Svar på remiss gällande förslag till: **Föreskrifter och allmänna råd om säkerhetsrevision och säkerhetsskanning, Diarienummer MCF 2026-06325**

Svarande organisation: **Stiftelsen för Internetinfrastruktur (Internetstiftelsen)**

Intern referens: **Legal**

För generella kommentarer välj "Generellt" under kolumn Kapitel.
För kommentarer som gäller allmänna råd välj "Allmänna råd" under kolumn annars välj det kapitel du vill lämna synpunter på.
Välj i kolumn Paragraf vilken paragraf du vill lämna synpunkt på
Välj i kolumn Punkt vilken punkt i paragrafen dina kommetarer avser både om de avser paragraf eller allmännt råd.

Synpunkter på konsekvensutredningen lämnas på filken Konsekvensutredningen

Vänligen skicka dina svar i excelformat för att underlätta sammanställningen av synpunkter.

Synpunkter föreskrifter och allmänna råd

Kapitel	§	Punkt	Synpunkt	Förslag till ändring	Kommentar
kap. 1	3		"Viktig samhällsfunktion" är ett nytt begrepp.		Se över om inte befintligt begrepp kan användas, istället för en ny definition.
kap. 1	3		Säkerhetsrevision = Revisionen ska kunna visa på nivån av cybersäkerhet i systemen		Den är svår att tillämpa, vad innebär nivå? Cybersäkerhetslagen kräver att säkerhetsåtgärder ska vara “lämpliga och proportionella” och utgå från risk, och den anger även att åtgärderna ska bedömas om de är effektiva i sin implementering eller inte.
kap. 2	4		Felstavning "säkerhetsrevsion"		
kap. 2	1		Det bör också framgå att kraven ska gälla de personer som faktiskt utför uppdraget, inte bara den juridiska personen.		
kap. 2	2	Allmänna råd	Bör det finnas en karenstid efter rådgivningsuppdrag hos den granskade verksamhetsutövaren?		Allmänna rådet säger att tillsynsmyndigheten “bör inte anlita” organ med affärsrelationer, rådgivningsuppdrag eller andra beroendeförhållanden.
kap. 2	2	2	Texten säger att information inte får nyttjas för annat än revisionen. Det är bra, men den bör även reglera eller åtminstone nämna krav på säker hantering, åtkomstbegränsning, lagring, överföring, gallring/radering, hantering av sårbarhetsinformation och incidentrapportering om revisionsmaterial röjs.		Detta är särskilt viktigt eftersom revision och skanning kan ge mycket känslig information om svagheter i samhällsviktiga system.
kap. 2	4		Det bör tydliggöras vilka krav, kriterier eller bedömningsgrunder som avvikelser ska bedömas mot. Detta är viktigt för att säkerhetsrevisioner ska bli jämförbara, rättssäkra och användbara som underlag i tillsynen.		Det bör framgå om avvikelser ska bedömas mot cybersäkerhetslagen, föreskrifter, tillsynsmyndighetens uppdrag, verksamhetsutövarens egna styrande dokument, avtal, standarder eller en kombination av dessa.
kap. 2	4		Det bör framgå vad resultatet minst ska innehålla: omfattning, metod, granskningskriterier, avgränsningar, iakttagelser, avvikelser, riskbedömning, allvarlighetsgrad, bevisning/underlag, begränsningar och eventuella rekommendationer.		Risken är att det ser väldigt olika ut hos olika verksamhetsutövare.

kap. 2	5		Formuleringen att revisionen inte ska vålla större kostnad eller olägenhet än nödvändigt är rimlig. Men den bör inte kunna användas för att begränsa en nödvändig granskning. Det kan därför vara värt att föreslå ett förtydligande om att revisionen ska vara proportionerlig i förhållande till risk, verksamhetens betydelse och granskningens syfte.		
kap. 2	10		"Information om identifierade brister och sårbarheter ska hanteras så att uppgifterna inte röjs för obehöriga. "		Överväg tydligare hänvisning till sekretess-regler?
kap. 3	1		"har rådighet över."		Det är något löst begrepp. Överväg att tydliggöra "ha rådighet över". Bestämmelsen riskerar annars att skapa osäkerhet vid just de vanligaste fallen: molntjänster, utkontrakterad drift, koncernmiljöer, delade plattformar och leverantörskedjor. En verksamhetsutövare kan ha ansvar för säkerhetsåtgärder i ett system utan att ha obegränsad rätt att låta en tillsynsmyndighet skanna hela den tekniska miljön.
kap. 3	4		Det bör förtydligas i kapitel 2 paragraf 4 vad som är tillräckligt även vid en säkerhetsrevision då det kan tolkas som att det är tillräckligt för oberoende organ är det att likställa med intern och externrevision? Medan det i denna punkt står "En säkerhetsskanning ska utföras av en tillsynsmyndighet eller av en av tillsynsmyndigheten anlitad extern aktör."		
kap. 3	5		Den externa aktören.		Överväg Allmänna råd om den externa aktörens lämplighet och oberoende, jämför under kap. 2 1 §.
kap. 3	6		bör förtydligas vad är sektorskritiskt system, samt vem avgör detta?		kan kopieras in från föreskriften säkerhetsåtgärder då sektorskritisk system beskrivs där i 1kap., Ordförklaringar, 4§