelserna i förordning (EU) 2018/1139. Den bör också följa förordning (EU) nr 376/2014. | |