Helena Andersson
Avdelningen för risk- och sårbarhetsreducerande arbete
Verksamheten för samhällets informations- och cybersäkerhet
073-026 11 33

Konsekvensutredning rörande reviderade föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet

A. Allmänt

1.1 Beskrivning av problemet och vad man vill uppnå

1.1.1 Informationssäkerhet – beroenden och utmaningar

Bristande informationssäkerhet, det vill säga bristande tillgänglighet till informationen när den behövs eller brister när det gäller spårbarhet respektive skydd mot obehörig åtkomst eller förändring, kan få både allvarliga och direkta konsekvenser för såväl enskilda och organisationer som samhället i stort.

Svenska myndigheter hanterar idag en mängd information med stor betydelse för en rad olika samhällsfunktioner. Denna information behöver kunna skyddas mot obehörig åtkomst (skydd av informationens konfidentialitet) men behöver även vara tillgänglig för behöriga när den ska användas (skydd för informationens tillgänglighet). I vissa fall är behovet av tillgänglighet så högt att några avbrott i praktiken inte är acceptabla. Informationen behöver även skyddas mot obehöriga förändringar (skydd av informationens riktighet). För att säkerställa att dessa behov upprätthålls är det av grundläggande betydelse att det i efterhand går att spåra vem som har gjort vad i myndigheternas system (skydd av informationens spårbarhet) – något som även befintlig lagstiftning ställer krav på.

Säkerhet för information uppnås inte enbart genom att införa olika säkerhetsåtgärder utan det är även av grundläggande vikt att på ett systematiskt sätt fortlöpande styra arbetet med informationssäkerhet i syfte att planera, genomföra, kontrollera, följa upp, utvärdera, rapportera och förbättra säkerheten i myndighetens informationshantering. Detta ger sammantaget möjlighet att upprätthålla en lämplig nivå av säkerhet som är anpassad till bland annat verksamhetens behov, rättsliga krav samt identifierade hot och risker. Som stöd för ett sådant systematiskt arbete används ett *ledningssystem för informationssäkerhet* (LIS).

LIS beskriver en process för informationssäkerhetsarbete inom en verksamhet som består av policy, regler, förslag till skyddsåtgärder och processer. LIS utgår ifrån att det är nödvändigt med en helhetssyn på informationssäkerhet som

täcker in alla delar. Skälet till det är att man inte kan åstadkomma god säkerhet utan tydliga regler, personella resurser, tekniska skyddsåtgärder, administrativa rutiner och uppföljning, d.v.s. samma komponenter som krävs i vilket annat kvalitetsarbete som helst.

1.1.2 Skäl för revidering

Det finns flera skäl till att författningen om statliga myndigheters informationssäkerhet, MSBFS 2009:10, behöver revideras. Ett skäl är att de standarder som författningen hänvisar till har upphört att gälla och ersatts av nya versioner. En annan grundläggande anledning är att MSB:s kartläggning av myndigheternas tillämpning av de nu gällande föreskrifterna uppvisar påtagliga brister, vilket ställer krav på åtgärder. Behovet av förbättrad informationssäkerhet har även uppmärksammats av Riksrevisionen i en granskningsrapport från 2014[1] samt i utredningen ”Informations- och cybersäkerhet i Sverige”, SOU 2015:23.

Uppdaterade standarder

Enligt det uppdrag som MSB har att utfärda föreskrifter om statliga myndigheters informationssäkerhet ska myndigheten beakta nationella och internationella standarder när föreskrifter meddelas. I de nu gällande föreskrifterna om statliga myndigheters informationssäkerhet MSBFS 2009:10 hänvisas det till de ledande standarderna på området, det vill säga standarderna för *ledningssystem för informationssäkerhet* ISO/IEC 27001 och ISO/IEC 27002. Dessa standarder har nyligen ersatts av nyare utgåvor.

MSB bedömer att de förändringar som de nya versionerna av standarderna innebär ger i sig tillräckliga skäl att se över föreskriftens utformning i sin helhet vilket även kan påverka sättet på vilket standarderna beaktas i författningen.

Bristande efterlevnad av nu gällande krav och nya utmaningar

En central fråga för MSB i samband med revideringen av MSBFS 2009:10 är att säkerställa att författningen utgör ett ändamålsenligt stöd för myndigheternas informationssäkerhetsarbete.

Statliga myndigheter har sedan 2008, genom både föreskrifter från Verva och MSB, haft krav på sig att arbeta systematiskt med informationssäkerhet och i detta utföra informationsklassning och riskanalyser, ta fram en informationssäkerhetspolicy och hantera identifierade risker. Särskilda krav har ställts på att följa upp och utvärdera myndighetens informationssäkerhetsarbete.

I syfte att följa upp och kartlägga de statliga myndigheternas arbete med informationssäkerhet genomförde MSB under våren 2014 en enkätundersökning. I enkätundersökningen ställdes dels frågor med koppling

[1] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23, http://www.riksrevisionen.se/PageFiles/20759/RIR_2014_23_infos%c3%a4kerhet_Anpassad.pdf

till föreskrifterna, dels frågor som hade till syfte att belysa utvecklingen på it- och informationshanteringsområdet av betydelse för informationssäkerhets-arbetet. Enkäten skickades ut till samtliga statliga myndigheter som omfattades av MSB:s föreskrifter och drygt 95 % besvarade den. Kartläggningen gav en god bild av hur myndigheterna själva uppfattade sitt arbete med informationssäkerhet och hur de arbetade med föreskrifternas olika krav. Resultaten sammanställdes i rapporten ”*En bild av myndigheternas informationssäkerhetsarbete 2014*”.[2]

Även om några få resultat uppvisade en bättre situation än väntat tydliggjorde kartläggningen att det fanns ett stort antal påtagliga brister där det tydligt framgick att många myndigheter inte uppfyllde föreskrifternas krav på informationssäkerhet.

Som nämndes ovan uppmärksammade även Riksrevisionen behovet av förbättrad informationssäkerhet. Riksrevisionen sammanfattade kartläggningens resultat i sin granskningsrapport på följande sätt:

”Enskilda svar i uppföljningen kan uppfattas som positiva. En samlad läsning av svaren visar dock att även om 84 % av myndigheterna uppger att de har en informationssäkerhetspolicy så svarar 38 % att kompetens, mandat eller resurser är otillräckliga för att utföra arbetet på ett tillfredsställande sätt, 42 % att det saknas regler för vad riskanalysen ska omfatta eller när den ska ske och 65 % att de saknar kontinuitetsplan. Riksrevisionens bedömning är därför att en stor andel myndigheter inte har centrala delar av ett systematiskt informationssäkerhetsarbete på plats.”

Mot bakgrund av detta rekommenderade Riksrevisionen i sin granskningsrapport att ”MSB bör lämna de myndigheter som inte uppfyller kraven i föreskrifterna om statliga myndigheters informationssäkerhet (MSBFS 2009:10) det stöd som är nödvändigt, så att de uppnår efterlevnad inom rimlig tid”.[3]

Den senaste utvecklingen inom teknik och tjänsteområdet är ytterligare en utmaning som ställer nya krav på informationssäkerhetsarbetet. Många myndigheter använder sig idag av gemensamma e-förvaltningstjänster och har utkontrakterat sin informationshantering. Myndigheternas informationshantering har därför, ibland till och med i stora delar, förändrats och utvecklats i förhållande till hur det såg ut när de nu gällande föreskrifterna trädde ikraft. Även detta är ett skäl till en översyn av föreskrifterna om statliga myndigheters informationssäkerhet.

---

[2] Rapporten är publicerad på MSB:s webbplats https://www.msb.se/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014/

[3] Riksrevisionen, Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23, s 13

Bristernas orsaker

De påvisade bristerna ger en tydlig indikation på att stödet för myndigheternas systematiska informationssäkerhetsarbete inte varit tillräckligt. Olika brister kan dock vara av olika allvarlig karaktär och ha olika påverkan på säkerheten i en organisations informationshantering. MSB har med anledning av detta kompletterat kartläggningens resultat med en konsekvensanalys för att kunna bedöma hur allvarliga de påvisade bristerna är ur ett informationssäkerhetsperspektiv.

För att närmare utreda orsakerna bakom dessa brister, och hur de kan motverkas genom revidering av föreskrifterna MSBFS 2009:10, har MSB analyserat ca 35 olika rapporter från revisioner och granskningar av informationssäkerhet hos ett 20-tal myndigheter. MSB har i mars 2015 även genomfört djupintervjuer med informationssäkerhetschefen eller motsvarande på 13 olika myndigheter.

Efter genomförda analyser har MSB gjort bedömningen att orsakerna till de brister som påvisats i myndigheternas systematiska informationssäkerhetsarbete är flera. Det handlar exempelvis om nya utmaningar vad gäller hot och sårbarheter, en snabb utveckling på it-området, nya informationssäkerhetskrav genom användning och utveckling av gemensamma it-tjänster samt bristande kravställning när det gäller systematiskt och riskbaserat arbete med informationssäkerhet. Bristerna behöver åtgärdas, särskilt med beaktande av den betydelse myndigheternas informationshantering har för samhällets funktioner.

1.1.3 Vad som behöver åstadkommas

MSB gör bedömningen att det finns ett tydligt behov av att vidta åtgärder för att ytterligare förbättra och konkretisera stödet för statliga myndigheters informationssäkerhetsarbete. Vid sidan av behovet av ytterligare vägledningar och annat stöd har genomförda analyser, både av granskningsrapporter och djupintervjuer, även visat på betydelsen av central styrning och tydliga krav på området.

Innan föreskrifter fanns på området var ofta informationssäkerhetsarbetet av lägre prioritet för många myndigheter. Av de myndigheter som själva hanterar sin information och informationssäkerhet har idag en övervägande majoritet en informationssäkerhetspolicy och har även utsett en informationssäkerhetschef eller motsvarande för att leda och samordna arbetet. Båda åtgärder är uttryckliga krav i nu gällande föreskrifter.[4]

Föreskrifterna bidrar till och utgör ett viktigt stöd för myndigheternas informationssäkerhetsarbete. Enkätresultat och analyser visar dock på, mot bakgrund av påvisade brister och orsaker, ett behov av att skapa ännu tydligare

[4] Uppgifterna framgår av rapporten ”En bild av myndigheternas informationssäkerhetsarbete” och är publicerad på MSB:s webbplats https://www.msb.se/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014/

krav på systematiskt och riskbaserat informationssäkerhetsarbete. Dessutom behöver kraven utformas på ett sådant sätt att de ger ett ännu starkare stöd för ett processbaserat arbete där exempelvis informationsklassning används som underlag för riskanalysarbetet. Föreskrifterna i sin nuvarande utformning har inte heller visat sig vara tillräckligt konkreta när det gäller resurser och ansvar. Dessa huvudpunkter behöver åtgärdas genom tydligare inriktning i nya föreskrifter. Närmare om vilka åtgärder som behöver vidtas framgår av 1.1.4.

Vid sidan av mer konkreta skrivningar i föreskrifterna tillhandahåller MSB stöd i form av exempelvis vägledningar och information. Stödet bedöms dock inte kunna ersätta mer konkret inriktning av arbetet i föreskriftsform utan endast komplettera denna.

1.1.4 Bedömda revideringsbehov för föreskrifterna

Mot bakgrund av det underlag som sammanställts inför översynen av föreskrifterna om statliga myndigheters informationssäkerhet, gör MSB bedömningen att flera av de brister som påvisats i de statliga myndigheternas informationssäkerhetsarbete behöver hanteras. I flera frågor bedömer MSB att det finns ett behov av en tydligare reglering på området.

Följande behov av revidering har bedömts behöva omhändertas genom föreskriftsförändringar.

Tillämpningsområdet

Vad gäller tillämpningsområdet är regleringen i stort sett identisk med MSBFS 2009:10. Ett undantag är dock införandet av en ny föreskrift rörande förhållandet då en myndighet överlåter till en annan myndighet att administrera sin informationshantering eller informationssäkerhet.

Den genomförda enkätundersökningen visade att ungefär en tredjedel av de statliga myndigheterna har överlåtit administrationen av all sin informationshantering eller all sin hantering av informationssäkerhet till en annan myndighet. Av de myndigheter som överlåtit administrationen hade dock ca 30 % inte reglerat förutsättningarna för och kraven på hur informationen ska hanteras och skyddas hos den andra myndigheten.

En överlåtelse kan, oavsett myndighetens storlek, aldrig innebära att ansvaret för informationssäkerheten överlåts. Detta gäller även om en annan myndighet administrerar informationshanteringen eller informationssäkerheten. Ansvaret innebär bland annat att den myndighet som äger och ansvarar för informationen behöver definiera förutsättningarna för arbetet. Det handlar exempelvis om att tydliggöra hur skyddsvärd den egna informationen är. Otydliga förutsättningar och krav kan innebära att informationen inte ges det skydd som den behöver.

Av de nu gällande allmänna råden till MSBFS 2009:10 framgår redan att en myndighet kan överlåta till en annan myndighet att utföra de uppgifter som åligger myndigheten men att detta inte påverkar ansvaret för informationen.

Enkätresultatet indikerar dock att det finns en brist på kunskap om vikten av en sådan överlåtelse och vad den innebär för det praktiska arbetet. MSB ser därför ett behov av att i de nya föreskrifterna tydliggöra detta.

Begreppsförklaringar

Avsnittet som innehåller begreppsförklaringar är nytt. MSB har här valt att närmare förklara vad som i författningens föreskrifter och allmänna råd närmare avses med ett antal centrala begrepp. Det handlar med andra ord inte om definitioner.

I föreskrifterna förtydligas vad som i föreskrifterna avses med informationssäkerhet. I de allmänna råden förklaras ytterligare ett antal begrepp.

Begreppet informationssäkerhet är av grundläggande betydelse för myndigheternas informationssäkerhetsarbete. Det huvudsakliga syftet med att införa begreppsförklaringarna är att skapa en samsyn hos berörda myndigheter rörande innebörden av begreppen. Genom att förklara ett antal av nyckelbegreppen kan författningstexten dessutom förenklas.

Ledningssystem för informationssäkerhet

Avsnittet med rubriken ledningssystem för informationssäkerhet är nytt. Här har föreskrifter som tydliggör myndighetens ansvar och ledningssystemets omfattning samlats. Inledningsvis förtydligas vilken information som myndigheterna ansvarar för. Dessutom betonas ledningssystemets betydelse och vikten av att utforma ledningssystemet på ett sådant sätt att det får en nära koppling till verksamheten och dess risker. Att med hjälp av ledningssystemet förtydliga både myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete ses även som centralt. Detta innebär att myndigheterna ska se till att ett antal roller och funktioner kommer på plats för att skapa förutsättningar för informationssäkerhetsarbetet. Vidare betonas att myndigheten ska se till att de befattningshavare som behöver utses för att leda och samordna arbetet får de befogenheter som krävs.

Redan i inledningen av *standarden ISO/IEC 27001* tydliggörs att allt organisationerna gör ska utgå från dess förutsättningar, miljö, intressenter och krav. Det viktiga med detta är betoningen på situationsanpassning – informationssäkerheten och hela ledningssystemet ska vara anpassat till den specifika verksamheten. Det finns även ett fokus på risker i standarden vilket uttrycks genom att flera krav ställs på hur informationssäkerhetsrisker bland annat ska identifieras, bedömas, hanteras och förebyggas. Dessutom betonas vikten av ledningens engagemang för informationssäkerhetsarbetet på ett tydligt sätt. Ledningen ska visa engagemang genom att exempelvis tillse att det för verksamheten finns avpassade mål, dokumenterad policy, tilldelade resurser, samt utdelat ansvar för informationssäkerhet inklusive återkoppling tillbaka till ledningen. Krav ställs även på att ledningen ska skapa medvetenhet om informationssäkerhet.

Enkätundersökningen visade brister på flera punkter avseende ledningens aktivitet för att främja informationssäkerhet. Närmare 30 % av de myndigheter som besvarade samtliga frågor i enkäten[5], det vill säga de som själva hanterar sin information och informationssäkerhet, saknade exempelvis en informationssäkerhetspolicy som beslutats av ledningen. Dessutom hade endast 75 % av de myndigheter som besvarade samtliga frågor i enkäten utsett en informationssäkerhetschef eller motsvarande.

Problembilden rörande ledningens roll och engagemang bekräftades i de *fördjupade analyser* som MSB genomförde. Det framkom bland annat att ledningen i många fall inte uppfattade sin egen betydelse för att ett fungerande och effektivt informationssäkerhetsarbete skulle komma till stånd i hela organisationen. Dessutom lyftes behovet av att den befattningshavare som hade till uppgift att driva informationssäkerhetsfrågorna hade rätt stöd, resurser och befogenhet för uppgiften.

På en övergripande nivå har enkätresultatet samt övrigt underlag gett en bild av att de organisatoriska förutsättningarna hos många myndigheter idag snarare försvårar än underlättar ett systematiskt informationssäkerhetsarbete. Det handlar både om otydlighet rörande de olika rollernas uppgifter och om de faktiska förutsättningarna dessa roller har att bedriva när det gäller att bedriva informationssäkerhetsarbete.

MSB ser med anledning av detta ett behov av att i föreskrifterna ställa krav på att myndigheterna bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett LIS. Denna uppgift är nära kopplad till myndighetens förmåga att genomföra sina uppdrag. Av ledningssystemet ska det ansvar som myndighetsledningen och andra delar av myndigheten har för informationssäkerhetsarbetet framgå. Att säkerställa att utpekade roller har de befogenheter som krävs för att bedriva informationssäkerhetsarbetet ingår också.

Närmare krav på myndigheternas informationssäkerhetsarbete

Avsnittet om arbete med informationssäkerhet påminner i delar om de tidigare föreskrifterna eftersom paragraferna tar upp flera av stegen i ett systematiskt informationssäkerhetsarbete, som informationsklassning och riskanalys. Inledningsvis betonas vikten av att informationssäkerhetsarbetet ska drivas, samordnas, utvärderas och löpande utvecklas. Informationssäkerhetsarbetet förutsätter en adekvat resurstilldelning samt att myndighetens ledning löpande ges tillräckligt med information för att kunna utöva beslutsunderlag. Nya krav på aktiviteter som ska underlätta kravställning på informationssäkerhet har införts i föreskrifterna. Det handlar om kravet på att myndigheterna ska

[5] Enkäten distribuerades till 351 myndigheter och sammanlagt fick MSB svar från drygt 95%. 227 av dessa myndigheter uppgav att de själva hanterade sin information och informationssäkerhet och besvarade samtliga frågor i enkäten. Övriga myndigheter, vars informationshantering eller informationssäkerhet i sin helhet hanteras av en annan myndighet, besvarade endast ett fåtal frågor i enkäten, främst om hur förhållandet till den andra myndigheten reglerats.

kartlägga sina verksamhetsprocesser och deras informationsbehov. Krav ställs även på att myndigheterna arbetar med att skapa en säkerhetskultur genom utbildning och övning. Dessutom följer krav på dokumentation och på ett processinriktat informationssäkerhetsarbete, där varje steg bygger på det föregående samt att dessa steg ska utgå från beslutade modeller. Av de beslutade modellerna som ska stödja det systematiska informationssäkerhetsarbetet ska det framgå vid vilka tidpunkter och vid vilka situationer informationsklassning och riskanalys ska göras.

Av *standarden ISO/IEC 27001* framgår att organisationen ska se till att det finns resurser för informationssäkerhetsarbetet, att de befattningar som är relevanta för informationssäkerhetsarbetet har tilldelats ansvar och befogenheter samt att organisationen ska arbeta med kompetens och medvetenhet. Dessutom ska organisationen införa åtgärder som sedan ska kunna utvärderas för att möta de risker och möjligheter som identifierats. I samband med det ska en riskanalysprocess tas fram, riskernas ägare identifieras, säkerhetsåtgärder för att skydda informationen väljas, införas och dokumenteras. Dessutom ska mätbara tydliga mål för informationssäkerheten sättas upp, kommuniceras och följas upp.

Enkätresultatet visade på flera brister hos myndigheter vilka behöver åtgärdas. Även om styrande dokument fanns på plats i de flesta myndigheter kontrollerade endast 26 % av myndigheterna[6] om de efterlevs. Dessutom uppgav myndigheterna att av ”de som leder och samordnar informationssäkerhetsarbetet” hos myndigheterna uppges 38 %[7] sakna tillräcklig kompetens, resurser eller mandat för att utföra uppdraget på ett tillfredsställande sätt. Den sistnämnda siffran lyfts särskilt upp av Riksrevisionen i sin granskning av informationssäkerheten i den civila statsförvaltningen.[8] När det gällde informationsklassning och riskanalys visade det sig att en majoritet av myndigheterna[9], 67 % respektive 78 %, har en informationsklassningsmodell respektive en metod för riskanalys. Däremot saknades i stor utsträckning både regler när modellerna och metoderna skulle användas och vem som var ansvarig för arbetet. Tydliga brister fanns när det gällde att bedriva informationssäkerhetsarbetet som en process. Endast 36 % av myndigheterna[10] uppgav att riskanalysen var kopplad till modellen för informationsklassning. Endast 4 av 10 myndigheter[11] använde sedan resultatet från riskanalysen som stöd vid kontinuitetsplaneringen. Dessutom uppgav fler än hälften av de myndigheter som besvarade hela enkäten att de saknar tydliga regler kring uppföljning av resultatet av riskanalysen. Storleken på myndigheten påverkade i princip inte resultatet.

[6] Av de myndigheter som besvarade hela enkäten.
[7] Av de myndigheter som besvarade samtliga frågor i enkäten
[8] RiR 2014:23 s 49
[9] Av de myndigheter som besvarade hela enkäten.
[10] Av de myndigheter som besvarade hela enkäten.
[11] Av de myndigheter som besvarade hela enkäten.

Även djupintervjuer och granskningsrapporter stödde bilden av att det fanns brister i det processuella arbetet.

Ett systematiskt informationssäkerhetsarbete förutsätter dock inte bara aktivitet från de som har utpekade roller och ansvar rörande informationssäkerhetsarbetet. Även de som arbetar med myndighetens olika verksamheter har en viktig uppgift genom att formulera vilka behov av skydd olika informationsmängder har.

För att hela organisationen ska kunna bidra till informationssäkerhetsarbetet på det sätt som behövs krävs både förståelse för frågorna och ett tydliggörande av uppgiften. MSB har därför sett behov av att både ställa krav som syftar till att det skapas en säkerhetskultur i organisationen och att ansvaret för respektive informationsmängder tydliggörs genom att informationsägare ska pekas ut.

Eftersom enkätresultatet och djupintervjuerna visade på att det fanns brister när det gällde att knyta de olika stegen i informationssäkerhetsarbetet till varandra, har MSB bedömt att det processuella och stegvisa arbetet behöver förtydligas i modeller som myndigheten beslutat. Dessutom införs ett särskilt krav på att kartlägga verksamhetsprocesserna, och den information dessa behöver. Detta har till syfte att ytterligare underlätta identifieringen av informationssäkerhetskrav.

De påtagliga brister som påvisades i enkäten när det gällde struktur kring hur informationsklassning och riskanalysarbetet bedrivs, exempelvis när det gällde ansvar och tidpunkt, har också föranlett MSB att ytterligare tydliggöra att dessa uppgifter ska framgå.

It-incidenthantering och kontinuitet i informationshantering

Avsnittet är nytt och reglerar myndighetens interna hantering av it-incidenter samt kontinuitetshantering.

I standarden utvecklas hur incidenthantering ska kunna utformas för att vara ett stöd. Det samma gäller kontinuitetshantering.

Av enkäten framgick att 26 % av de myndigheter som besvarade enkäten i sin helhet inte hade någon process för incidenthantering och incidentrapportering. Något som ökar risken för att incidenter inte omhändertas på rätt sätt och försvårar möjligheterna att lära sig av inträffade incidenter. Några av de mest påtagliga bristerna som kunde visas med stöd av enkätens resultat var kopplade till myndigheternas kontinuitetsplanering. Här framgick att endast drygt 3 av 10 myndigheter[12] hade en kontinuitetsplan samt att endast en tredjedel av dessa även hade övat sin kontinuitetsplan.

Med hänsyn till de påvisade bristerna har MSB valt att särskilt lyfta fram it-incidenthantering och kontinuitetshantering i en särskild paragraf.

[12] Av de som besvarat enkäten i sin helhet.

Tillämpning av standarder

I nu gällande föreskrifter hänvisas till de två standarderna ISO/IEC 27001 och ISO/IEC 27002. Den förstnämnda innehåller krav på ett LIS medan den andra ger stöd för utformning av olika typer av säkerhetsåtgärder. Med hänsyn till att MSB nu byggt ut föreskrifterna och där lyft in flera av de krav som ställs i de reviderade standarderna gör MSB bedömningen att behovet av att därutöver direkt peka på standarderna i föreskrifterna har minskat. Standarderna är dock av stor betydelse som stöd för ett systematiskt informationssäkerhetsarbete. MSB väljer därför att även fortsättningsvis tydliggöra standardernas betydelse för myndigheternas informationssäkerhet genom att anvisa standarderna som stöd för arbetet i de allmänna råden.

1.2 Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

Det finns anledning att resonera kring olika handlingsalternativ för att hantera den problematik som pekats på i föregående avsnitt. Nedan beskrivs de huvudsakliga alternativen.

- Föreskrifterna förändras inte med undantag från en uppdaterad referens till de nya versionerna av standarderna ISO/IEC 27001 och ISO/IEC 27002 kombinerad med utbildningsinsatser.
- Författningens utformning och innehåll ses över i sin helhet i syfte att på ett aktivt sätt stödja statliga myndigheters systematiska informationssäkerhetsarbete. Arbetet inkluderar även att säkerställa att författningens föreskrifter utformas i linje med de uppdaterade standarderna.

MSB har under flera år arbetat metodiskt med att ta fram stöd i olika former för informationssäkerhetsarbete. På www.informationssäkerhet.se finns ett metodstöd för införande av ett ledningssystem som är framtaget i samarbete med en rad olika organisationer, både offentliga och privata aktörer. Ytterligare stöd finns på www.msb.se. MSB har, tillsammans med övriga myndigheter i samverkansgruppen för informationssäkerhet (SAMFI)[13], även sedan 2011 anordnat en årlig konferens för offentlig sektor om informationssäkerhet. Dessutom håller MSB föredrag och presentationer samt driver en rad nätverk inom området. Trots insatserna kan dock konstateras att säkerhetsnivån ännu inte är tillräcklig hos statliga myndigheter. MSB gör därför bedömningen att det, vid sidan av ytterligare vägledning och stöd, behövs tydligare styrning och inriktning i form av mer konkreta krav i föreskrifterna.

[13] I SAMFI ingår Försvarsmakten, Försvarets Materielverk, Försvarets Radioanstalt, Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen.

1.3 Uppgifter om vilka som berörs av regleringen

Författningen berör endast statliga myndigheter med undantag för Regeringskansliet, kommittéväsendet och Försvarsmakten. För utlandsmyndigheterna gäller föreskrifterna endast i den omfattning som anges av regeringen i föreskrifter.

1.4 Uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på

MSB har enligt sin instruktion[14] i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet. Vidare har MSB med stöd av 34 § förordningen (2006:942) om krisberedskap och höjd beredskap rätt att utfärda föreskrifter om statliga myndigheters informationssäkerhet, vilket myndigheten även har gjort. När föreskrifter meddelas ska enligt 34 § KBF nationell och internationell standard beaktas. De nu gällande föreskrifterna utfärdade MSB den 1 februari 2010.

I betänkandet *Informations- och cybersäkerhet i Sverige*, SOU 2015:23, föreslås att en ny förordning rörande statliga myndigheters informationssäkerhet ska införas. MSB gör bedömningen att myndighetens förslag på nya föreskrifter om statliga myndigheters informationssäkerhet ligger i linje med förordningsförslaget i betänkandet.

1.5 Uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Idag är det en självklarhet att en myndighet har kostnader för att skydda sin information. I denna kostnad ingår till exempel tekniska skyddsåtgärder i it-system och administrativa kostnader för rutiner samt förvaltning av tekniken. En stor del av utgifterna för informationssäkerhet består av personalkostnader. Utöver kostnader för personal som är särskilt utsedd att samordna och leda säkerhetsarbetet måste även ledningen ägna sig åt säkerhetsfrågor. Dessutom behövs personal som handlägger behörighetsadministration, övervakar brandväggar, uppdaterar virusskydd, följer upp säkerheten, utbildningar, etc.

Det är svårt att på ett normerande sätt ange hur stor del av en verksamhets kostnader som bör läggas på informationssäkerhet. Varje organisation har att förhålla sig till en unik situation när det gäller verksamhet, geografisk och fysisk placering av lokaler, förhållanden till omvärlden m.m.

En vanlig modell är att bedöma minskade skadekostnader som resultat av skyddsåtgärder. Exempelvis kan negativa effekter av incidenter av olika slag såsom rättsförluster, störningar i verksamheten, obehörig åtkomst och skada för tredje man i många fall bedömas kostnadsmässigt.

---

[14] 11 a § Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Ett väl genomfört, riskbaserat och systematiskt informationssäkerhetsarbete kan innebära minskade kostnader. Det finns exempel på att organisationer efter riskanalys och skyddsnivåklassificering funnit att man tillämpat skyddsåtgärder som inte varit relevanta eller helt verkningslösa när det gäller de hot som identifierats, med möjlighet till besparingar som följd.

I förslaget till reviderade föreskrifter för statliga myndigheters informationssäkerhet ställs, liksom i nu gällande föreskrifter, krav på att statliga myndigheter ska arbeta systematiskt med sin informationssäkerhet med stöd av ett LIS. I föreskriftsförslaget förtydligas dessutom att arbetet ska vara riskbaserat och att ledningssystemet ska utgå från verksamhetens behov. I denna del innebär inte föreskriftsförslaget någon kostnadsmässig skillnad jämfört med nu gällande föreskrifter. Det kan till och med vara så att den tydliga verksamhetskopplingen, vilken betonas i det nya förslaget, skulle kunna innebära att det nya förslaget på föreskrifter kan göra myndigheternas informationssäkerhetsarbete mer kostnadseffektivt.

I förslaget till reviderade föreskrifter skärps, i vissa avseenden, kraven på informationssäkerhetsarbetets utformning. Detta gäller exempelvis krav på utbildning och övning. Kraven kan kortsiktigt innebära viss kostnadsökning för myndigheterna jämfört med kraven i nuvarande reglering men kan i förlängningen bidra till att minska kostnader för it-incidenter. Det finns flera indikationer på att hoten som riktas mot och riskerna kring myndigheternas informationshantering stadigt ökar, bland annat på grund av den tekniska utvecklingen. Föreskriftsförslaget har som övergripande syfte att ytterligare förbättra stödet för myndigheternas systematiska och effektiva informationssäkerhetsarbete och därmed minska risken för kostnader och förtroendeförluster samt andra konsekvenser orsakade av avbrott, störningar och andra it-incidenter.

1.6 Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Föreskrifterna i sin föreslagna utformning främjar myndigheternas användning av ett LIS i former enligt internationell standard på området, ISO/IEC 27001. En sådan inriktning av myndigheternas informationssäkerhetsarbete bedöms följa samma linje som Europeiska unionen ger uttryck för i flera rättsakter. Exempelvis ställs uttryckliga krav på att berörda aktörer från och med den 16 oktober 2016 ska certifiera säkerheten i sina informationssystem enligt ISO 27001: *Ledningssystem för informationssäkerhet – Krav*.[15] Detta krav träffar

[15] Kommissionens delegerade förordning (EU) nr 907/2014 av den 11 mars 2014 om komplettering av Europaparlamentets och rådets förordning (EU) nr 1306/2013 vad gäller utbetalande organ och andra organ, ekonomisk förvaltning, avslutande av räkenskaper, säkerheter och användning av euron. http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014R0907&from=SV

bland annat svenska myndigheter med vissa särskilda uppdrag kopplade till utbetalningar av EU-stöd.

Europaparlamentet har yttrat sig positivt till användningen av standarden ISO/IEC 27001 i samband med e-förvaltning och rekommenderar uttryckligen att man, ”för att säkerställa kvaliteten vid tillhandahållandet av dessa tjänster [e-förvaltningstjänster], ser till att de överensstämmer med internationella standarder, normer och riktlinjer för god praxis, såsom ISO 27001 när det gäller informationssäkerhet, eller ISO 20000 vad beträffar kvaliteten på processerna för hantering av it-tjänster.”

Enligt MSB:s uppfattning är föreskriften ett viktigt steg mot att på rekommenderat sätt främja goda rutiner för informationssäkerhetsarbete och överensstämmer därför väl med det europeiska regelverket.

1.7 Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Enligt nuvarande planering kommer föreskrifterna att träda ikraft den 1 januari 2016.

MSB gör, bland annat på grund av resonemanget i 1.1.2, bedömningen att det sedan en tid finns ett behov av utökat stöd för och styrning av myndigheters informationssäkerhetsarbete i form av reviderade föreskrifter. Detta stöd bör därför komma på plats så snart som möjligt.

Med hänsyn till att regeringen planerat att en ny förordning om statliga myndigheters informationssäkerhet ska träda ikraft den 1 januari 2016, gör MSB även bedömningen att myndigheternas efterfrågan på mer stöd och styrning kommer att växa det närmaste året. MSB ser detta som ytterligare en anledning till att säkerställa att de nya föreskrifterna träder ikraft vid årsskiftet 2015/2016.

När det gäller informationsinsatser kommer MSB att i anslutning till ikraftträdandet använda flera kanaler för att uppmärksamma myndigheterna på de nyutkomna föreskrifterna.

B. Kommuner och landsting

Markera med x

(X) Regleringen bedöms inte få effekter för kommuner eller landsting.

( ) Regleringen bedöms få effekter för kommuner eller landsting.

C. Företag

Med företag avses här en juridisk eller en fysisk person som bedriver näringsverksamhet, det vill säga försäljning av varor och/eller tjänster

yrkesmässigt och självständigt. Att yrkesmässigt bedriva näringsverksamhet bör tolkas brett.

Markera med x

(x) Regleringen bedöms inte få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför inte någon beskrivning av punkterna i avsnitt B.

( ) Regleringen bedöms få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Konsekvensutredningen innehåller därför en beskrivning av punkterna i avsnitt B.

D. Samråd

I syfte att säkerställa att arbetet med att revidera föreskrifterna om statliga myndigheters informationssäkerhet baserades på rätt ingångsvärden genomförde MSB en rad ”tidiga samråd”. Detta skedde främst i form av drygt 10 stycken djupintervjuer där bland annat orsaker till brister, alternativa lösningar och konsekvenser av olika val diskuterades. Intervjuerna genomfördes innan arbetet med att utforma föreskriftsförslaget påbörjades. De myndigheter som intervjuades var av olika storlek och med olika typer av verksamhet. Dessutom presenterades förslaget på föreskrifter vid två tillfällen för olika intressenätverk/intresseorganisationer där möjlighet gavs att lämna synpunkter.

Av de synpunkter som framkom, både vid djupintervjuerna och vid presentationerna, blev det tydligt att det ses som positivt att MSB i föreskrifterna hänvisar till standarder på området, särskilt ISO/IEC 27001. De organisatoriska förutsättningarna anses av aktörerna vara av stor betydelse för informationssäkerhetsarbetet, och särskilt myndighetsledningens agerande. Ansvar och resurser för informationssäkerhetsarbetet behöver även säkerställas. Dessutom behöver hela organisationen engageras i informationssäkerhetsarbetet.

Synpunkterna som framkom vid de ”tidiga samråden” har legat till grund för MSB:s arbete med föreskrifter och allmänna råd för statliga myndigheters informationssäkerhet.

E. Kontaktpersoner

Kontaktperson vid frågor om konsekvensutredningen och de nya föreskrifterna om statliga myndigheters informationssäkerhet är Helena Andersson som lämpligast nås på helena.andersson@msb.se eller 010-240 41 33 alternativt 073-026 11 33.