Europeiska unionens
officiella tidning

SV
L-serien

2025/2540

12.12.2025

# KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/2540

**av den 9 december 2025**

**om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller fastställande av planen för inbördes granskning**

**(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) 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) ([1]), särskilt artikel 59.5, och

av följande skäl:

(1) Enligt artikel 59.4 i förordning (EU) 2019/881 ska den inbördes granskningen av nationella myndigheter för cybersäkerhetscertifiering utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och kommissionen. I syfte att uppnå likvärdiga standarder för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse bör kommissionen övervaka aspekter som rör efterlevnaden av denna förordning och säkerställa att inbördes utvärderingar utförs på ett enhetligt sätt i hela unionen. För att bidra till att identifiera god praxis, utmaningar och lärdomar kopplade till genomförandet av europeiska ordningar för cybersäkerhetscertifiering bör Europeiska unionens cybersäkerhetsbyrå (Enisa) ha möjlighet att delta i de inbördes utvärderingarna som observatör. För att stödja ett harmoniserat genomförande av bestämmelserna i denna förordning bör Enisa, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering, också tillåtas att utarbeta mallar.

(2) För att få till stånd en förutsägbar planering och effektiv resursfördelning bör de inbördes granskningarna av varje nationell myndighet för cybersäkerhetscertifiering utföras i enlighet med en fastställd tidsplan. Det bör vara möjligt för en nationell myndighet för cybersäkerhetscertifiering att begära att få skjuta upp sin inbördes granskning under exceptionella omständigheter, till exempel oväntad personalbrist eller fall av force majeure. Det är därför nödvändigt att fastställa formerna för bedömningen av en sådan begäran och säkerställa att den övergripande tidsplanen följs och att målen för mekanismen för inbördes utvärdering inte äventyras.

(3) För att alla medlemsstater faktiskt ska bidra till genomförandet av mekanismen för inbördes utvärdering och för att göra det möjligt för dem att dra nytta av ömsesidigt lärande bör de nationella myndigheterna för cybersäkerhetscertifiering i varje medlemsstat utföra två inbördes utvärderingar under en femårsperiod. Det bör därför inrättas ett rotationssystem som gör det möjligt för de nationella myndigheter för cybersäkerhetscertifiering i samtliga medlemsstater att organisera sitt deltagande. Det är också nödvändigt att fastställa kriterier som de nationella myndigheterna för cybersäkerhetscertifiering bör ta hänsyn till när de väljer ut företrädare som ska utföra inbördes utvärderingar, så att man förfogar över lämplig sakkunskap och kompetens. De nationella myndigheterna för cybersäkerhetscertifiering bör också få delta i inbördes utvärderingar som observatörer i syfte att övervaka och dra lärdom av processen. I sådana fall bör det inte krävas att myndighetsföreträdarna har samma sakkunskap och kompetens som förväntas av de företrädare för de nationella myndigheterna för cybersäkerhetscertifiering som utför de inbördes granskningarna.

(4) För att säkerställa att en nationell myndighet för cybersäkerhetscertifiering blir föremål för inbördes granskning av minst en nationell behörig myndighet som tillämpar samma strategi för utfärdande av certifikat på nivån ”hög” ör Enisa, när den uppmanar de nationella myndigheterna för cybersäkerhetscertifiering att uttrycka sitt intresse för att utföra inbördes granskning, ange huruvida den nationella myndighet för cybersäkerhetscertifiering som blivit föremål för inbördes granskning, direkt utfärdar certifikat på nivån ”hög”, använder den modell för förhandsgodkännande som avses i artikel 56.6 a i förordning (EU) 2019/881, beviljar en allmän delegering i enlighet med led b i den punkten eller använder en kombination av dessa alternativ.

([1]) EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) För att utvärderingskriterierna och förfarandena för utförandet av inbördes utvärderingar ska bli enhetliga i hela unionen, bör varje inbördes utvärdering alltid innehålla ett frågeformulär för självbedömning, en dokumentationsgranskning och ett besök på plats, åtföljt av intervjuer. Efter besöket på plats bör gruppen för inbördes granskning diskutera resultaten med den nationella myndighet som granskats, utarbeta ett utkast till rapport och överlämna den till den granskade myndigheten för synpunkter, i syfte att säkerställa konsensus när så är möjligt. Gruppen för inbördes bedömning bör lämna in slutrapporten, som kan innehålla riktlinjer eller rekommendationer för att möjliggöra förbättringar för granskade myndigheten, till den europeiska gruppen för cybersäkerhetscertifiering. Den europeiska gruppen för cybersäkerhetscertifiering bör också, på förslag från gruppen för inbördes bedömning, godkänna en sammanfattande rapport som ska göras tillgänglig för allmänheten.

(6) För att den information som erhålls vid den inbördes granskningen ska hanteras på ett säkert sätt bör gruppen för inbördes granskning använda säkra kommunikationskanaler, såsom en säker plattform för lagring och delning av dokument, och använda lämpliga skyddsåtgärder för konfidentiella uppgifter som delas mellan medlemmarna i gruppen för inbördes granskning. Enisa bör, med beaktande av bästa praxis hos nationella myndigheter för cybersäkerhetscertifiering, också kunna utarbeta riktlinjer för hur säker kommunikation kan uppnås, särskilt i syfte att säkerställa att den säkerhetsnivå som tillämpas av gruppen för inbördes granskning när den samlar in, delar och behandlar information anpassas till säkerhetsbehoven hos den granskade nationella myndigheten för cybersäkerhetscertifiering.

(7) För att underlätta samarbete och effektivt informationsutbyte mellan nationella myndigheter för cybersäkerhetscertifiering bör framför allt den europeiska gruppen för cybersäkerhetscertifiering bidra till utarbetandet av mallar och bistå kommissionen i genomförandet av denna förordning.

(8) Mekanismen för inbördes bedömning utgör en transeuropeisk digital offentlig tjänst i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/903 ([2]). Genom den här förordningen införs nya bindande krav som påverkar den tjänsten, och som sådan omfattas den av skyldigheten att göra en interoperabilitetsbedömning enligt artikel 3 i förordning (EU) 2024/903. En interoperabilitetsbedömning har därför utförts, och den resulterande rapporten kommer att offentliggöras på portalen för ett interoperabelt Europa.

(9) Vid utarbetandet av den här förordningen har kommissionen beaktat synpunkterna från den europeiska gruppen för cybersäkerhetscertifiering, och då även från dess undergrupp för inbördes granskning.

(10) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 66 i förordning (EU) 2019/881.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

*Artikel 1*

**Tidsplan, frekvens och kostnader för inbördes granskningar**

1. Den inbördes granskningen av nationella myndigheter för cybersäkerhetscertifiering ska utföras i enlighet med tidsplanen i bilaga I. Alla inbördes granskningar ska vara utförda det datum som anges i tidsplanen, och ska därefter utföras vart femte år.

2. Under exceptionella omständigheter får en nationell myndighet för cybersäkerhetscertifiering, som varit föremål för inbördes granskning, lämna in en vederbörligen motiverad begäran till kommissionen om att skjuta upp granskningen till efter det datum som anges i tidsplanen i bilaga I. Kommissionen ska, i samarbete med den europeiska gruppen för cybersäkerhetscertifiering som inrättats genom artikel 62 i förordning (EU) 2019/881, bedöma begäran och i god tid informera alla berörda parter om resultatet.

([2]) Europaparlamentets och rådets förordning (EU) 2024/903 av den 13 mars 2024 om åtgärder för en hög nivå av interoperabilitet inom den offentliga sektorn i hela unionen (förordningen om ett interoperabelt Europa) (EUT L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Om en medlemsstat i enlighet med artikel 58.1 i förordning (EU) 2019/881 har utsett

a) fler än en nationell myndighet för cybersäkerhetscertifiering på sitt territorium ska alla sådana myndigheter i den medlemsstaten genomgå inbördes granskning parallellt,

b) en eller flera nationella myndigheter för cybersäkerhetscertifiering från en annan medlemsstat, får de myndigheterna genomgå inbördes granskning i enlighet med den tidsplan som fastställts antingen för den utseende medlemsstaten eller för den medlemsstat där den utsedda nationella myndigheten för cybersäkerhetscertifiering eller de utsedda nationella myndigheterna för cybersäkerhetscertifiering är belägna, med avseende på de tillsynsuppgifter som utförs i den utseende medlemsstaten.

4. Europeiska unionens cybersäkerhetsbyrå (Enisa) ska på webbplatsen om europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med artikel 50 i förordning (EU) 2019/881 offentliggöra

a) information om tidsplanen i bilaga I,

b) den förteckning över nationella myndigheter för cybersäkerhetscertifiering som utför inbördes granskning och som underhålls i enlighet med artikel 2.5.

5. Varje nationell myndighet för cybersäkerhetscertifiering som deltar i den inbördes granskningen ska bära sina kostnader för deltagande.

*Artikel 2*

**Rotationssystem för myndigheter för cybersäkerhetscertifiering som utför inbördes granskning**

1. I enlighet med artikel 59.4 i förordning (EU) 2019/881 ska den inbördes granskningen utföras av minst två nationella myndigheter för cybersäkerhetscertifiering från andra medlemsstater och kommissionen. De nationella myndigheterna för cybersäkerhetscertifiering från varje medlemsstat ska delta i en inbördes granskning av minst två andra nationella myndigheter för cybersäkerhetscertifiering under varje period som anges i bilaga I.

2. De nationella myndigheterna för cybersäkerhetscertifiering från andra medlemsstater får, med en eller flera företrädare, delta i den inbördes granskningen som observatörer, med samtycke från den nationella myndighet för cybersäkerhetscertifiering som granskas inbördes, från den nationella myndighet för cybersäkerhetscertifiering som utför granskningen och från kommissionen.

3. En företrädare för Enisa får delta i den inbördes granskningen som observatör. Ytterligare företrädare får också, med med samtycke från den nationella myndighet för cybersäkerhetscertifiering som granskas inbördes, från den nationella myndighet för cybersäkerhetscertifiering som utför granskningen och från kommissionen, delta.

4. Observatörerna ska ha tillgång till samma information som de andra medlemmarna i gruppen för inbördes granskning, men får inte utföra uppgifter som rör utförandet av den inbördes granskningen.

5. Enisa, i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering, ska föreslå och underhålla den förteckning över nationella myndigheter för cybersäkerhetscertifiering som utför den inbördes granskningen enligt tidsplanen i bilaga I. Under ett givet år ska Enisa, i samarbete med kommissionen, be nationella myndigheter för cybersäkerhetscertifiering att ange om de önskar delta som observatörer i, eller utföra, de inbördes granskningar av nationella myndigheter för cybersäkerhetscertifiering i enlighet med tidsplanen i bilaga I för det kommande året.

6. Om fler än två nationella myndigheter för cybersäkerhetscertifiering uttrycker sitt intresse för att utföra den inbördes granskningen av samma nationella myndighet för cybersäkerhetscertifiering ska kommissionen och Enisa samråda med de myndigheter som uttryckt intresse och bestämma vilka myndigheter som ska utföra den inbördes granskningen.

7. Om under ett visst år inte tillräckligt många nationella myndigheter för cybersäkerhetscertifiering uttrycker sitt intresse för att utföra de inbördes granskningarna ska kommissionen, efter samråd med den europeiska gruppen för cybersäkerhetscertifiering, välja ut de nationella myndigheter för cybersäkerhetscertifiering som ska utföra de inbördes granskningarna. När kommissionen väljer ut myndigheter ska den ta hänsyn till skyldigheten för de nationella myndigheter för cybersäkerhetscertifiering i varje medlemsstat att delta i den inbördes granskning av minst två nationella myndigheter för cybersäkerhetscertifiering som avses i punkt 1.

*Artikel 3*

**Kriterier för sammansättningen av gruppen för inbördes granskning**

1. I god tid innan den inbördes granskningen inleds ska varje nationell myndighet för cybersäkerhetscertifiering som utför den inbördes granskningen utse en företrädare som ska genomföra den. Nationella myndigheter för cybersäkerhetscertifiering som utför inbördes granskning får utse fler än en företrädare om det behövs för att säkerställa att gruppen för inbördes granskning besitter den kompetens som krävs för att utföra den inbördes granskningen.

2. Företrädare för nationella myndigheter för cybersäkerhetscertifiering som utför inbördes granskning, med undantag av företrädare för nationella myndigheter för cybersäkerhetscertifiering som deltar som observatörer, ska

a) ha minst två års erfarenhet av att arbeta för den nationella myndighet för cybersäkerhetscertifiering som utför den inbördes granskningen, eller ha deltagit i minst två inbördes granskningar som observatör,

b) har tillräckliga kunskaper om det ramverk för cybersäkerhetscertifiering som fastställs i förordning (EU) 2019/881,

c) ha goda kunskaper i engelska och, om möjligt, i ett eller flera av de språk som talas i den medlemsstat där de nationella myndigheter för cybersäkerhetscertifiering som är föremål för den inbördes granskningen är belägna,

d) verka oberoende av den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen.

3. Nationella myndigheter för cybersäkerhetscertifiering som utför den inbördes granskningen ska säkerställa att alla risker för intressekonflikter som rör de utsedda företrädarna avslöjas för de andra nationella myndigheterna för cybersäkerhetscertifiering, kommissionen och Enisa innan den inbördes granskningen inleds. Den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen får invända mot att en viss företrädare utses i enlighet med punkt 5.

4. De nationella myndigheter för cybersäkerhetscertifiering som utför den inbördes granskningen ska välja en företrädare (gruppledaren) från någon av myndigheterna som samordnare för den inbördes granskningen.

5. Kommissionen ska informera den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen om namn och kontaktuppgifter för företrädarna för de nationella myndigheter för cybersäkerhetscertifiering som utför den inbördes granskningen innan den inleds. Om den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen vill invända mot en eller flera utsedda företrädare ska den inom två veckor lämna en tydlig motivering till kommissionen, informera Enisa och den europeiska gruppen för cybersäkerhetscertifiering, samt begära att den nationella myndighet för cybersäkerhetscertifiering som utför den inbördes granskningen utser en annan företrädare.

6. Om det förfarande som anges i punkt 5 orsakar onödiga förseningar i inledandet av den inbördes granskningen på grund av exceptionella omständigheter ska kommissionen, i samråd med Enisa och den europeiska gruppen för cybersäkerhetscertifiering, besluta om hur gruppen för inbördes granskning ska vara sammansatt.

*Artikel 4*

**Metod för den inbördes granskningen**

1. Den inbördes granskningen ska bedöma de aspekter som förtecknas i bilaga II, i enlighet med artikel 59.3 i förordning (EU) 2019/881.

2. Enisa får, i samarbete med den europeiska gruppen för cybersäkerhetscertifiering och kommissionen, utarbeta mallar för bedömningen av de processer som inrättats av den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen.

3. Den inbördes granskningen ska omfatta följande:

a) Ett frågeformulär för självbedömning.

b) Bedömning av relevant dokumentation.

c) Online-intervjuer eller fysiska intervjuer, eller både och.

d) Besök på plats.

4. Längden på den inbördes granskningen får överenskommas på förhand mellan gruppen som utför den inbördes granskningen och den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen, beroende hur omfattande och komplex verksamheten är hos den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen. Besöket på plats får inte pågå längre än tre arbetsdagar.

5. Samarbetsspråket ska vara engelska om inte annat överenskommits mellan gruppen som utför den inbördes granskningen, den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen och kommissionen. Den rapport över den inbördes granskningen som avses i artikel 5 ska författas på åtminstone engelska.

6. Den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen ska samarbeta med gruppen som utför den inbördes granskningen och ge den tillgång till den information och de handlingar som är nödvändiga för den inbördes granskningen. Den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen ska lämna in frågeformuläret för självbedömning och den senaste årliga sammanfattande rapport som antagits i enlighet med artikel 58.7 g i förordning (EU) 2019/881 minst 21 dagar före besöket på plats. Ytterligare handlingar ska lämnas in på begäran av gruppen som utför den inbördes granskningen inom 7 dagar från mottagandet av en sådan begäran.

7. Handlingarna ska vara författade på engelska om inte annat överenskommits i enlighet med punkt 5. Om handlingarna inte är författade på engelska kan gruppen som utför den inbördes granskningen begära att de handlingar som krävs för den inbördes granskningen översätts till engelska.

8. Innan gruppen som utför den inbördes granskningen utarbetar rapporten över den inbördes granskningen i enlighet med artikel 5 ska den diskutera preliminära resultat med den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen.

*Artikel 5*

**Rapport över den inbördes granskningen**

1. Senast 21 dagar efter utförandet av den inbördes granskningen ska gruppen som utförde granskningen utarbeta ett utkast till rapport över den inbördes granskningen med närmare uppgifter om den medlemsstat där den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen är belägen, de nationella myndigheter för cybersäkerhetscertifiering som utförde den inbördes granskningen, kommissionen och eventuella observatörer, samt resultaten och slutsatserna från den inbördes granskningen. Om det är nödvändigt, ska rapporten innehålla rekommendationer till förbättringar när det gäller de aspekter som omfattas av den inbördes granskningen.

2. Enisa får i samarbete med kommissionen och den europeiska gruppen för cybersäkerhetscertifiering utarbeta en mall för rapporten över den inbördes granskningen.

3. Efter att ha utarbetat utkastet till rapport över den inbördes granskningen i enlighet med punkt 1 ska gruppen som utförde den inbördes granskningen skicka rapporten till den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen med begäran om synpunkter som ska lämnas inom 14 dagar. Gruppen som utförde den inbördes granskningen ska utvärdera synpunkterna och, när så är möjligt, ta med dem i slutrapporten, i syfte att säkerställa konsensus. Om det råder oenighet ska svaret från den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen bifogas slutrapporten.

4. Slutrapporten ska skickas till den europeiska gruppen för cybersäkerhetscertifiering inom två månader från det att den inbördes granskningen utfördes, tillsammans med en sammanfattning, för offentliggörande. I enlighet med artikel 59.6 i förordning (EU) 2019/881 ska den europeiska gruppen för cybersäkerhetscertifiering granska rapporten och godkänna dess sammanfattning, som ska offentliggöras på webbplatsen för europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med artikel 50 i förordning (EU) 2019/881. Sammanfattningen ska också innehålla svaret från den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen eller delar av det, i samförstånd med den myndigheten.

5. Gruppen som utförde den inbördes granskningen ska anonymisera personuppgifter som den kan ha samlat in under den inbördes granskningen innan den skickar rapporten över den inbördes granskningen utanför gruppen.

*Artikel 6*

**Konfidentialitet**

1. Alla parter som deltar i inbördes granskningar ska respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de skyddar följande:

a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inbegripet källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/943 ([3]).

b) Ett effektivt genomförande av denna förordning.

c) Intressen som rör allmän och nationell säkerhet.

d) Integriteten i straffrättsliga eller administrativa förfaranden.

2. Gruppen som utförde den inbördes granskningen ska säkerställa att all information som erhålls vid den inbördes granskningen hanteras på ett säkert sätt. När den slutrapport och den sammanfattning som avses i artikel 5.4 har utarbetats ska gruppen som utförde den inbördes granskningen, även eventuella observatörer, radera eller förstöra alla handlingar, utom slutrapporten och sammanfattningen, som har samlats in eller skapats som en del av den inbördes granskningen.

3. Enisa får, med beaktande av bästa praxis hos de nationella myndigheterna för cybersäkerhetscertifiering, i samarbete med den europeiska gruppen för cybersäkerhetscertifiering, utarbeta riktlinjer för säker och konfidentiell kommunikation.

([3]) Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

*Artikel 7*

**Kapacitetsuppbyggnad**

Enisa ska analysera de sammanlagda resultaten av de inbördes granskningarna och betona de viktigaste lärdomar som dragits och bästa praxis för att bidra till kapacitetsuppbyggnad för de nationella myndigheterna för cybersäkerhetscertifiering och till underhållet av europeiska ordningar för cybersäkerhetscertifiering. Denna analys kan, när så är lämpligt, innehålla utbildning och ytterligare riktlinjer för de nationella myndigheterna för cybersäkerhetscertifiering, utarbetade i samarbete med den europeiska gruppen för cybersäkerhetscertifiering.

*Artikel 8*

**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 9 december 2025.

*På kommissionens vägnar*
Ursula VON DER LEYEN
*Ordförande*

*BILAGA I*

**Tidsplan för nationella myndigheter för cybersäkerhetscertifiering som omfattas av en inbördes granskning**

Nationella myndigheter för cybersäkerhetscertifiering i följande medlemsstater ska omfattas av en inbördes granskning senast den 31 december 2026 och därefter vart femte år.

Belgien, Malta, Slovakien, Sverige, Tjeckien, Tyskland

Nationella myndigheter för cybersäkerhetscertifiering i följande medlemsstater ska omfattas av en inbördes granskning senast den 31 december 2027 och därefter vart femte år.

Estland, Grekland, Italien, Nederländerna, Slovenien, Ungern

Nationella myndigheter för cybersäkerhetscertifiering i följande medlemsstater ska omfattas av en inbördes granskning senast den 31 december 2028 och därefter vart femte år.

Bulgarien, Danmark, Irland, Kroatien, Litauen, Spanien

Nationella myndigheter för cybersäkerhetscertifiering i följande medlemsstater ska omfattas av en inbördes granskning senast den 31 december 2029 och därefter vart femte år.

Finland, Lettland, Luxemburg, Polen, Rumänien, Österrike

Nationella myndigheter för cybersäkerhetscertifiering i följande medlemsstater och EES-/Eftaländer ska omfattas av en inbördes granskning senast den 31 december 2030 och därefter vart femte år.

Cypern, Frankrike, Island, Liechtenstein, Norge, Portugal

*BILAGA II*

## Metod för inbördes granskning

### II.1 Åtskiljande av certifierings- och tillsynsverksamhet

I samband med den bedömning av huruvida de certifierings- och tillsynsverksamheter som avses i artikel 59.3 a i förordning (EU) 2019/881 hålls åtskilda vid den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen ska den inbördes granskningen åtminstone omfatta följande:

a) En detaljerad beskrivning av hur den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen fungerar, i vilken de olika enheter och/eller avdelningar som deltar i genomförandet av förordning (EU) 2019/881 tydligt identifieras.

b) En jämförelse av verksamheten vid den nationella myndighet för cyberhetssäkerhetscertifiering som är föremål för den inbördes granskningen med de verksamheter som förtecknas i artikel 58.7 i förordning (EU) 2019/881.

c) Om den nationella myndighet för cyberhetssäkerhetscertifiering som är föremål för den inbördes granskningen utfärdar certifikat, en förklaring som visar att dess certifieringsverksamhet och de tillsynsverksamheter som fastställts enligt led b inte står i strid med varandra.

### II.2 Övervakning och kontroll av efterlevnaden av reglerna för överensstämmelse med certifikaten

I samband med den bedömningen av förfaranden för övervakning och kontroll av efterlevnaden av reglerna om IKT-produkters, IKT-tjänsters, IKT-processers och utlokaliserade säkerhetstjänsters överensstämmelse med europeiska cybersäkerhetscertifikat, som avses i artikel 59.3 b i förordning (EU) 2019/881, vid den nationella myndighet för cybersäkerhetscertifiering som är föremål för den inbördes granskningen ska den inbördes granskningen åtminstone omfatta följande:

a) Kvalitet på och grad av detalj för beskrivningen av dessa processer och förfaranden och i vilken utsträckning de är dokumenterade.

b) Huruvida och i vilken utsträckning sådana processer och förfaranden omfattar relevanta europeiska ordningar för cybersäkerhetscertifiering.

c) Huruvida den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning faktiskt är behörig att inspektera organ för bedömning av överensstämmelse som utfärdar certifikat och, om så nödvändigt, återkalla certifikaten.

d) Omfattningen av samarbetet mellan den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning och berörda marknadskontrollmyndigheter.

e) Huruvida den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning har en mekanism för att behandla klagomål från fysiska eller juridiska personer, vilket krävs enligt artikel 58.7 f i förordning (EU) 2019/881, inbegripet bevis för huruvida fysiska och juridiska personer har rätt att lämna in klagomål samt har rätt till effektiva rättsmedel i enlighet med artiklarna 63 och 64 i den förordningen.

### II.3 Övervakning och verkställande av tillverkares och tillhandahållares skyldigheter

I samband med bedömningen av de förfaranden som den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning har för övervakning och verkställande av de skyldigheter som tillverkare eller tillhandahållare, som utför självbedömning av överensstämmelse, har enligt med artikel 59.3 c i förordning (EU) 2019/881 ska den inbördes granskningen åtminstone omfatta följande:

a) Huruvida den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning har infört sådana förfaranden och i vilken utsträckning dessa har dokumenterats, i synnerhet om den har inrättat en mekanism för att ta emot och hantera information från externa källor.

b) Huruvida och i vilken utsträckning sådana förfaranden omfattar relevanta europeiska ordningar för cybersäkerhets-certifiering.

c) Huruvida och i vilken utsträckning den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning utför egna undersökningar och huruvida omfattningen av undersökningarna täcker de skyldigheter som tillverkare har enligt artikel 53.2 och 53.3 i förordning (EU) 2019/881 och i motsvarande europeiska ordningar för cybersäkerhetscertifiering.

d) Huruvida det finns ett förfarande för informationsutbyte mellan certifieringsverksamhet och tillsynsverksamhet vid den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning som är relevant för att övervaka och verkställa tillverkares och tillhandahållares skyldigheter.

II.4 **Övervakning, bemyndigande och kontroll av organen för bedömning av överensstämmelse**

I samband med bedömningen av de förfaranden som den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning har för övervakning, bemyndigande och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse, i enlighet med artikel 59.3 d i förordning (EU) 2019/881, ska den inbördes granskningen åtminstone omfatta följande:

a) Kvalitet på och grad av detalj för beskrivningen av sådana förfaranden och i vilken utsträckning de är dokumenterade, inbegripet när det gäller samarbete med det nationella ackrediteringsorganet.

b) Central statistik över antalet bemyndiganden som beviljats, tillfälligt upphävts eller återkallats, det totala antalet organ för bedömning av överensstämmelse som är aktiva, antalet certifikat som har utfärdats och antalet korrigerande åtgärder som den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning har vidtagit.

c) Personalens sakkunskap och de förfaranden via vilka den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning övervakar och utövar tillsyn över verksamheten vid organen för bedömning av överensstämmelse, i de fall den nationella myndighet för cybersäkerhetscertifiering som är föremål för inbördes granskning tillåter utfärdande av europeiska cybersäkerhetscertifikat med nivån ”hög” efter förhandsgodkännande eller efter allmän delegering av uppgiften i enlighet med artikel 56.6 i förordning (EU) 2019/881.