Myndigheten för civilt försvars författningssamling

Utgivare: Anna Asp
ISSN 3119-2394

MCFFS 2026:12
Utkom från trycket
den 18 juni 2026

Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsrevision och säkerhetsskanning;

beslutade den 15 juni 2026.

Myndigheten för civilt försvar föreskriver[1] följande med stöd av 38 § 7 p. cybersäkerhetsförordningen (2025:1507).

Allmänna råd har en annan juridisk status än föreskrifter. De är inte tvingande. Deras funktion är att förtydliga innebörden i lag, förordning och föreskrifter och att ge generella rekommendationer om deras tillämpning.

1 kap. Inledande bestämmelser

Tillämpningsområde

1 § Dessa föreskrifter och allmänna råd innehåller bestämmelser om sådan säkerhetsrevision och säkerhetsskanning som avses i 3 kap. 5–7 §§ cybersäkerhetslagen (2025:1506).

2 § Bestämmelserna i 2 kap. ska endast tillämpas när en tillsynsmyndighet anlitar ett oberoende organ för att utföra en säkerhetsrevision.

Ordförklaringar

3 § Uttryck i dessa föreskrifter och allmänna råd har samma betydelse som i cybersäkerhetslagen.

4 § I dessa föreskrifter och allmänna råd avses med

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen (NIS 2-direktivet).

Begrepp	Betydelse
digital miljö	den samlade mängden system som verksamhetsutövaren använder för att bedriva intern verksamhet och tillhandahålla externa tjänster. Består av produktionsmiljö och, i tillämpliga fall, utvecklings-, test- respektive utbildningsmiljö,
sektorskritiska system	ett system som är nödvändigt för att kunna bedriva intern verksamhet eller tillhandahålla externa tjänster inom sektorsverksamhet,
system	nätverks- och informationssystem enligt 1 kap. 2 § p. 16 cybersäkerhetslagen,
säkerhetsrevision	granskning i syfte att bedöma om de säkerhetsåtgärder som verksamhetsutövaren har vidtagit för att skydda system och för att säkerställa efterlevnad av kraven i cybersäkerhetslagen med tillhörande reglering är ändamålsenliga och effektiva,
säkerhetsskanning	skanning av system för att upptäcka sårbarheter eller osäker konfiguration,
viktig samhällsfunktion	en samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet.

2 kap. Säkerhetsrevision

Syfte och val av oberoende organ för säkerhetsrevision

1 § Vid en säkerhetsrevision ska det bedömas vilken nivå av cybersäkerhet som verksamhetsutövaren har och om säkerhetsåtgärderna uppfyller de krav som ställs i cybersäkerhetslagen med tillhörande reglering.

2 § Det oberoende organ som anlitas för att utföra en säkerhetsrevision ska vara en juridisk person eller enskild näringsidkare som tillhandahåller

personal med tillräcklig kunskap utifrån uppdragets utformning och vid behov kunskap om den verksamhet som granskningen avser.

Allmänna råd

Vid tillsynsmyndighetens bedömning av det oberoende organets lämplighet för uppdraget bör det oberoende organets egen nivå av cybersäkerhet, tid och resurser för att kunna utföra uppdraget samt förekomst av relevant certifiering beaktas.

Vid bedömning av tillräcklig kunskap utifrån uppdragets utformning bör kunskaper inom cybersäkerhet, granskningsmetodik och säkerhetsrevision hos det oberoende organets personal beaktas.

3 § Tillsynsmyndigheten ska säkerställa att det oberoende organ som anlitas för att utföra en säkerhetsrevision

1. genomför uppdraget opartiskt, självständigt och objektivt,
2. inte under uppdragets genomförande är bundna av sekretessavtal eller andra motsvarande överenskommelser med verksamhetsutövaren som inskränker tillsynsmyndighetens tillgång till relevant information,
3. kan skydda information relaterad till uppdraget på ett säkert sätt,
4. inte nyttjar information som erhållits i samband med säkerhetsrevisionen för annat än genomförande av den aktuella säkerhetsrevisionen, och
5. förstör informationen när uppdraget är genomfört om inte annat har avtalats med verksamhetsutövaren som är föremål för tillsyn.

Allmänna råd

Tillsynsmyndigheten bör inte anlita ett oberoende organ som har affärsrelationer, rådgivningsuppdrag eller andra beroendeförhållanden till den verksamhetsutövare som är föremål för granskning. Tillsynsmyndigheten bör begära att det oberoende organet informerar tillsynsmyndigheten om sådan intressekonflikt uppstår under uppdraget.

Det oberoende organets genomförande av säkerhetsrevision

4 § Tillsynsmyndigheten ska i samband med att en säkerhetsrevision inleds upplysa verksamhetsutövaren om

1. uppdragets omfattning,

2. möjligheten att informera tillsynsmyndigheten om eventuella brister i det oberoende organets genomförande av säkerhetsrevisionen, och
3. på vilket sätt information enligt 2 p. ska lämnas.

5 § Tillsynsmyndigheten ska säkerställa att det oberoende organ som anlitas för att utföra en säkerhetsrevision dokumenterar avvikelser från efterlevnad av kraven i cybersäkerhetslagen med tillhörande reglering.

6 § I en säkerhetsrevision ingår att kontrollera både utformningen och tillämpningen av säkerhetsåtgärder.

En säkerhetsrevision ska utformas på ett sådant sätt att den inte vållar större kostnad eller olägenhet för verksamhetsutövaren än vad som är nödvändigt.

7 § Säkerhetsrevisionen ska inkludera åtminstonde följande moment:

1. granskning av relevant dokumentation,
2. intervjuer med berörd personal,
3. tekniska kontroller av system och segment, samt
4. vid behov, kontroll av lokaler.

Momenten i punkterna 2–4 ska, om inte särskilda skäl talar emot, utföras på plats hos verksamhetsutövaren.

Allmänna råd

En säkerhetsrevision bör omfatta både tekniska och icke-tekniska moment, såsom granskning av en verksamhetsutövarens digitala miljö, interna regler och arbetssätt, avtal eller överenskommelse om utkontraktering samt övrig dokumentation.

8 § Säkerhetsrevisionen ska genomföras enligt en metodik som möjliggör en systematisk och riskbaserad granskning av verksamhetsutövarens organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder. Den metodik som används ska dokumenteras.

Tillsynsmyndigheten ska säkerställa att säkerhetsrevisioner hos verksamhetsutövare utförs på ett effektivt och likvärdigt sätt.

Allmänna råd

Det oberoende organet bör som stöd vid utformning av metodiken och genomförande av säkerhetsrevisionen använda revisionsmetodik enligt nedan etablerade standarder eller motsvarande:

- Bedömning av överensstämmelse – Krav på organ som reviderar och certifierar ledningssystem (ISO/IEC 17021-1:2015).
- Bedömning av överensstämmelse – Krav på verksamhet inom olika typer av kontrollorgan (ISO/IEC 17020:2012).
- Informationsteknik – Säkerhetstekniker – Vägledning för revision av ledningssystem för informationssäkerhet (ISO/IEC 27007:2020).

- International standard on assurance engagements 3000 (revised) assurance engagements other than audits or reviews of historical financial information (Effective for assurance reports dated on or after December 15, 2015).
- Informationssäkerhet, cybersäkerhet och integritetsskydd – Krav på organ som tillhandahåller revision och certifiering av informationssäkerhetssystem – Del 1: Allmänt (ISO/IEC 27006-1:2024, IDT).

Det oberoende organet bör i sin granskning av organisatoriska, tekniska, driftrelaterade och fysiska säkerhetsåtgärder utgå ifrån standarder som ger stöd för den specifika revisionen.

9 § Innan en säkerhetsrevision inleds ska tillsynsmyndigheten ha godkänt säkerhetsrevisionens omfattning och tillvägagångssätt.

10 § Om en sårbarhet som inte tidigare har publicerats upptäcks i verksamhetsutövarens digitala miljö vid en säkerhetsrevision ska tillsynsmyndigheten säkerställa att det oberoende organet utan dröjsmål och på lämpligt sätt informerar verksamhetsutövaren och tillsynsmyndigheten om sårbarheten.

11 § Efter genomförd säkerhetsrevision ska tillsynsmyndigheten säkerställa att det oberoende organet sammanställer resultatet av genomförd revision i en skriftlig rapport. Rapporten och övrig relevant dokumentation ska överlämnas till tillsynsmyndigheten på det sätt tillsynsmyndigheten har anvisat.

Allmänna råd

En skriftlig rapport bör innehålla eventuellt identifierade sårbarheter, övrig information som framkommit under säkerhetsrevisionen samt förslag på åtgärder.

3 kap. Säkerhetsskanning

Syfte, omfattning och utförare

1 § Tillsynsmyndigheten ska genom säkerhetsskanning bedöma effektiviteten av genomförda säkerhetsåtgärder i verksamhetsutövarens digitala miljö.

2 § En säkerhetsskanning ska utföras av en tillsynsmyndighet. För genomförandet kan tillsynsmyndigheten anlita en extern aktör. En säkerhetsskanning ska utföras av personal med för uppdraget tillräcklig kunskap.

Allmänna råd

Vid bedömning av tillräcklig kunskap för uppdraget bör personalens kunskaper om följande beaktas:

- relevanta skanningsmetoder och risker,
- hur automatiserade och manuella verktyg används, samt
- hur negativa konsekvenser för verksamhetsutövaren kan minimeras.

3 § Tillsynsmyndigheten ska säkerställa att en säkerhetsskanning genomförs i den omfattning som är nödvändig för tillsynen och endast avser system som verksamhetsutövaren har rådighet över inom ramen för sin verksamhet.

4 § Tillsynsmyndigheten ska säkerställa att en säkerhetsskanning genomförs på ett sådant sätt att negativ inverkan på funktionaliteten i systemen och övriga negativa konsekvenser för verksamhetsutövaren minimeras.

Allmänna råd

Säkerhetskanningar bör ske med automatiserade verktyg i den mån det är lämpligt i förhållande till syftet med åtgärden.

5 § Tillsynsmyndigheten ska vid anlitande av en extern aktör för utförande av en säkerhetsskanning säkerställa att den externa aktören

1. inte under uppdragets genomförande är bundna av sekretessavtal eller andra motsvarande överenskommelser med verksamhetsutövaren som inskränker tillsynsmyndighetens tillgång till relevant information,
2. kan skydda information relaterad till uppdraget på ett säkert sätt,
3. inte nyttjar information som erhållits i samband med säkerhetsskanningen för annat än genomförande av den aktuella säkerhetsskanningen, och
4. förstör informationen när uppdraget är genomfört om inte annat har avtalats med verksamhetsutövaren som är föremål för tillsyn.

Metod och riskbaserat urval

6 § Vid val av metod för utförande av en säkerhetsskanning ska tillsynsmyndigheten beakta systemens betydelse för verksamheten.

Identifieras betydande risk för negativa konsekvenser för verksamhetsutövaren ska alternativa metoder för säkerhetsskanning övervägas och om säkerhetsskanning alls ska genomföras.

7 § Innan en tillsynsmyndighet beslutar att utföra en säkerhetsskanning ska den säkerställa att

1. val av verksamhetsutövare och av vilka system som ska skannas har skett utifrån en riskbaserad metod, och
2. de metoder som ska användas för att genomföra skanningen är lämpliga i förhållande till de identifierade riskerna och de system som ska skannas.

Tillsynsmyndighetens bedömning och beslut enligt 1–2 p. ska dokumenteras.

Allmänna råd

Vid tillsynsmyndighetens val av verksamhetsutövare för en säkerhetsskanning bör verksamhetsutövarens betydelse för viktiga samhällsfunktioner beaktas. Vid tillsynsmyndighetens val av vilka system som ska skannas bör följande beaktas:

- om systemet är sektorskritiskt,
- integrationer och beroenden,
- tidigare incidenter eller rapporterade sårbarheter,
- exponering mot internet, och
- teknisk riskprofil, såsom system som är kända för att innehålla sårbarheter.

8 § Innan en säkerhetsskanning genomförs ska tillsynsmyndigheten, om inte särskilda skäl talar emot, tillsammans med verksamhetsutövaren

1. bedöma risken för driftpåverkan,
2. planera genomförandet så att belastningen på systemen minimeras,
3. ta fram en plan för att kunna avbryta säkerhetsskanningen, och
4. bedöma behovet av att säkerställa förmåga att återställa de system som kan påverkas negativt.

Informationsskyldighet

9 § Tillsynsmyndigheten ska säkerställa att verksamhetsutövaren utan dröjsmål och på lämpligt sätt informeras om brister och sårbarheter som upptäckts vid säkerhetsskanningen för att skyndsamt kunna vidta åtgärder.

Denna författning träder i kraft den 1 oktober 2026.

Myndigheten för civilt försvar

MIKAEL FRISELL

Ida Sahlin
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Beställningsadress:
Norstedts Juridik, 106 47 Stockholm
Telefon: 08-657 95 00
E-post: order@forlagssystem.se
Webbadress: www.nj.se/offentligapublikationer
Beställningsnummer: 19126-12