Underlag 1.

Några myndigheters rapportering om informationssäkerhet i årsredovisningen

Årsredovisningar år 2009

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR TILLRÄCKLIG

Inga.

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR OTILLRÄCKLIG

Läkemedelsverket

Ledningssystemet för informationssäkerhet SS-ISO/IEC 27001:2006 är under uppbyggnad.

MYNDIGHETER DÄR MAN AV ÅRSREDOVISNINGEN DELVIS KAN UTLÄSA NÅGOT OM INFORMATIONSSÄKERHETEN

Ekobrottsmyndigheten (EBM), Premiepensionsmyndigheten (PPM), Riksgälden, Statistiska centralbyrån (SCB), Statens Jordbruksverk (Jordbruksverket), Strålsäkerhetsmyndigheten samt Åklagarmyndigheten.

SCB

- Säkerhetsorganisationens resurser har under 2009 fortsatt varit ansträngda, dels på grund av att säkerhetschefen (överdirektören) tjänstgjort som t.f. generaldirektör i stort sett hela året, dels beroende på engagemang i implementeringen av ett nytt driftavtal. Detta har sammantaget medfört en sänkt ambitionsnivå i genomförandet av förbättringsåtgärder jämfört med den verksamhetsplaneringen.
- En utredning om framtida säkerhetsorganisation har slutförts och avrapporterats. Utifrån utredningens rapportförslag har beslut fattats om och bemanning genomförts av en ny säkerhetsorganisation.
- Infört en standardiserad pc-plattform som har gett SCB ökade möjligheter att kontrollera installerade licensierade programvaror. Efter genomfört projekt är cirka 80 procent av myndighetens användare inte längre så kallade lokala administratörer över disponerad pc, vilket bedöms ge en avsevärd ökning av säkerhetsnivån på pc-området.
- Webbapplikationer för insamling och publicering har testats utifrån ett säkerhetsperspektiv.
- Genomfört ett så kallade penetrationstest mot ett tiotal utpekade applikationer med höga tillgänglighets eller sekretesskrav. Efter slutförda tester kunde konstateras att förekomsten av generella

applikationsrelaterade brister (säkerhetsluckor) var jämnt förekommande i de testade applikationerna
- Genomfört ett antal riskanalyser av prioriterade statistikprodukter som ska ligga till grund för kontinuitetsplaner
- Upphandlat stöd för analys av den interna behörighetshanteringen.

Åklagarmyndigheten
- Har påbörjat en säkerhetsanalys av myndighetens skyddsvärda verksamhet. Syftet är att få en övergripande bild av riskerna inom verksamheten samt av beredskapsnivån för eventuella kriser.
- Har påbörjat ett arbete med att definiera en säkerhetsstandard. Den innehåller policys och riktlinjer samt en miniminivå för Åklagarmyndighetens verksamhetsskydd.
- Har upphandlat ett incidentrapporteringssystem. Systemet kommer att driftsättas under 2010.

Årsredovisning 2010

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR TILLRÄCKLIG

Inga.

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR OTILLRÄCKLIG

Ekobrottsmyndigheten, Kriminalvården, Pensionsmyndigheten (tidigare PPM) samt Åklagarmyndigheten.

Ekobrottsmyndigheten
- Enligt LIS-föreskrifterna ska alla myndigheter införa ett ledningssystem för informationssäkerhet. Som ett led i detta arbete har Ekobrottsmyndigheten påbörjat en nulägesanalys av informationssäkerheten vid myndigheten.

Kriminalvården
- En IT-strategi har beslutats. Strategin beskriver hur organisationen för IT ser ut och hur Kriminalvården ska arbeta med IT-frågor på alla nivåer i organisationen
- Kriminalvårdens IT-råd, har inrättats och haft flera möten under året. IT-rådet ska stödja en god strategisk styrning och samordning av myndighetens IT-verksamhet
- Kompetensen har förstärkts genom rekrytering av en informationssäkerhetsansvarig och en IT-säkerhetsansvarig, båda placerade på huvudkontoret. Den informationssäkerhetsansvariga rapporterar direkt till generaldirektören.
- På varje region och på en del särskilda enheter har informationssäkerhetsombud utsetts.

- Inom myndigheten pågår nu ett omfattande arbete med att klassa alla informationstillgångar i olika skyddsnivåer och hantera dem enligt de regler som gäller för respektive skyddsnivå.
- Som ett resultat av klassningen kommer under början av 2011 hanteringsregler för klassad information att beslutas och genomföras i alla delar av organisationen.
- I IT-infrastrukturen påbörjas införandet av olika säkerhetsnivåer anpassade till informationsklassningens olika nivåer. Arbetet inleds med införandet av en gemensam grundsäkerhetsnivå.
- Under 2011 kommer inom det pågående LIS-projektet ett antal nya riktlinjer med genomförandeplaner att tas fram för beslut.
- En grundläggande utbildning i informationssäkerhet planeras också för 2011.
- Under nästa verksamhetsår kommer även ett projekt att startas för att integrera en PKI-struktur och smarta kort i Kriminalvårdens IT-infrastruktur.
- För att öka förmågan att hantera informationssäkerhetsrisker kommer riktade riskanalyser att genomföras.
- Arbete pågår också för att integrera och hantera informationssäkerhetsincidenter i myndighetens system för incidentrapportering.

MYNDIGHETER DÄR MAN AV ÅRSREDOVISNINGEN DELVIS KAN UTLÄSA NÅGOT OM INFORMATIONSSÄKERHETEN

Försäkringskassan, Riksgälden, Socialstyrelsen, Strålsäkerhetsmyndigheten samt kraftnät.

Svenska kraftnät

- En viktig del i driftsäkerheten är även att analysera och åtgärda brister i IT-säkerheten. Det sker både vad gäller teknik, regler och rutiner samt arbete med beteende och en tydlig ansvarsfördelning. SCADA–säkerhet är en ny satsning inom informations- och driftsystem, som etablerades under 2010.

Årsredovisningar 2011

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR TILLRÄCKLIG

Inga.

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR OTILLRÄCKLIG

Ekobrottsmyndigheten, Finansinspektionen, Kriminalvården, SCB, Socialstyrelsen samt Åklagarmyndigheten.

Finansinspektionen

- Internrevisionen har under året granskat it-säkerheten på Finansinspektionen. Granskningen visar på ett antal brister rörande styrning, styrdokument, ansvar och rutiner.
- Under 2011 har Finansinspektionens it-strategi kompletterats med en sourcingstrategi för it. Den långsiktiga målsättningen är att bygga upp en beställarorganisation med både djup verksamhetskunskap och it-kunskap. Syftet är att åstadkomma bättre, resurseffektiv styrning och kontroll av it-verksamheten.

MYNDIGHETER DÄR MAN AV ÅRSREDOVISNINGEN DELVIS KAN UTLÄSA NÅGOT OM INFORMATIONSSÄKERHETEN

Försäkringskassan, Konjunkturinstitutet, Pensionsmyndigheten, Riksgälden samt Svenska kraftnät.

Pensionsmyndigheten

- Pensionsmyndigheten klassas som en samhällsviktig verksamhet och behandlar även information som har betydelse för rikets säkerhet, vilket bland annat ställer särskilda krav på myndighetens it-miljö. Med anledning av detta har myndigheten beslutat att lägga ut delar av drift en på en extern leverantör, Logica, som kommer tillhandahålla tjänster som datahallar, lagring samt backup.
- Med de nya tjänsterna och den nya tekniska plattform som har implementerats parallellt i två datahallar kommer myndigheten att möta de krav på redundans, tillgänglighet och katastrofsäkring som ställs på myndigheten.
- Pensionsmyndigheten arbetar aktivt med att säkerställa att it-verksamheten lever upp till externa och interna krav på it-säkerhet inom både utveckling och drift. Till hjälp görs revisioner samt olika tester för att se att det inte finns några sårbarheter efter stora releaser.

Årsredovisningar 2012

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR TILLRÄCKLIG

Inga.

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR OTILLRÄCKLIG

Ekobrottsmyndigheten, Finansinspektionen, Socialstyrelsen samt Åklagarmyndigheten.

Finansinspektionen

- Behov av förbättringar på informationssäkerhetsområdet har framkommit både genom de riskanalyser Finansinspektionen genomfört i arbetet med intern styrning och kontroll och genom en granskning på området som internrevisionen genomförde 2011.

- Ett omfattande arbete med att planera och påbörja införandet av ett antal förbättringsåtgärder på området har gjorts under året.
- Styrande dokument om informationssäkerhet, systemförvaltning och ändringar i it-miljön har omarbetats och fastställts. Arbete återstår att fortsatt implementera de nya reglerna och rutiner kopplade till dem.

MYNDIGHETER DÄR MAN AV ÅRSREDOVISNINGEN DELVIS KAN UTLÄSA NÅGOT OM INFORMATIONSSÄKERHETEN

Diskrimineringsombudsmannen, Kemikalieinspektionen, Konjunkturinstitutet, Kronofogdemyndigheten, Pensionsmyndigheten, Riksgälden, Rikspolisstyrelsen samt Svenska kraftnät.

Årsredovisningar 2013

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR TILLRÄCKLIG

Riksgälden samt Svenska kraftnät.

Riksgälden

- Under 2013 gjordes en översyn av de styrande dokumenten för operativ riskhantering, och rapporteringsprocessen för operativa risker förbättrades för att skapa en tydligare övergripande bild av risknivån.
- Riksgälden har ett väl fungerande ledningssystem för säkerhet. Det visar de uppföljningar och granskningar av systemet som genomfördes 2013. Ledningssystemet ger ett strukturerat och systematisk sätt att arbeta med säkerhet såväl för medarbetare som för IT-system och information. Det är baserat på standarden ISO-27001 och 27002.
- En central del av säkerhetsarbetet är att löpande göra risk- och sårbarhetsanalyser. Därmed kan brister identifieras och rätt åtgärder sättas in.
- Riksgälden utvecklar också säkerheten genom åtgärder där verksamheten engageras. Exempelvis genomfördes under 2013 utbildningar i informationssäkerhet för alla medarbetare.

Svenska kraftnät

- En viktig del i driftsäkerheten är även att analysera och åtgärda brister i IT-säkerheten. Det sker både vad gäller teknik, regler och rutiner samt genom arbete med beteende och en tydlig ansvarsfördelning.
- Målet för säkerhetsarbetet inom Svenska kraftnät är att det ska integreras i organisationens kärnverksamhet. Genom detta skapas bättre förutsättningar för verksamhetsstyrning av säkerhetsarbetet samt hantering av aktuella risker.

- Under verksamhetsåret har arbetet med översyn av verkets interna säkerhetsregelverk fortgått, och riktlinjer och anvisningar för vissa prioriterade områden har tagits fram.
- En mätning av informationssäkerheten inom verkets olika verksamhetsgrenar har genomförts i syfte att undersöka om befintlig säkerhet i organisationen är anpassad till de risker som verksamheten utsätts för. Säkerhetsnivån bedömdes vara god.
- I enlighet med kraven i säkerhetsskyddsförordningen har en säkerhetsanalys gjorts av Svenska kraftnäts verksamhet.
- Enligt Försvarsmaktens föreskrifter om signalskydd har en översyn av signalskyddsinstruktionen för samtliga signalskyddssystem vid Svenska kraftnät genomförts. Årlig internkontroll har gjorts på två system.

MYNDIGHETER DÄR DET AV ÅRSREDOVISNINGEN FRAMGÅR ATT INFORMATIONSSÄKERHETEN ÄR OTILLRÄCKLIG

Socialstyrelsen.

MYNDIGHETER DÄR MAN AV ÅRSREDOVISNINGEN DELVIS KAN UTLÄSA NÅGOT OM INFORMATIONSSÄKERHETEN

Arbetsförmedlingen, Finansinspektionen, Konjunkturinstitutet, Kriminalvården, Pensionsmyndigheten, Rikspolisstyrelsen, Trafikverket samt Åklagarmyndigheten.

Pensionsmyndigheten

- I början av året påbörjades en informationsklassning av myndighetens webbplats med fokus på e-tjänster. Den genomfördes under året och kommer resultera i ett antal aktiviteter i förvaltning under nästa år för att förbättra dagens e-tjänster ur ett säkerhetsperspektiv.
- Under året har en ny version av it-strategin tagits fram, förankrats och beslutats. Grunden för strategin fokuserar på hur myndigheten upprätthåller en säker leverans av sina informationssystem, hur it bidrar i den konstanta förändringen samt hur myndigheten leds genom den digitalisering som sker i samhället.
- Under 2013 har två interna revisioner genomförts med syfte att ur ett oegentlighetsperspektiv utvärdera den tekniska miljön kring premiepensionssystemet och myndighetens nätverk och i det sammanhanget bedöma om säkerhetsläget är tillfredsställande.
- Sammanfattningsvis har myndigheten en bra säkerhetsnivå, men det har ändå konstaterats att det finns ett antal brister som behöver åtgärdas.
- Myndigheten har påbörjat ett arbete för att höja it-säkerheten genom att införa åtgärder som kommer att eliminera eller reducera risken för att de konstaterade bristerna utnyttjas.