EKONOMISTYRNINGSVERKET

Remissvar

Datum
2015-09-09
ESV dnr
3.4 - 573/2015
Handläggare
Annika Alexandersson
Ange handläggare 2

Ert datum
2015-09-15
Er beteckning
Ju2015/2650/SSK

Justitiedepartementet

Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten

Ekonomistyrningsverket (ESV) svarar på remissen om strategi och åtgärder för säker informations – och cybersäkerhet i staten. ESV avgränsar sitt svar till följande tre mål i den av utredningen föreslagna strategin. De tre målen är att stärka styrning och tillsyn inom området, att staten ska ställa tydliga krav vid upphandling på it-området och att samtliga statliga myndigheter rapporterar it-incidenter. När det gäller de förslag som berör statlig internrevision, intern styrning och kontroll samt myndighetsförordningen (2007:515) svarar ESV utifrån de uppgifter som framgår av vår instruktion. Sammanfattningsvis vill ESV framföra att:

- ESV anser att informationssäkerhetsområdet är viktigt för internrevisionen men att det inte behövs ytterligare reglering. Den statliga internrevisionens uppgift enligt internrevisionsförordning (2006:1228) är att granska myndighetens interna styrning och kontroll i all verksamhet som myndigheten bedriver och/eller ansvarar för, vilket även omfattar informationssäkerhet. ESV avstyrker därför förslaget som rör internrevisionsförordningen.

- ESV avstyrker förslaget om ett tillägg i myndighetsförordningen eftersom vi anser att det redan i dag framgår tydligt att myndighetens ledning ansvarar för hela myndighetens verksamhet inför regeringen (Myndighetsförordning (2007:515) 3 §). Informationssäkerhet ingår som en del av myndighetens verksamhet. Det finns därför inget behov att i myndighetsförordningen (2007:515) införa ett tillägg för att särskilt förtydliga myndighetsledningens ansvar för att upprätthålla säkerheten i myndighetens informationshantering.

- ESV avstyrker förslaget om att i förordningen (2000:605) om årsredovisning och budgetunderlag införa en bestämmelse om att en tilläggsupplysning om genomförd internrevision och status för myndighetens informationssäkerhetsarbete ska lämnas i myndighetens årsredovisning. ESV anser inte att det är sakligt motiverat att ha särskilda intyganden för enskilda områden. Ett övergripande intygande lämnas redan i dag av myndighetensledningarna när det gäller myndigheter med internrevision.

Drottninggatan 89
Box 45316
104 30 Stockholm

Tfn 08-690 43 00
Fax 08-690 43 50
www.esv.se
registrator@esv.se

Bankgiro 5052-6854

Org.nr/F-skattebevis
202100-5026
SE202100502601 (EU)

Faktureringsadress
Ekonomistyrningsverket
FE 27
838 73 Frösön

- ESV välkomnar regeringens initiativ inom området informationssäkerhet men vill samtidigt inte att regleringen ska ha en sådan omfattning att den riskerar att hämma säkerhetsutvecklingen i staten genom en alltför centralstyrd skyddsnivålösning. ESV:s uppfattning är att det är viktigt att styrmodellen är balanserad så att den inte begränsar myndighetens eget ansvar och försvårar för myndigheterna att anpassa sig till nya situationer.

- ESV stöder inte utredningens förslag till uppgifter för det föreslagna statliga myndighetsrådet. Av de uppgifter som föreslås i förslaget till ny förordning är det endast uppgiften att rådet ska fungera som referens- och beredningsgrupp som ESV anser vara lämplig.

- ESV stöder förslaget att ta fram en standard för informationssäkerhet och att denna ska användas vid kravställning i upphandling men vill påpeka att detta redan idag görs i stor utsträckning.

- ESV stöder förslaget att den nya upphandlingsmyndigheten får i uppdrag att ge stöd till myndigheter i informationssäkerhetsfrågor kopplade till upphandling.

- ESV stöder inte utredningens förslag att det bör införas krav på att rapportera vilken leverantör som en statlig myndighet har valt då ramavtal rörande IT-lösningar används.

- ESV är tveksam till utredningens förslag att för tjänster och produkter som ska användas för kommunikation inom staten tillämpa lagen om upphandling på försvars- och säkerhetsområdet, om upphandling enligt lagen om offentlig upphandling inte medger att nödvändiga krav ställs. ESV tror att detta kan motverka vissa syften med offentlig upphandling bland annat vad gäller god konkurrens.

- ESV anser inte att det är möjligt att utifrån den konsekvensutredning som gjorts bedöma vad utredningens förslag kommer att kosta eller hur det ska finansieras.

- ESV stöder förslaget om att införa en ny förordning för statliga myndigheters informationssäkerhet.

ESV lämnar även synpunkter som mer direkt berör utformningen av och begrepp i den av utredningen föreslagna förordningen.

Styrning och tillsyn av informationssäkerheten i staten stärks

a) Utredningen föreslår att en nationell styrmodell för informationssäkerhet etableras för att skapa ett systematiskt informationssäkerhetsarbete i statlig verksamhet. Förslaget avser i första hand de statliga myndigheterna och ska vara normerade för dem men styrmodellen kan på sikt utvecklas till att omfatta hela den offentliga sektorn.

ESV anser att en central styrmodell som omfattar skyddsnivåer[1] och skyddsåtgärder riskerar att hämma säkerhetsutvecklingen i staten. En centralstyrd skyddsnivålösning kan svårligen fungera i praktiken med dagens informationsflöden och teknikutveckling. Det är viktigt att styrmodellen är balanserad och inriktar sig enbart på kravnivåer.[2] En alltför strikt styrningsmodell är i konflikt med 5 § i den föreslagna förordningen gällande myndigheters ansvar. Konflikten och otydligheten gällande ansvar gör att strategin blir svår att genomföra och dess praktiska tillämning svår att granska.

b) Utredningen föreslår att det bör inrättas ett statligt myndighetsråd för informationssäkerhet bestående av företrädare för de relevanta myndigheterna på området.

ESV är tveksam till om ett råd sammansatt med företrädare från myndigheterna är tillräckligt för uppgiften att bistå med expertkompetens. De som sitter i rådet har inte möjlighet att från sin ordinarie anställning även arbeta med andra myndigheters informationssäkerhet. Förutom tidsaspekten så innebär expertstödet även risk för att rådet tar över myndigheternas ansvar enligt § 5 i den föreslagna förordningen. En annan brist är att förslaget inte samlar expertis från övrig offentlig sektor (kommuner och landsting).

ESV anser inte att det är lämpligt att Rådet ska ha den verkställande uppgiften att åtgärda brister i statens verksamhet. Rådet kan inte, som det är beskrivet med myndigheternas ansvar, se 5 § i förslaget till ny förordning, säkerställa att strategin verkställs. Rådets uppgift bör vara att stödja strategins genomförande enligt § 18 genom att enbart vara beredning- och remissinstans.

c) Utredningen föreslår att en ny förordning för statliga myndigheters informationssäkerhet bör införas för att tydliggöra ett ökat ansvar för det praktiska säkerhetsarbetet inom myndigheterna.

ESV stöder förslaget att införa en ny förordning. Vi har dock några synpunkter på förslaget och hade gärna sett att en ordlista bifogats till utredningen.

---

[1] Skyddsnivå – Hur myndigheten ska skydda sin information.
[2]. Kravnivå – olika krav på informationssäkerhet som myndigheten ska uppfylla.

Enligt 7 § i förslaget till ny förordning står det att myndigheten ska följa utvecklade krav och skyddsnivåer.

ESV anser att det vore bättre att begränsa detta till kravnivåer då myndigheter redan har ansvar för kravnivåernas uppfyllande, vilket ger skyddsnivån för information. I 5 § skriver man att varje myndighet ansvarar för att upprätthålla en tillräcklig nivå av informationssäkerhet. Användning av skyddsnivåer kan misstolkas och felaktigt lägga ansvaret för bedömning av vilket skydd man behöver utanför myndigheten. (Se även förslaget till ny säkerhetsskyddslag.)

I 10 § i förslaget till ny förordning anges att kraven i § 5-9 bara gäller "i tillämpliga delar" om man är en s.k. värdmyndighet.

ESV anser att tillämpning av § 5-9 bör gälla även för en värdmyndighet[3]. Detta eftersom informationssäkerheten alltid ska motsvara de krav som följer med den anlitande myndighetens information och som värdmyndigheten i sin tur hanterar. Det är också svårt att tolka vad som motiverar undantag och därmed att bedöma efterlevnaden hos en värdmyndighet.

Enligt 17 § i förslaget till ny förordning ska IT-incidenter rapporteras in till MSB.

ESV anser att begreppet" IT-incidenter" är för brett då det omfattar alla typer av IT relaterade händelser vilket är en ohanterlig mängd och i sammahanget innehåller en mängd ointressanta uppgifter. ESV anser att begreppet IT-säkerhetsincidenter är att föredra om det enbart är teknikknutet, alternativt informationssäkerhetsincidenter om man avser att få med även fysiska eller administrativa händelser som påverkar informationssäkerheten.

I 18 § i den föreslagna förordningen står det att rådet har till uppgift att "utgöra en gemensam beredning- och remissinstans på informationssäkerhetsområdet". Vidare står det i 18 § att rådet ska" utveckla krav- och skyddsnivåer".

ESV anser att detta kan tolkas som att rådet skulle ansvara för att utveckla både krav och skyddsnivåer. ESV anser att det är olämpligt att lägga ansvaret för utveckling av krav och skyddsnivåer på en beredning- och remissfunktion.

d) Utredningen anser att myndigheternas internrevision behöver utvecklas till att inkludera uppföljning och kontroll av myndigheternas informationssäkerhet samt att myndighetsledningens ansvar för att upprätthålla säkerhet i sin informationshantering bör förtydligas genom ett författningsreglerat rapporteringskrav. (Sammanfattningen sidan 17.)

[3] Värdmyndighet - Exempelvis Statens servicecenter och ESV (Hermes, Avropa).

ESV delar inte bedömningen att regelverket för internrevision behöver utökas till att inkludera uppföljning och kontroll av myndigheternas informationssäkerhet. ESV vill här påpeka att ansvaret för myndighetens uppföljning och kontroll inte ligger på internrevisionen. Man brukar här tala om de tre ansvarslinjerna. Första ansvarslinjen är den interna kontrollen i myndighetens operativa verksamhet. Den andra ansvarslinjen är myndighetens egen uppföljning och kontroll av den operativa verksamheten. Den tredje ansvarslinjen är internrevisionens granskning och bedömning av att den interna kontrollen och uppföljningen i myndigheten har fungerat på avsett vis. Internrevisionen ska med andra ord granska den interna uppföljningen och kontrollen, inte utföra den. Förslaget verkar bygga på missförstånd vad gäller internrevisionens roll och ansvar samt innebörden av den reglering som redan finns på plats. Det kan även vara så att utredningen har förväxlat de "interna revisioner" som ska genomföras enligt ISO 27001 med statlig internrevision som ska genomföras enligt Internrevisionsförordning (2006:1228).

Enligt internrevisionsförordningens 6 § ska internrevisionen omfatta den verksamhet som myndigheten bedriver och ansvarar för. Där ingår även informationssäkerhet.

Utredningen föreslår även att det i myndighetsförordningen (2007:515) införs ett tillägg för att förtydliga myndighetsledningens ansvar för att upprätthålla säkerheten i myndighetens informationshantering. (Avsnitt 9.2.5)

ESV tillstyrker inte utredarens förslag då vi anser att det redan i dag framgår tydligt att myndighetens ledning ansvarar för hela myndighetens verksamhet inför regeringen (Myndighetsförordning (2007:515) 3 §). Informationssäkerhet ingår som en del av myndighetens verksamhet.

ESV anser att informationssäkerhet redan innefattas i myndigheternas interna styrning och kontroll, så det är oklart vad förslaget med denna punkt i strategin tillför för nytt. Betänkandet tar upp också upp den nuvarande tolkningen på sidan 89:

Utredningen föreslår att det i förordningen (2000:605) om årsredovisning och budgetunderlag införs en bestämmelse om att en tilläggsupplysning om genomförd internrevision och status för myndighetens informationssäkerhetsarbete ska lämnas i myndighetens årsredovisning. (Avsnitt 9.2.5)

För de 67 internrevisionsmyndigheterna lämnar myndighetsledningarna redan i dag ett intygande i årsredovisningen att den interna styrningen och kontrollen är betryggande. ESV anser inte att det är sakligt motiverat att ha särskilda intyganden för enskilda områden när ett övergripande intygande redan lämnas. Om det finns brister inom området informationssäkerhet så bör det redan i dag redovisas som en brist i den interna styrningen och kontrollen. Det man däremot kan diskutera är om

det finns ett behov av att myndigheterna lämnar en beskrivning av sitt informationssäkerhetsarbete i årsredovisningen och om antalet myndigheter som lämnar en bedömning av sin interna styrning och kontroll ska utökas.

Utredningen föreslår att internrevisionen ska genomföra granskningar inom området informationssäkerhet varje år. (Avsnitt 9.2.5)

Statlig internrevision utgår från risk och väsentlighet. Internrevisionen genomför en analys av myndighetens risker. Riskanalysen ska enligt god internrevisionssed även omfatta informationssäkerhet.[4] Utifrån riskanalysen tar internrevisionen fram ett förslag till revisionsplan. Revisionsplanen ska godkännas av myndighetens ledning. Myndighetsledningen kan göra en annan bedömning av myndighetens risker och besluta om ändringar i förslaget till revisionsplan. Internrevisionen brukar inte granska alla områden varje år men följer alltid upp att myndigheten har åtgärdat de iakttagelser som internrevisionen tidigare har rapporterat. Det är myndighetsledningens ansvar, inte internrevisionens, att säkerställa att det finns en tillräcklig intern styrning och kontroll i myndighetens processer.

Mot bakgrund av ovanstående avstyrker ESV förslaget om att internrevisionens årligen skulle granska informationssäkerhet.

Staten ställer tydliga krav som upphandlare av tjänster som innehåller informationshantering eller av it-tjänster

a) Utredningen anser att statlig upphandling på it-området bör innehålla hänvisning till för staten gällande standarder och krav på certifiering i de situationer där säkerhetsnivåer har fastställts för respektive myndighet.

ESV stöder förslaget att ta fram en standard för informationssäkerhet och att denna ska användas vid kravställning i upphandling. Detta görs dock redan idag i stor utsträckning.

ESV tillstyrker också förslaget om att den nya upphandlingsmyndigheten får i uppdrag att stödja myndigheter i informationssäkerhetsfrågor kopplade till upphandling.

b) Utredningen anser att Myndigheten för samhällsskydd och beredskap bör ges i uppdrag att ta fram minimikrav på säkerhet i vanligt förekommande it-produkter som används av statliga myndigheter.

Vad gäller förslaget att ta fram skyddsnivåer som anger minimikrav finns, som utredningen nämner, både för- och nackdelar. ESV anser att det är viktigt att beakta förslaget kan leda till att myndigheterna inte tänker på vad som är bäst i varje enskild situation om det finns färdiga säkerhetsåtgärder/skyddsnivåer. Samtidigt

[4] International Professional Practice Framework (IPPF) 2013, standard 2120.A1

kan förslaget leda till att myndigheterna blir bättre som beställare på området. Ett alternativ skulle vara att ge MSB i uppdrag att stödja och vägleda upphandlande myndigheter istället för att ta fram färdiga skyddsprofiler.

c) Utredningen anser att det bör införas krav på att rapportera vilken leverantör som en statlig myndighet har valt då ramavtal rörande it-lösningar används.

ESV stöder inte i förslaget att det bör införas ett krav på att rapportera vilken leverantör en statlig myndighet valt då ramavtal rörande it-lösningar används. ESV har svårt att förstå vad syftet med ett sådant register skulle vara och vad det skulle bidra till. ESV menar också att det inte är helt okomplicerat för den myndighet som ska ta emot all rapportering att hålla registret uppdaterat.

d) Utredningen anser att när det gäller tjänster och produkter som ska användas för kommunikation inom staten bör upphandlande myndighet överväga möjligheten arr tillämpa lagen om upphandling på försvars- och säkerhetsområdet, om upphandling enligt lagen om offentlig upphandling inte medger att nödvändiga krav ställs.

ESV ställer sig frågan om inte ett överdrivet användande av LUFS kan komma att motverka vissa syften med offentlig upphandling, bland annat vad gäller god konkurrens.

Konsekvensutredningen

ESV har följande synpunkter på utredningens konsekvensutredning:

a) Utredningen föreslår att förslaget finansieras genom en omdisponering av medel från utgiftsområdena 06, 02 eller 22. (Sammanfattningen sidan 20.)

Någon närmare precisering av varifrån eller hur denna omdisponering ska göras har inte lämnats. Utan att en närmare precisering av hur medel ska omdisponeras kan inte frågan om finansiering av lämnade förslag anses vara behandlade i tillräcklig omfattning av utredningen.

ESV anser att det kommer att innebära att mycket resurser tillförs för att ta fram skyddsnivåer samtidigt som det egentliga skyddet och medföljande kostnader uppstår hos respektive myndighet där också ansvaret ligger. Det är oklart vad den egentliga kostnaden kommer att vara.

Under avsnitt 10.2.1 står även att en nationell styrmodell förutsätter en väl utvecklad kunskapsstyrning. Kunskapsstyrning måste antas innebära kunskapsöverföring i någon form. Kunskapsöverföringen innebär normalt ett ökat resursbehov både för den personal som ska överföra kunskap men även för framtagandet av informations- och utbildningsmaterial.

Det är inte möjligt att ta ställning till de kostnadsbedömningar vad gäller MSB som utredningen har lämnat i konsekvensanalysen. I konsekvensutredningen antas det finnas behov av ett visst antal tjänster för att hantera en ökad arbetsbelastning på MSB. För att kunna bedöma om dessa kostnadsökningar är rimliga finns det ett behov av att ta del av de beräkningar kopplade till den ökade arbetsbelastningen (antal ärenden, tid per ärende m.m.) som de ökade arbetsuppgifterna genererar. En ytterligare precisering av beräkningarna som ligger bakom bedömningarna vore värdefullt att få ta del av.

ESV anser att kostnaden för expertstödet till andra myndigheter borde ha särredovisats i konsekvensanalysen.

Generaldirektör Mats Wikströmhar beslutat i detta ärende. Utredare Annika Alexandersson har varit föredragande. I beredningen har också avdelningschef Eva Lindblom, avdelningschef Peter Öhlén, informationssäkerhetsansvarig Anne Samuelsson, utredare Karolin Knutsen-Öy, utredare Patrick Freedman och enhetschef Tina J Nilsson medverkat.

Mats Wikström
Generaldirektör

Annika Alexandersson
Utredare