Europeiska unionens råd

Bryssel den 31 oktober 2022
(OR. en)

14128/22

Interinstitutionellt ärende:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

I/A-PUNKTSNOT

från:	Rådets generalsekretariat
till:	Ständiga representanternas kommitté (Coreper II)/rådet
Föreg. dok. nr:	10097/5/22 REV 5
Komm. dok. nr:	7474/22 + ADD 1
Ärende:	Förslag till Europaparlamentets och rådets förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer – Allmän riktlinje

INLEDNING

1. Den 22 mars 2022 antog kommissionen förslaget till Europaparlamentets och rådets förordning om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer. Förslaget var en av åtgärderna i EU:s strategi för cybersäkerhet för ett digitalt decennium[1] som syftar till att stärka unionens kollektiva resiliens mot cyberhot.

[1] 14133/20.

I sina slutsatser av den 22 mars 2022 om denna strategi[2] betonade rådet att cybersäkerhet är ”avgörande för den offentliga förvaltningens och institutionernas funktion på både nationell nivå och EU-nivå och för vårt samhälle och ekonomin som helhet”.

2. Kommissionens förslag, som grundar sig på artikel 298 i fördraget om Europeiska unionens funktionssätt, syftar till att förbättra cybersäkerhetsnivån vid unionens institutioner, organ och byråer genom att inrätta en gemensam ram, med vederbörlig hänsyn till varje unionsentitets autonomi. Mer specifikt är förslagets mål att

   – stärka CERT-EU:s (autonom interinstitutionell datorincidenthanteringsorganisation för unionens entiteter) mandat och finansiering,

   – inrätta en interinstitutionell struktur (den interinstitutionella cybersäkerhetsstyrelsen – IICB) med företrädare för alla unionsentiteter för att säkerställa ett korrekt genomförande av förordningen,

   – införa en skyldighet för unionsentiteterna att dela (icke-sekretessbelagd) information om incidenter med CERT-EU och att rapportera betydande hot, sårbarheter och incidenter och

   – att främja samordning och samarbete vid betydande incidenter.

3. Europaparlamentet har utsett Henna Virkkunen (EPP) till föredragande i utskottet för industrifrågor, forskning och energi, som är det utskott som är ansvarigt. Förslaget till betänkande offentliggjordes den 7 oktober 2022.

4. Europeiska datatillsynsmannen lämnade sitt yttrande den 17 maj 2022[3].

[2] 6722/21.
[3] 9252/22.

5. I rådet inleddes behandlingen av förslaget i den övergripande arbetsgruppen för cyberfrågor under det franska ordförandeskapet den 29 mars 2022. Det franska ordförandeskapet utarbetade den första kompromisstexten, som diskuterades i arbetsgruppen i juni 2022, och överlämnade en lägesrapport[4] till rådet den 21 juni 2022.

6. Under det tjeckiska ordförandeskapet ägnade arbetsgruppen åtta möten[5] åt diskussioner om förslaget och om flera på varandra följande kompromisstexter.

7. Den 23 maj 2022 begärde ordförandeskapet ett yttrande från rådets säkerhetskommitté om de aspekter av förslaget som rör informationssäkerhet och särskilt säkerhetsskyddsklassificerade uppgifter. Säkerhetskommittén avgav sitt yttrande den 19 september 2022[6]. Såsom säkerhetskommittén föreslog har säkerhetsskyddsklassificerade EU-uppgifter uttryckligen undantagits från förordningens tillämpningsområde. Bestämmelserna om undantag från delnings- och rapporteringsskyldigheter avseende information som mottagits utanför unionsentiteterna har ändrats i enlighet med detta.

8. Den 28 oktober 2022 nådde den övergripande arbetsgruppen för cyberfrågor en överenskommelse om ordförandeskapets kompromisstext som återges i bilagan.

---

4 9719/22.

5 Den 6 och 20 juli, 13, 21 och 28 september samt 5, 19 och 28 oktober 2022.

6 12603/22 + COR 1.

DE VIKTIGASTE FRÅGORNA

9. Medlemsstaterna välkomnade förslaget som lägligt och som ett komplement till det framtida direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet) och stödde dess allmänna mål. Medlemsstaterna efterlyste dock ytterligare anpassningar till NIS 2, ökad ömsesidighet i informationsutbytet mellan unionsentiteterna och medlemsstaterna, och pekade på att vissa av de föreslagna åtgärderna är alltför frivilliga. Medlemsstaterna meddelade också att de föredrog att hänvisningarna till den gemensamma cyberenheten, vars mandat och sammansättning ännu inte har fastställts, tas bort.

10. På grundval av diskussionerna i den övergripande arbetsgruppen för cyberfrågor har följande punkter identifierats som de viktigaste politiska frågorna:

a) Anpassning till det framtida NIS 2-direktivet

Såsom medlemsstaterna har begärt har ytterligare anpassningar gjorts till det framtida NIS 2-direktivet, bl.a.

- har ett antal definitioner (artikel 3) anpassats till definitionerna i NIS 2,
- har en ny artikel 7a införts om frivilliga sakkunnigbedömningar, i linje med NIS 2, anpassade till unionsentiteternas behov,
- har rapporteringsskyldigheterna i artikel 20 anpassats till dessa skyldigheter i NIS 2.

b) Den interinstitutionella cybersäkerhetsstyrelsens (IICB) sammansättning (artikel 9)

Efter diskussioner om lämpligt deltagande av medlemsstaternas företrädare i IICB:s arbete nåddes en kompromiss genom ett uttalande från rådet till protokollet.

c) Institutionell autonomi

En balanserad strategi valdes mellan medlemsstaternas vilja att stärka efterlevnadsmekanismerna och behovet av att respektera principen om institutionell autonomi, särskilt när det gäller revisioner och disciplinåtgärder (artikel 11).

Slutligen ströks hänvisningen till en viss procentandel av it-budgeten för cybersäkerhet från skäl 8.

SLUTSATS

11. Coreper uppmanas att

a) godkänna kompromisstexten enligt bilagan, som sedan kommer att utgöra mandat för förhandlingarna med Europaparlamentet,

b) uppmana rådet att godkänna kompromisstexten enligt bilagan vid mötet den 18 november 2022 och att ta rådets uttalande i addendumet till detta dokument till protokollet.

BILAGA

2022/0085 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om åtgärder för en hög gemensam cybersäkerhetsnivå vid unionens institutioner, organ och byråer

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 298,

med beaktande av fördraget om upprättandet av Europeiska atomenergigemenskapen, särskilt artikel 106a,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) I den digitala tidsåldern är informations- och kommunikationsteknik en hörnsten i en öppen, effektiv och oberoende unionsadministration. Ny teknik och de digitala systemens ökade komplexitet och sammankopplingar förstärker cybersäkerhetsriskerna och gör unionsadministrationen mer sårbar för cyberhot och incidenter, vilket i slutändan utgör ett hot mot administrationens driftskontinuitet och kapacitet att säkra sina data. Ökad användning av molntjänster, allmänt utbredd användning av it, omfattande digitalisering, distansarbete och framväxande teknik och konnektivitet är i dag centrala inslag i all verksamhet inom unionens administrativa entiteter, men den digitala resiliensen är ännu inte tillräckligt inbyggd.

(2) Unionens […] **entiteter** konfronteras med ett cyberhotlandskap i ständig utveckling. Hotaktörernas taktik, metoder och förfaranden utvecklas hela tiden, samtidigt som de främsta motiven bakom angrepp förändras föga, från att stjäla värdefull icke-offentlig information till att tjäna pengar, manipulera den allmänna opinionen eller undergräva digital infrastruktur. De utför sina cyberangrepp i en allt snabbare takt med alltmer sofistikerade och automatiserade kampanjer, riktar in sig på exponerade attackytor som bara blir större och är snabba att utnyttja sårbarheter.

(3) Unionens **entiteter** […] har sammankopplade it-miljöer och integrerade dataflöden, och deras användare har ett nära samarbete. Denna sammankoppling innebär att alla störningar, även om de inledningsvis endast berör en […] **unionsentitet**, kan få större kaskadeffekter med långtgående och långvariga negativa konsekvenser för de andra. Dessutom är vissa unionsentiteters it-miljöer sammankopplade med medlemsstaternas it-miljöer, så att en incident hos en unionsentitet kan utgöra en risk för cybersäkerheten i medlemsstaternas it-miljöer och vice versa. **Vidare hanterar unionsentiteterna stora mängder ofta känslig information från medlemsstaterna, och incidenter kan därför även inverka negativt på medlemsstaterna. Unionsentiteternas cybersäkerhet är därför av stor betydelse även för medlemsstaterna**. **Incidentspecifik information kan också underlätta upptäckt av liknande cyberhot eller cyberincidenter som påverkar medlemsstaterna.**

(4) Unionens […] **entiteter** är attraktiva mål som konfronteras med mycket avancerade och resursstarka hotaktörer, liksom även andra hot. Samtidigt varierar cyberresiliensens nivå och mognad och förmågan att upptäcka och hantera skadlig cyberverksamhet avsevärt mellan dessa entiteter. För att den europeiska administrationen ska fungera är det därför nödvändigt att unionens […] **entiteter** uppnår en hög gemensam cybersäkerhetsnivå genom **genomförande av cybersäkerhetsåtgärder,** […] informationsutbyte och samarbete.

(5) Direktivet [förslag till NIS 2] om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen syftar till att ytterligare förbättra cybersäkerhetsresiliensen och incidenthanteringskapaciteten hos offentliga och privata entiteter, nationella behöriga myndigheter och organ samt unionen som helhet. Det är därför nödvändigt att unionens […] **entiteter** följer detta genom att säkerställa regler som är förenliga med direktivet [förslag till NIS 2] och som återspeglar dess ambitionsnivå.

(6) För att uppnå en hög gemensam cybersäkerhetsnivå är det nödvändigt att varje […] **unionsentitet** inrättar en intern ram för hantering, styrning och kontroll av cybersäkerhetsrisker vilken säkerställer en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker […]. **Ramen bör fastställa strategier för cybersäkerhet, inbegripet förfaranden för att bedöma effektiviteten i genomförda cybersäkerhetsåtgärder. Ramen bör bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på unionsentitetens information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, äktheten, integriteten eller konfidentialiteten hos uppgifter som lagras, överförs, behandlas eller är tillgängliga via nätverks- och informationssystem. Ramen bör återspegla resultaten från riskanalysen, och ta hänsyn till alla relevanta tekniska, operativa och organisatoriska risker för den berörda unionsentitetens cybersäkerhet.**

(6a) För att hantera de risker som identifierats inom ramen bör varje unionsentitet säkerställa att lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder vidtas. Dessa bör omfatta de områden, inbegripet cybersäkerhetsåtgärder som fastställs i denna förordning för att stärka cybersäkerheten för varje unionsentitet.

(6b) De tillgångar och risker som identifierats enligt ramen samt de slutsatser som härleds från regelbundna mognadsbedömningar bör återspeglas i en cybersäkerhetsplan som upprättas av varje unionsentitet. Cybersäkerhetsplanen bör innefatta anpassade cybersäkerhetsåtgärder som syftar till att öka den berörda unionsentitetens övergripande cybersäkerhet.

(6c) Säkerställandet av cybersäkerheten är en kontinuerlig process och således bör samtliga åtgärders lämplighet och ändamålsenlighet regelbundet ses över mot bakgrund av de föränderliga riskerna, tillgångarna och unionsentiteternas mognad. Ramen bör ses över med jämna mellanrum och åtminstone vart tredje år. Cybersäkerhetsplanen bör ses över åtminstone vartannat år eller efter varje mognadsbedömning eller varje översyn av ramen.

(6d) Unionsentiteter bör med jämna mellanrum utbyta relevant information, inbegripet vad beträffar relevanta incidenter och cyberhot samtidigt som konfidentiell behandling och lämpligt skydd säkerställs för den information som den rapporterande unionsentiteten tillhandahåller.

(6e) En mekanism för att säkerställa ett effektivt informationsutbyte, samordning och samarbete mellan unionens entiteter vid större incidenter bör inrättas. Av denna bör de inblandade unionsentiteternas roller och uppgifter klart framgå. Den utbytta informationen bör beaktas av den utsedda kontaktpunkten för EU-CyCLONe när relevant information delas med EU-CyCLONe som ett bidrag till den gemensamma situationsmedvetenheten.

(7) Skillnaderna mellan unions[...] **entiteter**na kräver flexibilitet i genomförandet eftersom samma lösning inte passar alla. Åtgärderna för en hög gemensam cybersäkerhetsnivå bör inte omfatta några skyldigheter som direkt inkräktar på unions**entiteternas** utövande av sitt uppdrag eller deras institutionella autonomi. Dessa [...] **unionsentiteter** bör därför fastställa sina egna ramar för hantering, styrning och kontroll av cybersäkerhetsrisker **och cybersäkerhetsplaner** och anta [...] cybersäkerhets [...] **åtgärder**. **Vid genomförandet av sådana åtgärder bör vederbörlig hänsyn tas till befintliga synergier mellan unionsentiteterna så att resurserna hanteras på ett korrekt sätt och kostnader optimiseras. Det bör också vederbörligen beaktas att åtgärderna inte på ett negativt sätt inverkar på unionsentiteternas effektiva informationsutbyte och samverkan med andra unionsentiteter och nationella behöriga myndigheter.**

(8) För att inte ålägga unions**entiteterna**oproportionella finansiella och administrativa bördor bör riskhanteringskraven för cybersäkerhet stå i proportion till den risk som det berörda nätverks- och informationssystemet utgör, med beaktande av den senaste utvecklingen i fråga om sådana åtgärder. Varje unions**entitet** bör sträva efter att anslå en tillräcklig procentandel av sin IKT-budget för att förbättra sin cybersäkerhetsnivå; **Mognadsbedömningen bör också utvärdera om unionsentitetens cybersäkerhetsutgifter står i proportion till de risker entiteten utsatts för.**

(9) En hög gemensam cybersäkerhetsnivå kräver att cybersäkerhet övervakas av den högsta ledningsnivån för varje unions[...]**entitet. [...] Den högsta ledningsnivån bör utöva tillsyn över genomförandet av denna förordning, inbegripet inrättandet av ramen för riskhantering, styrning och kontroll samt cybersäkerhetsplaner, vilket också innefattar cybersäkerhetsåtgärder.** Att etablera en cybersäkerhetskultur, dvs. dagliga cybersäkerhetsrutiner, är en viktig del av en **ram** [...] för cybersäkerhet vid alla unions**entiteter**.

(10) [...] [...] **Cybersäkerhets**åtgärderna bör utgöra en del av **[...] planen** för cybersäkerhet och specificeras ytterligare i vägledningar eller rekommendationer som utfärdas av CERT-EU. Vid fastställandet av åtgärder och riktlinjer bör vederbörlig hänsyn tas till **den senaste utvecklingen och, i förekommande fall, relevanta europeiska och internationella normer samt** relevant EU-lagstiftning och EU-politik, inbegripet riskbedömningar och rekommendationer som utfärdats av samarbetsgruppen för nät- och informationssäkerhet, såsom EU:s samordnade riskbedömning och EU:s verktygslåda för 5G-cybersäkerhet. Dessutom kan certifiering av relevanta IKT-produkter, IKT-tjänster och IKT-processer krävas enligt särskilda EU-ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. **Där så är lämpligt bör CERT-EU samarbeta med Enisa.**

(11) I maj 2011 beslutade generalsekreterarna för unionens institutioner och organ att inrätta en förkonfigurationsgrupp för en incidenthanteringsorganisation för unionens institutioner, organ och byråer (CERT-EU) som övervakas av en interinstitutionell styrelse. I juli 2012 bekräftade generalsekreterarna de praktiska arrangemangen och enades om att behålla CERT-EU som en permanent entitet för att fortsätta att förbättra den övergripande it-säkerheten vid unionens institutioner, organ och byråer som ett exempel på synligt interinstitutionellt samarbete inom cybersäkerhet. I september 2012 inrättades CERT-EU som en arbetsgrupp inom Europeiska kommissionen med ett interinstitutionellt mandat. I december 2017 ingick unionens institutioner och organ ett interinstitutionellt avtal om organisationen och driften av CERT-EU[7]. Denna [...] **förordning** bör [...] **innehålla en vittomfattande uppsättning regler om organisationen och driften av CERT-EU. Bestämmelserna i den här förordningen har företräde framför bestämmelserna i det interinstitutionella avtalet om organisationen och driften av CERT-EU som ingicks i december 2017**.

[...]

[7] EUT C 12, 13.1.2018, s. 1.

(13) Många cyberangrepp är en del av bredare kampanjer som inriktas på grupper av unions**entiteter** eller intressegrupper som inbegriper unions**entiteter**. För att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder bör unions**entiteter** underrätta CERT-EU om [...] cyberhot, [...] sårbarheter, **tillbud och** [...] incidenter och dela med sig av lämpliga tekniska detaljer som gör det möjligt att upptäcka eller begränsa samt vidta åtgärder mot liknande cyberhot, **sårbarheter, tillbud och** incidenter i andra unions[...]**entiteter**. Enligt samma tillvägagångssätt som i direktiv [förslag till NIS 2] bör **unions**entiteter som blir medvetna om en betydande incident vara skyldiga att lämna en [...] **tidig varning** till CERT-EU inom 24 timmar. Sådant informationsutbyte bör göra det möjligt för CERT-EU att sprida informationen till andra unions**entiteter** samt till lämpliga motparter, för att bidra till att skydda unionens IKT-miljöer och unionens motparters IKT-miljöer mot liknande incidenter[...].

(13a) I denna förordning fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att minska den potentiella spridningen av betydande incidenter och gör det möjligt för unionsentiteter att söka stöd, och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar enskilda unionsentiteters motståndskraft mot cyberhot. I detta avseende, bör den här förordningen innefatta rapportering om incidenter som, enligt en inledande bedömning som utförs av unionsentiteten, skulle kunna orsaka allvarliga driftstörningar i unionsentitetens verksamhet eller ekonomiska förluster för den berörda unionsentiteten eller ha en inverkan på andra fysiska eller juridiska personer genom att åsamka materiell eller immateriell skada. Denna inledande bedömning bör bland annat beakta de påverkade nätverks- och informationssystemen, särskilt deras betydelse för unionsentitetens funktionssätt, cyberhotets allvar och tekniska egenskaper, eventuella underliggande sårbarheter som utnyttjas samt unionsentitetens erfarenhet av liknande incidenter. Sådana indikatorer som i vilken omfattning unionsentitetens funktionssätt påverkas, hur länge en incident pågår eller antalet fysiska eller juridiska personer som påverkas kan spela en viktig roll vid bestämningen av huruvida driftsstörningen är allvarlig.

(13b) Då infrastrukturen och nätverken för den relevanta unionsentiteten och den medlemsstat där unionsentiteten är belägen, är sammankopplade är det avgörande att nämnda medlemsstat utan oskäligt dröjsmål underrättas om en betydande incident inom denna unionsentitet. I detta syfte bör den drabbade unionsentiteten underrätta CERT-EU´s nationella motpart, som utsetts av medlemsstaten i enlighet med direktivet [förslag NIS 2] inom samma tidsram som den bör rapportera om en betydande incident till CERT-EU. CERT-EU bör även underrätta denna nationella motpart när det får kännedom om en betydande incident inom medlemsstaten, såvida incidenten inte redan inrapporterats av den drabbade unionsentiteten.

(14) Utöver att ge CERT-EU fler uppgifter och en utökad roll bör det, **i syfte att främja en hög gemensam cybersäkerhetsnivå vid unionens entiteter** inrättas en interinstitutionell cybersäkerhetsstyrelse (IICB) som bör **ha en exklusiv roll** [...] [...] **när det gäller att** övervaka unions**entiteternas** genomförande av denna förordning och **när det gäller att** övervaka CERT-EU:s genomförande av allmänna prioriteringar och mål samt tillhandahålla strategisk ledning för CERT-EU. IICB bör **därför** säkerställa att institutionerna företräds och inkludera företrädare för byråer och organ genom unionsbyråernas nätverk. **Organisationen och driften av IICB bör regleras ytterligare i dess inre arbetsordning som kan innehålla närmare bestämmelser om IICB:s regelbundna möten, inbegripet årliga sammankomster på politisk nivå där företrädare för den högsta ledningsnivån för varje medlem i IICB skulle göra det möjligt för IICB att hålla strategiska diskussioner och ge strategisk vägledning. IICB kan vidare inrätta en verkställande kommitté som bistår den i dess arbete och delegera vissa av sina uppgifter och befogenheter till denna kommitté, särskilt vad beträffar uppgifter som kräver** [...] **särskild kompetens av sina medlemmar, som t. ex. godkännandet av tjänstekatalogen och eventuella senare uppdateringar av denna, arrangemangen för servicenivåavtal, bedömningar av dokument och rapporter som unionsentiteter inlämnat till IICB enligt denna förordning eller uppgifter som hör samman med utarbetande av beslut om efterlevnadsåtgärder som meddelas av IICB och övervakningen av deras genomförande. IICB bör fastställa den verkställande kommitténs arbetsordning, inbegripet dess uppgifter och befogenheter.**

(15) CERT-EU bör stödja genomförandet av åtgärder för en hög gemensam cybersäkerhetsnivå genom förslag till vägledningar och rekommendationer till IICB eller genom att utfärda uppmaningar till åtgärder. Sådana vägledningar och rekommendationer bör godkännas av IICB. Vid behov bör CERT-EU utfärda uppmaningar till åtgärder där man beskriver brådskande säkerhetsåtgärder som unions[...] **entiteter** uppmanas att vidta inom en fastställd tidsram. **IICB får ge CERT-EU i uppdrag att utfärda, dra tillbaka eller ändra ett förslag till vägledningar eller rekommendationer, eller en uppmaning till åtgärder.**

(16) IICB bör övervaka efterlevnaden av denna förordning samt uppföljningen av vägledningar och rekommendationer och uppmaningar till åtgärder [...]. IICB bör i tekniska frågor stödjas av tekniska rådgivande grupper i en sammansättning som IICB anser lämplig vilka bör arbeta i nära samarbete med CERT-EU, unions[...]**entiteter** och andra intressenter i enlighet med vad som är nödvändigt. **[...] Om IICB konstaterar att unionsentiteter inte har tillämpat eller genomfört denna förordning, inbegripet vägledningar, rekommendationer eller uppmaningar till åtgärder som utfärdats enligt denna förordning, får IICB, utan att det påverkar de interna förfarandena för unionsentiteten i fråga, vidta efterlevnadsåtgärder. Ordningen med efterlevnadsåtgärder bör användas progressivt beroende på hur allvarlig överträdelsen är. När IICB antar efterlevnadsåtgärder bör den följaktligen börja med en varning som är den minst ingripande åtgärden, och om det visar sig nödvändigt, trappa upp till den allra strängaste åtgärden som består i att utfärda en rekommendation om ett tillfälligt stopp för dataflöden till den berörda unionsentiteten, som ska tillämpas i undantagsfall då den berörda entitetens bristande efterlevnad av dess skyldigheter enligt denna förordning varit långvarig, avsiktlig och /eller allvarlig.**

(16a) En varning är den minst ingripande efterlevnadsåtgärden för att komma till rätta med en unionsentitets konstaterade tillkortakommanden. Den innehåller rekommendationer om att ändra entitetens cybersäkerhetsdokument inom en fastställd tidsram. Varningen bör vara tillgänglig för all unionsentiteter utom i de fall då varningens målgrupp begränsats på lämpligt sätt i enlighet med den här förordningen.

(16b) IICB kan också rekommendera att en revision av en unionsentitet ska utföras. Unionsentiteten får använda sin interna revisionsfunktion i detta syfte. IICB kan också begära att en revision ska utföras av en tredjeparts revisionstjänst, t. ex. en ömsesidigt överenskommen tjänsteleverantör från den privata sektorn.

(16c) På grundval av resultaten av en revision som utförts på rekommendation eller begäran av IICB, får IICB vidare begära att unionsentiteten ser till att hanteringen, styrningen och kontrollen av cybersäkerhetsrisker sker i enlighet med bestämmelserna i denna förordning.

(16d) Då medlemsstaterna med relevanta unionsentiteter delar information som kan vara känslig till sin karaktär är cybersäkerheten hon adressaten till sådan information avgörande för medlemsstaterna. Följaktligen kan IICB i undantagsfall då unionsentitetens bristande efterlevnad av dess skyldigheter varit långvarig, avsiktlig och /eller allvarlig, som en sista utväg utfärda en vägledning till alla medlemsstater och unionsentiteter med en rekommendation om att tillfälligt stoppa unionsentitetens dataflöden, som bör gälla till dess att cybersäkerhetsförhållandena inom den aktuella entiteten korrigerats. Vägledningen bör delges alla medlemsstater och unionsentiteter genom lämpliga säkra kommunikationskanaler.

(16e) **För att säkerställa att den här förordningen genomförs på ett korrekt sätt bör IICB, om den anser att en unionsentitets kontinuerliga bristande efterlevnad av den här förordningen direkt föranletts av handling eller underlåtenhet av en av dess anställda, inbegripet på högsta ledningsnivå, begära att den berörda unionsentiteten ska vidta lämpliga åtgärder mot vederbörande, i enlighet med tjänsteföreskrifterna och andra motsvarande regler som äger tillämpning inom vissa unionsentiteter. Sådana åtgärder kan bland annat innefatta disciplinära förfaranden och, i förekommande fall, i det särskilda fallet med unionsorgan, en begäran till den behöriga myndigheten att vidta nödvändiga åtgärder för att eventuellt avsätta den person som kan vara ansvarig för kontinuerlig bristande efterlevnad av denna förordning.**

(17) CERT-EU bör ha i uppdrag att bidra till säkerheten i IKT-miljön för alla unions**entiteter**. **När CERT-EU överväger huruvida man ska lämna teknisk rådgivning eller yttra sig över relevanta politiska frågor på begäran av en unionsentitet bör styrelsen säkerställa att detta inte hindrar fullgörandet av dess övriga uppgifter enligt denna förordning.**

(17a) CERT-EU bör fungera som motsvarighet till den utsedda samordnaren för unions[...]**entiteterna** när det gäller samordnad information om sårbarheter till det europeiska sårbarhetsregister som avses i artikel 6 i direktiv [förslag NIS 2] **och bör ta fram en policy för hantering av sårbarheter, som innefattar frivillig samordnad information om sårbarheter.**

[...]

(19) CERT-EU bör också fullgöra den roll som föreskrivs i direktiv [förslag NIS 2] när det gäller samarbete och informationsutbyte med nätverket av enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). I enlighet med kommissionens rekommendation (EU) 2017/1584[8] bör CERT-EU dessutom samarbeta och samordna insatserna med berörda parter. För att bidra till en hög cybersäkerhetsnivå i hela unionen bör CERT-EU utbyta incidentspecifik information med nationella motparter. CERT-EU bör också samarbeta med andra offentliga och privata motparter, även vid Nato, efter förhandsgodkännande från IICB.

[8] Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

(20) För att stödja operativ cybersäkerhet bör CERT-EU utnyttja tillgänglig expertis hos Europeiska unionens cybersäkerhetsbyrå **(Enisa)** genom strukturerat samarbete i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881[9]. Vid behov bör särskilda arrangemang mellan de båda entiteterna inrättas för att definiera det praktiska genomförandet av detta samarbete och undvika dubbelarbete. CERT-EU bör samarbeta med **Enisa** [...] om hotbildsanalys och regelbundet dela med sig av sin hotbildsrapport till byrån.

[...]

(22) **CERT-EU:s verksamhet och informationshantering enligt denna förordning kan inbegripa behandling av personuppgifter.** Alla personuppgifter som behandlas enligt denna förordning bör behandlas i enlighet med dataskyddslagstiftningen, inklusive Europaparlamentets och rådets förordning (EU) 2018/1725[10]. **Om personuppgifter i enlighet med denna förordning överförs till andra mottagare som är etablerade i unionen än unionsentiteter bör detta ske i enlighet med artikel 9 i förordning (EU) 2018/1725.**

---

9 Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

10 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).

(23) CERT-EU:s och unions[...]**entiteternas** hantering av information ska stämma överens med **tillämpliga** regler [...] om informationssäkerhet.

(23a) När information utbyts används synliga markeringar för att ange att mottagarna av informationen ska följa begränsningar när de delar den, särskilt på grundval av sekretessavtal, eller informella sekretessavtal såsom Traffic Light Protocol eller andra tydliga indikationer från avsändaren. Traffic Light Protocol ska förstås som ett sätt att ge information om eventuella begränsningar i fråga om ytterligare spridning av informationen. Protokollet används i nästan alla enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och i vissa centrum för informationsutbyte och analys.

(24) **Denna förordning och de nya uppgifter som tilldelats CERT-EU kommer inte att påverka de totala utgifterna inom ramen för den fleråriga budgetramen.** Eftersom CERT-EU:s tjänster och uppgifter ligger i alla unions**entiteters** intresse bör varje unions**entitet** med IKT-utgifter bidra med en skälig andel till dessa tjänster och uppgifter. Dessa bidrag påverkar inte budgetautonomin för unions[...]**entiteter**. **Alla unionsentiteter och deras förvaltningar bör säkerställa att deras resurser optimeras på nuvarande nivå och stärka effektivitetsvinsterna, bland annat genom att fördjupa det interinstitutionella samarbetet på cybersäkerhetsområdet. Därför bör en gemensam strategi för sammanslagning av administrativa utgifter ges företräde framför individualiserade utgifter för unionsentiteter.**

(25) IICB bör, med CERT-EU:s hjälp, se över och utvärdera genomförandet av denna förordning och rapportera sina resultat till kommissionen. På grundval av dessa uppgifter bör kommissionen rapportera till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén. **Dessutom uppmanas Europeiska revisionsrätten att regelbundet utvärdera hur CERT-EU fungerar.**

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Kapitel I
ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. I denna förordning fastställs **åtgärder som syftar till att uppnå en hög gemensam cybersäkerhetsnivå inom unionsentiteterna** [...]:

2. Därför föreskrivs följande i denna förordning:

c) Skyldigheter för **varje** unions[...] **entitet** att inrätta **en** [...] ram för hantering, styrning och kontroll av cybersäkerhetsrisker.

d) Skyldigheter när det gäller riskhantering, rapportering [...] **och informationsdelning** på cybersäkerhetsområdet för unionens **entiteter**.

e) Regler om organisationen, **funktionssätt**et och driften av den [...] **autonoma interinstitutionella datorincidenthanteringsorganisationen** för unionens **entiteter** (CERT-EU) och om organisationen, **funktionssättet** och driften av den interinstitutionella cybersäkerhetsstyrelsen (**IICB**).

f) Regler för övervakning av genomförandet av denna förordning.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på [...] alla unions[...]**entiteter** och på [...] [...] CERT-EU och **IICB** [...].

2. Denna förordning ska tillämpas utan att det påverkar den institutionella autonomin enligt fördragen.

3. Med undantag för artikel 12.7 ska denna förordning inte tillämpas på nätverks- och informationssystem som hanterar säkerhetsskyddsklassificerade Eu-uppgifter (EUCI).

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *Unions[...]**entiteter***: de unionsinstitutioner, unionsorgan, unions**kontor** och unionsbyråer som inrättats genom, eller på grundval av, fördraget om Europeiska unionen, fördraget om Europeiska unionens funktionssätt eller fördraget om upprättandet av Europeiska atomenergigemenskapen.

2. *Nätverks- och informationssystem*: **ett** nätverks- och informationssystem enligt [...] **definitionen i** artikel 4.1 i direktiv [förslag till NIS 2].

3. *Säkerhet i nätverks- och informationssystem:* säkerhet i nätverks- och informationssystem **enligt** [...] **definitionen i** artikel 4.2 i direktiv [förslag till NIS 2].

4. *Cybersäkerhet*: cybersäkerhet **enligt** [...] **definitionen i artikel 2.1 i förordning (EU) 2019/881.**

5. *Högsta ledningsnivå*: en chef eller ett lednings- eller samordnings- och tillsynsorgan på den högsta administrativa nivån **med beslutsbefogeneheter**, med beaktande av styrningsarrangemangen på hög nivå inom varje unions**entitet**.

5a. *Tillbud*: ett tillbud enligt definitionen i artikel 4.4a i direktiv [förslag till NIS 2].

6. *Incident*: incident [...] **enligt definitionen i** artikel 4.5 i direktiv [förslag till NIS 2].

[...]

8. *Betydande **incident***: [...] varje incident **som leder till en störningsnivå som kräver mer resurser än vad som finns att tillgå vid en unionsentitet och överträffar CERT-EU:s förmåga att reagera på den eller som har betydande konsekvenser för åtminstone två unionsentiteter**. [...]

9. *Incidenthantering*: incidenthantering [...] **enligt definitionen i** artikel 4.6 i direktiv [förslag till NIS 2].

10. *Cyberhot*: cyberhot [...] **enligt definitionen i** artikel 2.8 i förordning (EU) 2019/881.

[...]

12. *Sårbarhet*: sårbarhet i den mening som avses i artikel 4.8 i direktiv [förslag till NIS 2].

[...]

14. [...] *Risk*: **risk i den mening som avses i artikel 4.7b i direktiv [förslag till NIS 2]**[...].

[...]

[...]

Artikel 3a

Behandling av personuppgifter

1) Behandling av personuppgifter enligt denna förordning som utförs av CERT-EU, IICB eller unionsentiteter ska utföras i enlighet med förordning (EU) 2018/1725.

2) CERT-EU, IICB och unionens entiteter ska behandla och utbyta personuppgifter i den utsträckning som är nödvändig och uteslutande i syfte att fullgöra sina respektive skyldigheter enligt denna förordning.

Kapitel II
ÅTGÄRDER FÖR EN HÖG GEMENSAM CYBERSÄKERHETSNIVÅ

Artikel 4

Ram för hantering, styrning och kontroll av risker

1. Varje unions**entitet** [...] ska inrätta en egen [...] ram för hantering, styrning och kontroll av cybersäkerhetsrisker (*ramen*) till stöd för entitetens uppdrag [...]**.** [...] **Ramen** ska övervakas av entitetens högsta ledningsnivå för att säkerställa en effektiv och ansvarsfull hantering av alla cybersäkerhetsrisker. Ramen ska ha införts senast den ... [15 månader efter denna förordnings ikraftträdande].

2. Ramen ska omfatta hela den icke-säkerhetsskyddsklassificerade it-miljön för **unionsentiteten** [...] i fråga, inbegripet alla it-miljöer på plats, **nätverk för operativ teknik**, utkontrakterade tillgångar och tjänster i molnbaserade miljöer eller som förvaltas av tredje part, mobila enheter, interna nätverk, företagsnätverk som inte är anslutna till internet och alla enheter som är anslutna till it-miljön. Ramen ska **vara baserad på en allriskstrategi och på en mognadsbedömning i enlighet med artikel 6 som omfattar alla relevanta tekniska, operativa och organisatoriska risker som kan påverka cybersäkerheten vid den berörda unionsenheten** [...].

2a. **Ramen ska fastställa policy för cybersäkerhet, inbegripet mål och prioriteringar för säkerhet i nätverks- och informationssystem, samt policy och förfaranden för att bedöma effektiviteten i genomförda riskhanteringsåtgärder för cybersäkerhet och definiera personalens roller och ansvarsområden.**

2b. Ramen ska ses över med regelbundna mellanrum och åtminstone vart tredje år mot bakgrund av de föränderliga riskerna, tillgångarna och unionsentiteternas mognad.

3. Varje unions**entitets** [...] högsta ledningsnivå ska övervaka att **dess** [...] organisation fullgör sina skyldigheter i fråga om hantering, styrning och kontroll av cybersäkerhetsrisker, utan att det påverkar det formella ansvaret för efterlevnad och riskhantering på andra ledningsnivåer inom respektive ansvarsområden.

3a. **När så är lämpligt och utan att det påverkar dess ansvar för genomförandet av denna förordning får varje unionsentitets högsta ledningsnivå delegera särskilda skyldigheter enligt förordningen till andra höga tjänstemän inom den berörda entiteten. Oavsett eventuell delegering av särskilda skyldigheter kan den högsta ledningsnivån hållas ansvarig om entiteter inte uppfyller sina skyldigheter enligt denna förordning.**

3b. Varje unionsentitets högsta ledningsnivå ska säkerställa att unionsentiteterna godkänner en cybersäkerhetsplan som omfattar riskhanteringsåtgärder för cybersäkerhet, i enlighet med deras riskanalys, så att ramen genomförs i enlighet med denna förordning.

[...]

5. Varje unions**entitet** [...] ska utse en lokal cybersäkerhetsansvarig eller motsvarande funktion som ska fungera som dess gemensamma kontaktpunkt för alla aspekter av cybersäkerhet.

Den lokala cybersäkerhetsansvarige ska underlätta genomförandet av denna förordning och regelbundet lämna lägesrapporter om genomförandet direkt till den högsta ledningsnivån.

Utan att det påverkar den lokala cybersäkerhetsansvariges funktion som gemensam kontaktpunkt i varje unionsentitet får en unionsentitet delegera vissa av den lokala cybersäkerhetsansvariges uppgifter ifråga om genomförandet av denna förordning till CERT-EU på grundval av ett servicenivåavtal mellan den unionsentiteten och CERT-EU. IICB ska besluta om tillhandahållandet av denna tjänst ska ingå i CERT-EU:s baslinjetjänster, med beaktande av den berörda unionsentitetens personalresurser och ekonomiska resurser. Varje unionsentitet ska utan onödigt dröjsmål meddela CERT-EU om utsedda lokala cybersäkerhetsansvariga och alla senare ändringar av befattningen. CERT-EU ska föra en regelbundet uppdaterad förteckning över utsedda lokala cybersäkerhetsansvariga.

6. Varje unionsentitets högre tjänstemän i den mening som avses i artikel 29.2 i tjänsteföreskrifterna[11] eller andra tjänstemän på likvärdig nivå ska regelbundet genomgå särskild utbildning för att skaffa sig tillräckliga kunskaper och färdigheter för att kunna förstå och bedöma cybersäkerhetsrisker och rutiner för hantering av cybersäkerhet och deras inverkan på entitetens verksamhet.

---

11 Rådets förordning nr 259/68 av den 29 februari 1968 om fastställande av tjänsteföreskrifter för tjänstemännen i Europeiska gemenskaperna och anställningsvillkor för övriga anställda i dessa gemenskaper, EGT L 56, 4.3.1968.

7. Varje unionsentitet ska ha effektiva mekanismer för att säkerställa att en lämplig andel av IKT-budgeten spenderas på cybersäkerhet. Vid fastställandet av denna andel ska vederbörlig hänsyn ska tas till ramen.

Artikel 5

Riskhanteringsåtgärder för [...] ***cybersäkerhet***

1. [...] **Varje unionsentitet ska, under övervakning av sin** högsta ledningsnivå [...] [...] **säkerställa att det vidtagits lämpliga och proportionella tekniska, operativa och organisatoriska åtgärder för att hantera de risker som identifieras enligt den ram som avses i artikel 4.1 och för att förebygga och/eller minimera konsekvenserna av incidenter. Med beaktande av den senaste utvecklingen och, i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska dessa åtgärder säkerställa en lämplig säkerhetsnivå i nätverk och informationssystem i förhållande till riskerna. Vid bedömningen av proportionaliteten i dessa åtgärder ska vederbörlig hänsyn tas till graden av entitetens exponering för risker, dess storlek, sannolikheten för att incidenter ska inträffa och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.**

[...]

3. Unionsentiteter ska i sina cybersäkerhetsplaner ta upp åtminstone följande specifika områden för genomförandet av riskhanteringsåtgärder för cybersäkerhet, i linje med IICB:s vägledningar och rekommendationer:

a) Policy för cybersäkerhet, vid specificeringen av de verktyg och åtgärder som krävs för att uppnå de mål och prioriteringar som avses i artiklarna 4 och 5.4.

b) Strategier för riskanalys och informationssystemens säkerhet.

c) Organisation av cybersäkerhet, inbegripet fastställande av roller och ansvarsområden.

d) Förvaltning av tillgångar, inbegripet inventering av digitala tillgångar och it-nätverkskartografi.

e) Säkerhets- och åtkomstkontroll för personal.

f) Driftssäkerhet.

g) Kommunikationssäkerhet.

h) Förvärv, utveckling och underhåll av system, inbegripet hantering och redovisning av sårbarheter.

i) Säkerhet i leveranskedjan, inbegripet säkerhetsrelaterade aspekter som rör förbindelserna mellan unionsentiteten och dess direkta leverantörer eller tjänsteleverantörer. Unionsentiteter ska ta hänsyn till de sårbarheter som är specifika för varje direkt leverantör och tjänsteleverantör och den övergripande kvaliteten på produkterna och deras leverantörers och tjänsteleverantörers cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling.

j) Incidenthantering och samarbete med CERT-EU, såsom underhåll av säkerhetsövervakning och loggning.

k) Hantering av driftskontinuitet, såsom reservförvaltning och katastrofhantering, och krishantering.

l) Främjande och utveckling av program för utbildning, kompetens, ökad medvetenhet, övning och fortbildning inom cybersäkerhet.

4. Unionsentiteter ska i sina cybersäkerhetsplaner ta upp åtminstone följande specifika riskhanteringsåtgärder för cybersäkerhet vid genomförandet av riskhanteringsåtgärder för cybersäkerhet, i linje med IICB:s vägledningar och rekommendationer:

a) Mål och prioriteringar när det gäller användningen av molntjänster i den mening som avses i artikel 4.19 i direktiv [förslag till NIS 2] och tekniska lösningar för att möjliggöra distansarbete.

b) Konkreta åtgärder för framtida användning av nolltillitsprinciper, inbegripet en säkerhetsmodell och en samordnad strategi för cybersäkerhet och systemhantering baserade på det faktum att det finns en hotbild både inom och utanför traditionella nätverksgränser.

c) Införande av flerfaktorsautentisering som standard i nätverks- och informationssystem.

d) Inrättande av säkerhet i leveranskedjan för programvara genom kriterier för utveckling och utvärdering av säker programvara.

e) Förbättrade upphandlingsregler för att underlätta en hög gemensam cybersäkerhetsnivå genom

i) att undanröja avtalsmässiga hinder som begränsar informationsutbytet från leverantörer av it-tjänster om incidenter, sårbarheter och cyberhot med CERT-EU,

ii) att införa en avtalsenlig skyldighet att rapportera incidenter, sårbarheter och cyberhot samt att ha lämpliga åtgärder för hantering och övervakning av incidenter.

f) Användning av kryptografi och kryptering, särskilt totalsträckskryptering.

g) Säkra kommunikationssystem inom organisationen.

Artikel 6

Mognadsbedömningar

1. Varje unions**entitet** [...] ska**, när så är lämpligt med stöd av specialiserad tredjepart,** genomföra **en** [...] mognadsbedömning av cybersäkerheten minst vart tredje år, omfattande alla delar av deras IKT-miljö enligt beskrivningen i artikel 4, med beaktande av relevanta vägledningar och rekommendationer som antagits i enlighet med artikel 13.

2. På rekommendation av CERT-EU och efter samråd med Europeiska unionens cybersäkerhetsbyrå (Enisa) ska IICB, inom 4 månader efter denna förordnings ikraftträdande, anta metodriktlinjer för genomförandet av mognadsbedömningar.

3. Efter slutförd mognadsbedömning [...] ska unionsentiteterna överlämna bedömningen till IICB. Den första mognadsbedömningen ska utföras senast [12 månader efter denna förordnings ikraftträdande].

Artikel 7

Cybersäkerhetsplaner

1. Som en uppföljning av slutsatserna från mognadsbedömningen och med beaktande av de tillgångar och risker som identifierats i enlighet med artikel 4 ska varje unions**entitets** [...] högsta ledningsnivå godkänna en cybersäkerhetsplan utan onödigt dröjsmål efter inrättandet av [...] ramen, [...] **antagandet av riskhanteringsåtgärderna för** cybersäkerhet [...] **och utförandet av mognadsbedömningen, och senast 21 månader efter denna förordnings ikraftträdande**. **Cybersäkerhets**planen ska syfta till att öka den **berörda unions**entitetens [...] övergripande cybersäkerhet och ska därigenom bidra till att [...] stärka en hög gemensam cybersäkerhetsnivå vid alla unions**entiteter** [...] . [...] **Cybersäkerhets**planen ska åtminstone omfatta **riskhanteringsåtgärderna för cybersäkerhet enligt artikel 5** [...]. **Cybersäkerhets**planen ska ses över minst **vartannat** [...] år, **eller** efter [...] **varje** mognadsbedömning [...] som utförts i enlighet med artikel 6 **eller varje översyn av ramen i enlighet med artikel 4.**

2. [...]

3. Cybersäkerhetsplanen ska **ta hänsyn till** [...] alla tillämpliga vägledningar och rekommendationer som utfärdats **i enlighet med artikel 13** [...].

4. **Efter det att cybersäkerhetsplanen slutförts ska unionsentiteten överlämna den till IICB.**

Artikel 7a

Sakkunnigbedömning

1. IICB ska, på rekommendation av CERT_EU och efter samråd med Enisa, senast den ... [24 månader efter denna förordnings ikraftträdande], med utgångspunkt i metoden för sakkunnigbedömningar och metoden för självbedömning i enlighet med artikel 16 i direktiv [NIS 2-förslaget] och vid behov med anpassning till unionsentiteternas behov, fastställa metoden för och de organisatoriska aspekterna av en sakkunnigbedömning i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt stärka den kapacitet och policy för cybersäkerhet som krävs av unionsentiteterna för att genomföra denna förordning. Det är frivilligt att delta i sakkunnigbedömningar. Företrädare för medlemsstaterna får delta i sakkunnigbedömningen som observatörer. Sakkunnigbedömningarna ska utföras av cybersäkerhetsexperter som utsetts av minst två andra unionsentiteter än den unionsentitet som granskas och de ska omfatta minst ett av följande:

i) Nivå av genomförande av de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som avses i artiklarna 5 och 20.

ii) Kapacitetsnivå, inbegripet tillgängliga ekonomiska, tekniska och mänskliga resurser.

iii) Nivå av genomförande av den ram för informationsutbyte som avses i artikel 19.

iv) Särskilda frågor av sektorsöverskridande slag.

2. Unionsentiteter får ange särskilda frågor som nämns i punkt 1 iv för granskning. Granskningens omfattning, inbegripet de frågor som angivits, ska meddelas till de deltagande unionsentiteterna innan sakkunnigbedömningen inleds.

3. Innan sakkunnigbedömningen inleds får unionsenheterna göra en självbedömning av de aspekter som ska granskas och låta de utsedda experterna ta del av denna självbedömning.

4. Sakkunnigbedömningar ska inbegripa fysiska eller virtuella besök på plats och distansbaserade utbyten. Med tanke på principen om gott samarbete ska de unionsentiteter som är föremål för sakkunnigbedömningen förse de utsedda experterna med den information som krävs för bedömningen, utan att det påverkar tillämpningen av nationell lagstiftning eller unionslagstiftning om skydd av känsliga eller säkerhetsskyddsklassificerade uppgifter. All information som erhålls genom en sakkunnigbedömning får endast användas för detta ändamål. De experter som deltar i sakkunnigbedömningen får inte lämna ut känsliga eller säkerhetsskyddsklassificerade uppgifter som erhållits under denna bedömning till någon tredje part.

5. Efter genomgången sakkunnigbedömning i unionsentiteterna ska samma aspekter inte vara föremål för ytterligare sakkunnighetsbedömningar i dessa unionsentiteter under de två år som följer på slutförandet av sakkunnighetsbedömningen, såvida inte unionsentiteterna så själva begär eller instämmer med efter ett förslag från IICB.

6. Unionsentiteterna ska säkerställa att alla risker för intressekonflikter som rör de utsedda experterna redovisas för övriga unionsentiteter och IICB innan sakkunnigbedömningen inleds. De unionsentiteter som är föremål för sakkunnigbedömningen får, av vederbörligen motiverade skäl som meddelas de unionsentiteter som utser experterna, invända mot utseendet av vissa experter.

7. Experter som deltar i sakkunnigbedömningar ska utarbeta rapporter om resultat och slutsatser av dessa. Unionsentiteterna ska ges möjlighet att lämna synpunkter på respektive utkast till rapporter, vilka ska bifogas rapporterna. Rapporterna ska innehålla rekommendationer för att möjliggöra förbättring av aspekter som ingår i sakkunnigbedömningen. Rapporterna ska vid behov föreläggas IICB och CSIRT-nätverket. Unionsentiteter under granskning kan besluta att offentliggöra sin rapport eller en redigerad version av den.

Artikel 8

Genomförande

1. [...]

2. Vägledningar och rekommendationer som utfärdas i enlighet med artikel 13 ska stödja genomförandet av bestämmelserna i detta kapitel.

3. På IICB:s begäran ska unionsentiteterna rapportera om särskilda aspekter av detta kapitel.

Kapitel III
INTERINSTITUTIONELL CYBERSÄKERHETSSTYRELSE

Artikel 9

Interinstitutionell cybersäkerhetsstyrelse

1. Härigenom inrättas en interinstitutionell cybersäkerhetsstyrelse (IICB).

2. IICB ska ansvara för att

   a) övervaka **unionsentiteternas** [...] genomförande av denna förordning,

   b) övervaka CERT-EU:s genomförande av de allmänna prioriteringarna och målen och ge CERT-EU strategisk ledning.

3. IICB ska bestå av följande:

   a) En företrädare som utsetts av var och en av följande:

      i) Europaparlamentet.

      ii) Europeiska rådet

      iii) Europeiska unionens råd.

      iv) Europeiska kommissionen.

      v) Europeiska unionens domstol.

      vi) Europeiska centralbanken.

vii) Europeiska revisionsrätten.

viii) Europeiska utrikestjänsten.

ix) Europeiska ekonomiska och sociala kommittén.

x) Europeiska regionkommittén.

xi) Europeiska investeringsbanken.

xii) Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning.

xiii) Europeiska unionens cybersäkerhetsbyrå.

b) Tre företrädare som av unionsbyråernas nätverk (EUAN) på förslag av dess rådgivande IKT-kommitté utses att företräda intressena för de byråer och organ som driver sin egen it-miljö. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3a. Ledamöterna får bistås av en suppleant. Ordföranden får bjuda in andra företrädare för de **entiteter** [...] som förtecknas ovan eller för andra **unionsentiteter** att delta i IICB:s möten utan rösträtt.

4. IICB ska själv anta sin arbetsordning.

5. IICB ska utse en ordförande bland sina ledamöter, i enlighet med sin arbetsordning, för en period på [...] **två** år. Ordförandens suppleant ska bli ordinarie ledamot av IICB för samma period.

6. IICB ska sammanträda **minst tre gånger om året** på ordförandens initiativ, **och/eller** på begäran av CERT-EU **och/**eller på begäran av någon av dess ledamöter.

7. Varje ledamot av IICB ska ha en röst. IICB:s beslut ska fattas med enkel majoritet om inte annat föreskrivs i denna förordning. Ordföranden får inte rösta utom vid lika röstetal, då han eller hon får avge en utslagsröst.

8. IICB får agera genom ett förenklat skriftligt förfarande som inleds i enlighet med IICB:s interna arbetsordning. Enligt det förfarandet ska det relevanta beslutet anses vara godkänt inom den tidsram som fastställts av ordföranden, utom i de fall då en ledamot har invändningar.

9. TCERT-EU:s chef**, ordföranden för samarbetsgruppen för nät- och informationssäkerhet**, **ordföranden för EU-CyCLONe och ordföranden för CSIRT-nätverket,** eller **deras** [...] suppleanter, [...] **får**, om inte IICB beslutar något annat**,** delta i IICB:s möten **som observatörer**.

10. IICB:s sekretariat ska tillhandahållas av **Enisa** [...] **och ska vara ansvarigt inför IICB:s ordförande**.

11. De företrädare som utsetts av EUAN på förslag av den rådgivande IKT-kommittén ska vidarebefordra IICB:s beslut till **EUAN:s medlemmar** […]. Alla unionens byråer och organ ska ha rätt att med företrädarna eller IICB:s ordförande ta upp alla frågor som de anser att IICB bör uppmärksammas på.

12. [...]

13. IICB får **inrätta** […] en verkställande kommitté som ska bistå den i dess arbete och får delegera vissa av sina uppgifter och befogenheter till den**, särskilt de i artikel 10 c och 10 e**. IICB ska fastställa den verkställande kommitténs arbetsordning, inbegripet dess uppgifter och befogenheter och dess ledamöters mandatperioder.

14. IICB ska var tolfte månad lämna en rapport till rådet med närmare uppgifter om hur genomförandet av denna förordning fortskrider och särskilt om omfattningen av CERT-EU:s samarbete med dess nationella motparter i var och en av medlemsstaterna. Denna rapport ska utgöra underlag till tvåårsrapporten om cybersäkerhetsläget i unionen under samma tidsperiod i enlighet med artikel 15 i direktiv [förslaget till NIS 2].

Artikel 10

IICB:s uppgifter

Vid utövandet av sina uppgifter ska IICB särskilt

(a) [...] **på ett effektivt sätt övervaka och utöva tillsyn över tillämpningen av** denna förordning [...] **och ge stöd till unionsentiteter i deras arbete med att stärka sin cybersäkerhet**; **IICB får i det sammanhanget begära särskilda rapporter från CERT-EU och unionsentiteterna,**

aa) efter en strategisk diskussion anta en flerårig strategi för att höja cybersäkerhetsnivån i unionsentiteterna vilken regelbundet, minst vart femte år, ska utvärderas och vid behov ändras,

b) på grundval av ett förslag **som inlämnats av** [...] CERT-EU:s chef godkänna CERT-EU:s årliga arbetsprogram och övervaka dess genomförande,

c) på grundval av ett förslag från CERT-EU:s chef godkänna CERT-EU:s tjänstekatalog **och eventuella senare uppdateringar av den,**

d) på grundval av ett förslag från CERT-EU:s chef godkänna den årliga ekonomiska planeringen av inkomster och utgifter, inbegripet för personal, för CERT-EU:s verksamhet,

e) på grundval av ett förslag från CERT-EU:s chef godkänna formerna för servicenivåavtal,

f) granska och godkänna den årsrapport som utarbetats av CERT-EU:s chef och som omfattar CERT-EU:s verksamhet och förvaltning av medel,

g) godkänna och övervaka de nyckelprestandaindikatorer som har fastställts för CERT-EU på grundval av ett förslag från CERT-EU:s chef,

h) godkänna samarbetsavtal, servicenivåavtal eller avtal mellan CERT-EU och andra entiteter i enlighet med artikel 17,

i) inrätta [...] tekniska rådgivande grupper [...] för att bistå IICB i dess arbete, godkänna deras mandat och utse deras respektive ordförande,

j) **anta vägledningar och rekommendationer på grundval av ett förslag från CERT-EU i enlighet artikel 13 och ge CERT-EU i uppdrag att utfärda, dra tillbaka eller ändra ett förslag till vägledningar eller rekommendationer, eller en uppmaning till åtgärder,**

(k) ta emot och bedöma handlingar och rapporter som lämnats in av unionentiteter enligt denna förordning,

(l) stödja inrättandet av en informell grupp som samlar lokala cybersäkerhetsansvariga från alla entiteter och därigenom underlätta utbytet av bästa praxis och information i samband med genomförandet av denna förordning,

(m) utarbeta en cyberkrishanteringsplan för att stödja en samordnad hantering av större incidenter på operativ nivå som påverkar unionsentiteter och bidra till ett regelbundet utbyte av relevant information, särskilt om större incidenters konsekvenser och allvarlighetsgrad och möjliga sätt att begränsa dem.

Artikel 11

Kontroll av efterlevnad

1. IICB ska **i enlighet med artiklarna 9.2 och 10** effektivt övervaka hur union[...]**entiteterna** genomför denna förordning och antagna vägledningar, rekommendationer och uppmaningar till åtgärder. **I detta syfte får IICB begära den information eller dokumentation som är nödvändig för att bedöma huruvida unionsentiteterna tillämpar bestämmelserna i förordningen på ett korrekt sätt. Vid antagande av efterlevnadsåtgärder enligt denna artikel ska den berörda unionsentiteten inte ha rösträtt.**

2. Om IICB konstaterar att union[...]**sentiteterna** inte effektivt har tillämpat eller genomfört denna förordning eller vägledningar, rekommendationer och uppmaningar till åtgärder som utfärdats enligt denna förordning, får den, utan att det påverkar de interna förfarandena för unions[...]**entiteten** i fråga**, och efter att ha gett entiteten eller den berörda personen möjlighet att lägga fram sina synpunkter**,

a) utfärda en varning **för att åtgärda konstaterade brister inom en angiven tidsram, inbegripet rekommendationer om ändring av cybersäkerhetsdokument som antagits av unionsentiteterna på grundval av denna förordning**; när det är nödvändigt med tanke på en tvingande cybersäkerhetsrisk ska varningens målgrupp begränsas på lämpligt sätt,

aa) utfärda ett motiverat meddelande till en unionsentitet, om de brister som identifierats i den tidigare utfärdade varningen inte har åtgärdats i tillräcklig utsträckning inom en angiven tidsram, och formellt underrätta rådet, Europaparlamentet och kommissionen detta uttalande,

b) **i synnerhet utfärda** [...]

i) en rekommendation om att en revision av en unionsentitet ska utföras,

ii) en begäran om att en revision ska utföras av en tredje parts revisionstjänst,

c) begära att unionsentiteten ser till att hanteringen, styrningen och kontrollen av cybersäkerhetsrisker sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specificerat sätt och inom en angiven tidsperiod,

d) utfärda råd till alla medlemsstater och unionsentiteter med rekommendationer om tillfälligt stopp för dataflöden till unionsentiteten.

3. Om IICB har antagit åtgärder enligt punkt 2 a-d ska den berörda unionsentiteten lämna en detaljerad redogörelse för de åtgärder som vidtagits för att åtgärda de påstådda brister som IICB identifierat. Unionsentiteten ska lämna in denna redogörelse inom en rimlig tidsperiod som ska överenskommas med IICB.

4. **Om IICB anser att en unionsentitet fortlöpande bryter mot bestämmelserna i denna förordning till följd av handlingar eller försummelser från en tjänsteman eller annan anställd i unionen, inbegripet på högsta ledningsnivå, ska IICB begära att den berörda entiteten vidtar lämpliga åtgärder, även disciplinära åtgärder, i synnerhet i enlighet med bestämmelserna i tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i Europeiska unionen. För detta ändamål ska IICB överföra nödvändig information till den berörda entiteten.**

Kapitel IV
CERT-EU

Artikel 12

CERT-EU:s uppdrag och uppgifter

1. CERT-EU ska ha i uppdrag att bidra till it-miljöns säkerheten hos alla union[...]**sentiteter** genom att ge dem råd om cybersäkerhet, hjälpa dem att förebygga, upptäcka, begränsa och hantera incidenter och genom att fungera som deras nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering.

1a. CERT-EU ska samla in, hantera, analysera och dela information med unionsentiteterna om hot, sårbarheter och incidenter som rör icke sekretessbelagd IKT-infrastruktur. CERT-EU ska samordna hanteringen av incidenter på interinstitutionell nivå och på unionsentitetsnivå, bland annat genom att ombesörja eller samordna tillhandahållandet av specialiserat operativt stöd.

2. CERT-EU ska utföra följande uppgifter för union[...]**sentiteterna**:

a) Stödja dem vid genomförandet av denna förordning och bidra till samordningen av tillämpningen av denna förordning genom de åtgärder som förtecknas i artikel 13.1 eller genom ad hoc-rapporter som IICB begär.

b) [...] **Erbjuda standardiserade CSIRT-tjänster för alla entiteter i unionen genom** ett paket av cybersäkerhetstjänster som beskrivs i dess tjänstekatalog (baslinjetjänster).

c) Upprätthålla ett nätverk av kollegor och partner för att stödja de tjänster som beskrivs i artiklarna 16 och 17.

d) Uppmärksamma IICB på alla frågor som rör genomförandet av denna förordning och genomförandet av vägledningarna, rekommendationerna och uppmaningarna till åtgärder.

e) **På grundval av den information som avses i punkt 1a och** [...] **i nära samarbete med Enisa** bidra till EU:s cybersituationsmedvetenhet. **Denna information ska delas med IICB, CSIRT-nätverket och EU-Intcen.**

f) Fungera som motsvarighet till den utsedda samordnaren för de unionsentiteter som avses i artikel 6 i direktiv [förslag till NIS 2].

[...]

[...]

[...]

[...]

[...]

4. **Inom ramen för sina befogenheter ska** CERT-EU inleda ett strukturerat samarbete med [...]**Enisa** om kapacitetsuppbyggnad, operativt samarbete och långsiktiga strategiska analyser av cyberhot i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881.

5. CERT-EU får tillhandahålla följande tjänster som inte beskrivs i dess tjänstekatalog (avgiftsbelagda tjänster):

   a) Andra tjänster som stöder cybersäkerheten i unions[...]**entiteters** it-miljö än de som avses i punkt 2, på grundval av servicenivåavtal och förutsatt att det finns tillgängliga resurser.

   b) Andra tjänster som stöder union[...]**sentiteternas** cybersäkerhetsinsatser eller cybersäkerhetsprojekt än de som skyddar deras it-miljö, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

   c) Tjänster som stöder säkerheten i it-miljön hos andra organisationer än unions[...]**entiteterna** vilka har ett nära samarbete med unions[...]**entiteterna**, till exempel genom att ha tilldelats uppgifter och ansvar enligt unionsrätten, på grundval av skriftliga avtal och med förhandsgodkännande från IICB.

6. CERT-EU får anordna **eller delta i** cybersäkerhetsövningar eller rekommendera deltagande i befintliga övningar, i tillämpliga fall i nära samarbete med [...]**Enisa**, för att testa unions[...]**entiteternas cybersäkerhetsnivå**.

7. CERT-EU får stödja unions[...]**entiteterna** när det gäller incidenter i säkerhetsskyddsklassificerade it-miljöer om **de berörda** unions[...]**entiteterna** uttryckligen begär detta i enlighet med deras respektive förfaranden. **I detta fall ska bestämmelserna i artiklarna 19–21 i denna förordning inte tillämpas. Tillhandahållande av bistånd från CERT-EU enligt denna punkt ska inte påverka medlemsstaternas eller unionens bestämmelser om skydd av känsliga eller säkerhetsskyddsklassificerade uppgifter.**

8. CERT-EU ska informera unionsentiteterna om sina förfaranden och processer för incidenthantering.

9. CERT-EU får övervaka unionsentiteternas nättrafik med den berörda unionsentitetens samtycke.

10. CERT-EU får, om unionsentiteternas politiska avdelningar uttryckligen så begär, tillhandahålla teknisk rådgivning eller synpunkter i relevanta politiska ärenden.

11. CERT-EU ska i samarbete med Europeiska datatillsynsmannen stödja de berörda unionsentiteterna när de hanterar incidenter som leder till personuppgiftsincidenter.

Artikel 13

Vägledningar, rekommendationer och uppmaningar till åtgärder

1. CERT-EU ska stödja genomförandet av denna förordning genom att utfärda

   a) uppmaningar till åtgärder som beskriver brådskande säkerhetsåtgärder som unions[...]**entiteterna** uppmanas att vidta inom en fastställd tidsram; **utan onödigt dröjsmål efter mottagandet av uppmaningen till åtgärder ska den berörda unionsentiteten informera CERT-EU om hur dessa åtgärder har tillämpats**.

   b) förslag till IICB till vägledningar som riktar sig till alla eller en del av unions[...]**entiteterna**,

   c) förslag till IICB till rekommendationer som riktar sig till enskilda unions[...]**entiteter**.

2. Vägledningar och rekommendationer kan omfatta

   a) former för eller förbättringar av riskhanteringen för cybersäkerhet och **riskhanteringsåtgärderna** [...] för cybersäkerhet,

   b) former för mognadsbedömningar och cybersäkerhetsplaner, och

   c) när så är lämpligt, användning av gemensam teknik, arkitektur och tillhörande bästa praxis i syfte att uppnå interoperabilitet och gemensamma standarder**, inbegripet en samordnad strategi för säkerhet i leveranskedjan** [...]**.**

[...]

[...]

Artikel 14

CERT-EU:s chef

1. Kommissionen ska, efter att ha fått godkännande av två tredjedelar av IICB:s ledamöter, utnämna CERT-EU:s chef. IICB ska rådfrågas i alla skeden av förfarandet före utnämningen av CERT-EU:s chef, särskilt när det gäller att utarbeta meddelanden om den lediga tjänsten, granska ansökningar och utse uttagningskommittéer med avseende på tjänsten.

2. CERT-EU:s chef ska, inom sitt behörighetsområde och under ledning av IICB, ansvara för att CERT-EU fungerar väl. Han eller hon ska ansvara för att genomföra den strategiska ledning och rådgivning och de mål och prioriteringar som fastställts av IICB och för förvaltningen av CERT-EU, inbegripet av de ekonomiska resurserna och personalen. Han eller hon ska regelbundet rapportera till IICB:s ordförande.

3. CERT-EU:s chef ska stödja den behöriga delegerade utanordnaren i utarbetandet av den årliga verksamhetsrapport med finansiella och administrativa uppgifter, inbegripet resultaten av kontroller, som upprättas i enlighet med artikel 66.9 i budgetförordningen, och ska regelbundet rapportera till denne om genomförandet av åtgärder för vilka befogenheter har vidaredelegerats till CERT-EU:s chef.

4. CERT-EU:s chef ska årligen utarbeta en finansiell planering av administrativa inkomster och utgifter för dess verksamhet, förslaget till årligt arbetsprogram, förslaget till en tjänstekatalog för CERT-EU och översynen av denna, förslaget till formerna för servicenivåavtal och förslaget till nyckelprestandaindikatorer för CERT-EU vilka ska godkännas av IICB i enlighet med artikel 10.

Vid översynen av förteckningen över tjänster i CERT-EU:s tjänstekatalog ska CERT-EU:s chef beakta de resurser som tilldelats CERT-EU.

5. CERT-EU:s chef ska [...] lämna **års**rapporter till IICB [...] om CERT-EU:s resultat, finansiell planering, inkomster, genomförande av budgeten, servicenivåavtal och skriftliga avtal som ingåtts, samarbete med motparter och partner samt personalens uppdrag, inbegripet de rapporter som avses i artikel 10 [...]**a**.

Artikel 15

Ekonomiska frågor och personalfrågor

[...]

1a. Även om CERT-EU inrättades som en autonom interinstitutionell tjänsteleverantör för alla unionsentiteter ska CERT-EU integreras i den administrativa strukturen vid ett av kommissionens generaldirektorat i syfte att dra nytta av kommissionens stödstrukturer när det gäller administration, ekonomisk förvaltning och redovisning. Kommissionen ska informera IICB om CERT-EU:s administrativa lokalisering och eventuella ändringar därav. Detta upplägg ska utvärderas regelbundet, senast före utgången av varje flerårig budgetram som har fastställts i enlighet med artikel 312 i EUF-fördraget, för att göra det möjligt att vidta lämpliga åtgärder.

2. När det gäller tillämpningen av de administrativa och finansiella förfarandena ska CERT-EU:s chef handla under kommissionens överinseende.

3. CERT-EU:s uppgifter och verksamhet, inbegripet tjänster som tillhandahålls av CERT-EU i enlighet med artiklarna 12.2, [...] 12.4, 12.6 och 13.1 till unions[...]**entiteter** som finansieras genom den rubrik i den fleråriga budgetramen som är avsedd för europeisk offentlig administration, ska finansieras genom en särskild budgetpost i kommissionens budget. De tjänster som öronmärkts för CERT-EU ska anges i en fotnot till kommissionens tjänsteförteckning.

4. Unions[...]**entiteter**, andra än de som avses i punkt 3, ska lämna ett årligt ekonomiskt bidrag till CERT-EU för att täcka de tjänster som CERT-EU tillhandahåller i enlighet med punkt 3. Respektive bidrag ska baseras på riktlinjer som ges av IICB och som varje entitet och CERT-EU kommer överens om sinsemellan i servicenivåavtal. Bidragen ska utgöra en rättvis och proportionell andel av de totala kostnaderna för de tjänster som tillhandahålls. De ska tas emot under den särskilda budgetpost som avses i punkt 3 som inkomster avsatta för särskilda ändamål i enlighet med artikel 21.3 c i Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046[12].

5. Kostnaderna för de uppgifter som anges i artikel 12.5 ska återkrävas från de unions[...]**entiteter** som tar emot CERT-EU-tjänsterna. Inkomsterna ska avsättas för de budgetposter som stöder kostnaderna.

[12] Europaparlamentets och rådets förordning (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012 (EUT L 193, 30.7.2018, s. 1).

Artikel 16

CERT-EU:s samarbete med motparter i medlemsstaterna

1. CERT-EU ska **utan onödigt dröjsmål** samarbeta och utbyta information med nationella motparter i medlemsstaterna, **särskilt** [...] [...] [...] de CSIRT-enheter **som avses i artikel 9 i direktiv [förslag till NIS 2] och/eller i förekommande fall nationella behöriga myndigheter** och de gemensamma kontaktpunkter som avses i artikel 8 i direktiv [förslag till NIS 2], om cyberhot, sårbarheter och incidenter, om möjliga motåtgärder och om alla frågor som är relevanta för att förbättra skyddet av it-miljön vid unions[...]**entiteterna**, inbegripet genom det CSIRT-nätverk som avses i artikel 13 i direktiv [förslag till NIS 2].

1a. CERT-EU ska utan dröjsmål underrätta alla relevanta nationella motparter som avses i punkt 1 i en medlemsstat när centrumet får kännedom om betydande incidenter som inträffar inom den medlemsstatens territorium, såvida inte CERT-EU har vetskap om att den berörda unionsentiteten redan har rapporterat denna incident i enlighet med artikel 20.2a.

2. CERT-EU **ska utan onödigt dröjsmål** [...] utbyta incidentspecifik information med nationella motparter i medlemsstaterna för att underlätta upptäckt av liknande cyberhot eller incidenter **eller för att bidra till analysen av en incident** utan **att behöva inhämta** den berörda **unionsentitetens** [...] samtycke. CERT-EU **får inte** utbyta incidentspecifik information som avslöjar identiteten på målet för cybersäkerhetsincidenten [...] **såvida inte** [...]

   a) den berörda unionsentiteten har gett sitt samtycke,

   b) den berörda unionsentiteten redan har offentliggjort att den är berörd,

c) samtycke från den berörda unionsentiteten saknas men offentliggörandet av den berörda unionsentitetens identitet skulle öka sannolikheten för att incidenter på annat håll undviks eller mildras. Sådana beslut kräver godkännande från CERT-EU:s chef. Den berörda unionsentiteten ska informeras före offentliggörandet.

Artikel 17

CERT-EU:s samarbete med <u>andra</u> motparter [...]

1. CERT-EU får samarbeta med **andra** motparter [...] **i Europeiska unionen än de som anges i artikel 16**, inbegripet branschspecifika motparter, om verktyg och metoder, såsom teknik, taktik, förfaranden och bästa praxis, och om cyberhot och sårbarheter. För allt samarbete med sådana motparter [...] ska CERT-EU **från fall till fall** inhämta förhandsgodkännande från IICB**. CERT-EU ska informera alla relevanta nationella motparter som avses i artikel 16.1, i en medlemsstat där motparten är belägen, när CERT-EU upprättar samarbete med sådana motparter.**

2. CERT-EU får samarbeta med andra partner, såsom kommersiella entiteter, internationella organisationer, nationella entiteter eller enskilda experter utanför EU, för att samla in information om allmänna och specifika cyberhot, sårbarheter och möjliga motåtgärder. För ett bredare samarbete med sådana partner ska CERT-EU **från fall till fall** inhämta förhandsgodkännande från IICB**.**

3. CERT-EU får, **förutsatt att en överenskommelse eller ett avtal om sekretess har ingåtts med den relevanta partnern,** med samtycke från den **unionsentitet** [...] som berörs av en incident, lämna information om **den specifika** incidenten till partner **som avses i punkterna 1 och 2 endast i syfte att bidra** [...] till dess analys. **Sådana överenskommelser eller avtal om sekretess ska genomgå rättslig kontroll i enlighet med kommissionens relevanta interna förfaranden. För överenskommelser eller avtal om sekretess ska förhandsgodkännande från IICB inte krävas, men IICB:s ordförande ska informeras.**

4. **CERT-EU kan med IICB:s förhandsgodkännande undantagsvis ingå servicenivåavtal med andra entiteter än unionsentiteterna.**

Kapitel V
SAMARBETS- OCH RAPPORTERINGSKRAV

Artikel 18

Informationshantering

1. CERT-EU och unions[...]**entiteterna** ska respektera tystnadsplikt i enlighet med artikel 339 i fördraget om Europeiska unionens funktionssätt eller likvärdiga tillämpliga ramar.

2. Bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 1049/2001[13] ska tillämpas på allmänhetens begäranden om tillgång till handlingar som innehas av CERT-EU, inbegripet skyldigheten enligt den förordningen att samråda med övriga unions[...]**entiteter, och i förekommande fall medlemsstaterna,** när en begäran rör deras handlingar.

[...]

4. CERT-EU:s och unions[...]**entiteternas** hantering av information ska stämma överens med **tillämpliga** regler [...] om informationssäkerhet.

[...]

Artikel 19

[...] ***Informationsutbyte om cybersäkerhet***

-1. Unionsentiteterna får frivilligt förse CERT-EU med information om cyberhot, incidenter, tillbud och sårbarheter som berör dem. CERT-EU ska säkerställa att effektiva medel för kommunikation finns tillgängliga i syfte att underlätta informationsutbytet med unionsentiteterna. CERT-EU får ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser.

[13] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

1. För att [...] **kunna utföra sitt uppdrag och sina uppgifter enligt artikel 12** får CERT-EU [...] begära att unions[...]**entiteterna** lämnar information från sina respektive it-systeminventarier, **inbegripet information om cyberhot, tillbud, sårbarheter, angreppsindikatorer, cybersäkerhetsvarningar och rekommendationer avseende konfiguration av cybersäkerhetsverktyg för att upptäcka cyberincidenter** [...]. Den unions[...]**entitet** som mottar begäran ska utan onödigt dröjsmål översända den begärda informationen och eventuella senare uppdateringar.

2. Unions[...]**entiteterna** ska, på CERT-EU:s begäran och utan onödigt dröjsmål, förse centrumet med digital information som skapats genom användning av elektroniska enheter som är inblandade i respektive incident. CERT-EU kan ytterligare klargöra vilka typer av sådan digital information som behövs för situationsmedvetenhet och incidenthantering.

3. CERT-EU får **med unionsentiteterna** utbyta incidentspecifik information som avslöjar identiteten på den unions[...]**entitet** som berörs av incidenten endast med den entitetens samtycke. **Om samtycke nekas ska den berörda entiteten anföra vederbörligen motiverade skäl till CERT-EU.** [...]

4. Delningsskyldigheterna ska inte omfatta säkerhetsskyddsklassificerade EU-uppgifter och uppgifter **vars distribution utanför den mottagande unionsentiteten har uteslutits av informationskällan genom en synlig markering, såvida inte informationskällan** [...] **uttryckligen tillåter att denna information delas med CERT-EU.** [...]

Artikel 20

[...] ***Rapporteringsskyldigheter***

-1. En incident ska anses vara betydande om

a) den har orsakat, eller kan orsaka, allvarliga driftstörningar i unionsentitetens verksamhet eller ekonomiska förluster för den berörda unionsentiteten,

b) den har påverkat, eller kan påverka, andra fysiska eller juridiska personer genom att åsamka betydande materiell eller ideell skada.

1. Alla unions[...]**entiteter** ska **lämna in** [...] följande **till CERT-EU:** [...]

[...].

(a) Utan onödigt dröjsmål, och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, en tidig varning som i tillämpliga fall ska ange om den betydande incidenten antas ha orsakats av olagliga eller avsiktligt skadliga handlingar och har eller skulle kunna ha gränsöverskridande verkningar.

(b) Utan onödigt dröjsmål, och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, en incidentunderrättelse som i tillämpliga fall ska uppdatera den information som avses i led a och göra en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angepps**indikatorer**.

(c) På begäran av CERT-EU, en delrapport om relevanta statusuppdateringar.

(d) Senast en månad efter inlämningen av anmälan av en betydande incident som avses i led b, en slutrapport som minst ska innehålla följande:

i) En detaljerad beskrivning av den betydande incidenten, dess allvarlighetsgrad och dess konsekvenser.

ii) Den typ av hot eller grundorsak som sannolikt utlöst den betydande incidenten.

iii) Tillämpade och pågående avhjälpande åtgärder.

iv) I tillämpliga fall, den betydande incidentens gränsöverskridande konsekvenser.

(e) Vid pågående betydande incidenter vid tidpunkten för inlämnandet av den slutrapport som avses i led d, en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att incidenten har hanterats.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2a. Alla unionsentiteter ska inom samma tidsfrist dela med sig av den information som rapporteras i enlighet med punkt 1 till alla relevanta nationella motparter som avses i artikel 16.1 där de är belägna.

3. CERT-EU ska […] **var tredje** månad lämna in en sammanfattande rapport till […] **IICB, EU Intcen och CSIRT-nätverket** med anonymiserade och aggregerade data om […] cyberhot, […] sårbarheter **i enlighet med artikel 19, unionsentiteternas svar på uppmaningar till åtgärder i enlighet med artikel 13.1 a,** och betydande incidenter om vilka underrättelse lämnats i enlighet med punkt 1. **Denna rapport ska utgöra underlag till tvåårsrapporten om cybersäkerhetssituationen i unionen i enlighet med artikel 15 i direktiv [förslaget till NIS 2].**

4. IICB **ska,** […] **senast [sex månader efter dagen för denna förordnings ikraftträdande],** utfärda vägledningar eller rekommendationer **med ytterligare specificering av** […] formerna**, formatet för** och innehållet i **rapporteringen** […]. **Vägledningarna eller rekommendationerna ska vederbörligen beakta de bestämmelser som genomförs genom eventuella genomförandeakter i enlighet med artikel 20.11 i direktivet [förslaget till NIS 2].** CERT-EU ska sprida lämpliga tekniska detaljer för att möjliggöra proaktiv upptäckt, incidenthantering eller riskreducerande åtgärder hos unionens […] **entiteter**.

5. **Rapporteringsskyldigheterna** […] ska inte omfatta säkerhetsskyddsklassificerade EU-uppgifter och uppgifter **vars distribution utanför den mottagande unionsentiteten har uteslutits av informationskällan genom en synlig markering, såvida inte informationskällan** [...] **uttryckligen tillåter att denna information delas med CERT-EU.** [...]

Artikel 21

Incidenthantering – samordning och samarbete […]

1. I sin funktion som nav för utbyte av cybersäkerhetsinformation och samordning av incidenthantering ska CERT-EU främja informationsutbyte om cyberhot, sårbarheter och incidenter mellan

   a) unionens […] **entiteter**,

   b) de motparter som avses i artiklarna 16 och 17.

2. CERT-EU ska**, i tillämpliga fall i nära samarbete med Enisa i enlighet med artikel 7.7 d i cybersäkerhetsakten[14],** främja unionens […] **entiteters** samordning av incidenthantering, genom bland annat

   a) bidrag till konsekvent extern kommunikation,

   [...]

   c) optimal användning av operativa resurser,

   d) samordning med andra krishanteringsmekanismer på unionsnivå.

3. CERT-EU ska **i nära samarbete med Enisa** stödja unionens […] **entiteter** när det gäller situationsmedvetenhet om cyberhot, sårbarheter och incidenter.

---

14 EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

4. IICB ska**, senast [tolv månader efter dagen för denna förordnings ikraftträdande], på grundval av ett förslag från CERT-EU, anta** […] riktlinjer **eller rekommendationer** för samordning av incidenthantering och samarbete vid betydande incidenter. När en incident misstänks vara brottslig ska CERT-EU ge råd om hur incidenten ska rapporteras till de brottsbekämpande myndigheterna.

Artikel 22

Hantering av större incidenter […]

-1. För att stödja en samordnad hantering av större incidenter på operativ nivå som påverkar unionsentiteter och bidra till ett regelbundet utbyte av relevant information mellan unionsentiteter och med medlemsstaterna ska IICB, i nära samarbete med CERT-EU och Enisa, utarbeta en cyberkrishanteringsplan på grundval av den verksamhet som anges i artikel 21.2 som åtminstone ska innehålla följande delar:

a) Former för samordning och informationsflöde mellan unionsentiteter för hantering av större incidenter på operativ nivå.

b) Gemensamma operationella standardförfaranden (SOP).

c) En gemensam taxonomi för större incidenters allvarlighetsgrad och kriströskelpunkter.

d) Regelbundna övningar.

e) Uppgift om vilka säkra kommunikationskanaler som ska användas.

f) En kontaktpunkt för EU-CyCLONe, som ska dela relevant information med EU-CyCLONe som underlag för den gemensamma situationsmedvetenheten.

1. CERT-EU ska samordna unionens […] **entiteters** hantering av större **incidenter** […]. Centrumet ska föra en förteckning över den tekniska expertis som skulle behövas för incidenthantering i händelse av **större incidenter** […].

2. Unionens […] **entiteter** ska bidra till förteckningen över teknisk expertis genom att tillhandahålla en årligen uppdaterad förteckning över experter som finns tillgängliga inom respektive organisation med detaljerade uppgifter om deras specifika tekniska kompetens.

3. Efter en specifik begäran från en medlemsstat där den drabbade unionsentitetens är belägen och med […] godkännande **från den drabbade unionsentiteten** […] får CERT-EU också anlita experter från den förteckning som avses i punkt 2 för att bidra till hanteringen av **en** […] större **incident vid den unionsentiteten** […].

Kapitel VI
SLUTBESTÄMMELSER

Artikel 23

Inledande omfördelning av budgeten

Kommissionen ska föreslå en omfördelning av personal och ekonomiska resurser från unionens berörda […] **entiteter** till kommissionens budget. Omfördelningen ska få verkan samtidigt som den första budget som antas efter det att denna förordning träder i kraft.

Artikel 24

Översyn

1. IICB ska med bistånd av CERT-EU regelbundet rapportera till kommissionen om genomförandet av denna förordning. IICB får också rekommendera kommissionen att **se över** […] denna förordning.

2. Kommissionen ska rapportera om genomförandet av denna förordning till Europaparlamentet och rådet senast **36** […] månader efter denna förordnings ikraftträdande och därefter vart tredje år.

3. Kommissionen ska utvärdera hur denna förordning fungerar och rapportera till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén **senast** […] fem år efter dagen för ikraftträdandet. **Rapporten ska vid behov åtföljas av ett lagstiftningsförslag.**

Artikel 25

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

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

BILAGA II

[...]

[...]

[...]

[...]

[...]

[...]

[...]