CRA EVIDENCE WHITEPAPER

EU:s cyberresiliensförordning: praktisk guide till överensstämmelse

Whitepaper för tillverkare, importörer och distributörer av produkter med digitala element.

Version	1.0
Status	Levande dokument
Grund	Förordning (EU) 2024/2847

Ändringshistorik

Det här är ett levande dokument. Det uppdateras i takt med att kommissionens vägledning, harmoniserade standarder och marknadspraxis under CRA utvecklas.

Version	Datum	Beskrivning
1.0	17 maj 2026	Första publicering. Täcker tillämpningsområde, klassificering, väsentlig ändring, väsentliga krav, sårbarhetshantering, teknisk dokumentation, vägar för bedömning av överensstämmelse samt samspel med AI Act, Data Act, ESPR och produktansvar.

Innehåll

Sammanfattning

PÅ 60 SEKUNDER

Vad som omfattas: uppkopplad hårdvara och programvara som tillhandahålls på EU-marknaden. Säkerhet behandlas som ett krav på produktöverensstämmelse, inte som en frivillig bästa praxis.

När det börjar gälla: rapportering enligt artikel 14 från 11 september 2026. Fullständiga tekniska krav, dokumentationskrav och krav på CE-märkning från 11 december 2027.

Vad du måste ta fram: bedömning av cybersäkerhetsrisker, SBOM, teknisk dokumentation, användarinstruktioner, EU-försäkran om överensstämmelse, CE-märkning samt artikel 14-rapporter om incidenter och sårbarheter.

Vem som behöver agera

Tillverkare bär huvudansvaret. Importörer och distributörer har omsorgskontroller innan de tillhandahåller produkter.

Vad som förändras

Cybersäkerhet blir del av produktöverensstämmelse: säker design, sårbarhetshantering, dokumentation, CE-märkning och åtgärder efter marknadslansering.

Första tidsfristen

Rapportering enligt artikel 14 börjar **11 september 2026** för aktivt utnyttjade sårbarheter och allvarliga incidenter.

Full tillämpning

Full teknisk överensstämmelse gäller från **11 december 2027**. Äldre produkter omfattas efter en väsentlig ändring, men rapporteringen gäller fortsatt.

Bevisens ryggrad

Den tekniska dokumentationen behöver riskbedömning, SBOM, motivering av stödperioden, testbevis, instruktioner, försäkran och bevis för överensstämmelse med de väsentliga cybersäkerhetskraven.

Bedömningsväg

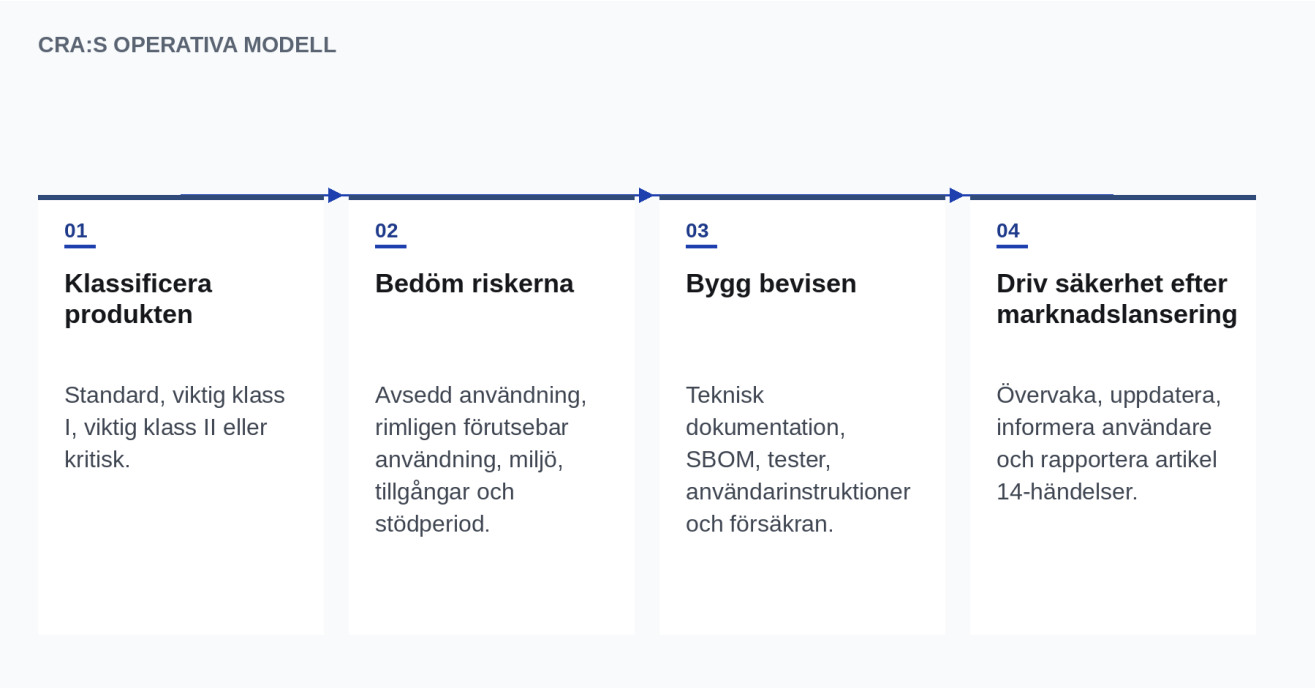
De flesta produkter kan använda modul A med självbedömning. Viktiga och kritiska produkter kan kräva anmält organ eller EU-cybersäkerhetscertifiering.

Vad är cyberresiliensförordningen?

Cyber Resilience Act (CRA), på svenska cyberresiliensförordningen och formellt Förordning (EU) 2024/2847, är EU:s första horisontella ramverk som gör cybersäkerhet till ett bindande krav för produkter med digitala element som tillhandahålls på EU-marknaden. Den auktoritativa texten finns på EUR-Lex.

CRA gäller tillverkare, importörer och distributörer av uppkopplad hårdvara och programvara. Den omfattar produkter från konsument-IoT till industriella styrsystem. Den praktiska förändringen är tydlig: cybersäkerhet ska utformas, bevisas, underhållas och övervakas som en del av produktöverensstämmelsen.

Bristande efterlevnad av de väsentliga cybersäkerhetskraven eller skyldigheterna i artikel 13 och 14 kan leda till sanktionsavgifter på upp till 15 miljoner euro eller 2,5 procent av den globala årsomsättningen, beroende på vilket belopp som är högst. Lägre nivåer gäller: upp till 10 miljoner euro eller 2 procent för överträdelse av andra angivna skyldigheter, och upp till 5 miljoner euro eller 1 procent för att lämna felaktig, ofullständig eller vilseledande information till anmälda organ eller marknadskontrollmyndigheter. Marknadskontrollmyndigheter kan också kräva korrigerande åtgärder, begränsa tillgängligheten, dra tillbaka produkter eller kräva återkallelser.



Viktiga datum för planering av överensstämmelse

CRA trädde i kraft **10 december 2024**. Det praktiska arbetet med överensstämmelse samlas kring tre milstolpar: anmälda organ i **juni 2026**, rapportering i **september 2026** och full teknisk överensstämmelse i **december 2027**.

NOTERING

Aktuellt läge för kommissionens vägledning: Europeiska kommissionen publicerade utkast till CRA-vägledning den 3 mars 2026. Samrådet stängde den 13 april 2026. Vägledningen är inte slutlig, men den är användbar som planeringsunderlag för utsläppande på marknaden, fri programvara och öppen källkod, stödperioder, väsentliga ändringar, produktklassificering, komponentgranskning, fjärrdatabehandling, sårbarhetshantering och överlapp med annan EU-lagstiftning. Gränsfrågor mot AI Act och DORA kan fortfarande behöva ytterligare vägledning.

10 december 2024

Ikraftträdande

Övergångsperioden börjar

11 juni 2026

Anmälda organ

Kapitel IV gäller

11 september 2026

Rapportering

Artikel 14 börjar gälla

11 december 2027

Full tillämpning

Tekniska krav, CE-märkning, dokumentation och bedömning av överensstämmelse

BÖRJA HÄR

Börja med rapporteringsberedskap. Tidsfristen i artikel 14 kommer före full teknisk överensstämmelse och gäller även produkter som redan finns på EU-marknaden.

Eftersom rapporteringen börjar **11 september 2026** bör rapporteringsberedskap vara det första genomförandespåret: **detektion, triage, användarkommunikation och myndighetsrapportering** måste fungera innan full teknisk överensstämmelse krävs.

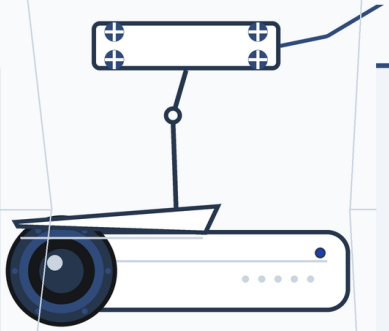
Produkter som släppts ut på marknaden före **11 december 2027** omfattas av de tekniska kraven i CRA bara om de genomgår en **väsentlig ändring** från det datumet. Rapporteringen fungerar annorlunda: artikel 14 gäller **alla produkter inom tillämpningsområdet**, inbegripet produkter som redan finns på EU-marknaden.

CRA över produktens livscykel

STEG 01
Fastställ omfattning
Omfattning, klassificering, supportperiod och riskbedömning

STEG 02
Utveckla säkert
Säkra defaults, kodanalys, SBOM och beroendekontroll

STEG 03
Validera och dokumentera
Säkerhetstester, vuln-triage, teknisk dokumentation och användarinfo



STEG 04
Släpp på marknaden
EU-försäkran om överensstämmelse, CE-märkning och releasebeslut

STEG 05
Övervaka och uppdatera
CVE:er, råd, exploitaktivitet, uppdateringar och offentliggörande

STEG 06
Ge support och samarbeta
Art. 14, användarinfo, myndighetsfrågor och supportslut

Uppkopplad IP-kamera, från produktplanering till eftermarknadssupport enligt CRA

Vilka produkter omfattas

Tillämpningsområde och undantag

CRA gäller hårdvaru- och programvaruprodukter där avsedd eller rimligen förutsebar användning omfattar en direkt eller indirekt dataanslutning till en enhet eller ett nätverk. Det omfattar datorer, smarttelefoner, nätverksutrustning, IoT-enheter, industriella styrsystem och databehandlingsapplikationer.

Följande kategorier är uttryckligen undantagna:

- Medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik som omfattas av förordningarna (EU) 2017/745 och 2017/746
- Fordonssystem som omfattas av förordning (EU) 2019/2144
- Luftfartsutrustning som omfattas av förordning (EU) 2018/1139
- Marin utrustning som omfattas av direktiv 2014/90/EU
- Produkter som utvecklats enbart för nationell säkerhet eller försvar
- Rent mekaniska produkter utan digitala element eller nätverksanslutning

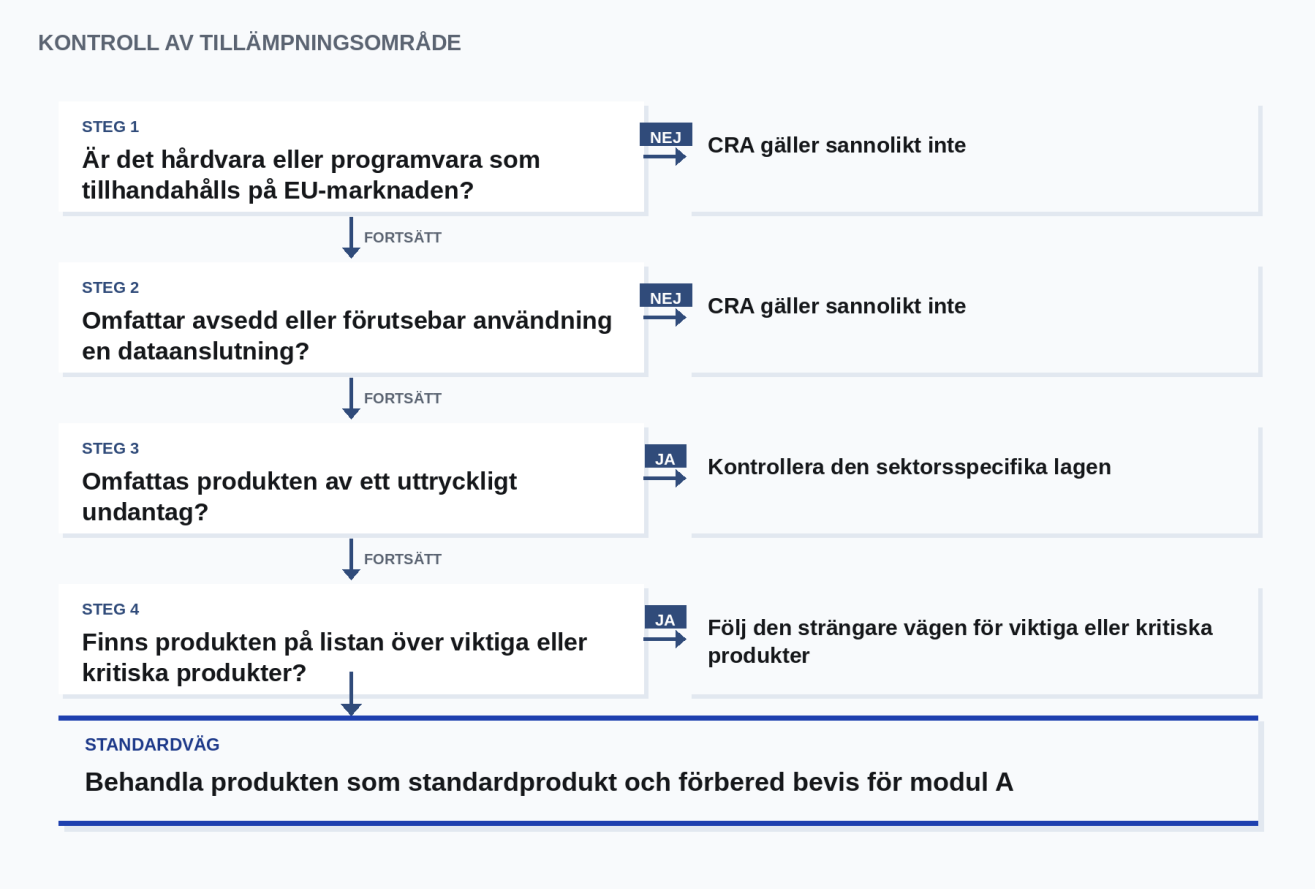
Om inget tydligt undantag gäller bör du behandla den uppkopplade produkten som en produkt inom CRA:s tillämpningsområde.

NOTERING

Skräddarsydda produkter: ett smalt undantag. Om du bygger en produkt anpassad för en enskild företagsanvändare, enligt ett skriftligt avtal mellan dig och den användaren, får du avvika från två krav: den säkra standardkonfigurationen (du måste fortfarande erbjuda en väg tillbaka till ett säkert ursprungsläge) och kostnadsfria säkerhetsuppdateringar (avtalet kan reglera en annan kommersiell grund). Allt annat gäller fullt ut: sårbarhetshantering, övriga produktsäkerhetskrav, rapportering enligt artikel 14, teknisk dokumentation, CE-märkning, bedömning av överensstämmelse och stödperioden. Det är inte ett generellt B2B-undantag; det omfattar inte standardprodukter som säljs till företag.

EKONOMISKA AKTÖRERS ANSVAR

Tillverkare	Utformar säkra produkter, bedömer risk, tar fram teknisk dokumentation, genomför bedömning av överensstämmelse, hanterar sårbarheter och rapporterar artikel 14-händelser.
Importör	Kontrollerar tillverkarens överensstämmelse, verifierar CE-märkning och dokumentation, håller försäkran tillgänglig och agerar på kända sårbarheter.
Distributör	Kontrollerar indikatorer för tillbörlig aktsamhet före leverans, verifierar nödvändig information och instruktioner, och tillhandahåller inte produkter som inte överensstämmer.



Produktklassificering styr bedömningsvägen

Produktkategorin styr hur du visar överensstämmelse.

Kategori	Exempel	Bedömning av överensstämmelse
Standard "oklassificerad"	Allmän programvara och uppkopplade konsumentprodukter som inte hör hemma i kategorierna viktig eller kritisk	Modul A: självbedömning
Viktig "klass I"	Identitetshantering, webbläsare, lösenordshanterare, antivirus, VPN, nätverkshantering, router, smart lås, säkerhetskamera och liknande produkter	Modul A endast när tillämpliga harmoniserade standarder, gemensamma specifikationer eller certifieringssystem tillämpas enligt kraven; annars modul B+C eller modul H
Viktig "klass II"	Hypervisorer, containerruntimes, brandväggar, IDS/IPS och manipulationsresistenta mikroprocessorer	Modul B+C, modul H eller ett tillämpligt europeiskt cybersäkerhetscertifieringssystem med minst assuransnivån "betydande"
Kritiska produkter	Säkra element, smartkort, smarta mätargateways och hårdvarusäkerhetsboxar	Europeisk cybersäkerhetscertifiering där det krävs och finns tillgängligt; annars gäller vägarna för klass II

De fyra produktkategorierna

Tabellen ovan visar exempel. Den fullständiga referensen, som du jämför produktens kärnfunktion mot, framgår nedan.

Standardprodukter

De flesta produkter hamnar här. Varje produkt med digitala element vars kärnfunktion inte matchar något i listorna över viktiga eller kritiska produkter nedan behandlas som standard. Vägen för bedömning av överensstämmelse är modul A med självbedömning.

Vanliga exempel:

- Smarta TV-apparater och streamingenheter.
- Nätverksskrivare och multifunktionsenheter för kontor.
- Bluetooth-högtalare och ljudprodukter för konsumenter.
- Programvara för mediaspelare.
- Spelkonsoler, e-läsare och liknande konsumentelektronik.
- Smarta köksapparater som ugnar, kylskåp och diskmaskiner utan säkerhetsfunktioner.
- Smarta glödlampor och uppkopplad belysning utan säkerhetsfunktioner.
- Aktivitetsarmband utan hälsoövervakande syfte.
- Allmänna mobilapplikationer som inte är webbläsare, lösenordshanterare eller VPN-appar.
- Programvara för kontorsproduktivitet som ordbehandlare och kalkylprogram.

Listan ovan är illustrativ. Listorna för viktiga och kritiska produkter nedan är uttömmande.

Viktiga produkter (klass I)

Obligatorisk bedömning av tredje part, om inte tillämpliga harmoniserade standarder, gemensamma specifikationer eller certifieringssystem tillämpas enligt kraven.

1. Programvara och hårdvara för identitetshantering och hantering av privilegierad åtkomst, inbegripet läsare för autentisering och åtkomstkontroll (inklusive biometriska läsare).
2. Fristående och inbäddade webbläsare.
3. Lösenordshanterare.
4. Programvara som söker efter, tar bort eller karantänsätter skadlig programvara.
5. VPN-produkter.
6. Nätverkshanteringssystem.
7. System för säkerhetsinformations- och händelsehantering (SIEM).
8. Starthanterare.
9. Programvara för publik nyckelinfrastruktur och utfärdande av digitala certifikat.
10. Fysiska och virtuella nätverksgränssnitt.
11. Operativsystem.
12. Routrar, modem avsedda för internetanslutning och switchar.
13. Mikroprocessorer med säkerhetsrelaterade funktioner.

14. Mikrokontroller med säkerhetsrelaterade funktioner.
15. ASIC- och FPGA-kretsar med säkerhetsrelaterade funktioner.
16. Allmänna virtuella assistenter för smarta hem.
17. Smarta hem-produkter med säkerhetsfunktioner (smarta dörrlås, säkerhetskameror, babyövervakningssystem, larmsystem).
18. Internetanslutna leksaker med interaktiva funktioner (tal, filmning, positionsspårning).
19. Personliga bärbara enheter med hälsoövervakande syfte (där förordningarna (EU) 2017/745 eller 2017/746 inte gäller), eller bärbara enheter avsedda för barn.

Viktiga produkter (klass II)

Obligatorisk bedömning av tredje part, strängare väg. Självbedömning är inte tillgänglig ens när harmoniserade standarder finns.

1. Hypervisorer och containerruntimes som stödjer virtualiserad körning av operativsystem och liknande miljöer.
2. Brandväggar, system för intrångsdetektering och intrångsskydd.
3. Manipulationsresistenta mikroprocessorer.
4. Manipulationsresistenta mikrokontroller.

Kritiska produkter

Europeisk cybersäkerhetscertifiering krävs där systemet finns tillgängligt. Annars gäller vägen för klass II.

1. Hårdvaruenheter med säkerhetsboxar.
2. Smarta mätargateways inom smarta mätarsystem enligt definitionen i artikel 2.23 i direktiv (EU) 2019/944, och andra enheter för avancerade säkerhetsändamål, inbegripet säker kryptobehandling.
3. Smartkort och liknande enheter, inbegripet säkra element.

Om produktens kärnfunktion matchar något i listorna för viktiga eller kritiska produkter hamnar produkten i den klassen. Om produkten integrerar något av listpunkterna som komponent men har en annan egen kärnfunktion ändrar integreringen inte klassen.

Så klassificerar du: kärnfunktion, inte integration

Listorna ovan säger vad kategorierna är. De säger inte hur du tillämpar dem på din produkt. CRA:s svar är ett enda begrepp: **kärnfunktion**.

Klassen avgörs av vad produktens kärnfunktion är, inte av vilka komponenter den integrerar. Matcha kärnfunktionen mot listorna för viktiga produkter och produkten är viktig (klass I eller klass II). Matcha den mot listan för kritiska produkter och produkten är kritisk. Matchar den ingen av listorna är produkten standard. Det är hela testet.

Den praktiska skyddsregeln ligger i andra meningen i artikel 7.1. Att integrera en viktig komponent flyttar inte den integrerande produkten till klassen viktig. Att bädda in ett brandväggsbibliotek i en smart hem-hub gör inte hubben till en brandvägg. Skäl 45 säger samma sak rakt ut: brandväggar och intrångsdetekteringssystem är viktiga klass II, men andra produkter som råkar integrera dem är det inte.

Använd den här sekvensen för att klassificera produkten själv.

1. **Beskriv produktens kärnfunktion i en mening.** Klarar du inte det faller resten av analysen. Fokusera på vad produkten inte skulle fungera utan.
2. **Kontrollera listorna för viktiga produkter ovan.** En matchning i klass I eller II gör produkten viktig.
3. **Kontrollera listan för kritiska produkter ovan.** En matchning gör produkten kritisk. En väg via europeisk cybersäkerhetscertifiering gäller där systemet finns tillgängligt; annars gäller vägen för klass II.
4. **Ingen matchning på någon lista.** Produkten är standard. Modul A med självbedömning är vägen.
5. **Dokumentera resonemanget.** Ett enkelt promemoria med kärnfunktionsbeskrivningen, listkontrollen och vald väg hör hemma i den tekniska dokumentationen.

Två genomarbetade exempel.

Smart hem-hub med inbäddad lösenordshanterare. Kärnfunktion: orkestrera rutiner mellan IoT-enheter i ett hem. Lösenordshanterarkomponenten, såld separat av sin egen tillverkare, är en viktig klass I-produkt i sig själv. Hubbens kärnfunktion är hemautomation, inte hantering av inloggningsuppgifter. Hubben förblir standard.

Operativsystem efter funktionsuppsättning. En produkt marknadsförs som en smart hem-apparat, men dess huvudfunktioner är initiering av hårdvara och kringutrustning, processplanering, minneshantering och ett systemanropsgränssnitt. Det är kärnfunktionen hos ett operativsystem. Operativsystem är en viktig klass I-produkt. Produkten är viktig klass I, oavsett marknadsföringen.

Om klassificeringen hamnar på en klass som överraskar resten av teamet behöver kärnfunktionsbeskrivningen en ny granskning innan ni skickar.

När molnet är en del av din produkt

De flesta produkter med digitala element lutar sig mot något utanför själva enheten: en molnbackend, en mobil följeslagarapp, en server för luftburna uppdateringar, en autentiseringsportal, ett system för enhetshantering. CRA behandlar inte allt det som din produkt. Det behandlas som del av produkten endast när **båda** dessa två villkor är uppfyllda:

- Programvaran har **utformats och utvecklats av ditt team eller under ditt ansvar**.
- Produkten **skulle inte utföra en av sina funktioner** utan den.

Om något av villkoren brister hamnar fjärrtjänsten utanför produktens gräns för CRA. En tredjeparts-SaaS som du inte äger, även om din produkt pratar med den, är inte en del av din produkt. En webbplats som marknadsför produkten utan att stödja dess funktioner är inte heller en del av produkten.

När en fjärrkomponent ingår i tillämpningsområdet ingår den **som del av produkten**. Den tekniska dokumentationen, bedömningen av överensstämmelse, försäkran om överensstämmelse, sårbarhetshanteringen och tidsfristerna för rapportering enligt artikel 14 omfattar då molnkomponenten tillsammans med enheten.

Använd den här matrisen för att avgöra fallet snabbt.

Komponent	Ingår som del av produkten?
Mobil följeslagarapp som paras med enheten	**Ja.** Du har utformat den, och enheten kan inte konfigureras eller användas utan den.
Molnbackend som lagrar och bearbetar enhetens data	**Ja.** Du har utformat den, och kontrollpanelen eller huvudfunktionen fungerar inte utan den.
Server för luftburna uppdateringar	**Ja.** Du har utformat den, och enheten kan inte ta emot säkerhetsuppdateringar utan den.
Autentiseringsportal som styr åtkomsten till enheten	**Ja.** Du har utformat den, och användarna kan inte logga in utan den.
Marknadsföringswebbplats för produkten	**Nej.** Den stödjer ingen produktfunktion.
Tredjeparts-SaaS som produkten integrerar med (du äger den inte)	**Nej.** Inte utformad av dig. Tredjepartsleverantören har egna skyldigheter under NIS 2.
Generisk molninfrastruktur som tjänsten körs på (IaaS eller PaaS)	**Nej.** Inte utformad av dig. Infrastrukturleverantören omfattas av NIS 2.

Ett vanligt mönster: en smart hem-enhet med en mobilapp, en uppdateringsserver och en molnbackend. Alla tre är utformade av tillverkaren, och enheten kan inte utföra sina marknadsförda funktioner utan dem. Alla tre är del av produkten. CRA-skyldigheterna gäller hela paketet. Om molnbackenden sedan pratar med en analys-SaaS från tredje part är den SaaS:en inte del av produkten. Tredjepartsleverantören har egna skyldigheter under NIS 2.

CRA kräver inte säkerhetsåtgärder för tillverkarens nätverk och informationssystem som helhet. Förordningen kräver säkerhet för de fjärrtjänster som är del av produkten. Linjen går vid produktens gräns, inte vid företagets gräns.

Din leveranskedja: vem gör vad enligt CRA

CRA lägger huvudskyldigheterna på dig som tillverkare, men importörer och distributörer har också uppgifter som påverkar hur din produkt når marknaden. Tre saker är värda att känna till.

Vem	Vad de kontrollerar före leverans	Vad de gör vid en sårbarhet	När de tar över dina skyldigheter
Importör	CE-märkning, EU-försäkran om överensstämmelse, användarinstruktioner på rätt språk, dina kontaktuppgifter på eller med produkten	Informerar dig utan onödigt dröjsmål; informerar marknadskontrollmyndigheterna direkt om produkten innebär en betydande cybersäkerhetsrisk	När de placerar din produkt under eget namn eller varumärke eller gör en väsentlig ändring
Distributör	CE-märkning, att du och importören gjort er del, att de obligatoriska dokumenten följer med produkten	Informerar dig utan onödigt dröjsmål; informerar marknadskontrollmyndigheterna direkt om produkten innebär en betydande cybersäkerhetsrisk; kan sluta tillhandahålla produkten	Samma utlösare som för importörer

För en tillverkare innebär det tre praktiska saker:

- Din CE-märkning, din EU-försäkran om överensstämmelse och dina användarinstruktioner måste vara korrekta och på rätt språk i det ögonblick en distributör kontrollerar dem. Kanalpartner är skyldiga att verifiera detta och kan vägra tillhandahålla produkten om något saknas eller är fel.
- Du behöver en tydlig och lätt tillgänglig kontaktväg som importörer och distributörer kan använda för att rapportera sårbarheter in i din sårbarhetshanteringsprocess. De kommer att använda den.
- Varje partner som märker om produkten, placerar den under eget namn eller varumärke eller gör en väsentlig ändring blir tillverkare för den varianten. Den fullständiga uppsättningen skyldigheter kring teknisk dokumentation, bedömning av överensstämmelse, rapportering och stödperiod flyttar då över till dem för den versionen. Se *När någon annan blir tillverkare* i nästa avsnitt för regeln om väsentlig ändring.

Väsentlig ändring: när förnyad överensstämmelse gäller

När din produkt är på marknaden delar CRA upp efterföljande förändringar i två läger. De flesta är rutin och kräver inget extra. Vissa är väsentliga. En väsentlig ändring behandlas, för CRA:s syfte, som en ny produkt som släpps ut på marknaden. Det betyder en ny bedömning av överensstämmelse, en uppdaterad teknisk dokumentation, en ny försäkran om överensstämmelse och CE-märkning på den nya versionen.

Testet är kort, och det ligger i definitionen av väsentlig ändring. En ändring är väsentlig om något av detta är sant:

- Den **påverkar överensstämmelsen** med de väsentliga cybersäkerhetskraven.
- Den **ändrar det avsedda ändamål** för vilket produkten har bedömts.

Om inget av detta gäller är ändringen inte väsentlig. Dokumentera resonemanget ändå och behåll det. Analysen är en del av bevisspåret.

Vad som inte räknas som väsentligt

Två undantag gör det mesta av jobbet i praktiken.

Säkerhetsuppdateringar och buggrättelser som minskar cybersäkerhetsrisken utan att ändra det avsedda ändamålet är inte väsentliga. Att patcha en känd sårbarhet, justera indatavalidering för att stänga en brist eller bygga om en komponent för att åtgärda en CVE hamnar alla på den här sidan av linjen.

Renovering, underhåll och reparation är inte heller automatiskt väsentliga. De blir väsentliga endast om de ändrar det avsedda ändamålet eller påverkar överensstämmelsen med de väsentliga cybersäkerhetskraven.

Mindre arbete med användargränssnittet hamnar också på den säkra sidan. Att lägga till ett språk, byta en ikonuppsättning eller putsa en skärmlayout är inte en väsentlig ändring i sig. Att lägga till ett nytt indataelement som kräver tillräcklig indatavalidering kan vara det.

Reservdelar

CRA undantar reservdelar på ett smalt och specifikt sätt. **Identiska reservdelar**, tillverkade enligt samma specifikationer som de komponenter de ersätter, ligger helt utanför förordningens tillämpningsområde. Funktionella ersättare gör det inte.

Använd den här matrisen för att avgöra fallet snabbt.

Ersättning	Värdprodukt släppt före 11 december 2027	Värdprodukt släppt 11 december 2027 eller senare
Identisk med den ursprungliga komponenten, samma specifikationer	Reservdelen ligger utanför CRA:s tillämpningsområde. Inga skyldigheter utlöses av bytet.	Reservdelen ligger utanför CRA:s tillämpningsområde. Inga skyldigheter utlöses av bytet.
Funktionellt likvärdig, annan design eller specifikation	Ersättaren är en CRA-produkt i sig. Värdprodukten har inga CRA-skyldigheter, eftersom den föregår tillämpningsdatumet.	Ersättaren är en CRA-produkt. Bedöm om bytet in i värdprodukten är en väsentlig ändring av värdprodukten enligt tvåstegstestet ovan.

Två praktiska följder. För det första bygger undantaget på identisk specifikation. En trådlös modul ombyggd på ett annat chipset är inte en identisk reservdel, även om kunden inte märker skillnaden. För det andra: tillverkaren som levererar en funktionell ersättare bär CRA-skyldigheterna för den delen, oavsett vem som tillverkade värdprodukten.

Programvaruuppdateringar och funktionsflaggor

Programvarureleaser är den vanligaste källan till frågor om väsentlig ändring. Tvåstegstestet avgör dem ändå.

En patch som åtgärdar en sårbarhet är inte väsentlig. En funktionsflagga som slår på en kapacitet som produkten aldrig bedömts för är det. En modelluppgradering som låter produkten ta beslut om nya kategorier av indata är det också. Om en release skickar både en rättelse och en ny funktion, utvärdera funktionen.

Bundling spelar mindre roll än substans. Om en funktionsuppdatering kommer på egen hand eller i samma release som en säkerhetspatch saknar betydelse för bedömningen.

Om du arbetar med funktionsflaggor eller stegvisa utrullningar är det aktivering för slutanvändare i produktion som räknas, inte leveransen av binären som innehåller flaggan.

Beslutet i praktiken

Använd den här sekvensen vid varje ändring innan den skickas.

1. **Ändrar förändringen produktens avsedda ändamål?** Om ja: väsentlig. Gör om bedömningen av överensstämmelse för den nya versionen.
2. **Påverkar förändringen överensstämmelsen med de väsentliga cybersäkerhetskraven?** Om ja: väsentlig. Gör om bedömningen av överensstämmelse för den nya versionen.
3. **Annars:** inte väsentlig. Dokumentera analysen och fortsätt under den befintliga tekniska dokumentationen.

Om produkten ligger i klassen viktig eller kritisk och vägen krävde en bedömning av tredje part första gången, sätter en väsentlig ändring dig tillbaka på samma väg. Underrätta tredje part i förväg om varje ändring som sannolikt är väsentlig. Självbedömning är inte en bakdörr för att i efterhand omklassificera en viktig produkt.

Följder när en ändring är väsentlig

En väsentlig ändring behandlas som en ny produkt som släpps ut på marknaden. För tillverkaren innebär det:

- Uppdatera den tekniska dokumentationen för den ändrade versionen.
- Gör om bedömningen av överensstämmelse längs den väg produktklassen kräver.
- Utfärda en ny EU-försäkran om överensstämmelse för den ändrade versionen.
- Anbringa CE-märkningen igen, med den nya försäkran på fil.
- Behåll dokumentationen för den tidigare versionen under hela bevarandetiden. Den nya versionen raderar inte den.

För programvaruprodukter särskilt kan du begränsa säkerhetsuppdateringar under stödperioden till den senaste version du har släppt ut på marknaden, förutsatt att användare av tidigare versioner kan flytta till den senaste versionen utan kostnad och utan ny hårdvara.

Enheter som redan sålts under den tidigare överensstämmelsen påverkas inte. Skyldigheten knyts till den ändrade versionen som tillhandahålls, inte till identiska enheter som föregår den.

När någon annan blir tillverkare

Om du inte är ursprunglig tillverkare och du genomför en väsentlig ändring behandlar CRA dig som tillverkare för den versionen. De fullständiga skyldigheterna i artiklarna 13 och 14 fästs vid dig. Samma regel gäller om du släpper ut produkten på marknaden under eget namn eller varumärke.

Det fångar fler situationer än team brukar förvänta sig:

- En systemintegratör som skickar ett kundspecifikt firmwarebygge med nya funktioner.
- En återförsäljare som vit-etiketterar en produkt och ändrar det marknadsförda avsedda ändamålet.
- En tjänsteleverantör som paketerar en tredjepartsenhet med egen firmware.

I varje fall ärver aktören som gjort ändringen tillverkarens skyldigheter för den versionen: teknisk dokumentation, bedömning av överensstämmelse, rapportering, sårbarhetshantering och resten. Etiketten "importör" eller "distributör" slutar skydda dem i samma stund som de korsar någon av linjerna.

Vad du behöver ha på plats

Använd avsnittet som en arbetslista. Den detaljerade vägledningen krav för krav följer längre fram.

Bedömning av cybersäkerhetsrisker

Innan en produkt släpps ut på marknaden behöver du en bedömning av cybersäkerhetsrisker på fil. Det är dokumentet som med dina egna ord förklarar varför produkten är säker att skicka och att behålla på marknaden.

Bedömningen bör omfatta:

- Produktens avsedda ändamål och de användningsfall du rimligen kan förutse
- De förhållanden och den miljö produkten kommer att fungera i
- De data och funktioner som behöver skyddas
- De hot som gäller och de kontroller du förlitar dig på för att hantera dem
- Den tid produkten förväntas vara i bruk

Hur de flesta team strukturerar arbetet. Trovärdiga metoder konvergerar mot samma steg: identifiera tillgångarna (data produkten hanterar, säkerhetsmaterial som nycklar och inloggningsuppgifter, funktioner vars förlust skulle skada användare), kartlägg var varje tillgång ligger eller rör sig, modellera hoten per tillgång och miljö med konfidentialitet, integritet och tillgänglighet som dimensioner, sätt poäng på påverkan och sannolikhet, besluta vilka restrisker som ska accepteras och vilka som ska begränsas, och bedöm sedan om efter varje ny omgång kontroller (varje ny nyckel, certifikat eller autentiseringsfunktion är en ny tillgång att analysera).

Hotmodellering. Steg tre ovan är det mest tekniska momentet och har egna etablerade tekniker. STRIDE kategoriserar hot som spoofing, tampering, repudiation, information disclosure, denial of service och elevation of privilege; brett använd, passar de flesta uppkopplade produkter. LINDDUN breddar bilden för produkter som hanterar personuppgifter, med linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness och non-compliance; användbar där dataskyddsregimen överlappar CRA-skyldigheterna. PASTA går igenom en sjustegsprocess från affärsmål till acceptans av restrisk; användbar för komplexa system där attackbilden driver designen. Ingen av dem är CRA-specifik, och CRA kräver ingen av dem. Välj den som passar produktens exponeringsprofil.

Var du hittar en utarbetad metod. CRA föreskriver ingen metod. Tysklands BSI publicerar Technical Guideline TR-03183, den mest detaljerade CRA-anpassade riskbedömningsmetoden i offentlig cirkulation. ENISA publicerar bredare implementeringsvägledning för CRA.

Håll bedömningen aktuell under hela stödperioden. När hotbilden, komponenterna eller användningsfallet ändras bör bedömningen följa med.

Fastställande av stödperiod

Varje produkt behöver en definierad stödperiod, och du måste publicera dess slutdatum vid köptillfället. Stödperioden är fönstret då du hanterar sårbarheter, skickar säkerhetsuppdateringar och håller den tekniska dokumentationen aktuell.

Hur lång den måste vara

Minst fem år. Om produkten förväntas vara i bruk i mindre än fem år ska stödperioden motsvara den förväntade användningstiden. Förväntas den vara i bruk längre ska stödperioden återspegla den längre användningen; produkter som routrar, operativsystem och industriella styrenheter motiverar ofta mer än fem år.

Faktorer att väga in

När du fastställer perioden ska du på ett proportionerligt sätt beakta:

- Användarnas rimliga förväntningar på produkten
- Produktens art, inbegripet dess avsedda ändamål
- All EU-lagstiftning som redan sätter en livslängd för produkten i denna kategori
- Stödperioder för jämförbara produkter på marknaden
- Tillgången till den driftsmiljö produkten är beroende av
- Stödperioderna för integrerade komponenter som tillhandahåller kärnfunktioner
- Eventuell vägledning från ADCO eller kommissionen för produktkategorin

Resonemanget bakom den valda perioden ska finnas i den tekniska dokumentationen. Marknadskontrollmyndigheter kan begära att få se det.

Vad du måste publicera

Ange slutdatumet för stödperioden vid köptillfället, med minst månad och år, på en lättillgänglig plats. Där produkten har ett användargränssnitt ska den visa ett meddelande när den når slutet av sin stödperiod.

Behållande av uppdateringar

Varje säkerhetsuppdatering som gjorts tillgänglig för användare under stödperioden ska förbli tillgänglig i minst tio år efter att den utfärdats, eller under resten av stödperioden, beroende på vilken period som är längst.

Tillbörlig aktsamhet vid komponenter

En produkt består av komponenter. Vissa har du skrivit, vissa har du köpt, vissa har du hämtat från ett öppet källkodsförråd. CRA behandlar produkten som en helhet vid bedömning av överensstämmelse, så komponenterna räknas också. Om en sårbarhet sitter i en komponent sitter den i din produkt. Om en komponent inte får säkerhetsuppdateringar får din produkt inte heller dem.

Tillverkare ska visa tillbörlig aktsamhet vid tredjepartskomponenter, inbegripet fria och öppna källkodskomponenter. Komponenterna får inte kompromettera produktens cybersäkerhet.

Hur mycket aktsamhet som räcker beror på den cybersäkerhetsrisk komponenten bär. Ett bibliotek som hanterar autentisering är inte detsamma som ett bibliotek för teckenrendering. Använd en eller flera av dessa kontroller, proportionellt mot risken:

1. **Kontrollera CE-märkning på komponenten.** Om komponenten själv är en CRA-produkt och leverantören har visat överensstämmelse finns CE-märkningen på komponenten. Det visar leverantörens eget CRA-arbete.
2. **Kontrollera historiken för säkerhetsuppdateringar.** En komponent som regelbundet skickar säkerhetsuppdateringar är en bättre risk än en som varit tyst i åratal. Leta efter ett releasetempo och en aktuell historik av säkerhetsråd.
3. **Kontrollera komponenten mot sårbarhetsdatabaser.** Den europeiska sårbarhetsdatabasen och publika CVE-databaser berättar vad som är känt om komponenten. En känd CVE utan patch är en varningssignal.
4. **Kör kompletterande säkerhetstester.** Där ovanstående inte räcker, testa komponenten i din integrationskontext: statisk analys, dynamisk analys, fuzzing eller en fokuserad säkerhetsgranskning.

För komponenter som integrerats innan deras egen leverantör fullt ut omfattas av CRA (så att ingen CE-märkning ännu finns) använd de tre andra kontrollerna i stället. Skyldigheten att visa tillbörlig aktsamhet pausar inte bara för att leveranskedjan håller på att komma ifatt.

Bevis att hålla på fil

Den tekniska dokumentationen ska visa din tillbörliga aktsamhet, inte bara påstå den. Behåll:

- En förteckning över tredjepartskomponenter i produkten, spårbar till versioner, inbegripet öppen källkod. SBOM är den naturliga platsen.
- Leverantörernas säkerhetsdokumentation du granskat: säkerhetspolicyer, program för sårbarhetsoffentliggörande, åtaganden om stödperiod.
- Integrationsrapporter som visar att komponenten beter sig säkert i din produkt.
- Säkerhetsklausuler i kontrakt eller SLA med kommersiella leverantörer: tidsfrister för sårbarhetsmeddelanden, åtaganden om stödperiod, eskaleringsregler.
- En förteckning över de mildrande åtgärder du lagt till på produktnivå där den tillbörliga aktsamheten visat på begränsningar hos komponenten: sandboxning, begränsade behörigheter, indatavalidering, nätverkssegmentering.

När du hittar en sårbarhet i en komponent

Om din tillbörliga aktsamhet eller övervakning efter marknadslansering identifierar en sårbarhet i en komponent måste du göra två saker. Först, informera personen eller den enhet som underhåller komponenten. Om komponenten är öppen källkod är det uppströmsprojektet. För det andra, hantera och åtgärda sårbarheten i din produkt inom samma tidsramar som för andra sårbarheter du upptäcker. Om du har tagit fram en rättelse, dela koden eller dokumentationen med underhållaren, i ett maskinläsbart format där det är tillämpligt.

CRA låter dig inte vänta på att komponentunderhållaren agerar innan du skyddar dina egna användare. Tidslinjen för din produkts sårbarhetshantering löper oberoende av uppströms.

De 13 produktsäkerhetskraven

Varje produkt med digitala element ska uppfylla tretton grundläggande säkerhetskrav när den släpps ut på marknaden, och fortsätta uppfylla dem under hela stödperioden. De utgör golvet för vad cybersäkerhet innebär i produkttermer enligt CRA.

De tretton kraven är:

- Inga kända sårbarheter som kan utnyttjas vid tidpunkten för utsläppande på marknaden
- Säker standardkonfiguration ur lådan
- Säkerhetsuppdateringar, inbegripet automatiska uppdateringar med undantagsmekanism
- Skydd mot obehörig åtkomst
- Konfidentialitet för lagrade, överförda och behandlade uppgifter
- Riktighet hos data, firmware och konfiguration
- Uppgiftsminimering
- Tillgång och resiliens, även mot överbelastningsattacker
- Ingen negativ påverkan på andra anslutna enheter eller nätverk
- Begränsad attackyta, inbegripet externa gränssnitt
- Minskad incidentpåverkan genom begränsning av utnyttjande
- Loggning av säkerhetsrelevant aktivitet, med möjlighet för användaren att välja bort den
- Säker och permanent borttagning av data samt portabilitet

Varje krav packas upp i detalj senare i guiden, med vad det innebär i praktiken och de bevis du bör ha på fil.

De 8 kraven på sårbarhetshantering

Tillverkare behöver också processer för sårbarhetshantering som löper under hela produktens stödperiod:

1. Identifiera och dokumentera sårbarheter (inkluderar programvaruförteckning, SBOM)
2. Riskhantering och snabba säkerhetsuppdateringar
3. Regelbundna säkerhetstester
4. Information om säkerhetsuppdateringar och offentlig redovisning av sårbarheter
5. Policy för samordnad delgivning av sårbarheter (CVD)
6. Kontaktpunkt för informationsutbyte och rapportering av sårbarheter
7. Säkra mekanismer för distribution av uppdateringar
8. Kostnadsfria säkerhetsuppdateringar med rådgivande meddelanden

Tidsfrister för rapportering enligt artikel 14

Dessa skyldigheter gäller från **11 september 2026**. De gäller tillverkare av produkter med digitala element inom tillämpningsområdet, även produkter som släppts ut på marknaden före **11 december 2027**. Mikroföretag och små företag är inte generellt undantagna från rapportering. Böteslättnaden för små företag är snäv: den gäller bara den första **24-timmarsfristen för tidig varning**.

CRA skiljer mellan tre nivåer av sårbarhetsstatus:

- **Sårbarhet:** en svaghet som kan utnyttjas

- **Sårbarhet som kan utnyttjas:** en svaghet som kan användas under verkliga förhållanden
- **Aktivt utnyttjad sårbarhet:** en sårbarhet där användning i en attack har bekräftats

När klockan börjar gå

Du står inte på klockan i det ögonblick en signal kommer in. Klockan börjar gå när du har gjort en första bedömning och har en rimlig grad av säkerhet att en sårbarhet i din produkt aktivt utnyttjas, eller att en allvarlig incident har komprometterat din produkts säkerhet. Tyngdpunkten ligger på en snabb första bedömning, inte på att vänta in att hela utredningen är klar. Om en kund, forskare, myndighet eller annan tredje part väcker frågan om en möjlig brist hos dig, bedöm den utan dröjsmål och starta klockan så snart den bedömningen ger dig den rimliga säkerheten.

När du upptäcker en **aktivt utnyttjad sårbarhet** gäller följande rapporteringstidslinje:

Tidsfrist	Vad krävs	Var rapporterar du
Inom 24 timmar	Tidig varning om aktivt utnyttjande	ENISA via nationell CSIRT
Inom 72 timmar	Sårbarhetsrapport: berörd produkt, allmän karaktär på utnyttjandet och sårbarheten, begränsningsåtgärder, korrigerande åtgärder som användarna kan vidta och känslighetsmärkning där det är relevant	ENISA via nationell CSIRT
Senast 14 dagar efter att en korrigerande eller begränsande åtgärd finns tillgänglig	Slutrapport: beskrivning av sårbarheten, allvarlighetsgrad, påverkan, tillgänglig information om illvilliga aktörer och detaljer om säkerhetsuppdateringen eller annan korrigerande åtgärd	ENISA via nationell CSIRT

När du upptäcker en **allvarlig incident** som påverkar produktens säkerhet gäller följande rapporteringstidslinje:

Tidsfrist	Vad krävs	Var rapporterar du
Inom 24 timmar	Tidig varning, inklusive om incidenten misstänks bero på olagliga eller illvilliga handlingar	ENISA via nationell CSIRT
Inom 72 timmar	Incidentrapport: incidentens karaktär, inledande bedömning, begränsningsåtgärder, korrigerande åtgärder som användarna kan vidta och känslighetsmärkning där det är relevant	ENISA via nationell CSIRT
Inom en månad efter 72-timmarsrapporten	Slutrapport: detaljerad incidentbeskrivning, allvarlighetsgrad, påverkan, sannolikt hot eller grundorsak och genomförda eller pågående begränsningsåtgärder	ENISA via nationell CSIRT

Anmälningarna uppdateras allt eftersom du får veta mer

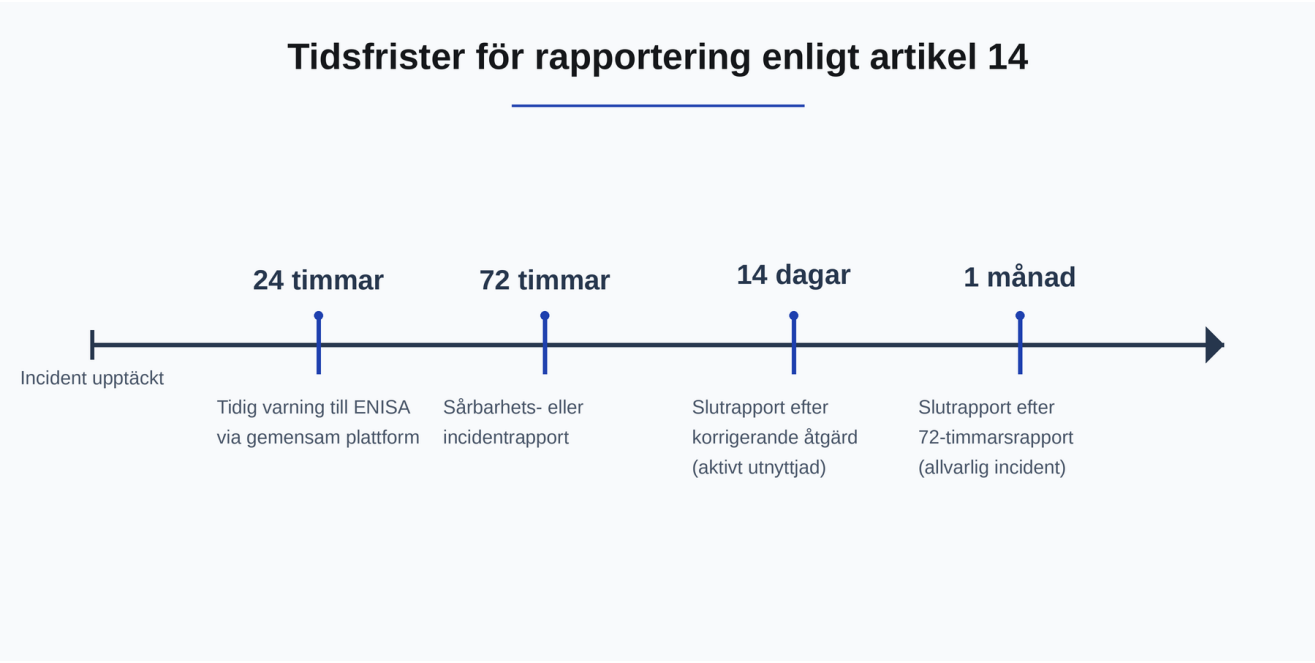
Inlämningarna vid 24 timmar, 72 timmar och 14 dagar (eller en månad) är steg i samma anmälan, inte separata inlämningar. Varje steg lägger till den information som inte var tillgänglig vid det föregående. Den CSIRT som utsetts till koordinator kan också begära en mellanliggande uppdatering när som helst. Du behöver inte upprepa information du redan lämnat.

Rapporter lämnas in via **CRA:s gemensamma rapporteringsplattform**, som dirigeras genom den nationella CSIRT:en i tillverkarens huvudsakliga medlemsstat, med samtidig åtkomst för ENISA.

Att informera dina användare

Efter att du blivit medveten ska du informera berörda användare om sårbarheten eller incidenten, och där det är lämpligt alla användare, om de åtgärder för att begränsa risk och korrigera situationen som de kan vidta. Det är inte detsamma som ett offentligt avslöjande. Skyldigheten är att få informationen till de användare som behöver den för att skydda sig, i proportion till risken. För produkter som används i känsliga eller väsentliga miljöer, begränsa detaljerad teknisk information till berörda kunder så länge sårbarheten är obegränsad; för tidiga offentliga detaljer kan göra utnyttjande enklare.

När sårbarheten är åtgärdad eller begränsad kan bredare offentliggörande bli lämpligt för att hjälpa användare verifiera att deras produkter inte längre är drabbade och för att höja allmän medvetenhet. Håll detaljgraden och tidpunkten i proportion till restrisken. Om du inte informerar användarna i tid kan CSIRT:en själv träda in och tillhandahålla informationen där den bedömer det proportionerligt och nödvändigt.



Aktivt utnyttjad sårbarhet

24 timmar	tidig varning
72 timmar	sårbarhetsrapport
14 dagar efter korrigerande åtgärd	slutrapport

Allvarlig incident

24 timmar	tidig varning
72 timmar	incidentrapport
en månad efter 72-timmarsrapporten	slutrapport

Korrigerande åtgärder när en produkt inte överensstämmer

Om du vet, eller har skäl att tro, att en produkt du släppt ut på marknaden, eller en av dina processer, inte överensstämmer med CRA:s väsentliga cybersäkerhetskrav, måste du agera omedelbart. Skyldigheten löper från utsläppandet på marknaden och under hela stödperioden.

De tre alternativen

1. **Bringa i överensstämmelse.** Åtgärda produkten eller processen. För programvaruprodukter är det vanligen en säkerhetsuppdatering eller en processändring. Tillämpa rättelsen på de versioner som stöds.
2. **Dra tillbaka.** Sluta tillhandahålla produkten på marknaden. Plocka den från din leveranskedja och från alla återförsäljare, integratörer och resellers som har lager.
3. **Återkalla.** Hämta tillbaka produkten från användare som redan har den. Använd det här när cybersäkerhetsrisken för användarna är betydande och en rättelse eller tillbakadragande inte räcker.

Valet är proportionerligt mot risken, inte en fast sekvens. En patchbar sårbarhet med en fungerande rättelse betyder vanligen *bringa i överensstämmelse*. En produkt som inte säkert kan åtgärdas i fält betyder vanligen *dra tillbaka* och, där den är i aktiv användning med betydande risk, *återkalla*.

Vad du också måste göra

- **Anmäl enligt artikel 14-kedjan** när bristen på överensstämmelse är en aktivt utnyttjad sårbarhet eller en allvarlig incident. Rapporteringstidslinjen finns ovan.
- **Informera användarna** om bristen och om de korrigerande åtgärder de själva kan vidta. Se *Att informera dina användare* ovan för proportionalitetsreglerna.
- **Samarbeta** med varje motiverad begäran från en marknadskontrollmyndighet, inbegripet att tillhandahålla den tekniska dokumentationen på ett språk de kan läsa.
- **Bevara bevis.** Behåll de underlag som visar vad du hittade, när du hittade det, vad du gjorde åt det och hur du kommunicerade med användare och myndigheter. Den tekniska dokumentationen och EU-försäkran om överensstämmelse ska förbli tillgängliga i minst tio år efter utsläppandet på marknaden, eller under hela stödperioden, beroende på vilken period som är längst.

Krav på produktdokumentation

Dokumentationen ska bevaras i **minst tio år** efter att produkten släppts ut på marknaden, eller under **hela stödperioden**, beroende på vilken period som är längst. På sammanfattande nivå behöver den tekniska dokumentationen åtta bevisfamiljer:

1. Allmän produktbeskrivning
2. Detaljer om design, utveckling och produktion (inbegripet SBOM)
3. Bedömning av cybersäkerhetsrisker
4. Fastställande av stödperiod
5. Tillämpade harmoniserade standarder och specifikationer
6. Testrapporter
7. EU-försäkran om överensstämmelse
8. Fullständig SBOM (på begäran från marknadskontrollmyndigheter)

Checklista för bedömningsvägen

Använd klassificeringstabellen ovan för att identifiera vägen. Spara sedan beslutet om väg i den tekniska dokumentationen tillsammans med de standarder, specifikationer, certifieringssystem eller bevis från anmält organ som motiverar beslutet.

Ett genomarbetat exempel. Samma nivåstruktur gäller för varje produkt med digitala element, inte bara säkerhetskameror.

Produktens cybersäkerhetskrav

a. Inga kända sårbarheter som kan utnyttjas vid utsläppande på marknaden

Skicka inte produkten med offentligt kända sårbarheter som kan utnyttjas och som förblir obehandlade. En känd sårbarhet kan komma från en publik databas, ett leverantörsmeddelande, en kundrapport eller din egen interna spårning.

För att uppfylla kravet:

- Kontrollera sårbarhetsdatabaser (inbegripet Common Vulnerabilities and Exposures, CVE) före varje release
- Använd statisk och dynamisk applikationssäkerhetstestning (SAST/DAST) i byggpipelinen
- Genomför beroendeskanning för alla tredjeparts- och öppna källkodskomponenter
- Dokumentera ditt beslut om riskacceptans eller mildring för varje identifierat fynd

b. Säker standardkonfiguration

Produkten ska vara säker att använda i sitt standardläge. Avaktivera onödiga tjänster, undvik svaga standardinloggningsuppgifter och håll varje osäkert idriftsättningsläge kort och kontrollerat. Skyldigheten kring standardkonfiguration kan varieras för skräddarsydda produkter som levereras till företagsanvändare genom skriftligt avtal, men en väg tillbaka till det ursprungliga säkra läget måste förbli tillgänglig.

För att uppfylla kravet:

- Avaktivera fjärråtkomstportar och felsökningsgränssnitt i standardbyggen
- Genomdriv starka standardmekanismer för autentisering
- Begränsa administrativa funktioner till behöriga användare
- Inför en säker fabriksåterställning som återställer alla inställningar och firmware till ett känt säkert läge och tar bort användardata

c. Säkerhetsuppdateringar, inklusive automatiska uppdateringar med undantagsmekanism

Produkten behöver en patchmekanism som kan hantera säkerhetsproblem efter driftsättning. Där automatiska uppdateringar är lämpliga, aktivera dem som standard och ge användarna ett tydligt sätt att skjuta upp eller välja bort.

För att uppfylla kravet:

- Inför kryptografisk signering och integritetsverifiering av uppdateringspaket
- Tillhandahåll skydd mot nedgradering och loggning av uppdateringshändelser
- Bygg meddelandesystem som varnar användarna om kommande uppdateringar
- Låt användarna skjuta upp eller avaktivera automatiska uppdateringar via ett tydligt konfigurationsgränssnitt

d. Skydd mot obehörig åtkomst

Åtkomstkontroller ska skydda både lokala och fjärrgränssnitt. Målet är att stoppa obehöriga användare från att nå funktioner, data, konfiguration eller hanteringsytor.

För att uppfylla kravet:

- Genomdriv policyer för lösenordskomplexitet och starka standardinloggningsuppgifter
- Inför flerfaktorsautentisering (MFA) där det är lämpligt
- Tillämpa rollbaserad åtkomstkontroll (RBAC) och hantering av sessionsutgång
- Logga misslyckade åtkomstförsök, använd anomalidetektering för att flagga obehörig aktivitet och lyft fram dessa händelser för granskning och rapportering

e. Konfidentialitet för lagrade, överförda och behandlade uppgifter

Känsliga uppgifter behöver skydd i vila, under överföring och under behandling.

För att uppfylla kravet:

- Använd standardiserade krypteringsalgoritmer (till exempel AES-256 för data i vila, TLS för data under överföring)
- Tillämpa säker nyckelhantering
- Separera konfidentiella data från icke-kritiska systemkomponenter
- Underhåll granskningsloggar för alla händelser av dataåtkomst

f. Riktighet hos data, firmware och konfiguration

Kravet omfattar systemet självt (firmware, programvara, konfigurationsfiler) och de data det hanterar (mätvärden, styrkommandon, användarindata).

För att uppfylla kravet:

- Inför säker uppstart och signerad firmware för att säkerställa att endast betrodd kod körs
- Använd körtidsverifiering för att upptäcka och rapportera manipulationsförsök
- Tillämpa kryptografisk hashning och digitala signaturer för att skydda dataintegriteten
- Bygg infrastruktur som kan generera, distribuera och verifiera kryptografiska nycklar över system- eller organisationsgränser

g. Uppgiftsminimering

Samla in och behandla bara de data som behövs för produktens avsedda ändamål. Det gäller personuppgifter och tekniska data.

För att uppfylla kravet:

- Genomför integritetspåverkansbedömningar eller övningar i dataskydd i designen för att identifiera onödiga dataflöden
- Ta bort eller gör valfri all oanvänd telemetri, diagnostik eller bakgrundsinsamling av data
- Inför konfigurerbara inställningar för datainsamling så att utökad insamling kan slås på eller av utifrån sammanhanget

h. Tillgång och resiliens, även mot överbelastningsattacker

Under incidenter eller attacker ska viktiga produktfunktioner förbli tillgängliga eller fallera på ett kontrollerat sätt.

För att uppfylla kravet:

- Inför circuit breakers, logik för omförsök, fallbackmekanismer och watchdog-timers
- Tillämpa resursgränser för att förhindra resursuttömning
- Använd hastighetsbegränsning och indatavalidering för att skydda mot överbelastningsscenarier
- Tillämpa nätverksfiltrering för att blockera överbelastningsförsök

i. Ingen negativ påverkan på andra anslutna enheter eller nätverk

Produkten ska inte störa andra system i samma miljö. Den ska bete sig förutsägbart och undvika överdriven användning av delade resurser.

För att uppfylla kravet:

- Inför trafikformning och begränsa användning av broadcast eller multicast
- Säkerställ följsamhet med specifikationer för kommunikationsprotokoll
- Använd självövervakning för att upptäcka och förhindra störande beteenden som nätverksöversvämning eller resursuttömning

j. Begränsad attackyta, inklusive externa gränssnitt

Minimera ingångspunkter och exponerad funktionalitet. Det omfattar fysiska portar, trådlösa gränssnitt, API:er, felsökningstjänster och onödiga programvarukomponenter.

För att uppfylla kravet:

- Avaktivera oanvända tjänster, portar och gränssnitt i produktionsbyggen
- Härda systemstandardvärden och begränsa användarbehörigheter
- Modularisera programvaruarkitekturen för att isolera komponenter från varandra
- Tillämpa principer för säker mjukvarudesign och genomför hotmodellering för att identifiera och ta bort onödig exponering

k. Minskad incidentpåverkan genom begränsning av utnyttjande

Räkna med att vissa attacker lyckas. Produktdesignen ska begränsa hur långt skada kan spridas.

För att uppfylla kravet:

- Separera systemkomponenter och kör dem i isolerade miljöer med sandboxning eller containerisering
- Genomdriv separation av behörigheter så att kritiska funktioner körs med minsta nödvändiga rättigheter
- Designa så att en kompromettering av en komponent inte kan ge en angripare kontroll över hela systemet

l. Loggning av säkerhetsrelevant aktivitet med möjlighet att välja bort

Registrera säkerhetsrelevant aktivitet, som åtkomstförsök och dataändringar, så att den kan övervakas och granskas. Användarna behöver en möjlighet att välja bort där CRA kräver det.

För att uppfylla kravet:

- Inför strukturerad loggning (till exempel JSON-loggar med tidsstämplar)
- Tillhandahåll lokal logglagring med loggrotation och alternativ för fjärrloggström
- Övervaka händelser som inloggningsförsök, konfigurationsändringar och programuppdateringar efter avvikelser
- Tillhandahåll en tydlig användarvänd mekanism för att avaktivera loggning där det är tillåtet

m. Säker och permanent borttagning av data samt portabilitet

Användarna behöver ett praktiskt sätt att ta bort data och inställningar permanent. Där data kan överföras till en annan produkt eller ett annat system ska överföringen vara säker.

För att uppfylla kravet:

- Inför en säker raderingsfunktion som skriver över lagringsområden eller raderar nycklar kryptografiskt
- Använd autentiserade och krypterade kanaler för dataportabilitetsöverföringar för att förhindra exponering under överföring

Krav på sårbarhetshantering

1. Identifiera och dokumentera sårbarheter

Du behöver veta vilka programvarukomponenter som finns i produkten och vilka kända sårbarheter som påverkar dem. En programvaruförteckning (SBOM) ger dig den maskinläsbara inventeringen.

För att uppfylla kravet:

- Integrera SBOM-generering direkt i CI/CD-pipelinen så att varje bygge producerar en aktuell komponentinventering
- Använd etablerade format som CycloneDX, SPDX eller SWID för interoperabilitet
- Kör automatiserad sårbarhetsskanning mot CVE-listor och databaser som CISA KEV och ENISA EUVD
- Underhåll SBOM som del av den tekniska dokumentationen under hela stödperioden och tillhandahåll den till marknadskontrollmyndigheter på begäran

2. Riskhantering och snabba säkerhetsuppdateringar

När sårbarheter hittas, åtgärda dem snabbt och leverera säkerhetsuppdateringar. Där det går, separera säkerhetspatchar från funktionsuppdateringar så att kritiska rättelser kan installeras snabbt.

För att uppfylla kravet:

- Designa uppdateringsmekanismen så att säkerhetsrättelser kan rullas ut utan att kräva en fullständig systemuppdatering
- Strukturera programvara och firmware så att kritiska komponenter kan patchas oberoende
- Leverera uppdateringar via säkra kanaler med integritetskontroller
- Underhåll register över uppdateringsaktivitet för att stödja spårbarhet och visa överensstämmelse

3. Regelbundna säkerhetstester

Säkerhetstestning är inte en engångsövning. Testa produkter genom hela livscykeln när hot, beroenden och produktbeteende förändras. Låt riskbedömningen styra typen och frekvensen av testning.

För att uppfylla kravet:

- Genomför penetrationstester för att simulera verkliga attacker
- Tillämpa statisk och dynamisk kodanalys för att identifiera säkerhetssvagheter
- Använd fuzz-testning för att avslöja brister i indatahantering
- Schemalägg och dokumentera formellt säkerhetskodgranskningar och arkitekturgranskningar, särskilt efter större design- eller funktionsändringar

4. Mottagning av sårbarheter, CVD-policy och rådgivande meddelanden

Täcker mottagning, samordnat offentliggörande och rådgivande skyldigheter (punkterna 4, 5 och 6 i sammanfattningen ovan) som i praktiken löper som ett arbetsflöde.

CRA pekar ut tre separata krav för hur du kommunicerar kring sårbarheter: ett sätt för människor att rapportera problem, en policy för samordnat offentliggörande och ett rådgivande meddelande när du skickar en rättelse. Så här ser varje skyldighet ut.

Mottagning

Ge rapportörer en tydlig och lätt tillgänglig väg in. Publicera en synlig kontaktmetod för sårbarhetsrapportering (dedikerad e-post eller webbformulär). Stödja säker kommunikation, till exempel genom att publicera en PGP-nyckel. Skyldigheten omfattar rapporter om din egen produkt och om de tredjepartskomponenter den innehåller.

Triage

Bekräfta varje rapport, logga den i ett spårningssystem, tilldela för granskning och lös inom definierade tidsramar. Skicka bekräftelse och statusuppdateringar tillbaka till rapportören. Där problemet sitter i en tredjepartskomponent, dirigera den vidare till uppströmsunderhållaren parallellt med din egen åtgärd.

Policy för samordnat offentliggörande av sårbarheter

Publicera en CVD-policy som sätter förväntningar för rapportörer och partner: kontaktmetod, förväntade svarstider, vad du åtar dig, vad du ber av dem. Samordna offentliggörandet för att skydda användarna samtidigt som rapportörens bidrag erkänns.

Rådgivande meddelanden vid rättelse

När en rättelse är tillgänglig, publicera ett rådgivande meddelande för den åtgärdade frågan. Inkludera CVE-identifieraren, de berörda produktversionerna, en standardiserad allvarlighetsgrad (till exempel CVSS) och tydlig, tillgänglig information om vad användarna ska göra. Skriv på ett språk som är tillgängligt för både tekniska administratörer och icke-tekniska användare.

Fördröjt offentligt offentliggörande

Du får skjuta upp offentligt offentliggörande endast där du har en vederbörligen motiverad anledning att cybersäkerhetsriskerna med ett omedelbart offentliggörande väger tyngre än fördelarna, och endast tills användarna haft möjlighet att tillämpa rättelsen. Dokumentera resonemanget.

5. Säkra mekanismer för distribution av uppdateringar

Uppdateringsmekanismen behöver vara pålitlig och motståndskraftig mot manipulation. Där automatiska uppdateringar är tekniskt möjliga minskar de tiden användare är exponerade.

För att uppfylla kravet:

- Skicka uppdateringar via säkra kanaler och verifiera dem genom digitala signaturer
- Tillämpa uppdateringar på ett sätt som förhindrar ofullständiga eller korrumperade installationer
- Använd differentiella eller modulära uppdateringar för att minska störning och leverera rättelser till system snabbare
- Underhåll uppdateringsloggar så att användare eller administratörer kan verifiera uppdateringsstatus

6. Kostnadsfria säkerhetsuppdateringar med rådgivande meddelanden

Leverera säkerhetsuppdateringar snabbt och utan extra kostnad, utom där ett separat avtal finns för skräddarsydda produkter till företag. Varje uppdatering behöver ett tydligt rådgivande meddelande som berättar för användarna vad som ändrats och vad de ska göra.

För att uppfylla kravet:

- Underhåll ett distributionssystem som kan informera användarna direkt eller tillämpa uppdateringar automatiskt, beroende på produktkontext
- Skriv rådgivande meddelanden på ett språk som både tekniska och icke-tekniska användare förstår
- Inkludera information om allvarlighetsgrad i rådgivande meddelanden där det är relevant
- Berätta för användarna vilken åtgärd de ska vidta, som att tillämpa uppdateringen, ändra en konfiguration eller hålla utkik efter tecken på kompromettering
- Sprid säkerhetsuppdateringar utan dröjsmål så snart de är tillgängliga, så att användarna inte lämnas exponerade medan rättelsen redan finns
- Publicera rådgivande meddelanden via en kanal som tillverkaren kontrollerar och länka till dem från produktens supportsida

Skyldigheterna att leverera kostnadsfritt och utan dröjsmål löper under hela den deklarerade stödperioden. Undantaget för skräddarsydda produkter ändrar bara den kommersiella grunden; rådgivande meddelanden gäller ändå.

Vad den tekniska dokumentationen ska innehålla

Teknisk dokumentation

Den tekniska dokumentationen är det centrala beviset på överensstämmelse med CRA. Den ska täcka de design-, tekniska och procedurmässiga åtgärder som använts för att uppfylla de väsentliga cybersäkerhetskraven. Den ska finnas **före utsläppandet på marknaden** och hållas aktuell under hela **stödperioden**.

Tekniska bevis i engineeringflödet

Steg 1	**Avgränsa och klassificera**	Produktens syfte, avsedd användning, beslut om utsläppande på marknaden, produktklass, standardväg.
Steg 2	**Arkitektur och risk**	Arkitektur, dataanslutningar, användningsvillkor, riskbedömning, riskreducering.
Steg 3	**Komponenter och SBOM**	Maskinläsbar SBOM, tredjepartskomponenter, leverantörsunderlag, sårbarhetsspårning.
Steg 4	**Bygg, testa, uppdatera**	Säkra standardvärden, härdning, testrapporter, säker uppdateringsmekanism, rådgivande meddelanden.
Steg 5	**Release och stöd**	Användarinstruktioner, EU-försäkran, CE-bevis, motivering av stödperiod, uppdateringsregister.

Den tekniska dokumentationen har åtta obligatoriska komponenter. Tillsammans förklarar de **vad produkten är**, **hur den byggts och testats**, **vilka risker som övervägts**, **vilka standarder som tillämpats** och **hur den kommer att stödjas** när den är på marknaden. Du behöver inte kopiera de juridiska rubrikerna, men varje ämne måste täckas.

Nr.	Komponent	Vad den måste innehålla
1	Allmän produktbeskrivning	Avsett ändamål och funktioner, relevanta programvaruversioner, foton eller illustrationer (för hårdvara), användarinformation och instruktioner
2	Detaljer om design, utveckling och produktion	Arkitekturbeskrivning (komponenter och interaktioner), programvaruförteckning (SBOM), processer för sårbarhetshantering (CVD-policy, kontaktpunkt, säkra uppdateringsmekanismer), produktions- och övervakningsprocesser inbegripet validering
3	Bedömning av cybersäkerhetsrisker	Dokumenterad analys av produktens risker, förklaring av hur varje väsentligt cybersäkerhetskrav tillämpas på produkten, mildring av identifierade risker
4	Fastställande av stödperiod	Dokumentation av de faktorer som använts för att sätta stödperioden, som användarförväntningar, jämförbara produkter och rättslig vägledning
5	Tillämpade harmoniserade standarder och specifikationer	Lista över harmoniserade standarder, gemensamma specifikationer eller EU-certifieringssystem som tillämpats; indikation om de tillämpats helt eller delvis; alternativa lösningar där standarder inte tillämpats
6	Testrapporter	Bevis för överensstämmelse för både produkten och processerna för sårbarhetshantering
7	EU-försäkran om överensstämmelse	Kopia av försäkran som kopplar den tekniska dokumentationen till skyldigheter kring CE-märkning
8	Fullständig SBOM (på begäran)	Marknadskontrollmyndigheter kan begära in den fullständiga SBOM:en för att verifiera överensstämmelse

En enda konsoliderad teknisk dokumentation kan täcka CRA och annan tillämplig EU-lagstiftning (till exempel direktivet om radioutrustning eller ESPR), förutsatt att alla tillämpliga skyldigheter ingår.

EU-försäkran om överensstämmelse

EU-försäkran om överensstämmelse är tillverkarens formella förklaring att produkten uppfyller de tillämpliga CRA-cybersäkerhetskraven. Varje försäkran ska innehålla:

- Produktnamn, typ och unika identifierare
- Tillverkarens namn och adress (eller tillverkarens representant)
- Förklaring om ensamt ansvar från leverantören
- Produktbeskrivning som säkerställer spårbarhet (valfritt med bild)
- Uttrycklig förklaring om överensstämmelse med relevant unionsrätt
- Hänvisningar till harmoniserade standarder, specifikationer eller certifieringar som använts
- Uppgifter om eventuellt inblandat anmält organ (namn, nummer, förfarande, certifikatnummer)
- Signaturblock: ort, datum, namn, funktion och underskrift av den som signerar

När den signerats är försäkran rättsligt bindande och bekräftar tillverkarens fulla ansvar för överensstämmelse med cybersäkerhetskraven.

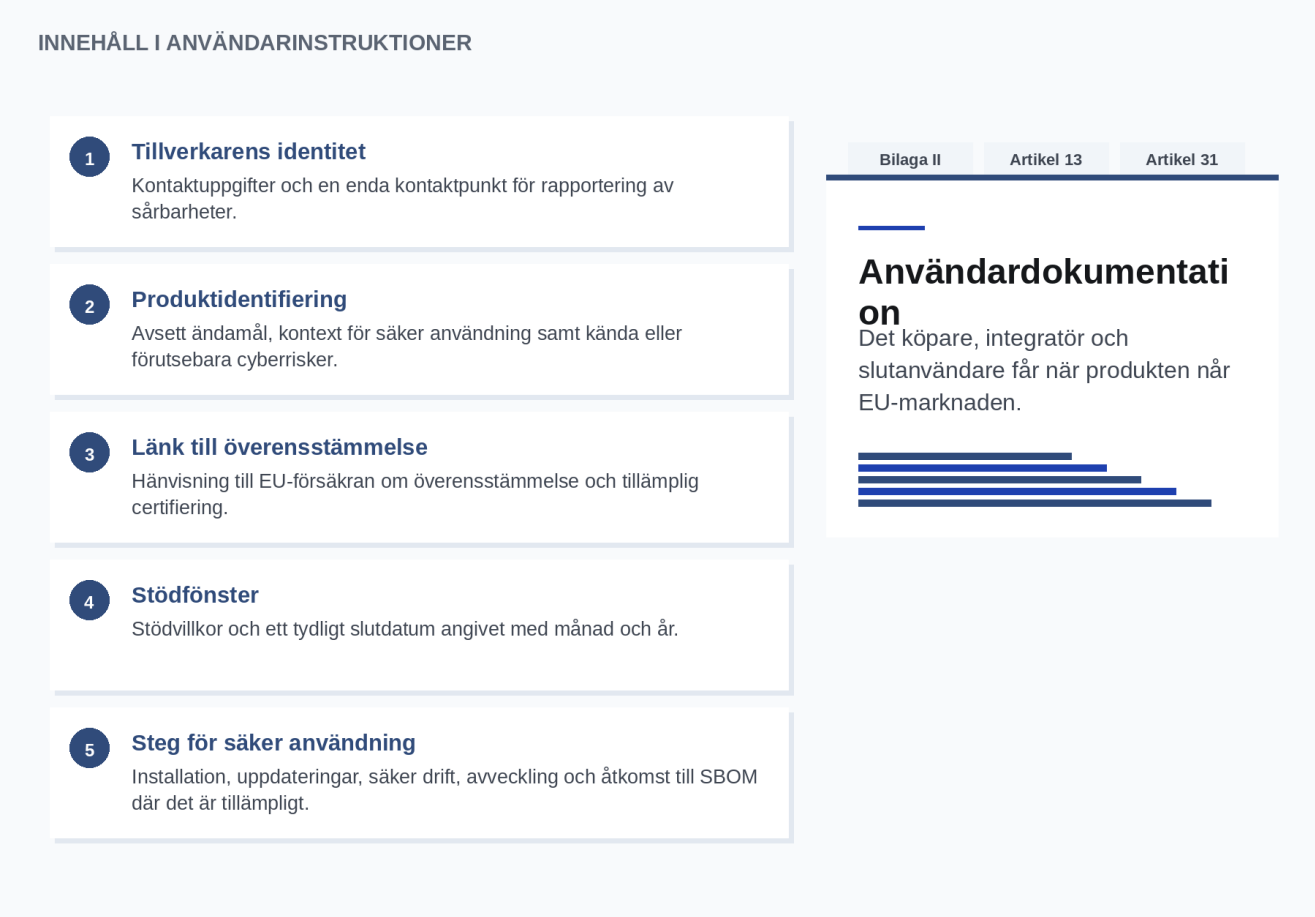
En förenklad försäkran är tillåten för användning på förpackningar eller i manualer, i formen: "Härmed försäkrar [tillverkare] att produkten [typ/beteckning] uppfyller Förordning (EU) 2024/2847. Den fullständiga texten till EU-försäkran om överensstämmelse finns på: [webbadress]." Den förenklade formen bevarar transparensen samtidigt som pappersarbetet minskar, och är särskilt användbar för små tillverkare eller portföljer med flera produkter.

Användarinformation och instruktioner

Användarinformation och instruktioner är ett villkor för att lagligt få släppa ut produkten på marknaden. Tillverkare ska hålla instruktionerna tillgängliga i **minst tio år** eller under hela **stödperioden**. Importörer och distributörer ska kontrollera att instruktionerna finns, är aktuella och tillhandahålls på rätt EU-språk innan de släpper ut eller levererar produkten.

Användarinstruktionerna ska innehålla:

- Tillverkarens identitet och kontaktuppgifter
- En enda kontaktpunkt för rapportering av sårbarheter
- Produktidentifiering, avsett ändamål och kontext för säker användning
- Kända eller förutsebara cyberrisker
- Länk till EU-försäkran om överensstämmelse
- Stödvillkor och ett tydligt slutdatum för stödet
- Steg-för-steg-säkerhetsinstruktioner för installation, uppdateringar, säker användning, avveckling och (om tillämpligt) integration och åtkomst till SBOM



Välj rätt väg för bedömning av överensstämmelse

Modul A: självbedömning

Modul A (intern produktionskontroll) låter dig själv-certifiera att din produkt uppfyller de väsentliga cybersäkerhetskraven, och ta fullt ansvar för både dess design och produktion. Vägen är tillgänglig för tillverkare av standardprodukter (oklassificerade). Den är också tillgänglig för viktiga produkter i klass I endast där relevanta harmoniserade standarder, gemensamma specifikationer eller europeiska cybersäkerhetscertifieringssystem finns tillgängliga och tillämpas enligt CRA:s vägregler.

Under modul A ska du:

- Förbereda omfattande teknisk dokumentation
- Detaljera produktens design, produktionsprocesser, cybersäkerhetsmekanismer och förfaranden för sårbarhetshantering
- Behålla löpande ansvar för fortsatt överensstämmelse under hela produktens livscykel
- Inrätta en plan för säkerhetsuppdateringar och sårbarhetshantering under produktens operativa liv
- Hålla register tillgängliga i minst tio år

Modulerna B och C: produktcentrerad bedömning

Modulerna B och C gäller där tredjepartsverifiering av en specifik produkttyp krävs. De gäller för viktiga produkter i klass I där tillverkaren inte har tillämpat, har tillämpat endast delvis eller inte kan tillämpa relevanta harmoniserade standarder, gemensamma specifikationer eller certifieringssystem. För viktiga produkter i klass II måste tillverkaren använda modul B+C, modul H eller ett tillämpligt europeiskt cybersäkerhetscertifieringssystem på minst "betydande" assuransnivå.

Modul B (EU-typkontroll): Ett anmält organ undersöker ett representativt produktprov och tillhörande teknisk dokumentation. Det verifierar överensstämmelse med alla väsentliga cybersäkerhetskrav och utfärdar ett intyg om EU-typkontroll när produktdesignen uppfyller CRA:s kriterier.

Modul C (överensstämmelse med typen, produktionskontroll): Tillverkaren säkerställer att alla produktionsenheter överensstämmer med den typ som godkänts under modul B. Tillverkaren anbringar CE-märkningen, utfärdar EU-försäkran om överensstämmelse och håller register tillgängliga i minst tio år. Tillsammans säkerställer modulerna B och C att en specifik produktmodell är tekniskt överensstämmande och att varje produktionsbatch förblir konsekvent med den godkända designen.

Modul H: processcentrerad bedömning (fullständig kvalitetssäkring)

Modul H (fullständig kvalitetssäkring) fokuserar på tillverkarens hela interna kvalitetssystem snarare än testning av enskilda produkter. Den är tillgänglig för viktiga produkter i klass I och klass II. Kritiska produkter använder certifieringsvägen där villkoren är uppfyllda; där dessa villkor inte är uppfyllda använder de samma vägar som finns tillgängliga för viktiga produkter i klass II.

Under modul H ska du:

- Inrätta och underhålla ett kvalitetssystem som täcker design, utveckling, produktion, testning och sårbarhetshantering för hela produktkategorin
- Lämna in kvalitetssystemet till ett anmält organ för utvärdering och godkännande

- Acceptera löpande tillsyn (revisioner, inspektioner och processgranskningar) av det anmälda organet för att verifiera kontinuerlig överensstämmelse

När det godkänts får du utfärda försäkran om överensstämmelse för alla produkter som tillverkas inom det kvalitetssystemet, utan att upprepa det anmälda organets undersökning för varje enskild produkttyp.

Den centrala skillnaden mellan vägarna:

- Modulerna B+C: fokus på produkten. En representativ produkttyp testas och certifieras.
- Modul H: fokus på processen. Tillverkarens hela design- och produktionssystem certifieras och övervakas.

CRA i EU:s bredare regelbild

CRA står inte ensam. Den praktiska frågan för en tillverkare är: var sparar mitt CRA-arbete in på arbete under en annan EU-regim, och var har jag fortfarande separata skyldigheter att köra parallellt?

Där ditt CRA-arbete kan återanvändas

- **AI-system med hög risk (AI Act, förordning 2024/1689).** Om din produkt är ett AI-system med hög risk som ligger inom CRA:s tillämpningsområde, anses uppfyllande av CRA:s väsentliga cybersäkerhetskrav uppfylla AI Acts cybersäkerhetskrav i den omfattning som täcks av din EU-försäkran om överensstämmelse. Förfarandet för bedömning av överensstämmelse går som regel via AI Act-regimen, med ett undantag för viktiga och kritiska CRA-produkter. CRA:s bedömning av cybersäkerhetsrisker måste väga in AI-specifika risker som data poisoning och fientliga attacker.
- **Konsoliderad riskbedömning med annan unionsrätt.** CRA tillåter uttryckligen att bedömningen av cybersäkerhetsrisker utgör del av en bredare riskbedömning som krävs av en annan unionsrättsakt, där produkten faller under båda regimerna. En bedömningsartefakt, två regulatoriska användningar.
- **En teknisk dokumentation över regimer.** Som redan noterats i avsnittet om teknisk dokumentation kan en enda konsoliderad teknisk dokumentation täcka CRA tillsammans med annan tillämplig unionsrätt, så länge varje regims skyldigheter hanteras. Användbart där samma produkt redan behöver dokumentation under direktivet om radioutrustning, förordningen om ekodesign för hållbara produkter eller annan produktlagstiftning.
- **Gemensamma definitioner av renovering, underhåll och reparation.** CRA importerar dessa definitioner från förordningen om ekodesign för hållbara produkter. När du analyserar om en serviceoperation räknas som en väsentlig ändring är ekodesigndefinitionerna referensen, inte en CRA-specifik term.

Där separata skyldigheter kvarstår

- **Allt annat i AI Act.** Cybersäkerhet är bara en skiva av AI Act. Riskklassificering, transparens, datauppsättningsstyrning, mänsklig tillsyn, övervakning efter marknadslansering av AI-beteende och resten är AI Act-skyldigheter som CRA inte adresserar. CRA-överensstämmande cybersäkerhet är ingen presumtion om AI Act-överensstämmelse som helhet.
- **Ekodesign och innehåll i digitalt produktpass.** Ekodesignkrav på energieffektivitet, hållbarhet, poängsättning av reparerbarhet och det digitala produktpassets hållbarhetsinnehåll ligger utanför CRA:s tillämpningsområde. CRA-bevisspåret kan stå bredvid ekodesignarbetet men ersätter det inte.
- **Data Act om IoT-dataåtkomsträttigheter.** Data Act ger användare avtalsmässiga rättigheter att få åtkomst till, dela och överföra de data deras uppkopplade produkter genererar. CRA täcker säkerheten för dessa data; den sätter inte åtkomsträttighetsregimen. Annan skyldighet, andra bevis.
- **Produktansvar för defekta produkter.** Produktansvarsdirektivet (2024/2853) håller kvar strikt ansvar på tillverkaren för skada orsakad av defekta produkter. CRA flaggar att avsaknad av säkerhetsuppdateringar efter marknadslansering kan vara den defekt som utlöser ansvar. Dina avtal, försäkringar och incidenthandböcker behöver ta höjd för den exponeringen oberoende av CRA-överensstämmelse.

Så hjälper CRA Evidence

CRA Evidence gör EU CRA-skyldigheter till verifierbara produktbevis och kombinerar en plattform för överensstämmelse med teknisk rådgivning.

Plattform

En plats för att hantera bevisen bakom CRA-beredskap:

- **SBOM- och komponentinventering:** CycloneDX-, SPDX- och HBOM-poster för produktversioner och releaser
- **CI/CD-automatisering av bevis:** CLI- och API-flöden för skanningar, SBOM-uppladdningar, release gates och granskningsposter
- **Signerad SBOM och härkomst:** versionsstyrda bevis, leverantörsintyg och poster för tillbörlig aktsamhet
- **Sårbarhetsarbete:** CISA KEV, EPSS, VEX, övervakning, triage och rapporteringsflöden
- **Teknisk dokumentation och CE-bevis:** EU-försäkransposter, bevarandehistorik och QR-länkade produktpass för överensstämmelse

Teknisk rådgivning

Fokuserat stöd för att översätta CRA-skyldigheter till tekniska beslut om produkt, arkitektur, releaseprocess och leverantörsmodell.

- **Sprint för teknisk beredskap:** gapgranskning av väsentliga krav, arkitekturrekommendationer och prioriterad åtgärdsplan
- **CRA-programledning:** ansvarsmodell, skyldighetsspårning, bevismilstolpar och underhåll av teknisk dokumentation
- **Plan för myndighets- och incidentrespons:** rapporteringsflöden, playbooks för förfrågningar, användarkommunikation och förberedda bevispaket
- **Regulatorisk samordning:** koppla CRA-bevis till Data Act, ESPR, AI Act, RED och sektorskrav
- **Tekniska workshops:** sessioner på distans eller plats med produkt, utveckling, säkerhet, compliance och leverantörer

Verktygsoberoende: CRA Evidence integreras med CycloneDX, SPDX, Grype, Trivy, CI/CD-pipelines och ärendehanterare.

Ett praktiskt första steg

Välj en produktfamilj. Kartlägg ansvarig, omfattningsbeslut, SBOM, sårbarhetsflöde, luckor i teknisk dokumentation och releasebevis. Det ger teamet en konkret CRA-bas utan att göra överensstämmelse till ett separat projekt.

Se vad CRA Evidence täcker för din produkt på craevidence.com/sv. Priser och planalternativ finns på craevidence.com/sv/priser.

Denna guide är framtagen av CRA Evidence och bygger på Förordning (EU) 2024/2847. Den är informativ och utgör inte juridisk rådgivning.