Remissvar: MSB 2025-13269

1. Sammanfattning

Det föreligger en stor diskrepans mellan MSB:s förslag till föreskrifter för cybersäkerhelagens (CSL) och NIS2 med dess genomförandeförordning. En klyfta skapas där svenska företag belastas med unika krav och särlösningar. MSB lägger vikten på informationssäkerhet CSL på cybersäkerhet och samhällsviktiga tjänsters funktion.

NIS2 har explicita krav på ledning och riskhanteringsåtgärder. Genomförandeförordningen som ensar och detaljerar de teknik- och metodkrav för av EU utpekade sektorer. För övriga sektorer. har MSB rätt att meddela föreskrifter.CSL syfte är en hög nivå av cybersäkerhet i samhället.

MSB:s förslag vilar på informationssäkerhet. MSB hävdar i sin konsekvensutredningen att cybersäkerhet och informationssäkerhet är likställda. Detta är fel.

Cybersäkerhet är att skydda nätverks- och informationssystemens förmåga att motstå en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer. Detta och inget annat gäller. (se CSL definition av cybersäkerhet och cyberhot).

MSB föreslagna föreskrifter har med informationssäkerhet som utgångspunkt skapat egen terminologi, egen struktur, egna formuleringar samt egna krav på specifika roller, detaljerad dokumentation, informationsklassning och tekniska särlösningar. Spårbarhet saknas mot CSL och EU-rättens uttalade syfte, en hög nivå av cybersäkerhet i samhället.(CSL 1 kap 1 §).

Det enklaste, mest kostnadseffektiva och rättssäkra sättet att implementera säkerhetskraven i CSL är att använda NIS2 genomförandeförordning. Genom att nyttja den med terminologi från CSL erhålls en enhetlig implementering med harmonisering, teknikneutralitet och tydlighet.

Om denna åtgärd ej genomförs, bör följande åtgärder övervägas:

- **Harmonisering med EU genomförandeförordning:** Omarbeta föreskrifterna så de med CSL terminologi speglar Bilaga 1 i genomförandeförordningen.
- **Inför Proportionalitet:** Inkludera klausuler som "där så är lämpligt" gällande MFA och kryptering, särskilt för OT-miljöer där driftsäkerhet måste gå före cybersäkerhet.
- **Ensa begreppen:** Ensa begreppen med CSL.
- **Fokusera på cybersäkerhet i stället för informationssäkerhet:** Skifta fokus från klassning av information till samhällsviktiga tjänsters funktion.

Genom att anpassa föreskrifterna till EU-rätten kan lagens syfte uppnås. Jag som skrivit detta remissvar är Ulf Dellborg, här finns min CV: https://.ension.se/konsult/sakerhetsexpert.

2. Konsekvenser avseende kostnader

Kostnadsökningar p g a lagstiftning är investeringar för att möta lagens mål och kostnader på grund av ineffektiv reglering. Här är fokuset ineffektiv reglering indelat i:

- **Administrativa kostnader:** Mest kostnadsdrivande är administrativ detaljstyrning i stället för tekniska utfall och riskbaserade åtgärder som i genomförandeförordningen.
- **Nya investeringar:** Krav på fysisk infrastruktur och hårdvara som tvingar fram ombyggnationer eller nyinvesteringar. En avvikelsen från EU:s teknikneutrala hållning.

2.1. Administrativa kostnader

2.1.1 Informationsklassning: Stora kostnader med mycket låg verkan

Verksamhetsutövarens information ska enligt 2 kap. 13 § klassas, innan en riskanalys genomförs. Konsekvensen är att man tvingas att klassa historiska och löpande datamängder. Risken är att energin läggs på att klassa mötesprotokoll i stället för att förhindra att cyberattack slår ut en samhällsviktig tjänst. Det viktiga är att klassa verksamhetsutövarnas tjänster, detta görs i efter en preliminär riskanalys, i kontextanalysen. Detta är ett betydligt mindre arbete än att klassa all information.

2.1.2 Nya regler relativt EU-rätten: Dubbelreglering

MSB krav "systematiskt och riskbaserat arbete" (2 kap. 1§) skapar stora kostnader. Spårbarhet mot NIS2 saknas. I propositionen till CSL bedöms kravet som en dubbelreglering. Kravet återinförs av MSB med hänvisningar till ISO 27000. Det är ett implicit krav på full certifiering mot ISO 27001. En kostnad på många miljoner kronor, utan legal nytta.

2.1.3 Egna begrepp: Begreppsförvirring

MSB inför en mängd egna begrepp. MSBs specifika krav på roller som "informationsägare" och "systemägare" (2 kap. 7 §) saknas i EU-rätten. "Utkontraktering" används när man troligen menar ”Säkerhet i Leveranskedjan”, digital miljö och system i stället för nätverks- och informationssystem, etc. För globala företag verksamma i Sverige innebär detta att styrdokument inte är användbara. För alla skapas kostnaden osäkerhet.

2.1.4 Detaljerade dokumentationskrav. Mycket arbete

MSB:s föreskrifter reglerar detaljer men missar bredd. Styrdokumentens utformning regleras på ett sätt som saknar motstycke i genomförandeförordningen. Detta skapar fokus på formalia snarare än på faktisk förmåga.

2.1.5 Ingen spårbarhet mot EU-rätt och CSL: Verksamhetsutövaren får skapa egen

Egen terminologi och struktur gör att genomförandeförordningens mappning mot NIS2 / CSL inte kan användas. Verksamhetsutövarna måste skapa denna spårbarhet själv. Aktörer som har tillsyn av både PTS och MSB måste upprätthålla parallella säkerhetssystem.

2.2. Infrastruktur och Fysisk Säkerhet

2.2.1 Kravet på fysiskt åtskilda sektioner

I 2 kap. 19 § ställer MSB krav på att redundanta system ska placeras i "fysiskt åtskilda sektioner". I genomförandeförordningen berörs tillgänglighet och "backup facilities". För en verksamhet med omfattande fysisk infrastruktur är konsekvenserna stora**.** Ett elnätsbolag med hundratals transformatorstationer måste ha dubbla enheter i samma teknikhus eller redundans via nätverket till en annan station. En tolkning av "fysiskt åtskilda sektioner" i produktionsmiljö innebär att två separata teknikhus måste vid varje station, med separata brandceller, kyla och strömförsörjning. Detta står inte i proportion till riskreduktionen.

2.2.2 Spårbarhet av Tid och UTC (SP)

Kravet i 3 kap. 28 § att tiden ska vara spårbar till UTC (SP) skapar en teknisk inlåsning. Verksamhetsutövare kan inte använda standardkonfigurationer i molntjänster eller routrar. Begreppet "robust tid" är odefinierat och kan tolkas som krav på lokal tidhållning. Även om robust tid är önskvärt, är kostnaden hög.

2.2.3 Kryptering i alla system

Kravet är att kryptering ska ske om informationen har "behov av utökat skydd". EU intar en mer nyanserad hållning, "om lämpligt". Detta är en kostnadsfråga. Inom OT krävs ofta byte av hårdvara. Det kan röra tusentals enheter. Gamla system kan ofta inte uppgraderas.

2.2.4 Certifieringskrav

I 3 kap. 2 § ställer MSB krav på att "identifiera och hantera behovet" av att välja system och tjänster som är certifierade enligt europeiska ordningar. Certifierade produkter är dyrare än standardprodukter. Om MSB:s krav tolkas strikt av tillsynsmyndigheter kan det tvinga offentlig sektor och kritisk infrastruktur att utesluta leverantörer som inte är certifierade.

3. Synpunkter per paragraf

2 kap. 1 §: Begreppet "Systematiskt och riskbaserat arbete"

- **Synpunkt:** Begreppet *"systematiskt och riskbaserat arbete"* saknar spårbarhet mot CSL och genomförandeförordning. Begreppet associeras med förslaget till formulering i SOU 2024:18 om "Systematiskt informationssäkerhetsarbete". Kravet kan tolkas som ett krav på efterlevnad av ISO 27001, i synnerhet när de allmänna råden hänvisar till ISO 27001. Där är syftet informationssäkerhet. NIS2 / CSL syfte är att skydda samhällsviktiga tjänster..
- **Motivering:** Kravet "systematiskt och riskbaserat informationssäkerhetsarbete" bedömdes i propositionen att redan följa av säkerhetskraven i CSL varför införandet av ett separat krav skulle innebära dubbelreglering.
- **Förslag:** Gör samma bedömning avseende dubbelreglering som i propositionen.

2 kap. 1 §: Angående "Identifiera och hantera behovet av standarder"

- **Synpunkt:** Kravet att "identifiera och hantera behovet av att använda relevanta standarder" är otydligt och skapar en onödig analysbörda.
- **Analys:** Det är myndighetens roll att förtydliga regler som ger efterlevnad av lagen. Att lägga ansvaret på varje verksamhetsutövare leder till rättsosäkerhet och varierad kravbild.
- **Förslag:** Skriv om genomförandeförordningen med CSL terminologi och översätt ENISAs guide till svenska. Detta ger konformitet och regelefterlevnad säkrad av EU.

2 kap. 3-5 §§: Interna regler och arbetssätt

- **Synpunkt:** MSB ställer detaljerade formaliakrav på styrdokument (datum, målgrupp, ansvarig roll specificerat i föreskrift).
- **Analys:** EU kräver att policys ska finnas och godkännas, men detaljerar inte metadatan. MSB:s krav är administrativt tunga utan att tillföra säkerhetsvärde.
- **Förslag:** Använd samma reglering som i genomförandeförordningen

2 kap. 7 §: Ledningens ansvar för säkerhetsåtgärder

- **Synpunkt:** MSB:s krav på att de specifika rollerna 'informationsägare' och 'systemägare' är en nationell särlösning. Även om dessa roller är vedertagna i svensk och ISO-baserad praxis, är de inte obligatoriska enligt NIS2. EU-rätten lägger ansvaret på ledningsorganet och kräver funktionell separation av uppgifter.
- **Analys:** MSB:s detaljerade krav på specifika titlar riskerar att skapa byråkratiska trösklar, särskilt i mindre organisationer som använder flexiblare rollbeskrivningar, samtidigt som kravet på 'etablerade metoder för säker utveckling' (3 kap. 4 § p 5) är för vagt jämfört med EU-förordningens explicita lista på tekniska principer.
- **Förslag:** Använd samma krav på roller som i genomförandeförordningen

2 kap. 9 §: Ledningens utbildning

- **Synpunkt:** Detta är den enda paragraf som genomskär alla sektorer, inklusive digital infrastruktur.
- **Konsekvens:** Här finns en tydlig harmonisering. Kravet är proportionerligt och nödvändigt för att aktivera ledningens ansvar enligt NIS2.

2 kap. 13 §: Informationsklassning

- **Synpunkt:** Kravet att klassa all information *innan* den behandlas i system är en ineffektiv metod för cybersäkerhet. Det är verksamhetsutövarens tjänster som först skall klassas. Detta görs i en preliminär riskanalys (jämför IEC 61508 och IEC 62443)
- **Analys:** Det är ologiskt att klassa information innan en riskanalys av verksamheten. För att kunna klassa information måste du veta vilka system som påverkar samhällsviktiga. Tjänster. Sedan skapar du säkerhetsåtgärder så tjänsten har nödvändig information. Att börja med att klassa all information är "bottom-up" när NIS2 kräver "top-down".
- **Förslag:** Ersätt med krav på *kritikalitetsbedömning av system och tjänster*, i linje med EU-förordningens "Asset Management".

2 kap. 14 §: Riskhantering, Begreppet "allriskperspektiv"

- **Synpunkt:** Begreppet "allriskperspektiv" i 2 kap. 14 § behöver förtydligas eller harmoniseras med NIS2-direktivets "all-hazards approach".
- **Motivering:** Riskanalysen riskerar att bli för abstrakt om den inte tydligt kopplas till *fysisk miljö och försörjningsberoenden (*el, kyla, telekom) i enlighet med EU-rätten.
- **Förslag:** Förtydliga i allmänna råd att "allrisk" inkluderar fysiska hot, miljöhot och leverantörsberoenden, samt att riskanalysen primärt ska syfta till att säkra den samhällsviktiga tjänstens leveransförmåga.

2 kap. 14 §: Riskhantering, Informationsklassning före Riskanalys

- **Synpunkt:** Kravet i 2 kap. 14 § p 3 att informationsklassning ska användas som *ingångsvärde* i riskanalysen bör ses över.
- **Motivering:** Att tvinga fram en fullständig informationsklassning *innan* riskanalys av systemen är ineffektivt och saknar stöd i genomförandeförordningen, och ISO 27001. MSB blandar ihop informationssäkerhet där skyddsobjektet är information med cybersäkerhet där skyddsobjektet är samhällsviktiga tjänster.
- **Förslag:** Ändra formuleringen så att *verksamhetsanalys* och *systemkritikalitet* utgör ingångsvärden, medan informationsklassning kan ske integrerat i riskprocessen.

2 kap. 15 §: Riskhantering, Begreppet "aggregering"

- **Synpunkt:** MSB introducerar begreppen aggregering. Begreppet "aggregering" som en specifik riskfaktor (där oklassad information blir skyddsvärd i mängd) är hämtat från Säkerhetsskyddslagen och svensk förvaltningspraxis, inte från NIS2.
- **Analys:** EU-regelverken fokuserar på tillgångshantering och skydd av tjänsters funktion. I NIS2 kontext är den primära risken avbrott i tjänsten, inte att någon pusslar ihop hemlig information (det är säkerhetsskydd). Detta lägger en extra analysbörda på företag att bedöma effekter av aggregering som inte krävs av genomförandeförordningen.
- **Förslag:** Ta bort kravet.

2 kap. 15 §: Riskhantering, "Användning av mobila system"

- **Synpunkt:** EU-förordningen är mer konkret. Den ställer krav på *"instructions regarding the secure configuration and operation of... mobile devices"*.
- **Analys:** Här är MSB mer processinriktad ("identifiera risker") medan EU är mer åtgärdsinriktad ("säkra konfigurationer"). MSB:s formulering kräver att varje organisation "uppfinner hjulet" genom att riskanalysera mobila enheter. EU:s strategi är att man ska införa "Best Practice", det är tydligare och lättare att revidera. MSB:s krav skapar administrativt merarbete (dokumentation) innan man säkrar enheten.
- **Förslag:** Använd samma reglering som i genomförandeförordningen

2 kap. 15 §: Riskhantering, "Utkontraktering"

- **Synpunkt:** I stället för begreppet ”utkontraktering” använder CSL termen ”säkerhet i leveranskedjan” vilket är ett bredare och mer modernt begrepp. Det täcker inte bara aktiv utkontraktering av verksamhet, utan även inköp av mjukvara, molntjänster och hårdvara.

- **Analys:** Termen "utkontraktering" (outsourcing) för tankarna till att flytta ut en hel process (t.ex. lön eller IT-drift). I en modern digital leveranskedja (SaaS, PaaS, bibliotek i kod) är "supply chain" mer relevant. Genom att använda ordet utkontraktering riskerar MSB att smalna av riskområdet jämfört med NIS2.
- **Förslag:** Använd samma reglering som i genomförandeförordningen

2 kap. 15 §: Enskilda felkällor

- **Synpunkt:** Krav på att identifiera enskilda felkällor (Single Points of Failure, SPOF), ett genomförandeförordningen bilaga 1 punkt 2.1.2.
- **Analys**: Utan krav på SPOF-analys riskerar verksamhetsutövare att genomföra. riskanalyser på en för hög abstraktionsnivå som missar kritiska beroenden i arkitekturen. Att hitta enskilda felkällor är vitalt för att säkra samhällsviktiga tjänsters funktion
- **Förslag:** Inför krav på SPOF-analys

2 kap. 16 § (Planering av säkerhetsåtgärder)

- Synpunkt: Bestämmelsen om riskhantering och åtgärdsplanering är för otydlig vad gäller ledningens ansvar för restrisker.
- Analys: MSB:s förslag anger att åtgärder ska motiveras utifrån "ledningens kriterier för riskacceptans". Detta skiljer sig markant från genomförandeförordningens punkt 2.1.1, där ledningsorganet aktivt ska acceptera restrisker. MSB:s formulering möjliggör en delegering där ledningen sätter generella kriterier men frikopplas från de faktiska besluten.
- **Förslag:** Harmonisera 2 kap. 16 § med EU-rätten.

2 kap. 17 §: Punkt 1: Insamling av information (Detektion)

- **Synpunkt:** Formuleringen är vag relativt genomförandeförordningen
- **Analys:** För "Relevanta Entiteter" ställer genomförandeförordningen (3.2) krav på automatiserad övervakning och specifikt loggning av relevant nätverkstrafik. MSB:s skrivning är vag. En verksamhetsutövare kan felaktigt tro att manuell rapportering från användare ("Servicedesk") uppfyller kravet i punkt 1,
- **Förslag:** Ensa med genomförandeförordningen.

2 kap. 17 §: Punkt 5 & 6: Återställning och Dokumentation

- **Synpunkt**: Kravet saknar koppling till kontinuitetsplanering och Business Impact Analysis.
- **Analys**: Genomförandeförordningen (3.1.2) har ett krav på överensstämmelse mellan incidentpolicy och kontinuitetsplan. MSB:s punkt 5 kan tolkas som endast ett krav på återställningsrutin. Återställningen ska ske i en prioriteringsordning (vilket EU kräver i punkt 4.1.2), riskerar verksamhetsutövaren att återställa fel system först.
- **Förslag**: Komplettera punkt 5 med kravet att återställningsrutinen ska vara synkroniserad med verksamhetens kontinuitetsplan (enligt 2 kap. 19-20 §§) för att säkerställa att affärskritiska beroenden respekteras.

2 kap. 17 §: Punkt 13: Rapportering av sårbarheter

- **Synpunkt:** Kravet på att rapportera sårbarheter (som inte är incidenter) avviker från harmoniseringen med EU:s genomförandeförordning och skapar onödiga säkerhetsrisker.
- **Analys:** EU-förordningen (6.10) fokuserar på att entiteter ska ha rutiner för avslöjande enligt nationell policy och att hämta information från CSIRT. Att tvinga entiteter att skicka information om sina "0-day"-sårbarheter till en central myndighetsdatabas innan en patch finns tillgänglig skapar en attraktiv måltavla (en så kallad "honeypot"). Dessutom är det otydligt hur detta förhåller sig till anonymitetsskyddet i NIS2-direktivet artikel 12.
- **Förslag:** Stryk kravet på obligatorisk rapportering av sårbarheter. Ersätt med ett krav på att ha en process för hantering och samordnat avslöjande av sårbarheter.

2 kap. 18 §: Kontinuitet och Fysisk Separation

- Synpunkt: Kravbilden för skydd av säkerhetskopior och verifiering av återställningsförmåga är för otydlig och harmoniserar inte med kraven i genomförandeförordningen.
- Analys: Genomförandeförordningen kräver i bilaga 1 punkt 4.2: Att säkerhetskopior för "Relevanta Entiteter" lagras fysiskt eller logiskt åtskilda från produktionssystemet, att regelbundna integritetskontroller av säkerhetskopiorna och regelbundna integritetskontroller av säkerhetskopiorna. MSB:s förslag är vagt och saknar dessa viktiga.
- Förslag: Lägg till genomförandeförordningens krav i föreskrifterna:

2 kap. 19 §: Kontinuitet och Fysisk Separation

- **Synpunkt:** MSB kräver att redundanta system ska placeras i "fysiskt åtskilda sektioner".
- **Analys:** Detta är ett långtgående krav som saknar direkt motsvarighet i EU-texten. MSB:s krav på fysisk separation i produktionsmiljö innebär för en processindustri eller ett elnätsbolag att man potentiellt måste bygga dubbla teknikhus vid varje ställverk eller pumpstation.
- **Förslag:** Använd samma reglering som i genomförandeförordningen

2 kap. 20 §: Kontinuitet i utvecklings-, test- och utbildningsmiljö.

- **Synpunkt:**ett krav som helt saknas i både genomförandeförordningen (EU) 2024/2690 och standarden ISO 27001.
- **Analys:** Kravet utgör en eller nationell särreglering. För en verksamhetsutövare innebär detta att efterlevnad av globala standarder och direkt tillämplig EU-lag inte är tillräckligt för att uppfylla svensk lag på denna punkt.
- **Förslag:** Ta bort kravet i nuvarande form. Nyttja kraven i genomförandeförordningen.

2 kap. 21-22 §§: Krishantering

- **Synpunkt:** .Total omskrivning och ny struktur. Spårbarhet saknas. Omöjliggör direkt användning av ENISA:s compliance-verktyg.
- **Analys:** Kravet utgör total omskrining av genomförandeförordningen och är en nationell särreglering som saknar spårbarhet till CSL.
- **Förslag:** Ta bort kravet i nuvarande form. Nyttja kraven i genomförandeförordningen.

2 kap. 23 §: Uppföljning och utvärdering.

- **Synpunkt:** .Total omskrivning och ny struktur. Spårbarhet saknas. Omöjliggör direkt användning av ENISA:s compliance-verktyg.
- **Analys:** Kravet är en trubbig styrning som missgynnar, agila arbetssätt och riskbaserad styrning. Det är en nationell särreglering som saknar spårbarhet till CSL.
- **Förslag:** Ta bort kravet i nuvarande form. Nyttja kraven i genomförandeförordningen.

2 kap. 24 §: Samordnare.

- **Synpunkt:** 2 kap. 24 § representerar en ambition att höja lägstanivån för cybersäkerhet i Sverige genom att tvinga fram en återkommande utvärdering ledd av en samordnare.
- **Analys:** Förslaget kolliderar med EU:s mer flexibla, processorienterade ansats och riskerar att skapa en parallell byråkrati för svenska företag. Kravet på specifika underlag, särskilt informationsklassning, avslöjar en kvardröjande syn på säkerhet som "skydd av data" snarare än "skydd av samhällsfunktioner", vilket är NIS2-direktivets kärna.
- **Förslag:** Ta bort kravet i nuvarande form. Nyttja kraven i genomförandeförordningen.

3 kap. 1 §: Fokus på administration i stället för förmåga

- **Synpunkt:** Formuleringen utgör en otydlig förenkling av kraven i NIS2 artikel 21.2.e och genomförandeförordningen.
- **Analys:** Formuleringen riskerar att tolkas som ett krav som inte tar hänsyn till tekniska realiteter för system med lång livscykel där skyddet ofta måste uppnås genom kompenserande åtgärder snarare än inbyggd säkerhet över tid. Fokus hamnar på administration i stället för förmåga
- **Förslag:** Använd samma reglering som i genomförandeförordningen

3 kap. 2 §: Angående spårbarhet och IKT-begreppet

- **Synpunkt:** MSB använder begreppet "IKT-produkter" på ett sätt som avviker från den terminologi ("Nätverks- och informationssystem") som används i CSL och NIS2-direktivet.
- **Motivering:** Detta skapar en begreppsförvirring och försvårar för verksamhetsutövare att använda befintliga ledningssystem (ISMS) för att visa efterlevnad.
- **Förslag:** Harmonisera begreppsanvändningen med CSL och inkludera en tydlig referensram för hur IKT-certifiering förhåller sig till ISO 27001.

3 kap. 2 §: Angående "Säkerhet i leveranskedjan" vs "Utkontraktering"

- **Synpunkt:** Kopplingen mellan 3 kap. 2 § och kraven på "utkontraktering" (2 kap. 15 §) är otydlig och riskerar att missa målet med NIS2:s fokus på säkerhet leveranskedjan.
- **Motivering:** Genomförandeförordningen ställer krav på en policy för säkerhet i leveranskedjan för alla leverantörer av IKT-produkter, inte bara vid "utkontraktering" av verksamhet. MSB:s terminologi riskerar att leda till missförstånd.
- **Förslag:** Byt terminologi från "utkontraktering" till "säkerhet i leveranskedjan" och tydliggör att kravet i 3 kap. 2 § omfattar anskaffning av både produkter och tjänster.

3 kap. 2 §: Ekonomiska konsekvenser

- **Synpunkt:** Konsekvensutredningen saknar en analys av kostnaderna för att b"identifiera och hantera behovet" av certifierade produkter.
- **Motivering:** Certifierade IKT-produkter är ofta betydligt dyrare än standardprodukter. Om MSB:s föreskrift tolkas strikt kan det tvinga offentlig sektor och kritisk infrastruktur att byta ut fungerande utrustning mot dyrare alternativ utan bevisad säkerhetsvinst.
- **Förslag:** MSB bör säkerställa att kravet är proportionerligt.

3 kap. 3 §: Angående "Lämpliga och proportionella" åtgärder

- **Synpunkt:** Begreppet "behov av säkerhet" i paragrafen behöver tydligare kopplas till proportionalitetsprincipen.
- **Motivering:** Utan en tydlig proportionalitetsklausul (som finns i NIS2 Artikel 21) riskerar 3 kap. 3 § att tolkas som att alla identifierade brister måste åtgärdas oavsett kostnad. För äldre system i industrin kan det vara tekniskt omöjligt att införa moderna skydd.
- **Förslag:** Inför en proportionalitetsklausul för att harmonisera med lagtexten.

3 kap. 3 §: Angående dokumentationskravet

- **Synpunkt:** Kravet på att dokumentera "hanteringen av behovet" riskerar att bli en administrativ inlåsning.
- **Motivering:** Fokus bör ligga på *att* åtgärder är införda och fungerar, inte på den processen bakom valet (som redan täcks av riskanalysen i 2 kap. 14 §). Detaljerade krav på dokumentation av varje enskilt val av åtgärd (snarare än "Statement of Applicability" som i ISO 27001) driver kostnader utan att höja säkerheten.
- **Förslag:** Förenkla kravet till att verksamhetsutövaren ska kunna redovisa vilka säkerhetsåtgärder som tillämpas för att skydda kritiska tillgångar.b

3 kap. 4 §: Fokus på administration i stället för förmåga

- **Synpunkt:** MSB:s förslag lägger fokus på dokumentation av processen (uppdaterade planer, involverade roller), medan EU-förordningen fokuserar på teknisk förmåga .
- **Motivering:** Ett dubbelt arbete för svenska företag som måste bygga säkra system enligt EU-standard men dessutom måste producera specifik svensk dokumentation.
- **Förslag:** Ensa med genomförandeförordningen.

3 kap. 4 §: kravet på "Etablerade metoder" (3 kap. 4 § p 5)

- **Synpunkt:** Begreppet "etablerade metoder" är för vagt.
- **Motivering:** NIS2 genomförandeförordning är betydligt mer specifik och nämner Zero Trust-arkitektur, Security-by-Design och säker kodning som etablerade metoder. MSB:s formulering ger ingen vägledning om vilken säkerhetsnivå som förväntas.
- **Förslag:** Ensa med genomförandeförordningen.

3 kap. 4 §: kravet på "Etablerade metoder" (3 kap. 4 § p 5)

- **Synpunkt:** Kravet på att informationsklassning och riskanalys ska vara *genomförd* (i dåtid) inför utveckling motverkar iterativt säkerhetsarbete.
- **Motivering:** I systemutveckling sker riskanalys och klassning kontinuerligt och iterativt. Att kräva en färdig riskanalys innan utveckling rimmar illa med *Security-by-Design*.
- **Förslag:** Formulera om till att riskanalys är en *integrerad del* av utvecklingslivscykeln.

3 kap. 4 §: Hantering av testdata (Saknas i MSB-förslaget)

- **Synpunkt:** Föreskrifterna saknar explicita krav på skydd av testdata, vilket är en allvarlig brist jämfört med EU-rätten.
- **Motivering:** EU 2024/2690 ställer explicita krav på anonymisering och sanering av data som används i testmiljöer. Detta är en av de vanligaste sårbarheterna i systemutveckling.
- **Förslag:** Inför ett explicit krav på hantering och skydd av data i utvecklings- och testmiljöer, i linje med genomförandeförordningen bilaga 1 punkt 6.2.2.

3 kap. 5-13 §§: Saknar spårbarhet

3 kap. 14 §: Utveckling och IT/OT-uppdelning

- **Synpunkt:** Begreppen "produktionsmiljöns it-segment" och "produktionsmiljöns ot-segment".Denna uppdelning saknar definition i CSL och genomförandeförordning.
- **Analys:** IT och OT konvergerar. Krav på "avskilda miljöer" för IT-segment men bara "riskidentifiering" för OT-segment är inkonsekvent och svårtolkat.
- **Förslag:** Ensa begreppen med genomförandeförordningen och CSL

3 kap. 15 §: Saknar spårbarhet

3 kap. 16 §: Digital identitet

- **Synpunkt:** Att "digitala identiteter som används i produktionsmiljön inte används i utvecklings-, test- och utbildningsmiljjö" är tekniskt och administrativt betungande.
- **Motivering:** Att tvinga fram helt separata identiteter för samma person i olika miljöer skapar en komplex struktur som är dyr att förvalta. EU:s genomförandeförordning ställer krav på separation av miljöer och data, men inte nödvändigtvis på identiteten.
- **Förslag:** Fokusera på funktionell separation.

3 kap. 17-18 §§: Saknar spårbarhet

3 kap. 19 §: Multifaktorautentisering (MFA)

- **Synpunkt:** Kravet på MFA vid åtkomst till system som behandlar information som vid informationsklassning bedömts ha behov av utökat skydd kan vara ofungerande.
- **Analys:** EU kräver MFA "in accordance with the classification of the asset". I t ex ett kontrollrum kan operatörer dela arbetsstation. Krav på MFA kan fördröja ingripanden vid driftstörningar. MSB:s krav riskerar här att sänka cybersäkerheten. Kostnaden för MFA i legacymiljöer kan vara stor om moderna autentiseringsprotokol lnte stöds.

3 kap. 20-27 §§: Saknar spårbarhet

3 kap. 28 §: Krave på UTC (SP)

- **Synpunkt:** Kravet på att tiden ska vara spårbar specifikt till "den svenska tillämpningen av koordinerad universell tid, UTC (SP)" bör tas bort eller ändras till en rekommendation.
- **Motivering:** En reglering som saknas i genomförandeförordningen. Där ska tiden vara synkroniserad med en tillförlitlig referenskälla (UTC) för att möjliggöra loggkorrelation. En svensk särreglering skapar hinder för användning av globala molntjänster och standardiserad hårdvara som ofta använder andra, likvärdiga UTC-källor.
- **Förslag:** ta bort kravet.

3 kap. 28 §: Robust tid

- **Synpunkt**: Begreppet "robust tid" är inte definierat.
- **Motivering**: Teknistk kan "robust tid" innebära lokal redundans för att klara avbrott i extern signal. Att införa detta brett är kostnadsdrivande utan proportion till risken.
- **Förslag:** Ensa med genomförandeförordningenL.

3 kap. 29-31 §§: Saknar spårbarhet

3 kap. 32 §: Kryptering

- **Synpunkt:** Binärt krav, kryptering *ska* ske om informationen har "behov av utökat skydd". MSB missar att specificera kraven på hur nycklarna skyddas.
- **Analys:** EU förespråkar en riskbaserad ansats där kryptering används "om lämpligt". I många OT-protokoll tillåter inte svarstiderna den latens som kryptering inför. Kryptering med dålig nyckelhantering är meningslös.
- **Förslag:** Ensa med genomförandeförordningenL.

3 kap. 33-42 §§: Saknar spårbarhet

4 kap. 1-8 §§: Saknar spårbarhet

5 kap. 1-4 §§: Saknar spårbarhet och skapar extra börda för offentlig förvaltning