Europeiska unionens
officiella tidning

SV
L-serien

2025/302

20.2.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/302

av den 23 oktober 2024

om fastställande av tekniska genomförandestandarder för tillämpningen av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller standardformulär, mallar och förfaranden för att finansiella entiteter ska kunna rapportera allvarliga IKT-relaterade incidenter och anmäla betydande cyberhot

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 ([1]), särskilt artikel 20 fjärde stycket, och

av följande skäl:

(1) För att säkerställa att finansiella entiteter rapporterar allvarliga incidenter till sina behöriga myndigheter på ett konsekvent sätt och för att säkerställa att de förser dessa myndigheter med uppgifter av god kvalitet bör det specificeras vilka datafält finansiella entiteter måste tillhandahålla i de olika skedena av den rapportering som avses i artikel 19.4 i förordning (EU) 2022/2554. Det är viktigt att denna information presenteras på ett sätt som möjliggör en samlad översikt över incidenten. Det är därför nödvändigt att fastställa en gemensam rapporteringsmall för dessa ändamål.

(2) Finansiella entiteter bör fylla i de datafält i rapporteringsmallen som motsvarar informationskraven för respektive anmälan eller rapport. Finansiella entiteter som redan har information som de ska lämna in i ett senare rapporteringsskede, dvs. i delrapporten eller slutrapporten, bör dock tillåtas att lämna in uppgifterna i förväg.

(3) Eftersom flera eller återkommande incidenter kan utgöra en allvarlig incident enligt artikel 8 i kommissionens delegerade förordning (EU) 2024/1772 ([2]) bör utformningen av rapporteringsmallen och datafälten göra det möjligt för finansiella entiteter att rapportera sådana återkommande incidenter.

(4) För att säkerställa korrekt och aktuell information bör rapporteringsmallen göra det möjligt för finansiella entiteter att, när de lämnar in del- och slutrapporten, uppdatera all information som lämnats tidigare och vid behov omklassificera allvarliga incidenter som icke-allvarliga.

(5) Den rättsliga identifieringen av entiteter bör anpassas till de identifikatorer som anges i de tekniska genomförandestandarder som antagits i enlighet med artikel 28.9 i förordning (EU) 2022/2554.

(6) Om finansiella entiteter utkontrakterar rapporteringsskyldigheten avseende allvarliga IKT-relaterade incidenter till en tredje part bör de behöriga myndigheterna känna till identiteten på den tredje part som utför rapporteringen för den finansiella entitetens räkning innan den första anmälan eller rapporterna lämnas in för att kontrollera den rapporterande tredje partens legitimitet.

([1]) EUT L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Kommissionens delegerade förordning (EU) 2024/1772 av den 13 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska standarder för tillsyn som specificerar kriterierna för klassificering av IKT-relaterade incidenter och cyberhot, fastställande av väsentlighetströsklar och närmare uppgifter om rapporter om allvarliga incidenter (EUT L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) För att enkelt kunna fastställa effekterna av en incident som inträffat hos eller orsakats av en tredjepartsleverantör och som påverkar flera finansiella entiteter inom en enda medlemsstat, och för att minska rapporteringsbördan för de finansiella entiteterna, bör rapporteringsmallen göra det möjligt att lämna in en aggregerad rapport som omfattar aggregerad information om incidentens inverkan på alla finansiella entiteter som påverkats och som har klassificerat incidenten som allvarlig.

(8) Rapporteringsmallen bör utformas på ett teknikneutralt sätt så att den kan användas i olika lösningar för incidentrapportering som redan finns eller som kan utvecklas för genomförandet av kraven i förordning (EU) 2022/2554.

(9) Utformningen av rapporteringsmallen och datafälten bör underlätta rapporteringen av allvarliga IKT-relaterade incidenter för tredje parter till vilka finansiella entiteter har utkontrakterat sin rapporteringsskyldighet i enlighet med artikel 19.5 i förordning (EU) 2022/2554.

(10) Denna förordning grundar sig på det förslag till tekniska genomförandestandarder som de europeiska tillsynsmyndigheterna har lagt fram för kommissionen.

(11) De europeiska tillsynsmyndigheterna har anordnat öppna offentliga samråd om de förslag till tekniska genomförandestandarder som den här förordningen grundas på, gjort en analys av möjliga kostnader och fördelar samt begärt råd från den bankintressentgrupp som inrättats i enlighet med artikel 37 i Europaparlamentets och rådets förordningar (EU) nr 1093/2010 ([3]), (EU) nr 1094/2010 ([4]) och (EU) nr 1095/2010 ([5]).

(12) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]) och avgav ett positivt yttrande den 22 juli 2024. All behandling av personuppgifter som omfattas av denna förordning bör utföras i enlighet med de tillämpliga principerna för och bestämmelserna om dataskydd i förordning (EU) 2018/1725.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Mall för rapportering av allvarliga IKT-relaterade incidenter

1. Finansiella entiteter ska använda mallen i bilaga I för att lämna in den första anmälan, delrapport och slutrapport som avses i artikel 19.4 i förordning (EU) 2022/2554 enligt följande:

a) Finansiella entiteter som lämnar in en första anmälan ska fylla i de datafält i mallen som motsvarar den information som ska tillhandahållas i enlighet med artikel 2 i kommissionens delegerade förordning (EU) 2025/301 ([7]), och får, om de redan har denna information, fylla i de datafält som inte behöver fyllas i vid en första anmälan men som krävs för en delrapport eller slutrapport.

([3]) Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (EUT L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Europaparlamentets och rådets förordning (EU) nr 1094/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska försäkrings- och tjänstepensionsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/79/EG (EUT L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Europaparlamentets och rådets förordning (EU) nr 1095/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska värdepappers- och marknadsmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/77/EG (EUT L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Kommissionens delegerade förordning (EU) 2025/301 av den 23 oktober 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2022/2554 vad gäller tekniska tillsynsstandarder som specificerar innehåll och tidsfrister för den första anmälan av, delrapporten och slutrapporten om allvarliga IKT-relaterade incidenter samt innehållet i den frivilliga anmälan av betydande cyberhot (EUT L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) Finansiella entiteter som lämnar in en delrapport ska fylla i de datafält i mallen som motsvarar den information som ska tillhandahållas i enlighet med artikel 3 i delegerad förordning (EU) 2025/301, och får, om de redan har den relevanta informationen, fylla i de datafält som inte behöver fyllas för delrapporten men som krävs för slutrapporten.

c) Finansiella entiteter som lämnar in en slutrapport ska fylla i de datafält i mallen som motsvarar den information som ska tillhandahållas i enlighet med artikel 3 i delegerad förordning (EU) 2025/301.

2. Finansiella entiteter ska säkerställa att informationen i den första anmälan samt i del- och slutrapporten är fullständig och korrekt.

3. Finansiella entiteter ska i möjligaste mån tillhandahålla uppskattade värden baserade på andra tillgängliga uppgifter och annan tillgänglig information om korrekta uppgifter inte finns tillgängliga vid tidpunkten för rapporteringen med avseende på den första anmälan eller delrapporten.

4. När finansiella entiteter lämnar in en delrapport eller slutrapport ska de använda mallen i bilaga I för att lämna all information som krävs och i tillämpliga fall uppdatera den information som tidigare tillhandahölls i den första anmälan eller i delrapporten.

5. Finansiella entiteter ska följa ordlistan och instruktionerna i bilaga II när de fyller i mallen i bilaga I.

Artikel 2

Gemensam inlämning av den första anmälan, delrapporten och slutrapporten

Finansiella entiteter får kombinera inlämningen av den första anmälan, delrapporten och slutrapporten genom att tillhandahålla två av dem eller alla samtidigt om den regelbundna verksamhet har återhämtat sig eller om analysen av de grundläggande orsakerna har slutförts och förutsatt att de tidsfrister som anges i artikel 5 i delegerad förordning (EU) 2025/301 uppfylls.

Artikel 3

Återkommande IKT-relaterade incidenter

Finansiella entiteter som tillhandahåller information om icke-allvarliga återkommande IKT-relaterade incidenter som kumulativt uppfyller villkoren för en allvarlig IKT-relaterad incident enligt artikel 8.2 i delegerad förordning (EU) 2024/1772 ska tillhandahålla denna information i aggregerad form.

Artikel 4

Användning av säkra elektroniska kanaler

1. Finansiella entiteter ska använda säkra elektroniska kanaler som har gjorts tillgängliga av deras behöriga myndighet för att lämna in den första anmälan samt delrapporten och slutrapporten.

2. Finansiella entiteter som inte kan använda de säkra elektroniska kanaler som tillhandahålls av deras behöriga myndighet ska informera sin behöriga myndighet om en allvarlig IKT-relaterad incident på ett annat säkert sätt i samförstånd med den behöriga myndigheten. Om den behöriga myndigheten så kräver ska de finansiella entiteterna lämna in den första anmälan eller del- eller slutrapporten på nytt, via den säkra elektroniska kanal som gjorts tillgänglig av deras behöriga myndighet så snart de har möjlighet att göra detta.

Artikel 5

Omklassificering av en allvarlig IKT-relaterad incident

Om den finansiella entiteten efter en ytterligare bedömning konstaterar att den IKT-relaterade incident som tidigare rapporterats vara allvarlig inte vid något tillfälle uppfyllde de klassificeringskriterier och tröskelvärden som anges i artikel 8 i delegerad förordning (EU) 2024/1772 ska den finansiella entiteten underrätta den behöriga myndigheten om att den har omklassificerat den IKT-relaterade incidenten från allvarlig till icke-allvarlig genom att tillhandahålla information om denna omklassificering i mallen i bilaga II till denna förordning i fälten för ”typ av rapport” och ”annan information”.

Artikel 6

Anmälan om utkontraktering av rapporteringsskyldigheter

1. Finansiella entiteter som har utkontrakterat skyldigheten att rapportera allvarliga IKT-relaterade incidenter i enlighet med artikel 19.5 i förordning (EU) 2022/2554 ska informera sin behöriga myndighet om detta arrangemang så snart utkontrakteringsarrangemanget har slutförts och senast före den första anmälan eller rapporteringen.

2. Finansiella entiteter ska förse den behöriga myndigheten med namn, kontaktuppgifter och identifikationskod för den tredje part som ska lämna in anmälningarna eller rapporterna om den allvarliga IKT-relaterade incidenten åt dem.

3. Finansiella entiteter ska informera sin behöriga myndighet så fort de inte längre utkontrakterar sina rapporterings-skyldigheter enligt artikel 19.5 i förordning (EU) 2022/2554.

Artikel 7

Aggregerad rapportering

1. En tredjepartsleverantör till vilken rapporteringsskyldigheter har utkontrakterats enligt artikel 19.5 i förordning (EU) 2022/2554 får använda mallen i bilaga I till denna förordning för att tillhandahålla aggregerad information om en allvarlig IKT-relaterad incident som påverkar flera finansiella entiteter i en enda anmälan eller rapport och lämna in denna anmälan eller rapport till den behöriga myndigheten för alla berörda finansiella entiteters räkning, förutsatt att samtliga följande villkor är uppfyllda:

a) Den allvarliga IKT-relaterade incident som ska rapporteras härrör från eller orsakas av en tredjepartsleverantör av IKT-tjänster.

b) Tredjepartsleverantören tillhandahåller den relevanta IKT-tjänsten till mer än en finansiell entitet eller till en koncern.

c) Den IKT-relaterade incidenten klassificeras som allvarlig av varje finansiell entitet som omfattas av den aggregerade anmälan eller rapporten.

d) Den allvarliga IKT-relaterade incidenten påverkar finansiella entiteter inom en enda medlemsstat och den aggregerade rapporten avser finansiella entiteter som står under samma behöriga myndighets tillsyn.

e) Behöriga myndigheter har uttryckligen tillåtit denna typ av finansiella entiteter att aggregera sin rapportering.

2. Punkt 1 ska inte tillämpas på kreditinstitut som anses vara betydande enligt artikel 2.16 i Europeiska centralbankens förordning (EU) nr 468/2014 ([8]), operatörer av handelsplatser och centrala motparter. De ska endast använda mallen i bilaga I för att lämna in anmälningar eller rapporter om allvarliga IKT-relaterade incidenter individuellt till sin behöriga myndighet.

3. Om de behöriga myndigheterna behöver information om den allvarliga IKT-relaterade incidentens enskilda effekter på en specifik finansiell entitet ska den finansiella entiteten på begäran av den behöriga myndigheten lämna in en individuell anmälan eller rapport om den allvarliga IKT-relaterade incidenten.

([8]) Europeiska centralbankens förordning (EU) nr 468/2014 av den 16 april 2014 om upprättande av ramen för samarbete inom den gemensamma tillsynsmekanismen mellan Europeiska centralbanken och nationella behöriga myndigheter samt med nationella utsedda myndigheter (ramförordning om den gemensamma tillsynsmekanismen [SSM]) (ECB/2014/17) (EUT L 141, 14.5.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Artikel 8

Anmälan av betydande cyberhot

1. Finansiella entiteter som anmäler betydande cyberhot till behöriga myndigheter i enlighet med artikel 19.2 i förordning (EU) 2022/2554 ska använda mallen i bilaga III till denna förordning och följa ordlistan och instruktionerna i bilaga IV till denna förordning.

2. Finansiella entiteter ska säkerställa att informationen i anmälan av betydande cyberhot är fullständig och korrekt.

Artikel 9

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 23 oktober 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

MALLAR FÖR RAPPORTERING AV ALLVARLIGA INCIDENTER

Fältets nummer	Datafält	
Allmän information om den finansiella entiteten		
1.1	Typ av inlämning	
1.2	Namnet på den entitet som lämnar in rapporten	
1.3	Identifieringskod för den entitet som lämnar in rapporten	
1.4	Typ av berörd finansiell entitet	
1.5	Namnet på den berörda finansiella entiteten	
1.6	LEI-kod för den berörda finansiella entiteten	
1.7	Namnet på den primära kontaktpersonen	
1.8	E-postadress till den primära kontaktpersonen	
1.9	Telefonnummer till den primära kontaktpersonen	
1.10	Namnet på den sekundära kontaktpersonen	
1.11	E-postadress till den sekundära kontaktpersonen	
1.12	Telefonnummer till den sekundära kontaktpersonen	
1.13	Namnet på det yttersta moderföretaget	
1.14	LEI-kod för det yttersta moderföretaget	
1.15	Rapporteringsvaluta	
Innehållet i den första anmälan		
2.1	Incidentens referenskod som tilldelats av den finansiella entiteten	
2.2	Datum och tidpunkt för upptäckten av den allvarliga IKT-relaterade incidenten	
2.3	Datum och tidpunkt då den IKT-relaterade incidenten klassificerades som allvarlig	
2.4	Beskrivning av den allvarliga IKT-relaterade incidenten	
2.5	Klassificeringskriterier som utlöste incidentrapporten	
2.6	Väsentlighetströsklar för klassificeringskriteriet Geografisk spridning	
2.7	Upptäckten av den allvarliga IKT-relaterade incidenten	

Fältets nummer	Datafält	
2.8	Indikation om huruvida den allvarliga IKT-relaterade incidenten har sitt ursprung hos en tredjepartsleverantör eller en annan finansiell entitet	
2.9	Aktivering av planen för driftskontinuitet, om aktiverad	
2.10	Annan relevant information	
Delrapportens innehåll		
3.1	Incidentens referenskod som tillhandahållits av den behöriga myndigheten	
3.2	Datum och tidpunkt då den allvarliga IKT-relaterade incidenten inträffade	
3.3	Datum och tidpunkt då tjänster, verksamheter eller insatser återställdes	
3.4	Antal berörda kunder	
3.5	Andel berörda kunder (i procent)	
3.6	Antal berörda finansiella motparter	
3.7	Andel berörda finansiella motparter (i procent)	
3.8	Inverkan på relevanta kunder eller finansiella motparter	
3.9	Antal berörda transaktioner	
3.10	Andel berörda transaktioner (i procent)	
3.11	Värdet på de berörda transaktionerna	
3.12	Uppgifter om huruvida siffrorna är faktiska eller uppskattade eller om det inte har förekommit någon inverkan	
3.13	Påverkan på anseendet	
3.14	Bakgrundsinformation om påverkan på anseendet	
3.15	Den allvarliga IKT-relaterade incidentens varaktighet	
3.16	Driftstopp	
3.17	Information om huruvida siffrorna för varaktighet och driftstopp är faktiska eller uppskattade	
3.18	Typer av effekter i medlemsstaterna	
3.19	Beskrivning av hur den allvarliga IKT-relaterade incidenten påverkar andra medlemsstater	
3.20	Väsentlighetströsklar för klassificeringskriteriet Dataförluster	
3.21	Beskrivning av dataförlusterna	

Fältets nummer	Datafält	
3.22	Klassificeringskriteriet Berörda kritiska tjänster	
3.23	Typ av allvarlig IKT-relaterad incident	
3.24	Andra typer av incidenter	
3.25	Hot och tillvägagångssätt som använts av den fientliga aktören	
3.26	Andra typer av tillvägagångssätt	
3.27	Information om berörda funktionella områden och affärsprocesser	
3.28	Berörda infrastrukturkomponenter som stöder affärsprocesser	
3.29	Information om berörda infrastrukturkomponenter som stöder affärsprocesser	
3.30	Inverkan på kundernas finansiella intressen	
3.31	Rapportering till andra myndigheter	
3.32	Specifikation av ”annan” myndighet	
3.33	Tillfälliga åtgärder som vidtagits eller planeras för återställning efter incidenten	
3.34	Beskrivning av alla tillfälliga åtgärder som vidtagits eller planeras för återställning efter incidenten	
3.35	Angreppsindikator	
Slutrapportens innehåll		
4.1	Högnivåklassificering av grundläggande orsaker till incidenten	
4.2	Detaljerad klassificering av grundläggande orsaker till incidenten	
4.3	Ytterligare klassificering av grundläggande orsaker till incidenten	
4.4	Andra typer av grundläggande orsaker	
4.5	Information om grundläggande orsaker till incidenten	
4.6	Sammanfattning av åtgärdandet av incidenten	
4.7	Datum och tid då de grundläggande orsakerna till incidenten hanterades	
4.8	Datum och tid då incidenten åtgärdades	
4.9	Information om datumet för det permanenta åtgärdandet av incidenten skiljer sig från det ursprungligen planerade genomförandedatumet	
4.10	Bedömning av risker för kritiska funktioner för resolutionssyften	
4.11	Information som är relevant för resolutionsmyndigheter	

Fältets nummer	Datafält	
4.12	Väsentlighetströskel för klassificeringskriteriet Ekonomiska effekter	
4.13	Belopp för direkta och indirekta bruttokostnader och bruttoförluster	
4.14	Belopp för finansiella återkrav	
4.15	Information om huruvida de icke-allvarliga incidenterna har varit återkommande	
4.16	Datum och tidpunkt för återkommande incidenter	

BILAGA II

ORDLISTA OCH INSTRUKTIONER FÖR RAPPORTERING AV ALLVARLIGA INCIDENTER

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
Allmän information om den finansiella entiteten					
1.1. Typ av inlämning	Ange vilken typ av incidentanmälan eller incidentrapport som lämnas in till den behöriga myndigheten.	Ja	Ja	Ja	Val: — Första anmälan, — Delrapport, — Slutrapport, — Allvarlig incident som omklassificerats som icke-allvarlig.
1.2 Namnet på den entitet som lämnar in rapporten	Fullständigt juridiskt namn på den entitet som lämnar in rapporten.	Ja	Ja	Ja	Alfanumeriskt värde
1.3 Identifieringskod för den entitet som lämnar in rapporten	Identifieringskod för den entitet som lämnar in rapporten. Om de finansiella entiteterna lämnar in anmälan/rapporten ska identifieringskoden vara en identifieringskod för juridiska personer (LEI-kod), som är en unik kod med 20 alfanumeriska tecken, på grundval av ISO 17442–1:2020. En tredjepartsleverantör som lämnar in en rapport för en finansiell entitet kan använda en identifieringskod i enlighet med de tekniska genomförandestandarder som antagits i enlighet med artikel 28.9 i förordning (EU) 2022/2554..	Ja	Ja	Ja	Alfanumeriskt värde
1.4 Typ av berörd finansiell entitet	Typ av entitet som avses i artikel 2.1 a–t i förordning (EU) 2022/2554 för vilken rapporten lämnas in. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska de olika typer av finansiella entiteter som omfattas av den aggregerade rapporten väljas.	Ja	Ja	Ja	Val (flera val kan göras): — Kreditinstitut, — Betalningsinstitut, — Undantaget betalningsinstitut, — Leverantör av kontoinformationstjänster, — Institut för elektroniska pengar, — Undantaget institut för elektroniska pengar, — Värdepappersföretag — Leverantör av kryptotillgångstjänster, — Emittent av tillgångsanknutna token, — Värdepapperscentral, — Central motpart, — Handelsplats, — Transaktionsregister,

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
						— Förvaltare av alternativa investeringsfonder, — Förvaltningsbolag, — Leverantör av datarapporteringstjänster, — Försäkrings- och återförsäkringsföretag, — Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet, — Tjänstepensionsinstitut, — Kreditvärderingsinstitut, — Administratör av kritiska referensvärden, — Leverantör av gräsrotsfinansieringstjänster, — Värdepapperiseringsregister.
1.5	Namnet på den berörda finansiella entiteten	Fullständigt juridiskt namn på den finansiella entitet som berörs av den allvarliga IKT-relaterade incidenten och som ska rapportera den allvarliga incidenten till sin behöriga myndighet enligt artikel 19 i förordning (EU) 2022/2554. Vid aggregerad rapportering: a) En förteckning över alla namn på de finansiella entiteter som berörs av den allvarliga IKT-relaterade incidenten, med ett semikolon emellan, b) Den tredjepartsleverantör som lämnar in en anmälan om en allvarlig incident eller en rapport på ett aggregerat sätt enligt artikel 7 i denna förordning ska ange namnen på alla finansiella entiteter som berörs av incidenten, med ett semikolon emellan.	Ja, om den finansiella entitet som berörs av incidenten är en annan än den entitet som lämnar in rapporten och vid aggregerad rapportering.	Ja, om den finansiella entitet som berörs av incidenten är en annan än den entitet som lämnar in rapporten och vid aggregerad rapportering	Ja, om den finansiella entitet som berörs av incidenten är en annan än den entitet som lämnar in rapporten och vid aggregerad rapportering	Alfanumeriskt värde
1.6	LEI-kod för den berörda finansiella entiteten	Identifieringskoden för juridiska personer (LEI-koden) för den finansiella entitet som berörs av den allvarliga IKT-relaterade incidenten, vilken tilldelats i enlighet med Internationella standardiseringsorganisationen. Vid aggregerad rapportering: a) En förteckning med alla LEI-koder för de finansiella entiteter som berörs av den allvarliga IKT-relaterade incidenten, med ett semikolon emellan,	Ja, om den finansiella entitet som berörs av den allvarliga IKT-relaterade	Ja, om den finansiella entitet som berörs av den allvarliga IKT-relaterade incidenten är en annan än	Ja, om den finansiella entitet som berörs av den allvarliga IKT-relaterade	En unik kod med 20 alfanumeriska tecken, på grundval av ISO 17442–1:2020

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
		b) Den tredjepartsleverantör som lämnar in en anmälan eller rapport om en allvarlig incident eller på ett aggregerat sätt enligt artikel 7 i denna förordning ska ange LEI-koderna för alla finansiella entiteter som berörs av incidenten, med ett semikolon emellan. Ordningsföljden för LEI-koderna och namnen på de finansiella entiteterna ska vara densamma.	incidenten är en annan än den entitet som lämnar in rapporten och vid aggregerad rapportering.	den entitet som lämnar in rapporten och vid aggregerad rapportering.	incidenten är en annan än den entitet som lämnar in rapporten och vid aggregerad rapportering	
1.7.	Namnet på den primära kontaktpersonen	Namn och efternamn på den finansiella entitetens primära kontaktperson. Vid aggregerad rapportering enligt artikel 7 i denna förordning, namnet på den primära kontaktpersonen för den entitet som lämnar in den aggregerade rapporten.	Ja	Ja	Ja	Alfanumeriskt värde
1.8	E-postadress till den primära kontaktpersonen	E-postadress till den primära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation. Vid aggregerad rapportering enligt artikel 7 i denna förordning, e-postadressen till den primära kontaktpersonen för den entitet som lämnar in den aggregerade rapporten.	Ja	Ja	Ja	Alfanumeriskt värde
1.9	Telefonnummer till den primära kontaktpersonen	Telefonnummer till den primära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation. Vid aggregerad rapportering enligt artikel 7 i denna förordning, telefonnumret till den primära kontaktpersonen för den entitet som lämnar in den aggregerade rapporten. Telefonnumret ska anges med alla internationella prefix (t.ex. +33XXXXXXXXX)	Ja	Ja	Ja	Alfanumeriskt värde
1.10	Namnet på den sekundära kontaktpersonen	Namn och efternamn på den sekundära kontaktpersonen eller namnet på den ansvariga gruppen för den finansiella entitet eller en entitet som lämnar in rapporten för den finansiella entitetens räkning	Ja	Ja	Ja	Alfanumeriskt värde
1.11	E-postadress till den sekundära kontaktpersonen	E-postadress till den sekundära kontaktperson eller en e-postadress till funktionsbrevlådan för gruppen som kan användas av den behöriga myndigheten för uppföljande kommunikation.	Ja	Ja	Ja	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
1.12	Telefonnummer till den sekundära kontaktpersonen	Telefonnummer till den sekundära kontaktpersonen eller en grupp som kan användas av den behöriga myndigheten för uppföljande kommunikation. Telefonnumret ska anges med alla internationella prefix (t.ex. +33XXXXXXXXX)	Ja	Ja	Ja	Alfanumeriskt värde
1.13	Namnet på det yttersta moderföretaget	Namnet på det yttersta moderföretaget för den koncern som den berörda finansiella entiteten tillhör, i tillämpliga fall.	Ja, om den finansiella entiteten tillhör en koncern.	Ja, om den finansiella entiteten tillhör en koncern.	Ja, om den finansiella entiteten tillhör en koncern.	Alfanumeriskt värde
1.14	LEI-kod för det yttersta moderföretaget	LEI-koden för det yttersta moderföretaget för den koncern som den berörda finansiella entiteten tillhör, i tillämpliga fall Tilldelas i enlighet med Internationella standardiseringsorganisationen.	Ja, om den finansiella entiteten tillhör en koncern.	Ja, om den finansiella entiteten tillhör en koncern.	Ja, om den finansiella entiteten tillhör en koncern.	En unik kod med 20 alfanumeriska tecken, på grundval av ISO 17442–1:2020.
1.15 Rapporteringsvaluta		Valutan som används för incidentrapporteringen	Ja	Ja	Ja	Valet fylls i med hjälp av valutakoder enligt ISO 4217
Innehållet i den första anmälan						
2.1	Incidentens referenskod som tilldelats av den finansiella entiteten	Unik referenskod som utfärdats av den finansiella entiteten och som otvetydigt identifierar den allvarliga IKT-relaterade incidenten. Vid aggregerad rapportering enligt artikel 7 i denna förordning, den referenskod för incidenten som tilldelats av tredjepartsleverantören.	Ja	Ja	Ja	Alfanumeriskt värde
2.2	Datum och tidpunkt för upptäckten av den IKT-relaterade incidenten	Datum och tidpunkt då den finansiella entiteten fick kännedom om den IKT-relaterade incidenten. För återkommande incidenter, det datum och den tidpunkt då den senaste IKT-relaterade incidenten upptäcktes.	Ja	Ja	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
2.3 Datum och tidpunkt då incidenten klassificerades som allvarlig	Datum och tidpunkt då den IKT-relaterade incidenten klassificerades som allvarlig enligt de klassificeringskriterier som fastställs i delegerad förordning (EU) 2024/1772.	Ja	Ja	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)
2.4 Beskrivning av den IKT-relaterade incidenten	Beskrivning av de mest relevanta aspekterna av den allvarliga IKT-relaterade incidenten. Finansiella entiteter ska tillhandahålla en översikt på hög nivå över följande information, såsom möjliga orsaker, omedelbara effekter, berörda system osv. Finansiella entiteter ska, om detta är känt eller rimligen kan förväntas, inkludera huruvida incidenten påverkar tredjepartsleverantörer eller andra finansiella entiteter, typen av leverantör eller finansiell entitet, deras namn, deras respektive identifieringskoder och typ av identifieringskod (t.ex. LEI-kod eller EUID). I efterföljande rapporter kan innehållet i fälten utvecklas med tiden för att återspegla den pågående förståelsen av den IKT-relaterade incidenten och beskriva all annan relevant information om den IKT-relaterade incidenten som inte har fastslagits i datafälten, inbegripet den finansiella entitetens interna allvarlighetsbedömning (t.ex. mycket låg, låg, medelhög, hög, mycket hög) och en indikation på nivån och namnet på de högsta beslutsstrukturer som har varit inblandade i reaktionen på den IKT-relaterade incidenten.	Ja	Ja	Ja	Alfanumeriskt värde
2.5 Klassificeringskriterier som utlöste incidentrapporten	Klassificeringskriterier enligt delegerad förordning (EU) 2024/1772 som har lett till att den IKT-relaterade incidenten fastställdes som allvarlig och efterföljande anmälan och rapportering. Vid aggregerad rapportering enligt artikel 7 i denna förordning, de klassificeringskriterier som har lett till att den IKT-relaterade incidenten har fastställts som allvarlig för minst en finansiell entitet.	Ja	Ja	Ja	Val (flera val kan göras): — Berörda kunder, finansiella motparter och transaktioner, — Påverkan på anseendet, — Varaktighet och driftstopp, — Geografisk spridning, — Dataförluster, — Berörda kritiska tjänster, — Ekonomiska effekter.
2.6 Väsentlighetströsklar för klassificeringskriteriet Geografisk spridning	EES-medlemsstater som berörs av den allvarliga IKT-relaterade incidenten Vid bedömningen av effekterna av den allvarliga IKT-relaterade incidenten i andra medlemsstater ska de finansiella entiteterna beakta artiklarna 4 och 12 i delegerad förordning (EU) 2024/1772.	Ja, om tröskelvärdet Geografisk spridning har uppnåtts.	Ja, om tröskelvärdet Geografisk spridning har uppnåtts.	Ja, om tröskelvärdet Geografisk spridning har uppnåtts.	Val (flera kan väljas) görs med hjälp av ISO 3166 ALPHA-2 för de berörda länderna

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
2.7	Upptäckten av den allvarliga IKT-relaterade incidenten	Beskrivning av hur den allvarliga IKT-relaterade incidenten upptäcktes.	Ja	Ja	Ja	Val: — It-säkerhet, — Personal, — Internrevision, — Extern revision, — Kunder, — Finansiella motparter, — Tredjepartsleverantör, — Angriparen, — Övervakningssystem, — Myndighet/organ/brottsbekämpande organ, — Annat.
2.8	Indikation om huruvida incidenten har sitt ursprung hos en tredjepartsleverantör eller en annan finansiell entitet	Indikation om huruvida den allvarliga IKT-relaterade incidenten har sitt ursprung hos en tredjepartsleverantör eller en annan finansiell entitet. Finansiella entiteter ska ange om den allvarliga IKT-relaterade incidenten har sitt ursprung hos en tredjepartsleverantör eller en annan finansiell entitet (inklusive finansiella entiteter som tillhör samma koncern som den rapporterande entiteten) och tredjepartsleverantörens eller den finansiella entitetens namn, identifieringskod och typ av identifieringskod (t.ex. LEI-kod eller EUID).	Ja, om incidenten har sitt ursprung hos en tredjeparts-leverantör eller en annan finansiell entitet.	Ja, om incidenten har sitt ursprung hos en tredjepartsle-verantör eller en annan finansiell entitet.	Ja, om incidenten har sitt ursprung hos en tredjepartsle-verantör eller en annan finansiell entitet.	Alfanumeriskt värde
2.9	Aktivering av planen för driftskontinuitet, om aktiverad	Uppgift om huruvida den finansiella entitetens åtgärder för driftskontinuitet har aktiverats formellt.	Ja	Ja	Ja	Boolesk (ja eller nej)
2.10	Annan relevant information	Ytterligare information som inte ingår i mallen. Finansiella entiteter som har omklassificerat en allvarlig IKT-relaterad incident som icke-allvarlig ska beskriva skälen till att den IKT-relaterade incidenten inte uppfyller, och inte förväntas uppfylla, kriterierna för att betraktas som en allvarlig IKT-relaterad incident.	Ja, om det finns annan information som inte omfattas av mallen eller	Ja, om det finns annan information som inte omfattas av mallen eller om den	Ja, om det finns annan information som inte omfattas av mallen eller	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
			om den allvarliga IKT-relaterade incidenten har omklassificerats som icke-allvarlig.	allvarliga IKT-relaterade incidenten har omklassificerats som icke-allvarlig	om den allvarliga IKT-relaterade incidenten har omklassificerats som icke-allvarlig	
Delrapportens innehåll						
3.1	Incidentens referenskod som tillhandahållits av den behöriga myndigheten	Unik referenskod som tilldelats av den behöriga myndigheten vid tidpunkten för mottagandet av den första anmälan för att otvetydigt identifiera den allvarliga IKT-relaterade incidenten.	Nej	Ja, om tillämpligt	Ja, om tillämpligt	Alfanumeriskt värde
3.2	Datum och tidpunkt för incidenten	Datum och tidpunkt då den allvarliga IKT-relaterade incidenten inträffade, om tidpunkten skiljer sig från den tidpunkt då den finansiella entiteten fick kännedom om den allvarliga IKT-relaterade incidenten. För återkommande allvarliga IKT-relaterade incidenter, det datum och den tidpunkt då den senaste allvarliga IKT-relaterade incidenten inträffade.	Nej	Ja	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)
3.3	Datum och tidpunkt då tjänster, verksamheter eller insatser återställdes	Information om datum och tidpunkt då tjänster, verksamheter eller insatser som berörs av den allvarliga IKT-relaterade incidenten återställdes.	Nej	Ja, om datafält 3.16 Driftstopp har fyllts i	Ja, om datafält 3.16 Driftstopp har fyllts i	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)
3.4	Antal berörda kunder	Antal kunder som berörs av den allvarliga IKT-relaterade incidenten som använder den tjänst som tillhandahålls av den finansiella entiteten. Vid bedömningen av antalet berörda kunder ska de finansiella entiteterna beakta artiklarna 1.1 och 9.1 b i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa det faktiska antal kunder som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. Vid aggregerad rapportering enligt artikel 7 i denna förordning, det totala antalet kunder som berörs hos alla finansiella entiteter.	Nej	Ja	Ja	Numeriskt heltal

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.5	Andel berörda kunder	Andel kunder som berörs av den allvarliga IKT-relaterade incidenten i förhållande till det totala antalet kunder som använder den berörda tjänst som tillhandahålls av den finansiella entiteten. Om mer än en tjänst berörs ska tjänsterna anges på ett aggregerat sätt. Finansiella entiteter ska vid sin bedömning beakta artiklarna 1.1 och 9.1 a i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa den faktiska andel kunder som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska en finansiell entitet dividera summan av alla berörda kunder med det totala antalet kunder hos alla berörda finansiella entiteter.	Nej	Ja	Ja	Uttryckt i procent – ett värde med upp till fem numeriska tecken inklusive upp till en decimal uttryckt som en procentandel (t.ex. 2,4 i stället för 2,4 %). Om värdet har fler än en siffra efter decimaltecknet och sista siffran är 5 eller högre ska de rapporterande motparterna alltid avrunda uppåt.
3.6	Antal berörda finansiella motparter	Antal finansiella motparter som berörs av den allvarliga IKT-relaterade incidenten och som har ingått ett avtal med den finansiella entiteten. Vid bedömningen av antalet berörda finansiella motparter ska de finansiella entiteterna beakta artikel 1.2 i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa det faktiska antal finansiella motparter som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. Vid aggregerad rapportering enligt artikel 7 i denna förordning, det totala antalet finansiella motparter som berörs hos alla finansiella entiteter.	Nej	Ja	Ja	Numeriskt heltal

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.7	Andel berörda finansiella motparter	Andelen finansiella motparter som berörs av den allvarliga IKT-relaterade incidenten i förhållande till det totala antalet finansiella motparter som har ingått ett avtal med den finansiella entiteten. Vid bedömningen av andelen berörda finansiella motparter ska de finansiella entiteterna beakta artiklarna 1.1 och 9.1 c i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa den faktiska andel finansiella motparter som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska summan av alla berörda finansiella motparter dividerat med det totala antalet finansiella motparter hos alla berörda finansiella entiteter anges.	Nej	Ja	Ja	Uttryckt i procent – ett värde med upp till fem numeriska tecken inklusive upp till en decimal uttryckt som en procentandel (t.ex. 2,4 i stället för 2,4 %). Om värdet har fler än en siffra efter decimaltecknet och sista siffran är 5 eller högre ska de rapporterande motparterna alltid avrunda uppåt.
3.8	Inverkan på relevanta kunder eller finansiella motparter	Alla fastställda effekter på relevanta kunder eller finansiella motparter som avses i artiklarna 1.3 och 9.1 f i delegerad förordning (EU) 2024/1772.	Nej	Ja, om tröskelvärdet för Betydelsen av kunder och finansiella motparter uppfylls	Ja, om tröskelvärdet för Betydelsen av kunder och finansiella motparter uppfylls	Boolesk (ja eller nej)
3.9	Antal berörda transaktioner	Antal transaktioner som berörs av den allvarliga IKT-relaterade incidenten. Vid bedömningen av effekterna på transaktioner ska de finansiella entiteterna beakta artikel 1.4 i delegerad förordning (EU) 2024/1772, inbegripet alla berörda inhemska och gränsöverskridande transaktioner som avser ett penningbelopp där minst en del av transaktionen genomförs i unionen.	Nej	Ja, om en transaktion har påverkats av incidenten	Ja, om en transaktion har påverkats av incidenten	Numeriskt heltal

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
		En finansiell entitet som inte kan fastställa det faktiska antal transaktioner som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. Vid aggregerad rapportering enligt artikel 7 i denna förordning, ange det totala antalet transaktioner som berörs hos alla finansiella entiteter.				
3.10	Andel berörda transaktioner	Andelen berörda transaktioner i förhållande till det dagliga genomsnittliga antalet inhemska och gränsöverskridande transaktioner som genomförs av den finansiella entiteten med anknytning till den berörda tjänsten. De finansiella entiteterna ska beakta artiklarna 1.4 och 9.1 d i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa den faktiska procentandelen av de transaktioner som berörs ska använda uppskattningar. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska en finansiell entitet summera antalet berörda transaktioner och dividera summan med det totala antalet transaktioner hos alla berörda finansiella entiteter.	Nej	Ja, om en transaktion har påverkats av incidenten	Ja, om en transaktion har påverkats av incidenten	Uttryckt i procent – ett värde med upp till fem numeriska tecken inklusive upp till en decimal uttryckt som en procentandel (t.ex. 2,4 i stället för 2,4 %). Om värdet har fler än en siffra efter decimaltecknet och sista siffran är 5 eller högre ska de rapporterande motparterna alltid avrunda uppåt.
3.11	Värdet på de berörda transaktionerna	Det totala värdet av de transaktioner som berörs av den allvarliga IKT-relaterade incidenten ska bedömas i enlighet med artiklarna 1.4 och 9.1 e i delegerad förordning (EU) 2024/1772. En finansiell entitet som inte kan fastställa det faktiska värdet av de transaktioner som berörs ska använda uppskattningar baserade på tillgängliga uppgifter från jämförbara referensperioder. En finansiell entitet ska redovisa det monetära beloppet som ett positivt värde. Vid aggregerad rapportering enligt artikel 7 i denna förordning, det totala värdet av de transaktioner som berörs hos alla finansiella entiteter.	Nej	Ja, om transaktioner har påverkats av incidenten	Ja, om en transaktion har påverkats av incidenten	Monetärt värde Finansiella entiteter ska rapportera datapunkten i enheter med en minsta noggrannhet motsvarande tusentals enheter (t.ex. 2,5 i stället för 2 500 euro).

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.12 Uppgifter om huruvida siffrorna är faktiska eller uppskattade eller om det inte har förekommit någon inverkan	Uppgifter om huruvida de värden som rapporteras i datafälten 3.4–3.11 är faktiska eller uppskattade, eller om det inte har förekommit någon påverkan.	Nej	Ja	Ja	Val (flera val kan göras): — Faktiska siffror för berörda kunder, — Faktiska siffror för berörda finansiella motparter, — Faktiska siffror för berörda transaktioner, — Uppskattningar för berörda kunder, — Uppskattningar för berörda finansiella motparter, — Uppskattningar för berörda transaktioner, — Ingen påverkan på kunder, — Ingen påverkan på finansiella motparter, — Ingen påverkan på transaktioner.
3.13 Påverkan på anseendet	Information om påverkan på anseendet till följd av den allvarliga IKT-relaterade incidenten enligt artiklarna 2 och 10 i delegerad förordning (EU) 2024/1772. Vid aggregerad rapportering enligt artikel 7 i denna förordning, de kategorier för påverkan på anseendet som gäller för minst en finansiell entitet.	Nej	Ja, om kriteriet Påverkan på anseendet uppfylls	Ja, om kriteriet Påverkan på anseendet uppfylls	Val (flera val kan göras): — Den allvarliga IKT-relaterade incidenten har tagits upp i medierna, — Den allvarliga IKT-relaterade incidenten har lett till upprepade klagomål från olika kunder eller finansiella motparter om tjänster riktade mot kunder eller kritiska affärsförbindelser, — Den finansiella entiteten kommer inte att kunna eller kommer sannolikt inte att kunna uppfylla lagstadgade krav till följd av den allvarliga IKT-relaterade incidenten, — Den finansiella entiteten kommer att eller kommer sannolikt att förlora kunder eller finansiella motparter med en väsentlig inverkan på dess verksamhet till följd av den allvarliga IKT-relaterade incidenten.
3.14 Bakgrundsinformation om påverkan på anseendet	Information om hur den allvarliga IKT-relaterade incidenten har påverkat eller skulle kunna påverka den finansiella entitetens anseende, inbegripet överträdelser av lag, lagstadgade krav som inte uppfyllts, antalet kundklagomål osv.	Nej	Ja, om kriteriet Påverkan på anseendet uppfylls.	Ja, om kriteriet Påverkan på anseendet uppfylls.	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	Bakgrundsinformationen ska omfatta typen av medier (t.ex. traditionella och digitala medier, bloggar eller strömningsplattformar) och medietäckning, inbegripet mediernas räckvidd (lokal, nationell eller internationell). Medietäckning ska i detta sammanhang inte innebära några få negativa kommentarer från följare eller användare av sociala nätverk. Den finansiella entiteten ska också ange om medietäckningen belyste betydande risker för dess kunder i samband med den allvarliga IKT-relaterade incidenten, inbegripet risken för den finansiella entitetens insolvens eller risken för förlust av medel. Finansiella entiteter ska också ange om de har lämnat information till medier som på ett tillförlitligt sätt har informerat allmänheten om den allvarliga IKT-relaterade incidenten och dess konsekvenser. Finansiella entiteter får också ange om det förekom felaktig information i medierna i samband med den IKT-relaterade incidenten, inbegripet information baserad på avsiktligt felaktig information som spreds genom fientliga aktörer, eller information som rör eller visar på förvanskning av den finansiella entitetens webbplats.				
3.15 Incidentens varaktighet	Finansiella entiteter ska mäta varaktigheten för den allvarliga IKT-relaterade incidenten från den tidpunkt då den allvarliga IKT-relaterade incidenten inträffade till den tidpunkt då incidenten åtgärdades. Finansiella entiteter som inte kan fastställa tidpunkten för den allvarliga IKT-relaterade incidenten ska mäta varaktigheten för den allvarliga IKT-relaterade incidenten från den tidigare av den tidpunkt då den finansiella entiteten upptäckte incidenten och den tidpunkt då den finansiella entiteten registrerade incidenten i nätverks- eller systemloggar eller andra datakällor. Finansiella entiteter som ännu inte vet när den allvarliga IKT-relaterade incidenten kommer att åtgärdas ska göra uppskattningar. Värdet ska uttryckas i dagar, timmar och minuter. När det gäller aggregerad rapportering enligt artikel 7 i denna förordning ska finansiella entiteter mäta den längsta varaktigheten för den allvarliga IKT-relaterade incidenten om det förekommer skillnader mellan finansiella entiteter.	Nej	Ja	Ja	DD:HH:MM

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.16 Driftstopp	Driftstopp mätt från den tidpunkt då tjänsten är helt eller delvis otillgänglig för kunder, finansiella motparter eller andra interna eller externa användare till den tidpunkt då den reguljära verksamheten eller verksamheten har återställts till den servicenivå som tillhandahölls före den allvarliga IKT-relaterade incidenten. Om driftstopp orsakar förseningar i tillhandahållandet av tjänster efter det att den reguljära verksamheten eller verksamheten har återställts, ska de finansiella entiteterna mäta driftstoppet från början av den allvarliga IKT-relaterade incidenten till den tidpunkt då den försenade tjänsten tillhandahålls. Finansiella entiteter som inte kan fastställa den tidpunkt då driftstoppet inleddes ska mäta driftstoppet från den tidigare tidpunkten av den tidpunkt då incidenten upptäcktes och den tidpunkt då den registrerades. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska finansiella entiteter mäta den längsta varaktigheten för driftstoppet om det förekommer skillnader mellan finansiella entiteter.	Nej	Ja, om incidenten har orsakat ett driftstopp	Ja, om incidenten har orsakat ett driftstopp	DD:HH:MM
3.17 Information om huruvida siffrorna för varaktighet och driftstopp är faktiska eller uppskattade	Uppgifter om huruvida de värden som rapporteras i datafälten 3.15 och 3.16 är faktiska eller uppskattningar.	Nej	Ja, om kriteriet Varaktighet och driftstopp uppfylls	Ja, om kriteriet Varaktighet och driftstopp uppfylls	Val: — Faktiska siffror, — Uppskattningar, — Faktiska siffror och uppskattningar, — Information saknas.
3.18 Typer av effekter i medlemsstaterna	Typer av effekter i respektive EES-medlemsstat. Angivelse om huruvida den allvarliga IKT-relaterade incidenten har påverkat andra EES-medlemsstater (än medlemsstaten för den behöriga myndighet till vilken incidenten rapporteras direkt), i enlighet med artikel 4 i delegerad förordning (EU) 2024/1772, och särskilt med hänsyn till effekternas betydelse i förhållande till a) drabbade kunder och finansiella motparter i andra medlemsstater, eller	Nej	Ja, om tröskelvärdet Geografisk spridning har uppnåtts	Ja, om tröskelvärdet Geografisk spridning har uppnåtts	Val (flera val kan göras): — Kunder, — Finansiella motparter, — Den finansiella entitetens filial, — Finansiella entiteter inom koncernen som bedriver verksamhet i respektive medlemsstat, — Finansmarknadsinfrastruktur, — Tredjepartsleverantörer som kan vara gemensamma för andra finansiella entiteter.

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	b) filialer eller andra finansiella entiteter inom koncernen som bedriver verksamhet i andra medlemsstater, eller c) finansmarknadsinfrastrukturer eller tredjepartsleverantörer som kan påverka finansiella entiteter i andra medlemsstater som de tillhandahåller tjänster till.				
3.19 Beskrivning av hur incidenten påverkar andra medlemsstater	Beskrivning av den allvarliga IKT-relaterade incidentens effekter och allvarlighetsgrad i varje berörd medlemsstat, inbegripet en bedömning av effekterna och allvarlighetsgraden för a) kunder, b) finansiella motparter, c) den finansiella entitetens filialer, d) andra finansiella entiteter inom koncernen som bedriver verksamhet i respektive medlemsstat, e) finansmarknadsinfrastrukturer, f) tredjepartsleverantörer som kan vara gemensamma för andra finansiella entiteter enligt vad som är tillämpligt i andra medlemsstater.	Nej	Ja, om tröskelvärdet Geografisk spridning har uppnåtts	Ja, om tröskelvärdet Geografisk spridning har uppnåtts	Alfanumeriskt värde
3.20 Väsentlighetströsklar för klassificeringskriteriet Dataförluster	Typer av dataförluster som den allvarliga IKT-relaterade incidenten medför i förhållande till uppgifternas tillgänglighet, äkthet, integritet och konfidentialitet. Finansiella entiteter ska vid sin bedömning beakta artiklarna 5 och 13 i delegerad förordning (EU) 2024/1772. Vid aggregerad rapportering enligt artikel 7 i denna förordning, de dataförluster som drabbar minst en finansiell entitet.	Nej	Ja, om kriteriet Dataförluster uppfylls	Ja, om kriteriet Dataförluster uppfylls	Val (flera val kan göras): — Tillgänglighet, — Äkthet, — Integritet, — Konfidentialitet.
3.21 Beskrivning av dataförlusterna	Beskrivning av hur den allvarliga IKT-relaterade incidenten påverkar tillgängligheten, äktheten, integriteten och konfidentialiteten för kritiska uppgifter i enlighet med artiklarna 5 och 13 i delegerad förordning (EU) 2024/1772. Information om påverkan på genomförandet av den finansiella entitetens affärsmål eller på uppfyllandet av lagstadgade krav. Som en del av den information som lämnas ska de finansiella entiteterna ange om de berörda uppgifterna är kunduppgifter, andra entiteters uppgifter (t.ex. finansiella motparter) eller den finansiella entitetens uppgifter.	Nej	Ja, om kriteriet Dataförluster uppfylls	Ja, om kriteriet Dataförluster uppfylls	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	Den finansiella entiteten får också ange vilken typ av uppgifter som berörs av incidenten – i synnerhet huruvida uppgifterna är konfidentiella och vilken typ av konfidentialitet det rörde sig om (t.ex. affärshemligheter, personuppgifter, tystnadsplikt, banksekretess, försäkringssekretess, betaltjänstsekretess osv.). Informationen kan också omfatta möjliga risker i samband med dataförluster, t.ex. huruvida de uppgifter som berörs av incidenten kan användas för att identifiera enskilda personer och skulle kunna användas av den fientliga aktören för att erhålla krediter eller lån utan deras samtycke, för att utföra nätfiskeattacker eller för att offentliggöra information. Vid aggregerad rapportering enligt artikel 7 i denna förordning, en allmän beskrivning av incidentens effekter på de berörda finansiella entiteterna. Om effekterna skiljer sig åt ska den specifika effekten på de olika finansiella entiteterna tydligt anges i beskrivningen av effekterna.				
3.22 Klassificeringskriteriet Berörda kritiska tjänster	Information om kriteriet Berörda kritiska tjänster. Finansiella entiteter ska beakta artikel 6 i delegerad förordning (EU) 2024/1772 i sin bedömning, inklusive information om — de berörda tjänster eller verksamheter som kräver auktorisation eller registrering eller som övervakas av behöriga myndigheter, eller — IKT-tjänster eller nätverks- och informationssystem som stöder kritiska eller viktiga funktioner hos den finansiella entiteten, och — karaktären hos den skadliga och obehöriga åtkomsten till den finansiella entitetens nätverks- och informationssystem. Vid aggregerad rapportering enligt artikel 7 i denna förordning, effekten på kritiska tjänster som gäller för minst en finansiell entitet.	Nej	Ja	Ja	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.23	Typ av incident	Klassificering av incidenter efter typ.	Nej	Ja	Ja	Val (flera val kan göras): — Cybersäkerhetsrelaterade, — Processfel, — Systemfel, — Extern händelse, — Betalningsrelaterad, — Annan (precisera).
3.24	Andra typer av incidenter	Andra typer av IKT-relaterade incidenter: Finansiella entiteter som har valt ”annan” typ av incidenter i datafältet 3.23 ska ange vilken typ av IKT-relaterad incident som det rör sig om.	Nej	Ja, om ”annan” typ av incidenter har valts i datafält 3.23	Ja, om ”annan” typ av incidenter har valts i datafält 3.23	Alfanumeriskt värde
3.25	Hot och tillvägagångssätt som använts av den fientliga aktören	Ange de hot och tillvägagångssätt som använts av den fientliga aktören, inbegripet a) social manipulering, inklusive nätfiske, b) samordnad överbelastningsattack, c) identitetsstöld, d) datakryptering för påverkan, inklusive utpressningsprogram, e) kapning av resurser, f) dataexfiltrering och datamanipulation, med undantag för identitetsstöld, g) förstöring av data, h) förvanskning, i) attack mot leveranskedjan, j) övrigt (specificera).	Nej	Ja, om typen av IKT-relaterad incident är ”cybersäkerhets-relaterad” i fält 3.23	Ja, om typen av IKT-relaterad incident är ”cybersäker-hetsrelaterad” i fält 3.23	Val (flera val kan göras): — Social manipulering (inklusive nätfiske), — Samordnad överbelastningsattack, — Identitetsstöld, — Datakryptering för påverkan, inklusive utpressningsprogram, — Kapning av resurser, — Dataexfiltrering och datamanipulation, inbegripet identitetsstöld, — Förstöring av data, — Förvanskning, — Attack mot leveranskedjan, — Annat (specificera).
3.26	Andra typer av tillvägagångssätt	Andra typer av tillvägagångssätt Finansiella entiteter som har valt ”annan” typ av tillvägagångssätt i datafält 3.25 ska ange vilken typ av tillvägagångssätt det rör sig om.	Nej	Ja, om ”annan” typ av tillvägagångs-sätt har valts i datafält 3.25	Ja, om ”annan” typ av tillvägagångs-sätt har valts i datafält 3.25	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.27	Information om berörda funktionella områden och affärsprocesser	Angivelse av de funktionella områden och affärsprocesser som påverkas av incidenten, inklusive produkter och tjänster. De funktionella områdena ska omfatta men är inte begränsade till följande: a) Marknadsföring och affärsutveckling. b) Kundtjänst. c) Produktförvaltning. d) Regelefterlevnad. e) Riskhantering. f) Finansiering och redovisning. g) HR och allmänna tjänster. h) Informationsteknik. Affärsprocesserna ska omfatta men är inte begränsade till följande: — Kontoinformation, — Aktuarietjänster, — Inlösen av betalningstransaktioner, — Autentisering/auktorisering, — Bemyndigande, — Introduktion av kund, — Förmånsförvaltning, — Hantering av utbetalning av förmåner, — Köp och försäljning av försäkringspaket mellan försäkringar, — Kortbetalningar, — Kontanthantering, — Kontantplacering eller kontantuttag, — Hantering av försäkringsanspråk, — Försäkring för skadeståndsprocesser, — Clearing, — Konglomerat för företagslån, — Kollektiva försäkringar, — Betalningar, — Förvaltning och förvaring av tillgångar, — Introduktion av kunder, — Datainsamling, — Databehandling, — Autogirering, — Exportförsäkringar, — Genomförande av handel på börser, — Placering av finansiella instrument, — Fondredovisning,	Nej	Ja	Ja	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	— Pengar på valutamarknad, — Investeringsrådgivning, — Investeringsförvaltning, — Utgivande av betalningsinstrument, — Låneförvaltning, — Utbetalning av livförsäkring, — Penningöverföring, — Beräkning av nettotillgångar, — Beställning, — Betalningsinitiering, — Tecknande av försäkringar, — Portföljförvaltning, — Uppbörd av premier, — Mottagning/överföring/utförande, — Återförsäkring, — Avveckling, — Transaktionsövervakning. Vid aggregerad rapportering enligt artikel 7 i denna förordning, de drabbade funktionella områden och affärsprocesser inom minst en finansiell entitet.				
3.28 Berörda infrastrukturkomponenter som stöder affärsprocesser	Information om huruvida infrastrukturkomponenter (servrar, operativsystem, programvara, applikationsservrar, mellanprogramvara, nätverkskomponenter osv.) som stöder affärsprocesser har påverkats av den allvarliga IKT-relaterade incidenten.	Nej	Ja	Ja	Val: — Ja, — Nej, — Information saknas.
3.29 Information om berörda infrastrukturkomponenter som stöder affärsprocesser	Beskrivning av den allvarliga IKT-relaterade incidentens effekter på infrastrukturkomponenter som stöder affärsprocesser, inbegripet maskinvara och programvara. Maskinvara omfattar servrar, datorer, datacentraler, växlar, routrar och nav. Programvara omfattar operativsystem, applikationer, databaser, säkerhetsverktyg, nätverkskomponenter osv. Ange vilka som avses. Beskrivningarna ska innehålla eller namnge berörda infrastrukturkomponenter eller infrastruktursystem och i förekommande fall a) versionsinformation, b) intern infrastruktur/delvis utkontrakterad/helt utkontrakterad – tredjepartsleverantörens namn,	Nej	Ja, om incidenten har påverkat infrastrukturkomponenter som stöder affärsprocesser	Ja, om incidenten har påverkat infrastrukturkomponenter som stöder affärsprocesser	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	c) huruvida infrastrukturen används av eller är delad mellan flera affärsfunktioner, d) relevanta arrangemang för motståndskraft/kontinuitet/återhämtning/utbytbarhet.				
3.30 Inverkan på kundernas finansiella intressen	Information om huruvida den allvarliga IKT-relaterade incidenten har påverkat kundernas ekonomiska intressen.	Nej	Ja	Ja	Val: — Ja, — Nej, — Information saknas.
3.31 Rapportering till andra myndigheter	Närmare uppgifter om vilka myndigheter som informerades om den allvarliga IKT-relaterade incidenten. Med hänsyn till skillnaderna till följd av medlemsstaternas nationella lagstiftning ska finansiella entiteter förstå begreppet brottsbekämpande myndigheter i stort sett som offentliga myndigheter som har befogenhet att lagföra it-brottslighet, inbegripet polis, brottsbekämpande organ och allmänna åklagare.	Nej	Ja	Ja	Val (flera val kan göras): — Polis/brottsbekämpande organ, — CSIRT, — Dataskyddsmyndighet, — Nationella cybersäkerhetsbyrån, — Inga, — Annan (förklara närmare).
3.32 Specifikation av ”annan” myndighet	Närmare uppgifter om ”annan” typ av myndigheter som informerades om den allvarliga IKT-relaterade incidenten. Om detta har valts i datafält 3.31. ”Annan” – beskrivningen ska innehålla mer detaljerad information om den myndighet till vilken den finansiella entiteten har lämnat information om den allvarliga IKT-relaterade incidenten.	Nej	Ja, om den finansiella entiteten har informerat ”annan” typ av myndighet om den allvarliga IKT-relaterade incidenten.	Ja, om den finansiella entiteten har informerat ”annan” typ av myndighet om den allvarliga IKT-relaterade incidenten	Alfanumeriskt värde
3.33 Tillfälliga åtgärder som vidtagits eller planeras för återställning efter incidenten	Angivelse om huruvida den finansiella entiteten har genomfört (eller planerar att genomföra) tillfälliga åtgärder som har vidtagits (eller planeras att vidtas) för återställning efter den allvarliga IKT-relaterade incidenten.	Nej	Ja	Ja	Boolesk (ja eller nej)

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
3.34 Beskrivning av alla tillfälliga åtgärder som vidtagits eller planeras för återställning efter incidenten	Informationen ska beskriva de omedelbara åtgärder som har vidtagits, inbegripet isolering av incidenten på nätverksnivå, aktiverade förfaranden för tillfälliga lösningar, blockerade USB-portar, aktiverad plats för katastrofåterhämtning och eventuella andra ytterligare säkerhetsåtgärder som har införts tillfälligt. Finansiella entiteter ska ange datum och tidpunkt för genomförandet av de tillfälliga åtgärderna och det datum då man förväntas återgå till den primära platsen. För alla tillfälliga åtgärder som inte har genomförts men som fortfarande planeras, ange det datum då de förväntas genomföras. Om inga tillfälliga åtgärder har vidtagits, ange orsaken.	Nej	Ja, om tillfälliga åtgärder har vidtagits eller planeras att vidtas (datafält 3.33)	Ja, om tillfälliga åtgärder har vidtagits eller planeras att vidtas (datafält 3.33)	Alfanumeriskt värde
3.35 Angreppsindikator	Information om den allvarliga IKT-relaterade incidenten som kan bidra till att identifiera skadlig aktivitet inom ett nätverks- eller informationssystem (angreppsindikatorer), i tillämpliga fall. Fältet gäller endast de finansiella entiteter som omfattas av Europaparlamentets och rådets direktiv (EU) 2022/2555 ([1]) och de finansiella entiteter som betraktas som väsentliga eller viktiga entiteter i enlighet med nationella bestämmelser som införlivar artikel 3 i direktiv (EU) 2022/2555, i förekommande fall. Den angreppsindikator som anges av den finansiella entiteten ska omfatta följande kategorier av uppgifter: a) IP-adresser. b) URL-adresser. c) Domäner. d) Filhashar. e) Uppgifter om sabotageprogram (namn på sabotageprogram, filnamn och var de finns, specifika registernycklar som är kopplade till aktivitet som rör sabotageprogram). f) Uppgifter om nätverksaktivitet (portar, protokoll, adresser, referenser, användaragenter, rubriker, specifika loggar eller distinkta mönster i nätverkstrafiken). g) Uppgifter om e-postmeddelanden (avsändare, mottagare, ämne, rubrik, innehåll).	Nej	Ja, om cybersäkerhetsrelaterad har valts som en typ av incident i datafält 3.23	Ja, om cybersäkerhetsrelaterad har valts som en typ av incident i datafält 3.23	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	h) DNS-begäranden och registerkonfigurationer. i) Aktiviteter på användarkonton (inloggningar, aktivitet på privilegierade användarkonton, eskalering av privilegier). j) Databastrafik (läsa/skriva), begäranden avseende samma fil. I praktiken kan denna typ av information omfatta data som avser bland annat indikatorer som beskriver mönster i nätverkstrafik som motsvarar kända attacker/ botnätmeddelanden, IP-adresser för maskiner som är infekterade med sabotageprogram (botar), data som avser ledningsservrar som används av sabotageprogram (vanligen domäner eller IP-adresser) och URL:er som avser platser för nätfiske eller webbplatser som observerats som värdar för sabotageprogram eller exploateringsverktyg.				
Slutrapportens innehåll					
4.1 Högnivåklassificering av grundläggande orsaker till incidenten	Högnivåklassificering av de grundläggande orsakerna till den allvarliga IKT-relaterade incidenten inom ramen för incidenttyperna, inbegripet följande högnivåkategorier: a) Illvilliga handlingar. b) Processfel. c) Systemfel/felfunktion. d) Mänskligt fel. e) Extern händelse.	Nej	Nej	Ja	Val (flera val kan göras): — Illvilliga handlingar, — Processfel, — Systemfel/felfunktion, — Mänskligt fel, — Extern händelse.
4.2 Detaljerad klassificering av grundläggande orsaker till incidenten	Detaljerad klassificering av de grundläggande orsakerna till den allvarliga IKT-relaterade incidenten inom ramen för incidenttyperna, inbegripet följande detaljerade kategorier med koppling till de högnivåkategorier som rapporteras i datafält 4.1: 1. **Illvilliga handlingar** (om du väljer detta alternativ ska du välja något av alternativen nedan): a) Avsiktliga interna åtgärder. b) Avsiktlig fysisk skada/manipulering/stöld. c) Bedrägeri. 2. **Processfel** (om du väljer detta alternativ ska du välja något av alternativen nedan): a) Otillräcklig övervakning eller bristande övervakning och kontroll.	Nej	Nej	Ja	Val (flera val kan göras): — Illvilliga handlingar: avsiktliga interna åtgärder, — Illvilliga handlingar: Avsiktlig fysisk skada/manipulering/stöld, — Illvilliga handlingar: bedrägeri, — Processfel: otillräcklig övervakning eller bristande övervakning och kontroll, — Processfel: otillräckliga/otydliga roller och ansvarsområden, — Processfel: misslyckad IKT-riskhanteringsprocess, — Processfel: otillräckliga eller bristfälliga IKT-åtgärder och IKT-säkerhetsåtgärder,

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	b) Otillräckliga/otydliga roller och ansvarsområden. c) Misslyckad IKT-riskhanteringsprocess. d) Otillräckliga eller bristfälliga IKT-åtgärder och IKT-säkerhetsåtgärder. e) Otillräcklig eller bristfällig IKT-projektledning. f) Inadekvata interna riktlinjer och förfaranden samt inadekvat dokumentation. g) Inadekvat förvärv, utveckling eller underhåll av IKT-system. h) Övrigt (specificera). 3. **Systemfel/felfunktion** (om du väljer detta alternativ ska du välja något av alternativen nedan): a) Maskinvarans kapacitet och prestanda: Allvarliga IKT-relaterade incidenter orsakade av maskinvaruresurser som visar sig vara otillräckliga i fråga om kapacitet eller prestanda för att uppfylla tillämpliga lagstiftningskrav. b) Maskinvaruunderhåll: Allvarliga IKT-relaterade incidenter till följd av inadekvat eller otillräckligt underhåll av maskinvarukomponenter, med undantag för ”Föråldrad/åldrande maskinvara”. c) Föråldrad/åldrande maskinvara: Denna typ av grundläggande orsaker inbegriper allvarliga IKT-relaterade incidenter till följd av föråldrade eller åldrande maskinvarukomponenter. d) Programvarans kompatibilitet/konfiguration: Allvarliga IKT-relaterade incidenter som orsakas av programvarukomponenter som är inkompatibla med andra programvaru- eller systemkonfigurationer, inbegripet allvarliga IKT-relaterade incidenter till följd av programvarukonflikter, felaktiga inställningar eller felkonfigurerade parametrar som påverkar systemets övergripande funktion. e) Programvarans prestanda: Allvarliga IKT-relaterade incidenter till följd av programvarukomponenter som uppvisar bristande prestanda eller ineffektivitet av andra skäl än de som anges under ”Programvarans kompatibilitet/konfiguration”, inbegripet allvarliga IKT-relaterade incidenter som orsakas av långsamma svarstider, överdriven resursförbrukning eller ineffektiva frågekörningar som påverkar programvarans eller systemets prestanda.				— Processfel: otillräcklig eller bristfällig IKT-projektledning, — Processfel: inadekvata interna riktlinjer och förfaranden samt inadekvat dokumentation, — Processfel: inadekvat förvärv, utveckling och underhåll av IKT-system, — Processfel: annat (specificera), — Systemfel: maskinvarans kapacitet och prestanda, — Systemfel: maskinvaruunderhåll, — Systemfel: föråldrad/åldrande maskinvara, — Systemfel: programvarans kompatibilitet/konfiguration, — Systemfel: programvarans prestanda, — Systemfel: nätverkskonfiguration, — Systemfel: fysisk skada, — Systemfel: annat (specificera), — Mänskligt fel: underlåtenhet, — Mänskligt fel: misstag, — Mänskligt fel: färdigheter och kunskaper, — Mänskligt fel: otillräckliga mänskliga resurser, — Mänskligt fel: felaktig kommunikation, — Mänskligt fel: annat (specificera), — Extern händelse: naturkatastrofer/force majeure, — Extern händelse: fel som rör tredje part, — Extern händelse: annan (specificera).

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	f) Nätverkskonfiguration: Allvarliga IKT-relaterade incidenter till följd av felaktiga eller felkonfigurerade nätverksinställningar eller felaktig eller felkonfigurerad nätverksinfrastruktur, inbegripet allvarliga IKT-relaterade incidenter som orsakas av fel i nätverkskonfigurationen, routningsproblem, felkonfigurering av brandväggar eller andra nätverksrelaterade problem som påverkar anslutning eller kommunikation. g) Fysisk skada: Allvarliga IKT-relaterade incidenter som orsakas av fysisk skada på IKT-infrastrukturen vilket leder till systemfel. h) Annan (specificera). 4. **Mänskligt fel** (om du väljer detta alternativ ska du välja något av alternativen nedan): a) Underlåtenhet (oavsiktlig). b) Misstag. c) Färdigheter och kunskap: Allvarliga IKT-relaterade incidenter till följd av bristande sakkunskap eller kompetens inom hantering av IKT-system eller IKT-processer som kan orsakas av bristfällig utbildning, otillräcklig kunskap eller brist på färdigheter som krävs för att utföra specifika uppgifter eller hantera tekniska utmaningar. d) Otillräckliga mänskliga resurser: Allvarliga IKT-relaterade incidenter som orsakas av brist på nödvändiga resurser, inbegripet maskinvara, programvara, infrastruktur eller personal, och i situationer där otillräckliga resurser leder till operativ ineffektivitet, systemfel eller oförmåga att tillgodose affärsbehov. e) Felaktig kommunikation. f) Övrigt (specificera). 5. **Extern händelse** (om du väljer detta alternativ ska du välja något av alternativen nedan): a) Naturkatastrofer/force majeure. b) Fel som rör tredje part.				

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	c) Övrigt (specificera). De finansiella entiteterna ska när det gäller återkommande allvarliga IKT-relaterade incidenter ta hänsyn till att den specifika uppenbara grundläggande orsaken till incidenten beaktas och inte de allmänna kategorierna i detta fält.				
4.3 Ytterligare klassificering av grundläggande orsaker till incidenten	Ytterligare klassificering av de grundläggande orsakerna till den allvarliga IKT-relaterade incidenten inom ramen för incidenttypen, inbegripet följande ytterligare klassificeringskategorier med koppling till de detaljerade kategorier som ska rapporteras i datafält 4.2. Fältet är obligatoriskt för slutrapporten om särskilda kategorier som kräver mer detaljerad information rapporteras i datafält 4.2. 2 **a Otillräcklig eller bristande övervakning och kontroll:** a) Övervakning av efterlevnaden av bestämmelser, b) Övervakning av tredjepartsleverantörer av tjänster, c) Övervakning och kontroll av avhjälpandet av sårbarheter, d) Identitets- och åtkomsthantering, e) Kryptering och kryptografi, f) Loggning. 2 **c Misslyckad IKT-riskhanteringsprocess:** a) Underlåtenhet att specificera korrekta risktoleransnivåer, b) Otillräckliga sårbarhets- och hotbedömningar, c) Otillräckliga riskhanteringsåtgärder, d) Bristfällig hantering av kvarstående IKT-risker. 2 **d Otillräckliga eller bristfälliga IKT-åtgärder och IKT-säkerhetsåtgärder:** a) Hantering av sårbarheter och programfixar, b) Hantering av förändringar, c) Kapacitets- och prestandahantering, d) Förvaltning av IKT-tillgångar och klassificering av information,	Nej	Nej	Ja	Val (flera val kan göras): — Övervakning av efterlevnaden av bestämmelser, — Övervakning av tredjepartsleverantörer av tjänster, — Övervakning och kontroll av avhjälpandet av sårbarheter, — Identitets- och åtkomsthantering, — Kryptering och kryptografi, — Loggning, — Underlåtenhet att specificera korrekta risktoleransnivåer, — Otillräckliga sårbarhets- och hotbedömningar, — Otillräckliga riskhanteringsåtgärder, — Bristfällig hantering av kvarstående IKT-risker, — Hantering av sårbarheter och programfixar, — Hantering av förändringar, — Kapacitets- och prestandahantering, — Förvaltning av IKT-tillgångar och klassificering av information, — Säkerhetskopiering och återställning, — Felhantering, — Inadekvat förvärv, utveckling och underhåll av IKT-system, — Otillräcklig eller misslyckad programvarutestning.

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
		e) Säkerhetskopiering och återställning, f) Felhantering. 2 **g Inadekvat förvärv, utveckling och underhåll av IKT-system:** a) Inadekvat förvärv, utveckling och underhåll av IKT-system, b) Otillräcklig programvarutestning eller misslyckad programvarutestning.				
4.4	Andra typer av grundläggande orsaker	Finansiella entiteter som har valt ”annan” typ av grundläggande orsak i datafältet 4.2 ska ange andra typer av grundläggande orsaker.	Nej	Nej	Ja, om ”annan” typ av grundläggande orsaker har valts i datafält 4.2.	Alfanumeriskt värde
4.5	Information om grundläggande orsaker till incidenten	Beskrivning av det händelseförlopp som ledde till den allvarliga IKT-relaterade incidenten och en beskrivning av på vilket sätt den allvarliga IKT-relaterade incidenten har en liknande uppenbar grundläggande orsak om incidenten klassificeras som en återkommande incident, inklusive en kortfattad beskrivning av alla underliggande orsaker och primära faktorer som bidrog till att den allvarliga IKT-relaterade incidenten inträffade. Om det har förekommit illvilliga handlingar, en beskrivning av tillvägagångssättet för de illvilliga handlingarna, inbegripet den metod, det tillvägagångssätt och de förfaranden som har använts, samt ingångsvektorn för den allvarliga IKT-relaterade incidenten, inbegripet en beskrivning av de utredningar och analyser som ledde till att de grundläggande orsakerna fastställdes, i tillämpliga fall.	Nej	Nej	Ja	Alfanumeriskt värde
4.6	Incidentlösning	Ytterligare information om de åtgärder som vidtagits/planerats för att permanent lösa den allvarliga IKT-relaterade incidenten och för att förhindra att incidenten inträffar igen. Lärdomar från den allvarliga IKT-relaterade incidenten.	Nej	Nej	Ja	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
		Beskrivningen ska innehålla följande punkter: 1. **Beskrivning av hur incidenten åtgärdats** a) Åtgärder som vidtagits för att permanent åtgärda den allvarliga IKT-relaterade incidenten (exklusive eventuella tillfälliga åtgärder), b) För varje åtgärd som vidtagits ska man ange om en tredjepartsleverantör och den finansiella entiteten har deltagit, c) Ange om förfarandena har anpassats till följd av den allvarliga IKT-relaterade incidenten, d) Ange eventuella ytterligare kontroller som har införts eller som planeras med tillhörande tidsplan för genomförandet. Potentiella problem som identifierats med avseende på tillförlitligheten hos de it-system som påverkats eller med avseende på de förfaranden eller kontroller som finns, i tillämpliga fall. De finansiella entiteterna ska tydligt ange hur de planerade avhjälpande åtgärderna kommer att hantera de identifierade grundläggande orsakerna och när den allvarliga IKT-relaterade incidenten förväntas ha åtgärdats permanent. 2. **Lärdomar** Finansiella entiteter ska beskriva resultaten av översynen efter incidenten.				
4.7	Datum och tid då de grundläggande orsakerna till incidenten hanterades	Datum och tid då de grundläggande orsakerna till incidenten hanterades.	Nej	Nej	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)
4.8	Datum och tid då incidenten åtgärdades	Datum och tid då incidenten åtgärdades.	Nej	Nej	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
4.9	Information om datumet för det permanenta åtgärdandet av incidenterna skiljer sig från det ursprungligen planerade genomförandedatumet	Beskrivning av orsaken till att datumet för det permanenta åtgärdandet av de allvarlig IKT-relaterade incidenterna skiljer sig från det ursprungligen planerade genomförandedatumet, i tillämpliga fall.	Nej	Nej	Ja	Alfanumeriskt värde
4.10	Bedömning av risker för kritiska funktioner för resolutionssyften	Bedömning av huruvida den allvarliga IKT-relaterade incidenten utgör en risk för kritiska funktioner i den mening som avses i artikel 2.1.35 i Europaparlamentets och rådets direktiv 2014/59/EU ([2]). Entiteter som avses i artikel 1.1 i direktiv 2014/59/EU ska ange om incidenten utgör en risk för kritiska funktioner i den mening som avses i artikel 2.1.35 i direktiv 2014/59/EU och som rapporteras i mall Z07.01 i kommissionens genomförandeförordning (EU) 2018/1624 ([3]) och kopplas till den specifika entiteten i mall Z07.02.	Nej	Nej	Ja, om incidenten utgör en risk för finansiella entiteters kritiska funktioner enligt artikel 2.1.35 i direktiv 2014/59/EU	Alfanumeriskt värde
4.11	Information som är relevant för resolutionsmyndigheter	Beskrivning av huruvida och i så fall hur den allvarliga IKT-relaterade incidenten har påverkat entitetens eller koncernens möjligheter till resolution. Entiteter som avses i artikel 1.1 i direktiv 2014/59/EU ska lämna information om huruvida och i så fall hur den allvarliga IKT-relaterade incidenten har påverkat entitetens eller koncernens möjligheter till resolution. Dessa entiteter ska också ange om den allvarliga IKT-relaterade incidenten påverkar den finansiella entitetens solvens eller likviditet och en potentiell kvantifiering av effekterna. Dessa entiteter ska också tillhandahålla information om inverkan på den operativa kontinuiteten, inverkan på entitetens resolutionsförmåga, eventuella ytterligare effekter på kostnader och förluster till följd av den allvarliga IKT-relaterade incidenten, inbegripet på den finansiella entitetens kapitalposition, och huruvida avtalsarrangemangen för användningen av IKT-tjänster fortfarande är stabila och fullt verkställbara vid resolution av entiteten.	Nej	Nej	Ja, om incidenten har påverkat entitetens eller koncernens möjlighet till resolution.	Alfanumeriskt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
4.12 Väsentlighetströskel för klassificeringskriteriet Ekonomiska effekter	Detaljerad information om de tröskelvärden som den allvarliga IKT-relaterade incidenten slutligen uppnår i förhållande till kriteriet Ekonomiska effekter som avses i artiklarna 7 och 14 i delegerad förordning (EU) 2024/1772.	Nej	Nej	Ja	Alfanumeriskt värde
4.13 Belopp för direkta och indirekta bruttokostnader och bruttoförluster	Totalt belopp för den finansiella entitetens direkta och indirekta bruttokostnader och bruttoförluster till följd av den allvarliga IKT-relaterade incidenten, däribland a) det belopp av exproprierade medel eller finansiella tillgångar som den finansiella entiteten är ansvarig för, b) kostnader för ersättning eller omplacering av programvara, maskinvara eller infrastruktur, c) personalkostnader, inbegripet kostnader för att byta ut, omplacera eller anställa extra personal, ersättning för övertid och ersättning av förlorad eller försämrad kompetens hos personalen, d) beloppet för avgifter på grund av avtalsförpliktelser som inte har fullgjorts, e) kostnaderna för gottgörelse av och kompensation för kunder, f) förlustbelopp på grund av uteblivna intäkter, g) kostnader i samband med intern och extern kommunikation, h) rådgivningskostnader, inklusive kostnader i samband med juridisk rådgivning, kriminaltekniska tjänster och saneringstjänster, i) övriga kostnader och förluster, inbegripet i) direkta avgifter, inklusive värdeminskningar och avvecklingskostnader, som redovisas i resultaträkningen och nedskrivningar till följd av den allvarliga IKT-relaterade incidenten, ii) avsättningar eller reserver som redovisas i resultaträkningen mot sannolika förluster i samband med den allvarliga IKT-relaterade incidenten,	Nej	Nej	Ja	Monetärt värde

Datafält	Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
	iii) förluster som ännu inte har beaktats, vilka utgörs av förluster till följd av den allvarliga IKT-relaterad incidenten som tillfälligt redovisas på övergångskonton eller interimskonton och ännu inte är redovisade i resultaträkningen, men som avses föras upp inom en tidsperiod som är i proportion till postens storlek och ålder, iv) väsentliga icke uppburna intäkter som är kopplade till avtalsenliga förpliktelser mot tredje part, däribland ett beslut att kompensera en kund till följd av den allvarliga IKT-relaterade incidenten – i stället för genom återbetalning eller direkt utbetalning – genom att avstå från justering av intäkter eller genom att sänka avtalsenliga avgifter för en viss framtida tidsperiod, v) periodrelaterade förluster, om de sträcker sig över mer än ett räkenskapsår och leder till rättslig risk. Finansiella entiteter ska vid sin bedömning beakta artikel 7.1 och 7.2 i delegerad förordning (EU) 2024/1772. Finansiella entiteter ska i denna uppgift inte ta med någon typ av finansiella återkrav. Finansiella entiteter ska redovisa det monetära beloppet som ett positivt värde. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska de finansiella entiteterna beakta de totala kostnaderna och förlusterna för alla finansiella entiteter. Finansiella entiteter ska rapportera datapunkten i enheter med en minsta noggrannhet motsvarande tusentals enheter.				
4.14 Belopp för finansiella återkrav	Totalt belopp för finansiella återkrav. Finansiella återkrav ska täcka den ursprungliga förlust som händelsen orsakade, skild från den tidpunkt då finansiella återkrav i form av tillgångar eller inflöden av ekonomiska förmåner erhålls.	Nej	Nej	Ja	Monetärt värde Finansiella entiteter ska rapportera datapunkten i enheter med en minsta noggrannhet motsvarande tusentals enheter.

Datafält		Beskrivning	Obligatoriskt för första anmälan	Obligatoriskt för delrapport	Obligatoriskt för slutrapport	Fälttyp
		Finansiella entiteter ska redovisa det monetära beloppet som ett positivt värde. Vid aggregerad rapportering enligt artikel 7 i denna förordning ska de finansiella entiteterna beakta det totala beloppet för finansiella återkrav för alla finansiella entiteter.				
4.15	Information om huruvida de icke-allvarliga incidenterna har varit återkommande	Information om huruvida mer än en icke-allvarlig IKT-relaterad incident har varit återkommande och tillsammans betraktas som en allvarlig incident i den mening som avses i artikel 8.2 i delegerad förordning (EU) 2024/1772. Finansiella entiteter ska ange om de icke-allvarliga IKT-relaterade incidenterna har varit återkommande och tillsammans betraktas som en allvarlig IKT-relaterad incident. Finansiella entiteter ska också ange antalet fall av sådana icke-allvarliga IKT-relaterade incidenter.	Nej	Nej	Ja, om den allvarliga incidenten omfattar mer än en icke-allvarlig återkommande incident.	Alfanumeriskt värde
4.16	Datum och tidpunkt för återkommande incidenter	Om finansiella entiteter rapporterar återkommande IKT-relaterade incidenter, datum och klockslag då den första IKT-relaterade incidenten inträffade.	Nej	Nej	Ja, för återkommande incidenter	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)

([1]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag och om ändring av rådets direktiv 82/891/EEG och Europaparlamentets och rådets direktiv 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU och 2013/36/EU samt Europaparlamentets och rådets förordningar (EU) nr 1093/2010 och (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Kommissionens genomförandeförordning (EU) 2018/1624 av den 23 oktober 2018 om fastställande i enlighet med Europaparlamentets och rådets direktiv 2014/59/EU av tekniska genomförandestandarder när det gäller förfaranden, standardformulär och mallar för den information som ska lämnas för upprättandet av resolutionsplaner för kreditinstitut och värdepappersföretag, och om upphävande av kommissionens genomförandeförordning (EU) 2016/1066 (EUT L 277, 7.11.2018, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

BILAGA III

MALLAR FÖR ANMÄLAN AV BETYDANDE CYBERHOT

Fältets nummer	Datafält	
1	Namnet på den entitet som lämnar in anmälan	
2	Identifieringskod för den entitet som lämnar in anmälan	
3	Typ av finansiell entitet som lämnar in anmälan	
4	Namnet på den finansiella entiteten	
5	LEI-kod för den finansiella entiteten	
6	Namnet på den primära kontaktpersonen	
7	E-postadress till den primära kontaktpersonen	
8	Telefonnummer till den primära kontaktpersonen	
9	Namnet på den sekundära kontaktpersonen	
10	E-postadress till den sekundära kontaktpersonen	
11	Telefonnummer till den sekundära kontaktpersonen	
12	Datum och tidpunkt då cyberhotet upptäcktes	
13	Beskrivning av det betydande cyberhotet	
14	Information om potentiella effekter	
15	Potentiella incidentklassificeringskriterier	
16	Status för cyberhotet	
17	Vidtagna åtgärder för att förhindra att hot förverkligas	
18	Anmälan till andra berörda parter	
19	Angreppsindikator	
20	Annan relevant information	

BILAGA IV

ORDLISTA OCH INSTRUKTIONER FÖR ANMÄLAN AV BETYDANDE CYBERHOT

Datafält	Beskrivning	Obligatoriskt	Fälttyp
1. Namnet på den entitet som lämnar in anmälan	Fullständigt juridiskt namn på den entitet som lämnar in anmälan.	Ja	Alfanumeriskt värde
2. Identifieringskod för den entitet som lämnar in anmälan	Identifieringskod för den entitet som lämnar in anmälan. Om de finansiella entiteterna lämnar in anmälan/rapporten ska identifieringskoden vara en identifieringskod för juridiska personer (LEI-kod), som är en unik kod med 20 alfanumeriska tecken, på grundval av ISO 17442–1:2020. Om en tredjepartsleverantör lämnar in en rapport för en finansiell entitet kan den använda en identifieringskod i enlighet med de tekniska genomförandestandarder som antagits i enlighet med artikel 28.9 i förordning (EU) 2022/2554.	Ja	Alfanumeriskt värde
3. Typ av finansiell entitet som lämnar in rapporten	Typ av entitet som avses i artikel 2.1 a–t i förordning (EU) 2022/2554 som lämnar in rapporten.	Ja, om rapporten inte tillhandahålls direkt av den berörda finansiella entiteten.	Val (flera val kan göras): — Kreditinstitut, — Betalningsinstitut, — Undantaget betalningsinstitut, — Leverantör av kontoinformationstjänster, — Institut för elektroniska pengar, — Undantaget institut för elektroniska pengar, — Värdepappersföretag, — Leverantör av kryptotillgångstjänster, — Emittent av tillgångsanknutna token, — Värdepapperscentral, — Central motpart, — Handelsplats, — Transaktionsregister, — Förvaltare av alternativa investeringsfonder, — Förvaltningsbolag, — Leverantör av datarapporteringstjänster,

Datafält		Beskrivning	Obligatoriskt	Fälttyp
				— Försäkrings- och återförsäkringsföretag, — Försäkringsförmedlare, återförsäkringsförmedlare och försäkringsförmedlare som bedriver förmedling som sidoverksamhet, — Tjänstepensionsinstitut, — Kreditvärderingsinstitut, — Administratör av kritiska referensvärden, — Leverantör av gräsrotsfinansieringstjänster, — Värdepapperiseringsregister.
4.	Namnet på den finansiella entiteten	Fullständigt juridiskt namn på den finansiella entitet som anmäler det betydande cyberhotet.	Ja, om den finansiella entiteten är en annan än den entitet som lämnar in anmälan.	Alfanumeriskt värde
5.	LEI-kod för den finansiella entiteten	Identifieringskoden för juridiska personer (LEI-koden) för den finansiella entitet som anmäler det betydande cyberhotet, vilken tilldelats i enlighet med Internationella standardiseringsorganisationen.	Ja, om den finansiella entitet som anmäler det betydande cyberhotet är en annan än den entitet som lämnar in rapporten.	En unik kod med 20 alfanumeriska tecken, på grundval av ISO 17442–1:2020.
6.	Namnet på den primära kontaktper-sonen	Namn och efternamn på den finansiella entitetens primära kontaktperson.	Ja	Alfanumeriskt värde
7.	E-postadress till den primära kontaktper-sonen	E-postadress till den primära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation.	Ja	Alfanumeriskt värde
8. Telefonnummer till den primära kontaktpersonen		Telefonnummer till den primära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation. Telefonnumret ska anges med alla internationella prefix (t.ex. +33XXXXXXXXX)	Ja	Alfanumeriskt värde
9.	Namnet på den sekundära kontaktper-sonen	Namn och efternamn på den sekundära kontaktpersonen för den finansiella entiteten eller en entitet som lämnar in anmälan för den finansiella entitetens räkning, om tillgängligt.	Ja, om namnet och efternamnet på den sekundära kontaktpersonen för den finansiella entiteten eller en entitet som lämnar in anmälan åt den finansiella entiteten finns tillgängligt.	Alfanumeriskt värde

Datafält		Beskrivning	Obligatoriskt	Fälttyp
10.	E-postadress till den sekundära kontaktpersonen	E-postadress till den sekundära kontaktpersonen eller en e-postadress till funktionsbrevlådan för gruppen som kan användas av den behöriga myndigheten för uppföljande kommunikation, om tillgänglig.	Ja, om en e-postadress till den sekundära kontaktpersonen eller en e-postadress till funktionsbrevlådan för gruppen som kan användas av den behöriga myndigheten för uppföljande kommunikation finns tillgänglig.	Alfanumeriskt värde
11. Telefonnummer till den sekundära kontaktpersonen		Telefonnummer till den sekundära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation, om tillgängligt. Telefonnumret ska anges med alla internationella prefix (t.ex. +33XXXXXXXXX).	Ja, om ett telefonnummer till den sekundära kontaktpersonen som kan användas av den behöriga myndigheten för uppföljande kommunikation finns tillgängligt.	Alfanumeriskt värde
12.	Datum och tidpunkt då cyberhotet upptäcktes	Datum och tidpunkt då den finansiella entiteten fick kännedom om det betydande cyberhotet.	Ja	ISO 8601 standard UTC (ÅÅÅÅ-MM-DD, tid: mm:ss)
13.	Beskrivning av det betydande cyberhotet	Beskrivning av de mest relevanta aspekterna av det betydande cyberhotet. Finansiella entiteter ska tillhandahålla a) en översikt på hög nivå över de mest relevanta aspekterna av det betydande cyberhotet, b) de relaterade risker som uppstår till följd av detta, inbegripet potentiella sårbarheter hos den finansiella entitetens system som kan utnyttjas, c) information om sannolikheten för att det betydande cyberhotet förverkligas och d) information om källan till informationen om cyberhotet.	Ja	Alfanumeriskt värde
14.	Information om potentiella effekter	Information om cyberhotets potentiella effekter på den finansiella entiteten, dess kunder eller finansiella motparter om cyberhotet har förverkligats	Ja	Alfanumeriskt värde
15.	Potentiella incidentklassificeringskriterier	De klassificeringskriterier som kunde ha utlöst en rapport om en allvarlig incident om cyberhotet hade förverkligats.	Ja	Val (flera val kan göras): — Berörda kunder, finansiella motparter och transaktioner, — Påverkan på anseendet, — Varaktighet och driftstopp, — Geografisk spridning, — Dataförluster, — Berörda kritiska tjänster, — Ekonomiska effekter.

Datafält	Beskrivning	Obligatoriskt	Fälttyp
16. Status för cyberhotet	Information om cyberhotets status för den finansiella entiteten och om det har skett några förändringar med avseende på hotaktiviteten. Om cyberhotet har upphört att kommunicera med den finansiella entitetens informationssystem kan statusen markeras som inaktiv. Om den finansiella entiteten har information om att hotet fortfarande är aktivt mot andra parter eller det finansiella systemet som helhet ska statusen markeras som aktiv.	Ja	Val: — Aktivt, — Inaktivt.
17. Vidtagna åtgärder för att förhindra att hot förverkligas	Information på hög nivå om de åtgärder som vidtagits av den finansiella entiteten för att förhindra att betydande cyberhot förverkligas, i tillämpliga fall.	Ja	Alfanumeriskt värde
18. Anmälan till andra berörda parter	Information om anmälan av cyberhotet till andra finansiella entiteter eller myndigheter.	Ja, om andra finansiella entiteter eller myndigheter har informerats om cyberhotet).	Alfanumeriskt värde
19. Angreppsindikator	Information om det betydande hotet som kan bidra till att identifiera skadlig aktivitet inom ett nätverks- eller informationssystem (angreppsindikatorer), i tillämpliga fall. Den angreppsindikator som anges av den finansiella entiteten kan omfatta, men är inte begränsad till, följande kategorier av uppgifter: a) IP-adresser, b) URL-adresser, c) Domäner, d) Filhashar, e) Uppgifter om sabotageprogram (namn på sabotageprogram, filnamn och var de finns, specifika registernycklar som är kopplade till aktivitet som rör sabotageprogram), f) Uppgifter om nätverksaktivitet (portar, protokoll, adresser, referenser, användaragenter, rubriker, specifika loggar eller distinkta mönster i nätverkstrafiken), g) Uppgifter om e-postmeddelanden (avsändare, mottagare, ämne, rubrik, innehåll), h) DNS-begäranden och registerkonfigurationer, i) Aktiviteter på användarkonton (inloggningar, aktivitet på privilegierade användarkonton, eskalering av privilegier), j) Databastrafik (läsa/skriva), begäranden avseende samma fil. Denna typ av information kan omfatta data som avser indikatorer som beskriver mönster i nätverkstrafik som motsvarar kända attacker/botnätmeddelanden, IP-adresser för maskiner som är infekterade med sabotageprogram (botar), data som avser ledningsservrar som används av sabotageprogram (vanligen domäner eller IP-adresser) och URL:er som avser platser för nätfiske eller webbplatser som observerats som värdar för sabotageprogram eller exploateringsverktyg.	Ja, om information om angreppsindikatorer i samband med cyberhotet finns tillgänglig.)	Alfanumeriskt värde
20. Annan relevant information	All annan relevant information om det betydande cyberhotet	Ja, om tillämpligt och om det finns annan information tillgänglig som inte ingår i mallen.	Alfanumeriskt värde

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj