



NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA

September 2026

Introduktion till föreskrifterna om säkerhetsåtgärder och ledningens utbildning

Cybersäkerhetslagen

Introduktion till föreskrifterna om säkerhetsåtgärder och ledningens utbildning

Denna publikation syftar till att ge en introduktion till föreskrifterna om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare enligt cybersäkerhetslagen (MCFFS 2026:11). Den riktar sig både till verksamhetsutövare och tillsynsmyndigheter.

Introduktionen beskriver föreskrifternas syfte och struktur samt förtydligar innebörden av centrala begrepp. Introduktionen innehåller även hänvisningar till annat stöd som kan användas i arbetet med säkerhetsåtgärder.

Introduktionen tillhandahåller endast information som stöd för tolkningen av regleringen, den inför inte några nya krav. Förtydliganden och förklaringar i denna introduktion ska inte betraktas som förhandsbesked om vad tillsynsmyndigheterna kan komma att bedöma i ett enskilt tillsynsärende.

NCSC kommer även att tillhandahålla en mer omfattande vägledning som stöd för tillämpningen av föreskrifternas enskilda krav på säkerhetsåtgärder. Den är planerad att publiceras runt årsskiftet 2026/2027.

John Billow

chef Nationellt Cybersäkerhetscenter - NCSC

Innehållsförteckning

1	Inledning	1
2	Innebörden av föreskrifter och allmänna råd	2
3	Tillsyn.....	2
4	Föreskrifternas utformning.....	3
4.1	Föreskrifternas disposition	4
4.2	Närmare om utformning av kraven.....	4
5	Uttryck och tidsangivelser.....	6
5.1	Beskrivning av hur krav ska omhändertas.....	6
5.2	Tidsfrister	7
5.3	Grundläggande begrepp	8
6	Hur kan man komma i gång med arbetet med föreskrifterna?	16
7	Befintligt stöd för arbetet.....	17
7.1	Metodstödet för systematiskt informationssäkerhetsarbete	17
7.2	Vägledning om säkerhetsåtgärder i informationssystem	17
7.3	Rekommendationer för skydd mot AI-förstärkta angrepp.....	18
7.4	ANTS	18
7.5	MISP-SE.....	18
7.6	Cybersäkerhetskollen	18
7.7	Mognadsdialogen	19
7.8	Säkerhet i leveranskedjor.....	19
7.8.1	Hoten mot de digitala leveranskedjorna - 50 rekommendationer för att stärka samhällssäkerheten	19
7.8.2	Verktygslåda för att förbättra säkerheten i IKT-leveranskedjan	19
7.9	Rekommendationer för att skydda ot-miljöer	20
7.9.1	Rekommendationer för beslutsfattare och organisationer.....	20
7.9.2	Fördjupade råd och rekommendationer för skydd av ot-miljöer ...	20
7.9.3	Vägledning om ot-säkerhet.....	20

1 Inledning

Cybersäkerhetslagen (2025:1506), härnäst kallad CSL, med tillhörande föreskrifter och allmänna råd syftar till att höja den generella cybersäkerhetsnivån i Sverige inom 18 utpekade sektorer som bedöms vara viktiga för samhällets funktion och ekonomi. För att nå dit ställer CSL bland annat krav på de som omfattas av lagen att vidta säkerhetsåtgärder.

Den 1 oktober 2026 träder föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare (MCFFS 2026:11) i kraft. Dessa förtydligar och kompletterar CSL:s bestämmelser om säkerhetsåtgärder och utbildning. CSL ställer bland annat krav på att en verksamhetsutövare ska vidta lämpliga och proportionella åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter (2 kap. 3 § CSL) samt att de som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder (2 kap. 4 § CSL).

Den 1 juli 2026 övergick föreskriftsrätten enligt cybersäkerhetsförordningen (2025:1507) från Myndigheten för civilt försvar (MCF) till Försvarets Radioanstalt (FRA). Det innebär att FRA tar över ansvaret för MCF:s föreskrifter enligt CSL och framtida revideringar. Föreskrifterna gäller oförändrat och bär MCF:s namn tills att de har reviderats.

2 Innebörden av föreskrifter och allmänna råd

Föreskrifter ("ska-krav") kompletterar och förtydligar bestämmelser i lag. De aktörer som träffas av bestämmelserna är skyldiga att efterleva såväl krav som finns i lag som i tillhörande föreskrifter.

Allmänna råd ("bör-krav") innehåller förtydliganden och konkreta förslag på tillvägagångssätt för att uppfylla föreskrifternas krav. Om en verksamhetsutövare inte kan uppfylla bör-kraven i enlighet med de allmänna råden kan verksamhetsutövaren vidta andra motsvarande åtgärder. Till skillnad från föreskrifter är allmänna råd inte juridiskt bindande.¹

3 Tillsyn

Cybersäkerhetsförordningen pekar ut ett antal myndigheter som tillsynsmyndigheter. En tillsynsmyndighet ska utöva tillsyn i sin sektor/sina sektorer över att cybersäkerhetslagen och de föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheterna ska bland annat bedriva tillsyn om föreskrifterna om säkerhetsåtgärder och ledningens utbildning följs.

NCSC vid FRA leder ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet är att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

¹ Myndigheternas föreskrifter (SB PM 2025:4) s. 44

<https://www.regeringen.se/contentassets/4a78b51adf5a41b09dc93f2bc2fe2846/myndigheternas-foreskrifter-pm-20254.pdf>

4 Föreskrifternas utformning

Föreskrifterna förtydligar CSL:s krav på säkerhetsåtgärder och ledningens utbildning. Kraven på cybersäkerhet är grupperade i organisatoriska, tekniska och driftrelaterade respektive fysiska säkerhetsåtgärder. Det övergripande syftet med föreskrifterna är att säkerställa:

- att verksamhetsutövaren bedriver ett systematiskt och riskbaserat cybersäkerhetsarbete utifrån ett allriskperspektiv²,
- en lägsta nivå av cybersäkerhet hos verksamhetsutövare som omfattas av CSL,
- att verksamhetsutövaren utformar sina säkerhetsåtgärder över lägsta nivån när den egna verksamheten har behov av det.

Kraven på säkerhetsåtgärder gällande organisatoriska, driftrelaterade och fysiska säkerhetsåtgärder anger en lägsta nivå. Genom att bedriva ett systematiskt och riskbaserat arbete i enlighet med 3 kap. skapar verksamhetsutövaren även en förmåga att kunna identifiera och hantera sitt behov av cybersäkerhet över lägsta nivån.

Vidtagandet av säkerhetsåtgärderna i föreskrifterna ska inte ses som fristående åtgärder eller som punkter som kan bockas av. Verksamhetsutövare behöver förstå sin verksamhet, sina system, sina leveranskedjor och sin omvärld. Den kunskapen gör det möjligt att förstå vilka risker som finns och vilka konsekvenser olika händelser kan få i verksamheten samt samhället i stort. Utifrån den bilden kan säkerhetsåtgärder vidtas, utformas och prioriteras så att de kontinuerligt motsvarar verksamhetens förutsättningar och behov.

Organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder kompletterar och förstärker varandra. En teknisk säkerhetsåtgärd, såsom säkerhetsloggning, får exempelvis bättre effekt när den stöds av en tydlig ansvarsfördelning, fungerande arbetssätt, rätt kompetens och tillgängliga resurser. På motsvarande sätt får organisatoriska säkerhetsåtgärder, såsom riskhantering, relevans först när de används för att stärka säkerheten i den digitala miljön.

Eftersom verksamheten, hoten och riskerna förändras över tid kan erfarenheter från den löpande verksamheten, förändringar, övningar, tester

² Begreppet "allriskperspektiv" är ett nyckelbegrepp som förklaras närmare i avsnitt 5.3.

och eventuella incidenter ge anledning att se över tidigare bedömningar och anpassa säkerhetsåtgärderna.

När det gäller ledningens utbildning och dess roll i arbetet med cybersäkerhet förtydligar föreskrifterna vilken kunskap och kompetens som ledningen behöver för att kunna fastställa mål och inriktning för verksamhetsutövarens cybersäkerhet, bedöma vilka säkerhetsåtgärder som verksamhetsutövaren behöver genomföra för att upprätthålla en lämplig nivå av cybersäkerhet utifrån identifierade risker samt övervaka genomförandet av säkerhetsåtgärderna.

4.1 Föreskrifternas disposition

Föreskrifterna är strukturerade enligt följande:

- Kapitel 2 innehåller krav på ledningens utbildning om säkerhetsåtgärder.
- Kapitel 3 innehåller krav på organisatoriska säkerhetsåtgärder. Kraven omfattar exempelvis systematiskt och riskbaserat arbete med cybersäkerhet, interna regler och arbetssätt, roller, ansvarsområden och befogenheter liksom omvärldsbevakning, informationsklassning och riskhantering samt uppföljning och utvärdering.
- Kapitel 4 omfattar krav på tekniska och driftrelaterade säkerhetsåtgärder. Kraven omfattar exempelvis säkerhetskonnfigurering, behörighetshantering, övervakning, säkerhetsloggning och logganalys, kryptering samt ändringshantering.
- Kapitel 5 innehåller krav på fysiska säkerhetsåtgärder rörande lokaler och tekniska försörjningssystem.
- Kapitel 6 innehåller sektorsspecifika krav. För närvarande endast riktade till verksamhetsutövare inom offentlig förvaltning. Kraven gäller system för kriskommunikation.
- Kapitel 7 reglerar möjligheterna till undantag från kraven i föreskrifterna.

4.2 Närmare om utformning av kraven

Kraven på en viss säkerhetsåtgärd inleds oftast med en målformulering som tydliggör varför en viss säkerhetsåtgärd ska vidtas. Med ett exempel hämtat från **3 kap. 10 § om omvärldsbevakning**:

För att hålla sig uppdaterad om hot, sårbarheter, teknisk utveckling, rättsliga krav och tillgängligt stöd av betydelse för verksamhetsutövarens cybersäkerhet, ska verksamhetsutövaren bedriva omvärldsbevakning.

Av regeln framgår att verksamhetsutövaren ska bedriva omvärldsbevakning med ett visst syfte som ska uppnås.

När det finns skäl har krav på att vidta en viss säkerhetsåtgärd konkretiserats ytterligare med en lägsta nivå. Detta är ett exempel hämtat från samma paragraf:

Verksamhetsutövaren ska inhämta relevant information från

- 1. leverantörer av den digitala miljöns hård- och mjukvara, och*
- 2. det nationella cybersäkerhetscentret (NCSC), vid Försvarets radioanstalt, och särskilt de däri ingående funktionerna nationell CSIRT-enhet och cyberkrishanteringsmyndighet.*

I exemplet tydliggörs från vilka källor verksamhetsutövaren minst ska inhämta information för sin omvärldsbevakning.

Vissa krav på säkerhetsåtgärder kompletteras med **allmänna råd**. Dessa ger rekommendationer och konkretiserar ytterligare hur verksamhetsutövaren bör uppfylla ”ska-kravet”. När det gäller omvärldsbevakning är de allmänna råden utformade på följande sätt:

Verksamhetsutövaren bör även som en del av sin omvärldsbevakning inhämta relevant information från

- relevanta tillsynsmyndigheter,*
- Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) hos det nationella cybersäkerhetscentret (NCSC), samt*
- Europeiska unionens cybersäkerhetsbyrå (ENISA).*

Det allmänna rådet rekommenderar ytterligare källor till information inom ramen för verksamhetsutövarens omvärldsbevakning. Om en verksamhetsutövare inte kan uppfylla bör-kraven i enlighet med de allmänna råden kan verksamhetsutövaren vidta andra åtgärder med motsvarande verkan, i det här fallet använda andra källor för att inhämta motsvarande relevant information.

5 Uttryck och tidsangivelser

I föreskrifterna används några ofta återkommande uttryck för att beskriva på vilket sätt eller inom vilken tidsfrist något ska göras. Dessa förklaras i detta avsnitt. Avsnittet innehåller även begrepp av grundläggande betydelse för förståelse av föreskrifterna. För att underlätta förståelsen av hur begreppen används i föreskrifterna ges förklaringar och exempel.

5.1 Beskrivning av hur krav ska omhändertas

Fastställa:

Begreppet används synonymt med besluta. Exempelvis fastställa interna regler och arbetssätt i 3 kap. 3 §.

Säkerställa:

Begreppet används när verksamhetsutövaren behöver verifiera att något finns eller är på ett visst sätt. Exempelvis ska enligt 3 kap. 8 § systemägaren, i de system denne ansvarar för, säkerställa att risker analyserats och att informationsägarens identifierade nivå av skydd uppnås.

Identifiera och hantera behovet av:

Formuleringen innebär att verksamhetsutövaren aktivt ska analysera och därefter ta ställning till om det finns behov av en viss åtgärd. Identifierat behov ska därefter omhändertas på ett ändamålsenligt sätt. Formuleringen ger verksamhetsutövaren flexibilitet i att själv utforma en säkerhetsåtgärd utifrån externa krav, interna behov och risk. Formuleringen används i exempelvis 3 kap. 12 § (riskhantering) enligt vilken verksamhetsutövaren ska identifiera och hantera behovet av att uppdatera genomförda riskanalyser vid förändrade hot och nya sårbarheter som kan påverka cybersäkerheten.

Om inte uppenbart obehövlig:

Formuleringen används för att beskriva något som ska vidtas, om inte verksamhetsutövaren bedömer att det absolut inte behövs. Som exempel kan nämnas att verksamhetsutövaren enligt 4 kap. 20 § (avseende krav på övervakning, säkerhetsloggning och logganalys) ska, om inte uppenbart obehövligt, ansluta sig till automatiska notifieringar av tekniska sårbarheter (ANTS) hos den nationella CSIRT-enheten³. För mer information om ANTS, se avsnitt 7.4.

³ CSIRT är en förkortning för ”Computer Security Incident Response Team”. Nationellt cybersäkerhetscenter vid FRA är Sveriges nationella CSIRT.

5.2 Tidsfrister

I föreskrifterna används tidsfrister när en åtgärd ska vara utförd. Uttrycken listas utifrån hur snabbt åtgärden ska vidtas. I detta avsnitt förklaras vad som avses med uttrycken.

Tabell 1 - Tidsfrister

Begrepp	Ev. definition	Förklaring
Skyndsamt	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Åtgärden är prioriterad och ska vidtas snarast.
Utan onödigt dröjsmål	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Åtgärden vidtas så snart det kan ske. ⁴
Inom 72 timmar	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Åtgärden vidtas så snart det är möjligt, dock senast inom 72 timmar från det att det som föranlett åtgärden gjorts tillgängligt.
Var tredje månad	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Åtgärden vidtas minst en gång vart tredje månad. Detta innebär dock ingen begränsning av åtgärden och den kan således vidtas med tätare frekvens än så.
Vid behov men minst en gång per år	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Åtgärden vidtas vid behov. Bedömningen kring när behov föreligger behöver göras från fall till fall. Om behov inte ansetts föreligga ska åtgärden genomföras minst en gång per år.
Acceptabla tider för otillgänglighet och bristande funktionalitet	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Denna tidsram ska vara sådan inom vilken otillgänglighet och bristande funktionalitet är acceptabel. Vad som utgör acceptabla tider för otillgänglighet och bristande funktionalitet för informationsbehandlingen bestämmer verksamhetsutövaren utifrån exempelvis externa krav, interna behov och identifierade risker.

⁴ Prop. 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 119

5.3 Grundläggande begrepp

Följande begrepp är av grundläggande betydelse för förståelse av föreskrifterna. Begreppen har delats in i följande kategorier:

1. nyckelbegrepp,
2. roller,
3. uttryck med särskild koppling till verksamhetsutövarens digitala miljö.

Tabell 2 - Nyckelbegrepp

Begrepp	Ev. definition	Förklaring och exempel
Allriskperspektiv	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Allriskperspektivet innebär att verksamhetsutövare ska sträva efter att bedöma alla risker för systemen som ska skyddas och att analysera alla möjliga orsaker till att en risk realiserar. ⁵ Det kan vara organisatoriska, tekniska och driftrelaterade risker och fysiska risker. Både medvetet illvilligt handlande och misstag räknas in. Som exempel kan nämnas väder- och klimatrelaterade risker, brand i datacenter, systemfel på grund av felkonfiguration eller utpressningsangrepp.
System	<i>Uttrycket framgår av 1 kap. 2 § 16 CSL: nätverks- och informationssystem: i cybersäkerhetslagens mening, dvs nätverks- och informationssystem: a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om</i>	En förkortning av nätverks- och informationssystem enligt 1 kap. 2 § p.16. CSL. Nätverk- och informationssystem (system i föreskrifterna) kan mycket förenklat sägas utgöras av följande: 1) Elektroniska kommunikationsnät, 2) En eller flera sammankopplade datorer, eller

⁵Prop. 2025/26:28 s. 244.

Begrepp	Ev. definition	Förklaring och exempel
	<i>elektronisk kommunikation,</i> b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller <i>c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas</i>	3) Digitala uppgifter som på något sätt hanteras i 1) eller 2). System kan vara av många olika slag. Som exempel kan nämnas system för hantering av fakturor, löner (it-system) och styrning av dammar, energiförsörjning, dricksvattenförsörjning och transporter (ot-system).
Cybersäkerhet	Uttrycket definieras i 1 kap. 2 § 5 CSL⁶ som: <i>all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot</i>	Begreppet cybersäkerhet har i andra sammanhang ibland haft en snävare betydelse med större tekniskt fokus, närmare det som brukar benämnas it-säkerhet. Ibland har begreppet använts för att beskriva endast skydd mot antagonistiska hot. Den legaldefinition som nu har fastslagits av EU innebär i stället att cybersäkerhet har fått en innebörd som i stort kan likställas med det som traditionellt beskrivs som informationssäkerhet.⁷ Exempelvis organisatoriska, tekniska och driftrelaterade samt fysiska åtgärder som behövs för att skydda system mot cyberhot.
Cyberhot	Definieras i 1 kap. 2 § 4 CSL som ⁸:	Cyberhot kan delas in i tre huvudsakliga kategorier:

⁶ Uttrycket definieras på samma sätt som i artikel 2.1 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 526/2103 (cybersäkerhetsakten).

⁷ Prop. 2025/26:28 s. 40.

⁸ Uttrycket definieras på samma sätt som i artikel 2.8 i cybersäkerhetsakten.

Begrepp	Ev. definition	Förklaring och exempel
	<i>en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informations-system, användare av dessa system och andra personer.</i>	• Mänskliga hot (kan vara både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag). • Tekniska hot (i form av systemfel). • Naturhot (som till exempel väderfenomen, jordbävningar) Samtliga hot kan leda till incidenter som kan påverka cybersäkerheten och leda till allvarliga konsekvenser för både enskilda och organisationer.
Sektorsverksamhet	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>sådan verksamhet som omfattas av cybersäkerhetslagen.</i>	Som utgångspunkt gäller CSL:s regler hela verksamhetsutövarens organisation och all verksamhet som verksamhetsutövaren bedriver.⁹ Den verksamhet som är anledningen till att man som organisation omfattas av CSL benämns i föreskrifterna sektorsverksamhet. En verksamhetsutövare kan bedriva både sektorsverksamhet och annan verksamhet, exempelvis är hälso- och sjukvård sektorsverksamhet medan att bedriva lunchrestauranger bedöms som annan verksamhet. I föreskrifterna ställs i vissa fall något skarpare krav på incidentrapportering eller att vidta säkerhetsåtgärder i sektorsverksamhet.
Viktiga samhällsfunktioner	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.</i>	Begreppet används när det är viktigt att förstå och tydliggöra hur den egna verksamheten och systemen påverkar samhällets funktionalitet. De viktiga samhällsfunktionerna är en utgångspunkt för samhällets arbete med beredskapsarbete. Kunskap om hur cybersäkerhet i den egna verksamheten bidrar till att upprätthålla

⁹ Det finns undantag för lagens tillämpning enligt 1 kap. 12 § CSL, bland annat för verksamhetsutövare som bedriver säkerhetskänslig verksamhet.

Begrepp	Ev. definition	Förklaring och exempel
		viktiga samhällsfunktioner ¹⁰ stärker arbetet med civilt försvar.

Tabell 3 - Roller

Begrepp	Ev. definition	Förklaring och exempel
Verksamhetsutövare	Definieras i 1 kap. 3–8 §§ CSL.	Den som omfattas av CSL.
Ledning	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En bedömning av vem som anses ingå i ledningen behöver göras från fall till fall då det skiljer sig åt beroende på aktuell verksamhetsutövares verksamhetsform. För aktiebolag och ekonomiska föreningar avser ledningen styrelsen och verkställande direktör samt ersättare för dessa. För handelsbolag och enkla bolag är bolagsmännen ansvariga för förvaltningen och är således att betrakta som ledningen. För myndigheter som står under regeringen är ledningen den som framgår av myndighetens instruktion eller annan författning. För kommuner och regioner utgörs ledningen av kommun- respektive regionstyrelsen. ¹¹
Samordnare	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för samordning av verksamhetsutövarens cybersäkerhetsarbete. Notera att rollen eller funktionen inte specifikt behöver benämnas som "samordnare" i verksamhetsutövarens

¹⁰ För ytterligare underlag rörande viktiga samhällsfunktioner hänvisas till MCF: <https://www.mcf.se/sv/amnesomraden/beredskap-for-kris-och-krig/beredskap-for-aktorer/samhallsviktig-verksamhet/viktiga-samhallsfunktioner/>.

¹¹ Prop. 2025/26:28, s. 99f.

Begrepp	Ev. definition	Förklaring och exempel
		organisation. I NCSC:s stöd benämns denna roll oftast CISO, den kan även exempelvis kallas informationssäkerhetssamordnare eller informationssäkerhetschef. ¹²
Informationsägare	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för informationsbehandling i system. Notera att rollen inte specifikt behöver benämnas som "informationsägare" i verksamhetsutövarens organisation. ¹³
Systemägare	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En eller flera roller eller funktioner hos verksamhetsutövaren med ansvar för säkerheten i system. Notera att rollen inte specifikt behöver benämnas som "systemägare" i verksamhetsutövarens organisation. ¹⁴

Tabell 4 - Begrepp kopplade till verksamhetsutövarens digitala miljö

Begrepp	Ev. definition	Förklaring och exempel
Digital miljö	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>den samlade mängden system som verksamhetsutövaren använder för att bedriva intern verksamhet och tillhandahålla externa tjänster. Består av produktionsmiljö och, i</i>	Verksamhetsutövarens samtliga system, det vill säga både de som används för den interna verksamheten och externa tjänster som verksamhetsutövaren tillhandahåller. Det inkluderar utkontrakterad informationsbehandling.

¹² Myndigheten för civilt försvar, Konsekvensutredning avseende föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare, (Konsekvensutredning) s. 41.

¹³ Konsekvensutredning s. 41.

¹⁴ Konsekvensutredning s. 41.

Begrepp	Ev. definition	Förklaring och exempel
	<i>tillämpliga fall, utvecklings-, test- respektive utbildningsmiljö.</i>	
Utkontrakterad informations-behandling	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Begreppet utkontrakterad informationsbehandling avser alla typer av tjänster som en verksamhetsutövare har anlitat en leverantör för, såsom drift- och molntjänster, ekonomitjänster, systemutveckling, säkerhet med flera. Verksamhetsutövaren kan utkontraktera informationsbehandling i hela eller delar av sin digitala miljö till en leverantör.
Sektorskritiskt system	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet.</i>	Verksamhetsutövaren behöver själv bedöma vilka system som är sektorskritiska inom dennes sektorsverksamhet. Sektorskritiska system innefattar sådana system som är nödvändiga för att verksamhetsutövaren långsiktigt ska kunna bedriva den sektorsverksamhet som specificeras i CSL. Det omfattar både system som används i tjänster som tillhandahålls externt och system som används internt om deras funktionalitet är central för att sektorsverksamheten ska kunna bedrivas enligt normalläge.
Information i behov av utökat skydd	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>information som på grund av externa krav kräver en viss nivå av</i>	Information i behov av utökat skydd på grund av externa krav kan ha sin grund i annan reglering eller avtal som verksamhetsutövaren ingått med andra organisationer. Exempel på detta kan vara hantering av

Begrepp	Ev. definition	Förklaring och exempel
	<i>skydd avseende konfidentialitet, riktighet inklusive autenticitet, eller tillgänglighet, alternativt information som verksamhetsutövaren vid värdering bedömer ha behov av motsvarande nivå av skydd.</i>	personuppgifter enligt dataskyddsförordningen (GDPR) eller regler för att skydda företagshemligheter enligt lagen (2018:558) om företagshemligheter. Verksamhetsutövaren kan också vid sin informationsklassning identifiera information i behov av utökat skydd.
Segment	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	Avser en indelning av digital miljö i olika nätverkssegment för att förhindra spridning och minimera konsekvenser av incidenter.
Ot-segment	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>ett nätverkssegment som är inrättat för cyberfysiska system.</i>	Nätverkssegment i den digitala miljön som verksamhetsutövaren har inrättat för system som används för att styra och övervaka fysiska enheter, fysiska processer och fysiska händelser. Sådana system kallas cyberfysiska system eller ot-system (ot är en förkortning för operativ teknik).
It-segment	Definieras i 1 kap. 4 § MCFFS 2022:11: <i>ett nätverkssegment som är inrättat för andra system än sådana system som placeras i ot-segment.</i>	Nätverkssegment som är inrättat för it-system. It-segment kan ha olika storlek och syften. I it-segment gäller föreskrifternas ordinarie krav på säkerhetsåtgärder, inte de anpassningar som gäller för ot-segment.
Produktionsmiljö	Definieras i 1 kap. 4 § MCFFS 2026:11: <i>de system i den digitala miljön som används för att bedriva verksamhet förutom de system som</i>	Produktionsmiljön används för verksamhetsutövarens ordinarie verksamhet, både sektorsverksamhet och annan verksamhet. Innehåller typiskt sett it- och, vid behov, ot-segment för systemadministration, centrala systemsäkerhetsfunktioner

Begrepp	Ev. definition	Förklaring och exempel
	<i>används för verksamhet i utvecklings- test- och utbildningsmiljö. Består av it-segment och ot-segment.</i>	verksamhetssystem och externt exponerade system. Kan även innehålla segment som används för andra uppgifter.
Utvecklingsmiljö	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En avskild del av den digitala miljön som verksamhetsutövaren använder för utvecklingsarbete som bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis utveckling av mjukvara till produktionsmiljön.
Testmiljö	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En avskild del av den digitala miljön som verksamhetsutövaren använder för att testa system där testningen bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis test av nyutvecklad mjukvara eller förändrad konfiguration av system.
Utbildningsmiljö	<i>Saknar definition i CSL och tillhörande föreskrifter.</i>	En avskild del av den digitala miljön som verksamhetsutövaren använder för intern utbildning av egna användare där utbildningen bedöms kunna påverka säkerheten i produktionsmiljön, exempelvis utbildning på ny eller uppdaterad mjukvara till produktionsmiljön. All utbildningsverksamhet bedrivs inte i utbildningsmiljön. Utbildning som en verksamhetsutövare exempelvis tillhandahåller externa aktörer som en del av sin sektorsverksamhet bedrivs i produktionsmiljön eftersom det hör till verksamhetsutövarens ordinarie verksamhet.

6 Hur kan man komma i gång med arbetet med föreskrifterna?

För en verksamhetsutövare som ännu inte har ett etablerat arbete kan en gapanalys ge en första samlad bild av nuläget. I gapanalysen jämförs det befintliga arbetet med tillämpliga bestämmelser. Analysen kan synliggöra:

- vad som redan finns på plats,
- vad som finns men kan behöva utvecklas,
- vad som saknas,
- vilka områden som behöver undersökas närmare.

Resultatet kan användas för att planera och prioritera det fortsatta arbetet utifrån risker och möjliga konsekvenser.

För mer stöd, se avsnitt *Gapanalys* i Metodstödet för systematiskt informationssäkerhetsarbete: <https://metodstod-informationssakerhet.msb.se/sv/analysera/gapanalys/>

7 Befintligt stöd för arbetet

Det finns flera olika slags stöd till organisationer som behöver komma i gång med eller vidareutveckla sitt arbete med cybersäkerhet. Det finns dels generell information om ett systematiskt och riskbaserat cybersäkerhetsarbete som bedöms vara relevanta, trots att de inte är anpassade till CSL. Dels finns det mer specifikt inriktat stöd med avseende på AI-hot. Vidare finns det ett antal olika kostnadsfria tjänster som avser stödja verksamhetsutövare i deras cybersäkerhetsarbete. Här följer en lista på stöd och tjänster som kan vara användbara.

7.1 Metodstödet för systematiskt informationssäkerhetsarbete

Metodstödet för systematiskt informationssäkerhetsarbete är en samling vägledningar och verktyg som förtydligar hur ett systematiskt arbete med informations- och cybersäkerhet kan utformas. Metodstödet bygger på standardserien ISO/IEC 27000.

Webbplatsen för Metodstödet för systematiskt informationssäkerhetsarbete kommer att överföras till ncsc.se i slutet av 2026. Notera att informationen på Metodstödet webbplats är aktuell och korrekt, även om flytten av webbplatsen kommer att överföras i slutet av 2026.

Här hittas Metodstödet för systematiskt informationssäkerhetsarbete:

<https://metodstod-informationssakerhet.msb.se/>

7.2 Vägledning om säkerhetsåtgärder i informationssystem

MCF har år 2023 publicerat en vägledning om säkerhetsåtgärder i informationssystem som stöd vid tillämpning av föreskrifter och allmänna råd (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter. Vägledningen riktar sig i första hand till de personer som utvecklar, hanterar och förvaltar en organisations digitala miljö. Fokus riktas främst mot tekniska och driftrelaterade samt fysiska säkerhetsåtgärder.

Vägledningen hittas här: <https://www.ncsc.se/siteassets/radgivning-och-stod/ovriga-publikationer/sakerhetsatgarder-i-informationssystem.pdf>

7.3 Rekommendationer för skydd mot AI-förstärkta angrepp

NCSC har tagit fram två olika rekommendationer avseende skydd mot AI-förstärkta angrepp. Den ena publikationen ger beslutsfattare och organisationer rekommendationer för att stärka skyddet mot AI-förstärkta cyberangrepp och hantera de säkerhetsrisker som följer av användningen av AI. För att ta del av dessa rekommendationer, se:

<https://www.ncsc.se/siteassets/publikationer/skydda-dig-mot-ai-forstarkta-angrepp-rek-for-beslutsfattare-och-organisationer.pdf>

Den andra rekommendationen avser tekniska och operativa åtgärder för att skydda verksamheten mot avancerade AI-förstärkta cyberhot. För att ta del av dessa rekommendationer, se:

<https://www.ncsc.se/siteassets/publikationer/skydd-mot-ai-forstarkta-angrepp-tekniska-och-operativa-atgarder.pdf>

7.4 ANTS

ANTS (Automatiska notifieringar om tekniska sårbarheter) är en kostnadsfri tjänst som är tillgänglig för alla svenska verksamheter, både i offentlig och privat sektor från NCSC/CERT-SE (den nationella CSIRT-enheten). ANTS hjälper till att övervaka verksameters angreppsytor på internet och notifierar verksamheter när det identifierats företeelser som kan behöva åtgärdas i dessa.

Här finns mer information om ANTS och hur man anmäler sig till tjänsten:

<https://cert.se/tjanster/ants/>

7.5 MISP-SE

MISP-SE (Malware Information Sharing Platform) är en nationell plattform för insamling, lagring, analys och informationsdelning som svenska verksamhetsutövare kan ansluta sig till kostnadsfritt. MISP-SE bidrar även till att skapa en lägesbild av aktuella cyberhändelser, både nationellt och inom specifika sektorer. Syftet är att stärka Sveriges samlade motståndskraft mot cyberangrepp genom delning av hotinformation. Tjänsten tillhandahålls av NCSC/CERT-SE.

För mer information om MISP-SE, se: <https://www.cert.se/tjanster/misp-se/>

7.6 Cybersäkerhetskollen

Cybersäkerhetskollen är samlingsnamnet för NCSC:s cybersäkerhetsmätningar Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. Med hjälp

av Cybersäkerhetskollen kan organisationer mäta nivån på sitt systematiska cybersäkerhetsarbete samt få stöd för förbättringsarbete. Verktöget kan användas när som helst av verksamheter som är behov av att följa upp nivån på sitt systematiska cybersäkerhetsarbete. Nationell mätning av nivån på det systematiska cybersäkerhetsarbetet genomförs vartannat år (udda år). Nästa genomförande är vårvinter 2027. Tills dess kommer innehållet i Cybersäkerhetskollen ses över utifrån cybersäkerhetslagen och tillhörande föreskrifter samt genomförd utvärdering.

Cybersäkerhetskollen är ett verktyg för ökad motståndskraft och ett stärkt civilt försvar. För mer information, se: <https://www.ncsc.se/sv/radgivning-och-stod/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/>

7.7 Mognadsdialogen

Ett sätt att diskutera cybersäkerhetsarbetet är att genomföra Mognadsdialogen, som är en strukturerad process där man tillsammans med ledningen kartlägger och bedömer verksamhetens nuvarande nivå av cybersäkerhet. Genom dialogen kan styrkor, svagheter och områden för förbättring identifieras, vilket skapar en gemensam förståelse för vad som behöver prioriteras i verksamheten framöver. För mer information om Mognadsdialogen, se här:

<https://www.ncsc.se/sv/radgivning-och-stod/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/mognadsdialogen/>

7.8 Säkerhet i leveranskedjor

7.8.1 Hoten mot de digitala leveranskedjorna - 50 rekommendationer för att stärka samhällssäkerheten

MCF (tidigare MSB) har publicerat en rapport som behandlar hoten mot leveranskedjor och ger rekommendationer för att stärka säkerheten. Rapporten hittas här: <https://www.ncsc.se/siteassets/radgivning-och-stod/ovriga-publikationer/hoten-mot-de-digitala-leveranskedjorna---50-rekommendationer-for-att-starka-samhallssakerheten.pdf>

7.8.2 Verkttyglåda för att förbättra säkerheten i IKT-leveranskedjan

EU har antagit en verkttyglåda för säkerhet i digitala leveranskedjor som tillhandahåller en sektorsövergripande och icke-bindande strategi för hur cybersäkerhet i digitala leveranskedjor ska identifieras, bedömas och hanteras. Verkttyglådan, som framtagits av EU-kommissionen och medlemsstater, syftar

till att stärka och harmonisera insatser för att förbättra säkerheten i digitala leveranskedjor inom unionen. Den är utformad inte bara för att stödja medlemsstaterna utan också för att hjälpa offentliga och privata aktörer i arbetet med att säkra digitala leveranskedjor. Du hittar rapporten här: <https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>

7.9 Rekommendationer för att skydda ot-miljöer

Det finns ett antal publikationer som avser skydd av ot-miljöer.

7.9.1 Rekommendationer för beslutsfattare och organisationer

NCSC:s publikation *Operativ teknik - En särskilt utsatt del av organisationers teknikmiljöer. Rekommendationer för beslutsfattare och organisationer* riktar sig till ledningen och lyfter vikten av styrning, ansvarsfördelning och ett riskbaserat arbetssätt för att skydda ot-miljöer.

Läs mer på: <https://www.ncsc.se/siteassets/publikationer/operativ-teknik---rekommendationer-for-beslutsfattare-och-organisationer.pdf>.

7.9.2 Fördjupade råd och rekommendationer för skydd av ot-miljöer

Fördjupade råd och rekommendationer för skydd av ot-miljöer ger mer tekniska råd. Den beskriver hur organisationer kan arbeta med exempelvis segmentering, åtkomstkontroller och övervakning för att minska risker. Läs mer på: <https://www.ncsc.se/siteassets/publikationer/fordjupade-rad-och-rekommendationer-for-skydd-av-ot-miljoer.pdf>

7.9.3 Vägledning om ot-säkerhet

Mycket av styrning och övervakning av den infrastruktur och de processer som behövs i samhällsviktiga verksamheter är beroende av industriella informations- och styrsystem, även kallade ot. Syftet med denna vägledning är att bidra med konkreta rekommendationer och stöd till arbetet med att bygga upp samt förbättra säkerheten i industriella informations- och styrsystem. Vägledningen *Ökad säkerhet i industriella informations- och styrsystem* hittas här: <https://www.ncsc.se/siteassets/radgivning-och-stod/ovriga-publikationer/vagledning-till-okad-sakerhet-i-industriella-informations--och-styrsystem.pdf>