RIKSREVISIONEN

Granskning av Sjöfartsverkets interna styrning och kontroll av informationssäkerheten

ISBN 91 7086 060 2
RiR 2005:27
Tryck: Riksdagstryckeriet, Stockholm 2005

Till
Regeringen
Näringsdepartementet

Datum 2005-11-17
Dnr 31-2004-1295

Sjöfartsverkets interna styrning och kontroll av informationssäkerheten

Riksrevisionen har granskat Sjöfartsverkets arbete med informationssäkerhet. Resultatet av granskningen redovisas i denna granskningspromemoria.

Företrädare för myndigheten har beretts tillfälle att faktagranska och lämna synpunkter på utkast till granskningspromemorian.

Promemorian överlämnas till regeringen i enlighet med 9§ lagen (2002:1022) om revision av statlig verksamhet m.m. Promemorian överlämnas samtidigt till Riksrevisionens styrelse.

Promemorian innehåller slutsatser och rekommendationer som avser Sjöfartsverket. Promemorian överlämnas därför även till Sjöfartsverket.

Revisionsdirektör *Dan Ljungberg* har beslutat i detta ärende. Revisionsdirektör *Björn Undall* har varit föredragande. Revisionsdirektör *Bengt EW Andersson*, revisor *Roland Fellman* (t.o.m. 2005-09-30), revisionsdirektör *Kent Gustafsson*, revisor *Nenus Jidah* samt revisor *Dan Melin* har medverkat vid den slutliga handläggningen.

Dan Ljungberg

Björn Undall

För kännedom
Finansdepartementet
Sjöfartsverket

Innehåll

Sammanfattning 7

1 Inledning 9
1.1 Bakgrund, syfte och revisionsfrågor 9
1.2 Bedömningskriterier 11
1.3 Metoder och tillvägagångssätt i granskningen 15
1.4 Läsanvisningar 15

2 SjöV och informationssäkerheten 17
2.1 SjöV:s verksamhet 17
2.2 Informationstillgångarna och SjöV:s egen bedömning av säkerheten för dessa 17

3 Kontrollmiljön 19
3.1 Bedömningskriterier 19
3.2 Iakttagelser 19
3.3 Bedömning 21

4 Riskanalys 23
4.1 Bedömningskriterier 23
4.2 Iakttagelser 24
4.3 Bedömning 25

5 Ledningens kontrollfunktioner samt införda skyddsåtgärder 27
5.1 Bedömningskriterier 27
5.2 Iakttagelser 28
5.3 Bedömning 29

6 Information och utbildning om informationssäkerhet 31
6.1 Bedömningskriterier 31
6.2 Iakttagelser 31
6.3 Bedömning 32

7 Uppföljning och förvaltning 33
7.1 Bedömningskriterier 33
7.2 Iakttagelser 34
7.3 Bedömning 34

8 Slutsatser och rekommendationer 37
8.1 Inledande lägesbeskrivning 37
8.2 Bedömning och slutsatser 37
8.3 Rekommendationer 43

Bilaga 1 SjöV:s IT-system 45
Bilaga 2 Komponenter i LIS 49
Källförteckning 55

Sammanfattning

Post- och telestyrelsens incidentcentrum, Sitic, konstaterar att nära en tredjedel av alla offentliga organisationer har utsatts för någon form av allvarligt dataintrång eller virusangrepp. Angreppen blir alltmer ”professionella”. Samtidigt lägger myndigheterna ut alltmer av sin verksamhet på Internet i form av elektroniska tjänster. Myndigheterna behöver därför arbeta med att skydda sin information och verksamhet. Det är både svårt och resurskrävande. Det är mot denna bakgrund som Riksrevisionen har ökat sina insatser i granskningen av informationssäkerhet inom staten. Denna granskning gäller Sjöfartsverkets (SjöV) arbete med sin informationssäkerhet.

Vad menas med informationssäkerhet?

Informationssäkerhet handlar om att rätt information ska finnas tillgänglig, att den inte ska kunna förvanskas eller vara möjlig att komma åt för obehöriga. Det ska också vara möjligt att spåra bakåt hur information använts och ändrats.

Riksrevisionen har i sin granskning utgått från en internationell standard för ledning av informationssäkerhetsarbete (SS-ISO/IEC 17799), den s.k LIS-standarden. Den täcker alla de områden som säkerhetsarbetet behöver omfatta, både det rent tekniska skyddet och det som handlar om att påverka de anställdas beteende.

Vad kan bristande informationssäkerhet leda till?

SjöV har ett ansvar för sjöfartens infrastruktur såsom farleder, isbrytare och nät för kommunikation med sjöfarten. Därutöver utförs viktiga tjänster som lotsning, sjötrafikinformation, inspektion och sjöräddning. Information från verkets IT-system är avgörande för många av dessa tjänster. Brister i Sjöfartsverkets informationssäkerhet kan få konsekvenser för svensk sjöfart och sjöfarten i Sverige. Dessa konsekvenser kan i sin tur medföra konsekvenser för samhället. Näringslivet kan påverkas genom försenade transporter och försämrad sjösäkerhet. Även rikets säkerhet skulle kunna påverkas då SjöV hanterar hemlig information. Konsekvenser för SjöV kan bli ett försämrat förtroende från omvärlden, minskad inre effektivitet och minskade intäkter.

Har SjöV ett fungerande system för informationssäkerhet?

Både ja och nej. SjöV har flera av de delar som enligt standarden tillsammans utgör ett LIS. Vissa delar av LIS är dock mindre väl utvecklade – funktioner som skapar överblick, rapportering, riskanalys, utbildning samt uppföljning och förvaltning av LIS. Dessa länkar i den kedja som ledningssystemets delar bör bilda saknas eller är för svaga. Dessa brister medför att SjöV:s LIS inte utgör en fullt ut lämpligt utformad och fungerande helhet. Praktiskt innebär bristerna bl.a. att SjöV:s möjligheter att systematiskt upptäcka och lära sig av erfarenheter i informationssäkerhetsarbetet och i användningen av LIS minskar. Det i sin tur minskar möjligheterna att driva ett effektivt förbättringsarbete som syftar till att stegvis förbättra LIS.

Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet. Svaret på den fråga som granskningen syftat till att besvara är därmed att SjöV inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

1 Inledning

1.1 Bakgrund, syfte och revisionsfrågor

Granskningen avser Sjöfartsverkets (SjöV) arbete med informationssäkerhet. Informationssäkerhet kan definieras i termerna:

- Tillgänglighet: att behöriga användare har tillgång till den information de är behöriga till i rätt tid och rätt omfattning.
- Riktighet: att information inte obehörigt ändras eller modifieras.
- Sekretess: att endast behöriga användare kommer åt information.
- Spårbarhet: att kunna se vem som gjort vad och vid vilken tidpunkt.

Informationssäkerhet handlar med andra ord både om att rätt information ska finnas tillgänglig för att verksamheten ska kunna ge god service och om att informationen inte ska förvanskas, förstöras eller komma obehöriga till del. Det ska också vara möjligt att i efterhand se vem som medverkat till att informationen använts eller ändrats i strid med myndighetens regler.

Informationssäkerheten är väsentlig i tiden därför att elektronisk förvaltning får insteg hos de flesta statliga myndigheter och allt större krav ställs på att sådana tjänster som tillhandahålls elektroniskt är säkra, inte minst för att medborgare och företagare ska ha förtroende för dessa tjänster. Med denna utveckling följer bl.a. att myndigheterna behöver se över och vid behov förstärka informationssäkerheten.

En rapport[1] från Sveriges IT-incidentcentrum, Sitic, som är en del av Post- och telestyrelsen visar att

- 21 % av offentliga[2] organisationer har någon gång varit med om IT-säkerhetsincidenter som medfört att information eller systemkomponenter blivit åtkomliga för obehörig att läsa, kopiera, ändra eller radera. Det kan alltså handla om dataintrång, ”hacking”.
- 10 % av offentliga organisationer har varit med om IT-säkerhetsincidenter som inneburit en utförlig kartläggning av deras system. Det handlar alltså om att obehörig letat efter sårbara punkter.
- 20 % av offentliga organisationer har varit med om IT-säkerhetsincidenter som medfört att system eller delar av system blev otillgängliga,

[1] Mörkertalsundersökningen, http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf.

[2] Det vill säga statliga och kommunala myndigheter enligt Sitics bearbetning av sin mörkertalsundersökning:

s.k. DOS-angrepp eller Denial of Service. Det kan alltså handla om att system/nätverk blivit överbelastat på grund av ett DOS-angrepp.

- 30 % av offentliga organisationer har varit med om IT-säkerhetsincidenter som inneburit ett allvarligt utbrott av skadlig kod med betydande konsekvenser för verksamheten. Det kan alltså handla om virus, maskar, trojaner m.m.

Sitics undersökning visar att både hot och incidenter är verklighet för svenska myndigheter i dag.

Brister i Sjöfartsverkets informationssäkerhet skulle kunna få konsekvenser för svensk sjöfart och sjöfarten i Sverige. Dessa konsekvenser skulle i sin tur kunna medföra konsekvenser för samhället. Näringslivet skulle kunna påverkas på grund av försenade transporter och försämrad sjösäkerhet. Även rikets säkerhet skulle kunna påverkas då SjöV hanterar hemlig information[3]. Konsekvenser för SjöV skulle kunna vara ett försämrat förtroende från omvärlden, minskad inre effektivitet och minskade intäkter.

Granskningen avser SjöV:s arbete med informationssäkerhet. Under arbetets gång har Riksrevisionen valt att fokusera på säkerheten för de IT-relaterade informationstillgångarna. Säkerheten för manuella register, brev och liknande informationssamlingar har alltså inte blivit föremål för någon granskning. Det som Riksrevisionen därmed har granskat är det som brukar kallas IT-säkerhet. Anledningen till vårt val är att skyddet av de IT-relaterade informationstillgångarna är den mest svårbemästrade delen av informationssäkerheten eftersom den förutsätter en väl strukturerad och fungerande samverkan mellan individer och många gånger mycket komplicerade tekniska system. Det är också så att det främst är denna del av myndighetens informationshantering som har att motstå en mängd nya hot.

I granskningen har tyngdpunkten legat på myndighetsledningens styrning och kontroll för att säkerställa säkerheten/skyddet av myndighetens IT-relaterade informationstillgångar, t.ex. systemdokumentation, informationsregister/databaser, programvaror och programlicenser. Denna styrning och kontroll benämns samlat för ledningssystem för informationssäkerhet (LIS). Denna avgränsning innebär bl.a. att faktiskt uppnådd säkerhet i enskilda system inte granskats. God informationssäkerhet kräver ett systematiskt säkerhetsarbete som leds utifrån noggranna analyser av bl.a. verksamhetens säkerhetsbehov, sårbarhet och risker. LIS är alltså en viktig förutsättning för god informationssäkerhet. Detta är bakgrunden till vårt val av LIS som fokus.

Revisionsfrågan är: arbetar myndigheterna, utifrån gängse normer, systematiskt med sin informationssäkerhet?

---

[3] Här avses information om vattendjupet utanför farlederna, något som anses vara av intresse för främmande makt.

1.2 Bedömningskriterier

Riksrevisionen har i sitt sökande efter revisionsfrågans ”gängse normer” utgått från ett flertal normkällor[4]. Efter genomgången valdes standarden Ledningssystem för informationssäkerhet – Riktlinjer för ledning av informationssäkerhet (SS-ISO/IEC 17799 och SS 627799) som den dominerande utgångspunkten för Riksrevisionens granskningskriterier. Nämnda standard, den s.k. LIS-standarden, utgör riktlinjer som enligt standarden ”bör betraktas som ett underlag för att utveckla organisationsspecifika riktlinjer. Allt som nämns i denna standard är kanske inte tillämpligt. Ytterligare åtgärder, som inte anges i denna standard, kan också vara nödvändiga.”[5] Samtidigt utgör standarden ”en gemensam grund för i princip alla organisationer”[6].

För Riksrevisionens beslut att använda LIS-standarden har följande faktorer haft betydelse:

- LIS-standarden visar sig vid Riksrevisionens genomgång av de olika normkällorna vara den mest fullständiga. Med det menas att den täcker alla de områden – länkarna i kedjan – som säkerhetsarbetet behöver omfatta för att det ska leda till att eftersträvad säkerhet ska kunna uppnås.
- Det är vidare den enda internationella standarden för informationssäkerhet som täcker hela detta område.
- Stora delar av både näringsliv och förvaltning har accepterat den som utgångspunkt för det egna arbetet med informationssäkerhet.
- Standardens innehåll (riktlinjerna) har visats sig vara stabilt. Standarden har efter tio år nu uppdaterats beträffande sin disposition men den är innehållsligt intakt.

Riksrevisionen har således valt att använda LIS-standarden för att precisera de kriterier som bör gälla för att informationssäkerhetsarbetet ska anses bedrivas enligt gängse norm. På en övergripande nivå finns emellertid också krav på myndigheter i detta avseende formulerade i lagar och förordningar.

---

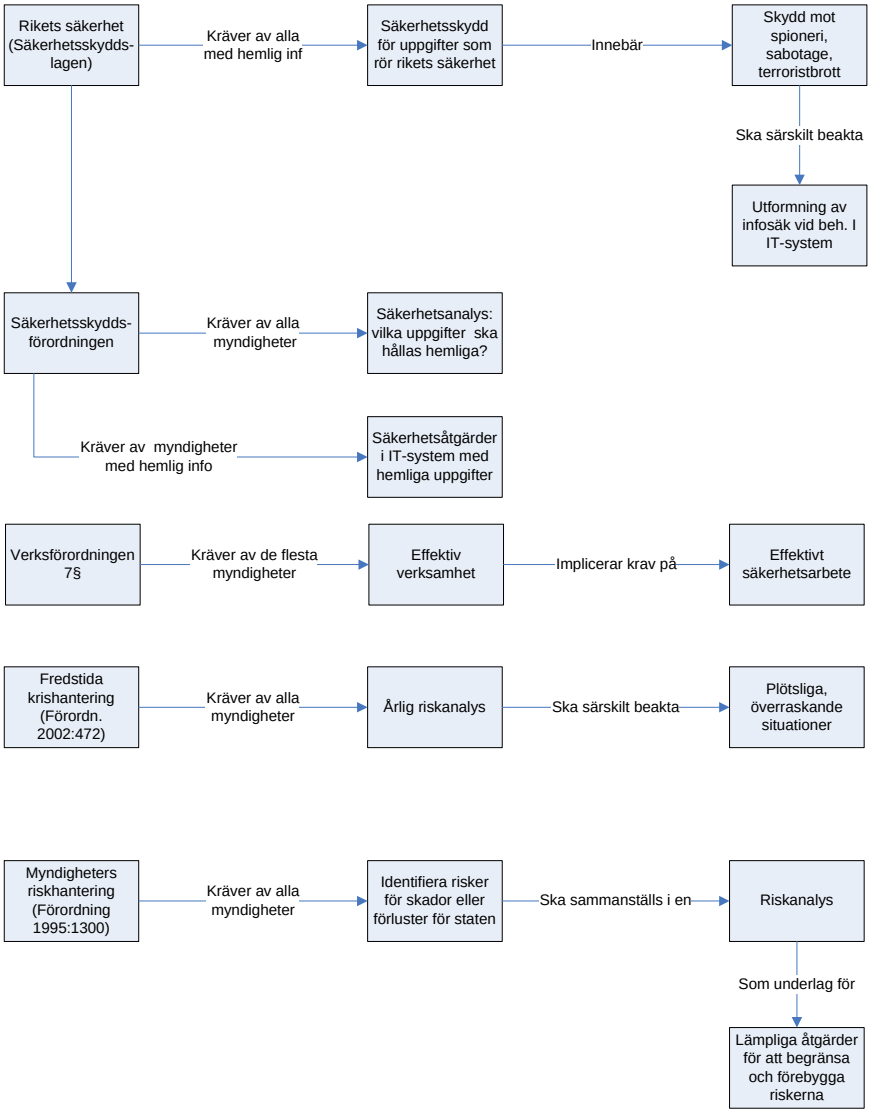
[4] Standarden Ledningssystem för informationssäkerhet, Krisberedskapsmyndighetens rekommendation BITS, Basnivå för IT-säkerhet, verksförordningen (1995:1322), förordning om myndigheters riskhantering (1995:1300), förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap, säkerhetsskyddsförordning (1996:633, 2000:888), Datainspektionens föreskrifter om bearbetning av personuppgifter i datorer, ”800-serien” från USA:s standardiseringsorgan NIST, COBIT, *Control Objectives for Information and related Technology,* erfarenheter från andra nationella revisionsorgan, bl.a. GAO i USA, OAG i Kanada samt erfarenheter från den svenska bank- och försäkringssektorn.

[5] SS-ISO/IEC 17799 s. 10.

[6] SS-ISO/IEC 17799 s. 10.

1.2.1 *Lagar och förordningar som berör informationssäkerhet*

Figur 1. Översikt över reglering av informationssäkerhet



Lagar och förordningar som berör informationssäkerhetsområdet beskrivs i grafen ovan[7]. De behandlar myndigheters riskhantering[8], åtgärder

[7] Redovisningen utgör ett urval som bedömts relevant. Därutöver finns bl.a. RPS föreskrifter (RPS FS 1996:9), skyddslagen (1990:217) och sekretesslagen (1980:100).

[8] Förordning (1995:1300) om myndigheters riskhantering.

för fredstida krishantering[9] samt skydd mot spioneri, sabotage och andra brott som kan hota rikets säkerhet[10].

Vad som berör **samtliga myndigheter** är:

- Kravet att utföra en *riskanalys* som identifierar risker för skador och förluster för staten (3§, förordning om myndigheters riskhantering).
- Kravet att vidta *lämpliga åtgärder* för att begränsa riskerna och förebygga skador eller förluster (3§, förordning om myndigheters riskhantering).
- Kravet att utföra årlig *risk- och sårbarhetsanalys* som ska identifiera sårbarhet och risker som *synnerligen allvarligt* kan påverka verksamheten. Särskilt ska beaktas situationer som uppstår hastigt, oväntat och utan förvarning, sådana som allvarligt påverkar samhällets funktionsförmåga samt myndighetens förmåga att hantera *mycket allvarliga* situationer inom ansvarsområdet (3§, förordning om åtgärder för fredstida krishantering och höjd beredskap).
- Kravet att utföra *säkerhetsanalys* som ska visa om myndigheten har information som ska hållas hemlig med hänsyn till rikets säkerhet (§5, säkerhetsskyddsförordning).

Vad som berör **vissa myndigheter**, de som enligt genomförd säkerhetsanalys har information som med hänsyn till *rikets säkerhet* ska hållas hemlig, är:

- Krav att det ska finnas det *säkerhetsskydd* som behövs som skydd mot spioneri, terroristbrott m.m. som kan hota rikets säkerhet (5§, säkerhetsskyddslagen) och som förebygger brister i informationssäkerhet som avser hemlig information (7 och 9§§, säkerhetsskyddslagen).
- Krav på *särskilda säkerhetsåtgärder* – behörighetskontrollsystem, händelseloggning, samråd med säkerhetsmyndigheterna i vissa fall, godkänd kryptering, inventering av hemliga handlingar – för de IT-system som används för hemlig information (12 §, säkerhetsskyddsförordningen). Regeringen har här alltså funnit anledning att formulera relativt konkreta krav på dessa myndigheters säkerhetsarbete till den del detta avser skydd av hemlig information.

Risker för skador och förluster för staten kan uppstå genom brister i informationssäkerheten för stora delar av den statliga informationen, och inte bara i den hemliga informationen. Riskhanteringsförordningen innehåller därmed implicit ett krav på riskanalys också beträffande informationssäkerhet. Vidare krävs att lämpliga skyddsåtgärder vidtas för att begränsa och förebygga riskerna. Riskhanteringsförordningen uppfattar därför

[9] Förordning (2002:472)om åtgärder för fredstida krishantering och höjd beredskap.
[10] Säkerhetsskyddslag (1996:627).

Riksrevisionen som den mest långtgående i kraven på alla myndigheters informationssäkerhetsarbete. Samtidigt avgränsas riskerna till sådana som har statsfinansiell betydelse. Risker för enskildas intressen lämnas därmed utanför om de inte föranleder ersättningsanspråk eller annan skada för staten.

Regeringen vill vidare i risk- och sårbarhetsanalysen lyfta upp riskerna för att hemlig information röjs eller förvanskas och på så sätt allvarligt påverkar (3§ krishanteringsförordningen) samhällets funktionsförmåga eller förmågan att hantera mycket allvarliga situationer.

1.2.2 LIS-standarden

Enligt Riksrevisionens tolkning av LIS-standarden ska åtgärder vidtas för skydd av all, enligt den enskilda myndighetens bedömning, *skyddsvärd information*. Det kan uppfattas innebära ett vidgat åtagande eftersom skyddsvärdet inte relateras till enbart rikets säkerhet eller till statsfinansiella förluster utan kan avse exempelvis enskilds integritet och hälsa eller hemliga förhållanden i företag. Det som enligt regelverket ska göras av alla myndigheter – riskanalys, risk- och sårbarhetsanalys samt säkerhetsanalys – inryms samtidigt i standardens krav på främst ledningssystemets riskanalysprocess respektive den del av riskanalysen som avser säkerhetsklassning av informationen.

Riksrevisionens slutsats är att ingenting i LIS-standarden motsäger regelverket. Skillnaderna är att regelverket täcker en mindre del av myndigheternas säkerhetsarbete (främst riskanalysen) och en mindre del av de statliga informationstillgångarna samt att regelverket är mindre preciserat med undantag för säkerhetsarbetet som gäller den hemliga informationen. LIS-standarden kan på så sätt sägas precisera kraven på myndigheternas arbete inom informationssäkerhetsområdet. Det ska tilläggas att det enligt Riksrevisionens bedömning även följer av verksförordningens § 7 – att myndighetens verksamhet ska bedrivas effektivt - att myndigheter ska bedriva ett effektivt säkerhetsarbete. Med detta krav följer bl.a. enligt Riksrevisionens bedömning att säkerheten för alla skyddsvärda informationstillgångar ska skötas i ett sammanhållet ledningssystem. LIS-standarden innehåller de mest väsentliga kraven på ett sådant ledningssystem.

Riksrevisionen har därför tagit fram ett granskningsprogram med kriterier och intervjufrågor som avser LIS och som baseras på LIS-standarden. Granskningsprogrammet har behandlats i seminarier med Swedish Standards Institute (SiS), Krisberedskapsmyndigheten, Statskontoret och en säkerhetschef inom bank- och försäkringssektorn.

I granskningsprogrammet har således LIS-standarden använts som utgångspunkt för kriterier för bedömning av myndighetens säkerhetsarbete.

Bedömningskriterierna avser myndighetens kontrollmiljö, riskanalys, kontrollfunktioner, information och utbildning samt uppföljning av och förvaltning. Bedömningskriterierna anges i inledning av kapitel 3-7.

1.3 Metoder och tillvägagångssätt i granskningen

Granskningen har genomförts på följande sätt:

- Myndigheten har först fått ett introduktionsbrev och en begäran att få ta del av myndighetens informationssäkerhetspolicy.
- Myndigheten har därefter fått besvara en webbenkät med frågor (dvs. en självutvärdering) om myndighetens syn på sin verksamhet och behovet av informationssäkerhet. Myndigheten redovisar vidare vilka delar av det ledningssystem för informationssäkerhet som standarden anger som finns i myndighetens ledningssystem för informationssäkerhet.
- Myndigheten har i nästa steg fått en lista som beskriver s.k. nyckeldokument som Riksrevisionen behöver för sin granskning. Myndigheten har sedan översänt dessa. Myndigheten har gjort en egen bedömningar vilka av dess dokument som motsvarar Riksrevisionens beskrivningar och som tillsammans ger en rättvisande bild av myndighetens arbete med informationssäkerhet.
- Efter det att Riksrevisionen gått igenom dokumenten har företrädare för myndigheten blivit intervjuade[11] med stöd av granskningsprogrammets intervjufrågor. Intervjuerna spelades in – efter att intervjupersonerna lämnat sitt medgivande – för att öka precisionen i tolkningarna av intervjuerna. Efter intervjuerna har en del kompletterande dokument överlämnats till revisionen.
- Myndigheten har sedan faktagranskat utkast till revisionsrapport.

Med denna stegvisa insamling av information har det varit möjligt att sprida den över en längre tidsperiod och därmed mindre belasta myndigheten. Det har samtidigt gjort det möjligt att fokusera insamlandet i efterföljande insamlingssteg utifrån resultaten av föregående steg.

1.4 Läsanvisningar

Begreppet ”systematisk” används på flera ställen. Det står för ett förfarande som till sin natur är metodiskt och av ledningen fastställt.

[11] Sju intervjuer gjordes: GD, avdelningschefer vid farleds- och sjötrafikavdelningarna, sektionschef, ekonomichef, IT-chef och IT-strateg.

Ett annat ord som används är ”tillräcklig”. Det är en bedömning som Riksrevisionen gör av hur långt vi bedömer att SjöV kommit i förhållande till vår tolkning av de krav som uttrycks i LIS-standarden.

I rapporten har redovisningen av granskningskriterier, iakttagelser och slutsatser strukturerats[12] enligt följande:

- kontrollmiljö,
- riskanalys,
- kontrollfunktioner,
- information och utbildning,
- uppföljning och utvärdering.

En beskrivning av Riksrevisionens bedömningskriterier för respektive komponent i modellen inleder kapitlen 3–7. Dessa kapitel behandlar Riksrevisionens iakttagelser och slutsatser.

Alla bedömningskriterier identifieras med fetstilta ledord i kapitlens inledande avsnitt om bedömningskriterier. I de därpå följande avsnitten om iakttagelser används dessa fetstilta ledord för att underlätta för läsaren. I vissa kapitel saknas iakttagelser beträffande en del av dessa kriterier. Riksrevisionen har under granskningens gång fokuserat på vissa kriterier och tillhörande frågor med ledning av de uppgifter som framkommit. Även de bedömningskriterier som inte motsvarats av iakttagelser har dock tagits med eftersom Riksrevisionen bedömt det vara av värde att redovisa även övriga kriterier. En mer fullständig redovisning kan t.ex. vara av värde för SjöV i myndighetens informationssäkerhetsarbete. Att ett kriterium inte tagits upp bland iakttagelserna innebär alltså inte att Riksrevisionen funnit att detta uppfylls av myndigheten. Bedömningarna som följer sist i varje kapitel tar endast upp de iakttagelser som utgör den huvudsakliga grunden för Riksrevisionens slutsatser.

[12] Committee of Sponsoring Organizations of the Treadway Commission (Coso) har beskrivit den interna styrningens och kontrollens olika beståndsdelar och deras samband i den s.k. Coso-modellen. Strukturen för denna rapport motsvarar dessa beståndsdelar.

2 SjöV och informationssäkerheten

2.1 SjöV:s verksamhet

SjöV[13] är en central förvaltningsmyndighet med ett sektorsansvar för sjöfarten. Verkets huvuduppgift är att verka för goda förutsättningar för både sjöfarten i Sverige och för svensk sjöfart.

Organisatoriskt är SjöV uppdelat på ett huvudkontor i Norrköping, med en central administration, samt en regional organisation bestående av sju sjötrafikområden och en sjöräddningscentral i Göteborg. Sjöfartsinspektionen, som är en ansvarsmässigt självständig del inom verket har, förutom sitt huvudkontor i Norrköping, tre regionala inspektionsområden.

Kärnverksamheten bedrivs i huvudsak inom två avdelningar. Farledsavdelningen ansvarar för att genomföra beslutade infrastrukturåtgärder avseende farleder, isbrytning och sjögeografisk information. Sjötrafikavdelningen leder och samordnar sjötrafikområdenas verksamhet avseende lotsning, sjötrafikinformation och sjöräddning.

2.2 Informationstillgångarna och SjöV:s egen bedömning av säkerheten för dessa

Inslaget av IT-stöd i SjöV:s processer är betydande och SjöV är starkt IT-beroende. Av särskild betydelse är SjöV:s infrastrukturtjänster i form av bl.a. sjögeografisk information och sjötrafikinformation till sjöfarten. Viktigare informationssystem[14] framgår av bilaga 1.

Det ställs stora krav på att den information som finns i SjöV:s informationssystem är säkerställd. Med detta menas att informationens riktighet, tillgänglighet och sekretess är skyddade. Kraven på kontinuitet i verksamheten är också stora.

Enligt Riksrevisionens enkät[15] till myndigheten betraktas informationssäkerhet som en viktig ledningsfråga.

Ett flertal faktorer i myndighetens verksamhet påverkar SjöV:s bedömning av informationssäkerhetens betydelse i verksamheten. SjöV framhåller i sitt svar på enkäten att omfattningen av IT-beroendet, omfattningen av e-

[13] I stora stycken hämtat från SjöV Årsredovisning 2004.

[14] Ett register – Systemlistan – över alla de informationssystem som används av SjöV hålls av IT-enheten.

[15] Webbenkäten finns i bilaga 1.

tjänster och exponeringen på Internet, vikten av kontinuitet samt volymen incidenter som särskilt betydelsefulla faktorer för utformningen av arbetet med informationssäkerhet/IT-säkerhet.

Sammantaget anser SjöV enligt enkätsvaret att myndigheten har en informationssäkerhet som är tillräcklig.

SjöV har valt en starkt decentraliserad organisering av sitt informationssäkerhetsarbete. Verksamhetscheferna[16] inom avdelningarna är systemägare. Bland systemägarens ansvar ingår ansvaret för skyddet av systemen. Ekonomidirektören är systemägare för IT-infrastrukturen[17] och ansvarar för alla de tekniska skyddsåtgärder som vidtagits (behörighetskontrollsystem, virusskydd m.m.). I IT-rådet lämnas information från avdelningarna angående bl.a. pågående projekt och viss samordning av informationssäkerhetsfrågor. Ekonomichefen leder IT-rådet och är i direktionen föredragande när det gäller informationssäkerhetsfrågor. Hon har en säkerhetscontroller till sin hjälp. Controllern har i huvudsak arbetat med råd och stöd till systemägarna. Han har även tagit fram, för verksledningens beslut, ett stort antal dokument som beskriver SjöV:s ledningssystem för informationssäkerhet.

[16] Chefer direkt underställda avdelningschefer.

[17] Med IT-infrastruktur avser SjöV det gemensamma generella tekniska IT-stöd, i form av program- och maskinvaror, som verksamheten ges tillgång till.

3 Kontrollmiljön

3.1 Bedömningskriterier

Kontrollmiljön är en del av myndighetskulturen och skapas av myndighetens ledning och chefer i interaktion med medarbetarna och omgivningen.

Verksledningen bör skapa tillräckliga **förutsättningar** för arbetet med informationssäkerheten. Viktiga förutsättningar är lämpliga organisatoriska former för arbetet med informationssäkerhet, uttalat stöd till dem som arbetar med informationssäkerhet samt resurser som står i paritet med ledningens krav på skyddet av informationstillgångarna.

Verksledningen i statliga myndigheter bör noga avväga[18] det **engagemang** som ska ägnas informationssäkerhetsfrågorna vid sidan av övriga ledningsuppgifter. Av särskild vikt är det att detta görs i sådana myndigheter som har informationstillgångar som är av avgörande betydelse för verksamheten, är sekretessbelagda eller har stora databaser som avser enskilda eller företag och som därmed kan vara känsliga om de sprids. Detta engagemang och tillhörande syn på betydelsen av intern styrning och kontroll av informationssäkerhetsarbetet bör också kommuniceras till medarbetarna.

Att verksledningen lägger vikt vid informationssäkerheten bör också framgå av att den skaffat sig tillräcklig **förtrogenhet** med de ledningsfrågor som informationssäkerhetsarbetet innehåller.

Verksledningen bör tillse att de krav och mål som ska gälla för informationssäkerheten tydligt förmedlas till alla berörda IT-användare inom myndigheten. Detta bör göras i ett sammanhållet övergripande policydokument, en **informationssäkerhetspolicy**. Medarbetarna bör delges vikten av att informationssäkerhetskraven och övriga krav i informationssäkerhetspolicyn uppfylls samt vilka konsekvenser som i annat fall uppstår för den enskilde medarbetaren.

3.2 Iakttagelser

Verksledningen har genom omfattande handböcker och andra dokument, däribland en **informationssäkerhetspolicy**, uttryckt sina krav på informationssäkerheten. Den samlade dokumentmängden anses dock av flera intervjuade vara svår att överblicka.

[18] Ledningen bör kunna beskriva sina överväganden på ett konsistent sätt.

En viktig **förutsättning** för LIS funktionssätt är välfungerande rapporteringsrutiner som gör att delegationsgivare och delegationstagare görs uppmärksamma på problem, möjligheter och behov av åtgärder. Verksledningen[19] samråder om och samordnar frågor av strategisk betydelse för verksamheten. Granskningen visar att frågor som rör informationssäkerhetens betydelse för verksamheterna inte finns på verksledningens mötesagenda som en återkommande rapporteringspunkt. Dessa frågor har delegerats till avdelningschefer i linjen, ekonomichefen, IT-rådet, Paraplygruppen[20], IT-chefen och IT-säkerhetscontrollern. Detta utgör i sig inget problem men förutsätter att delegationen följs upp på ett ändamålsenligt sätt av GD och de som vidaredelegerat. Detta sker alltså i mindre utsträckning i ledningsgruppen. Frågor om informationssäkerhet hanteras även mer sällan i respektive avdelningschefs egen ledningsgrupp. IT-rådets ordförande avgör efter diskussion i rådet vilka frågor som ska föras till myndighetsledningen. Detta sker främst i form av avvikelserapportering i anslutning till att problem har uppstått, t.ex. en rapport om allvarlig incident. En sådan rapport kommer till IT-rådets kännedom om berörd avdelningschef fått kännedom om den från berörd systemägare och beslutat att föra frågan vidare till IT-rådet eller om IT-säkerhetscontrollern fått kännedom[21] om den i sin kontakt med systemägaren. Avdelningschefen kan också ta upp frågan direkt i verksledningen. Någon dokumenterad rutin för rapportering till verksledningen, IT-rådet och avdelningscheferna finns inte.

Beträffande ledningens **engagemang** i informationssäkerhetsfrågor har detta delvis belysts i beskrivningen ovan av rapporteringens omfattning och bristande formalisering. Riksrevisionen delar emellertid verksledningens uppfattning att inrättandet av IT-controllertjänsten är ett tecken på att informationssäkerhet uppfattas som en viktig fråga och att controllerfunktionen utgör en viktig del av myndighetens LIS. Innehavaren av tjänsten har beklagligtvis efter drygt ett års sjukdom avlidit. Under denna tid har ledningen haft svårigheter[22] att upprätthålla en fokuserad controllerfunktion genom att controllerns arbetsuppgifter fördelats på flera personer som i motsvarande utsträckning inte befriats från ordinarie uppgifter. IT-chefens ordinarie roll kan dessutom anses vara svår att förena med controlleruppgifter.

---

[19] Här avses GD och hans avdelningschefer.

[20] Har som främsta uppgift att samordna IT-baserad verksamhetsutveckling. Har dock i mindre utsträckning, enligt protokollen, hittills ägnat sig åt informationssäkerhetsfrågor. Enligt SjöV kommer gruppen att mera uppmärksamma dessa frågor framöver.

[21] Controllern är mottagare av samtliga incidentrapporter. Sätts in i en pärm som förvaras i hans rum.

[22] Hanterades genom konsultinsatser och omfördelning av arbetsuppgifter till IT-strateg och IT-chef.

3.3 Bedömning

Informationssäkerhetspolicyn samt övriga styrande dokument och handböcker uttrycker kraven på informationssäkerheten på ett rimligt tydligt sätt, men deras styrande verkan kan ifrågasättas genom att de uppfattas som svåra att överblicka.

Systemägarna har fått en nyckelroll i arbetet med informationssäkerheten. Verksledningen har dock inte infört sådana rapporteringsrutiner att ledningen kan få en samlad kunskap om hur väl arbetet med informationssäkerhet i praktiken utförs i linjen. Motsvarande rutiner saknas också inom de olika avdelningarna. Enligt Riksrevisionens bedömning torde det vara svårt för verksledningen att med dessa förutsättningar skapa sig en tillförlitlig bild av om systemägarna med stöd av säkerhetscontrollern förmår verka för att kraven på informationssäkerhet uppfylls. Det finns också risk för att kunskapsläget har försämrats under de senaste två åren under vilka säkerhetscontrollern på grund av sjukdom inte fullt ut kunnat sköta sin informationsinhämtning och vidarerapportering. Utan formaliserade rapporteringsrutiner på avdelningsnivå – med bl.a. genomtänkta kriterier för vad som ska föras vidare till skilda instanser som styr selekteringen – och med nedsatt controllerkapacitet påverkas även IT-rådets funktionssätt oförmånligt. I dessa avseenden saknas viktiga förutsättningar för god informationssäkerhet.

De uppmärksammande bristerna skulle enligt Riksrevisionens bedömning ha motiverat en uppföljning av LIS ändamålsenlighet, men någon sådan har inte genomförts. Vidare prövas inte[23] heller nivån på myndighetens faktiskt uppnådda informationssäkerhet, vilket hade varit en naturlig åtgärd i den ovan beskrivna situationen. Därmed bedömer också Riksrevisionen att ledningens engagemang i informationssäkerhetsfrågorna har vissa brister.

Riksrevisionen bedömer sammantaget att kontrollmiljön har brister.

[23] Riksrevisionen bortser härvid från användningen av standardprogramvara för vissa tester av nätverket.

4 Riskanalys

4.1 Bedömningskriterier

Riskanalys är en viktig förutsättning för och del av myndighetens riskhantering. Riskhanteringen innefattar en process för riskanalys. Den omfattar analyser och bedömningar av väsentliga hot, risker och konsekvenser av genomförda hot. För att bedöma om en verksamhet har genomfört en adekvat riskanalys kan sex olika kriterier användas.

Som underlag för analysen behövs identifiering[24] av de skyddsvärda informationstillgångarna. De bör dokumenteras i en överblickbar **förteckning** eller databas.

Åtminstone de tillgångar som är strategiska för verksamheten bör åsättas en beslutad säkerhetsnivå – **informationsklassning** – med hänsyn till verksamhetens krav på säkerhet så att en prioritering av åtgärder kan göras.

Riskanalysen bör utföras med hjälp av beslutade och dokumenterade **metoder**[25]. Riskanalys bör årligen, och däremellan vid behov, uppdateras. Analysen bör omfatta **alla risker** för bristande tillgänglighet, riktighet, sekretess och spårbarhet som kan vara väsentliga i verksamheten.

Det bör finnas en tydlig och uppföljningsbar **åtgärdsplan** som förtecknar beslutade åtgärder[26] för att möta de risker som framkommit i analysen, t.ex. avbrottsplanering och förstärkning av skyddsåtgärder. Planen bör beskriva när åtgärderna ska vara genomförda och vem som ansvarar för deras genomförande.

I riskhanteringsarbetet ingår att ta hänsyn till **incidenter** för att på så sätt kunna skapa förutsättningar för att begränsa dem i framtiden. Incidenter bör systematiskt dokumenteras och rapporteras så att en bild av de upptäckta säkerhetsproblem som finns i myndighetens informationshantering kan skapas.

---

[24] Identifieringen bör omfatta: vilka de är, vem som är ägare/har ansvar för dem, var de finns samt vilka kopplingar till andra tillgångar respektive tillgång kräver när den används.

[25] Exempel på riskanalysmetoder är SBA Scenario, RiscPac, CRAMM, RA, ISAP, ISF Sprint och Proteus.

[26] Dvs. åtgärder och kontroller som vidtas för att uppfylla specificerade säkerhetskrav som avser en viss informationstillgång. Skyddsåtgärderna omfattar bl.a. organisation och ansvar, administrativa rutiner, personalsäkerhet, fysiskt skydd, driftrutiner samt utrustnings- och programvarubaserade funktioner. Åtgärderna kan även indelas i förebyggande skydd, detekterande skydd och återställningsrutiner.

4.2 Iakttagelser

Det finns en **förteckning** över informationssystem hos IT-avdelningen. Denna omfattar en delmängd, förvisso mycket viktig, av verkets informationstillgångar. Det finns dock ingen sammanställning[27] som gör det möjligt att överblicka SjöV:s informationstillgångar i vilken även t.ex. dokumentation av system och driftprocesser samt licenser finns tillgänglig.

En **klassificering** av informationstillgångarna påbörjades för ett par år sedan men slutfördes inte. Det finns ännu inget formellt beslutat regelverk för klassificering av informationstillgångar. Granskningen visar dock att cheferna inom SjöV är medvetna om de viktigaste säkerhetskraven på verksamheterna och däri ingående informationssystem. Kraven på informationen som används i verksamheterna gäller bl.a. dess konfidentialitet, korrekthet, aktualitet och tillgänglighet. Det finns ett GD-beslut från år 1999 om vilka informationssystem inom SjöV som ska anses vara kritiska för samhällets eller verksamhetens funktion. Detta beslut har inte senare uppdaterats med t.ex. förändringar beträffande vilka system som finns kvar, vilka som slagits ihop med andra eller vilka eventuella nya kritiska system som tillkommit. Beslutet utnyttjas inte heller som en grund för riskanalyser.

Den riskanalys som sker av tekniska system, IT-stöd och IT-infrastruktur i februari varje år utgår från förordningen om myndigheternas riskhantering[28] och har därför fokus på ekonomiska risker för staten. Riskanalysen, som utförs av systemägarna, är inte kopplad till någon mer systematisk omvärldsbevakning och omfattar därmed inte alla **väsentliga risker**. Den gjorda analysen presenteras inte för avdelningscheferna utan skickas direkt från systemägarna till ekonomiavdelningen. Effekterna av riskanalysen är främst att SjöV tecknar vissa försäkringar.

SjöV:s IT-strategi redovisar på en övergripande nivå en koppling mellan verkets strategiska målområden och hur IT-relaterade insatser (IT-baserad verksamhetsutveckling) kan bidra till att målen uppfylls. I strategin ingår ingen översiktlig analys av risker för att de angivna insatserna inte kan genomföras som tänkt och med önskat resultat, konsekvenserna för berörda verksamheter av störningar i utvecklingen av IT-stödet samt hur myndigheten ska hantera dessa risker.

Chefer inom SjöV är dock inte omedvetna om risker för störningar i deras verksamheter och konsekvenser av störningar för mottagarna av myndighetens tjänster. Frågor som diskuteras är vad som händer om data går förlorade och hur lång tid det tar att återställa data (tillgängligheten). Men det sker ingen systematisk och metodisk riskanalys som fokuserar informationssäkerhetsriskerna med utgångspunkt i ett verksamhetsper-

[27] I en verksamhet av SjöV:s omfattning bör det finnas en sammanhållen databas med sådana uppgifter.

[28] Förordningen (1995:1300) om myndigheters riskhantering.

spektiv och som omfattar samtliga IT-system. En årlig riskanalys av ovan nämnt slag kan inte ersättas av den rapportering som sker i IT-rådet. Inte heller analyseras förekomsten av interna hot.

Det saknas också beslut om val av och utbildning beträffande användning av specifika **metoder** och verktyg[29] för riskanalysen.

Den modell som SjöV valt för att decentralisera och delegera ansvar för systemen till linjen innebär att behovet av säkerhetsåtgärder tas fram för respektive system och hanteras sedan i beslutsprocessen för respektive systems förvaltning. **Åtgärdsplaner** finns alltså endast i meningen systemförvaltningsplaner. Insprängt i dessa planer, vid sidan av planerade förändringar i systemens funktionalitet, finns informationssäkerhetsinriktade åtgärder. Någon samlad bild av risker, beslutade informationssäkerhetsåtgärder samt genomförandeläget beträffande dessa finns inte och förmedlas alltså inte till ledningen. Visst stöd finns dock i IT-planen[30].

4.3 Bedömning

SjöV har inte skaffat sig de förutsättningar och rutiner som behövs för att kunna överblicka informationstillgångarna, säkerhetsåtgärderna – både redan vidtagna och beslutade men inte genomförda – och de kostnader som säkerhetsarbetet medför. De brister som framkommit ovan beträffande fokus och metodik i myndighetens riskanalys tillsammans med den begränsade överblick som framhållits torde medföra svårigheter att bedriva en effektiv riskanalys och riskhantering.

Riksrevisionen bedömer därför att SjöV:s hantering av risker relaterat till informationssäkerheten har brister.

[29] Tidigare använde SjöV SÅRB-metoden.

[30] På denna punkt anser SjöV att ”om de totala kostnaderna för ett system ökar mer än vad som är rimligt så märks det genom IT-planen, som är ett mycket viktigt instrument för oss i samband med budgetarbetet där beslut fattas om vad respektive system får kosta under kommande år”.

5 Ledningens kontrollfunktioner samt införda skyddsåtgärder

5.1 Bedömningskriterier

Med kontrollfunktioner avses i detta sammanhang de åtgärder som ledningen utformat för att förebygga, upptäcka och åtgärda brister i informationssäkerheten. Dessa kan exempelvis vara att formulera och införa policyer och regler för informationssäkerheten samt tekniska kontrollåtgärder såsom behörighetskontroller, loggningsförfaranden m.m. Kontrollfunktionerna utgör sammantagna en väsentlig del av myndighetens ledningssystem för informationssäkerhet (LIS).

Myndigheten bör ha ett LIS med **beslutade och dokumenterade komponenter.** LIS syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten. Ett väl fungerande LIS innebär därmed att de strategiska informationstillgångarna har ett tillräckligt och kostnadseffektivt skydd i förhållande till bedömda risker.

LIS bör normalt ha följande **omfattning** när det gäller komponenter[31]:

- informationssäkerhetspolicy
- process för incidentrapportering inklusive beslut om vilka incidenter som ska rapporteras till ledningen
- åtgärdsplan för informationssäkerhet
- kontinuitetsplan
- utsedd person med övergripande och samordnande ansvar för myndighetens informationssäkerhet
- Internetpolicy
- distansarbetspolicy
- e-postpolicy
- åtkomstpolicy[32]
- process för säkerhetskopiering av all verksamhetskritisk information.
- process för styrning av utveckling och förändringar i IT-miljö, IT-system och bemanning

[31] En del komponenter tas upp i särskilda avsnitt, bl.a. riskanalys och de som avser utbildning och information, och medtas därför inte i denna uppställning.

[32] Policy som reglerar åtkomst av informationstillgångar.

- tekniska skyddsåtgärder (behörighetskontrollsystem, virusskydd, brandväggar m.m.)
- processer för att kontrollera efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som bl.a. ovannämnda policykomponenter tillsammans bildar
- en till all personal kommunicerad skriftlig beskrivning av roller[33] i informationssäkerhetsarbetet och hur ansvar och befogenheter för myndighetens informationssäkerhet fördelats på dessa.
- processer för återkommande uppföljning och förvaltning av LIS.

Komponenterna bör vara utformade utifrån myndighetens särskilda behov och därvid beakta relevant "**best practice**"[34] inom aktuellt område.

De bör vidare vara väl **införda** i verksamheterna.

Komponenterna bör tillsammans utgöra en lämpligt utformad **helhet** genom sina inbördes samband samt utgöra en väl integrerad del i myndighetens (totala) ledningssystem.

5.2 Iakttagelser

Granskningen visar att SjöV har ett **LIS med dokumenterade och beslutade komponenter.**

SjöV:s LIS **omfattar** ett antal tekniska säkerhetsåtgärder i IT-infrastrukturen (behörighetskontrollsystem, program som automatiskt identifierar sårbarheter i nätverket, virusskydd, brandväggar m.m.) för att skydda sina informationstillgångar. Särskilda skyddsåtgärder har vidare införts för att skydda särskilt känsliga data (djupdata). LIS-komponenter av policykaraktär finns också framtagna. Det saknas emellertid väsentliga komponenter av organisatorisk karaktär: delar av processen för information och utbildning inom informationssäkerhetsområdet (tas upp i avsnitt 7.2), myndighetsövergripande kontinuitetsplan, liksom regler för hur de partiella kontinuitetsplanerna ska utformas och övas. Brister i riskanalysprocessen som bl.a. försvårar överblicken i denna krävande process har redovisats i avsnitt 4.2.

LIS-dokumentationen visar på god insikt i de grundläggande frågorna beträffande informationssäkerhet och LIS-standarden. I vissa fall har de dokumenterade reglerna mer karaktär av råd eller lärobokstext[35] än specifik reglering av frågor som rör just SjöV. Syftet med detta är enligt uppgift att sprida allmän information om IT-säkerheten och inte beskriva preciserade

[33] Exempelvis säkerhetschef, systemägare, användare, IT-styrgrupp m.fl.

[34] Myndigheten bör alltså informera sig om och dra nytta av de kunskaper som finns i standards såsom SS17799, NIST:s 800-serie av rapporter m.fl.

[35] Gäller bl.a. incidentrapporteringsavsnittet i säkerhetshandboken.

regler på detaljnivå per verksamhet. Det senare kan vara en konsekvens av att systemägare förväntas bestämma vad som ska gälla för de enskilda systemen. Det leder dock till att bl.a. incidentrapporteringsavsnittet i säkerhetshandboken blir onödigt abstrakt och fjärmat från myndighetens verksamhet. Det pågår inget arbete för att göra regelverket mera lättillgängligt och specifikt

Beträffande **införandet** har SjöV inte kunnat redovisa förekomsten av formella direktiv för IT-rådets ansvar och uppgifter inom informationssäkerhetsområdet. Rådet arbetar snarare reaktivt än proaktivt. Rapportering sker när systemägare eller ägaren av IT-infrastrukturen har ett problem att lösa. Rådet diskuterar inte på förhand vad som skulle kunna hända och vad som eventuellt behöver göras långsiktigt för att möta nya krav eller för att sänka kostnaderna för säkerhetsarbetet. Vidare är ledningens styrning av incidentrapporteringen relativt otydlig och svagt systematiserad. I dag är det varje systemägare som ska bedöma vad som ska betraktas som en rapporteringsvärd incident. Från intervjuerna framkommer att det är oklart för bl.a. systemägare vad som utgör sådana incidenter, när rapportering ska ske och med vilket hjälpmedel[36]. Dessa incidentrapporter förvaras i en pärm hos IT-säkerhetscontrollern, och erfarenheterna från incidenter och deras hantering delas inte på ett systematiskt sätt bland systemägarna. Viktiga rutiners resultat följs inte alltid upp, exempelvis att säkerhetskopieringsrutinerna som IT-avdelningen hanterar[37] för systemägarens räkning faktiskt fungerar (dvs. att backupkopior kan återläsas vid behov).

Incidentrapporteringsprocessen är därmed inte heller utformad i enlighet med vad som måste betraktas som "**best practice**". Detsamma gäller informations- och utbildningsprocessen samt myndighetens riskanalysprocess, enligt redovisade iakttagelser i avsnitt 4.2.

5.3 Bedömning

Ett flertal LIS-komponenter saknas eller har brister i sin utformning eller införande. Enligt Riksrevisionens bedömning har SjöV främst satsat resurser på tekniska säkerhetsåtgärder av standardkaraktär i sin IT-infrastruktur.

Sammantaget bedömer Riksrevisionen att dessa brister i LIS medför ökad risk för brister i informationssäkerheten

[36] Det finns dock ett särskilt Word-dokument för incidenter som rör IT-säkerheten.
[37] Det finns dokumenterade rutiner för säkerhetskopieringen som IT-enheten följer.

6 Information och utbildning om informationssäkerhet

6.1 Bedömningskriterier

Området information och utbildning avser ledningens åtgärder för att förse personalen med relevant information och kunskaper om informationstillgångar, säkerhetsåtgärder, incidenter och andra viktiga aspekter beträffande LIS. Området innefattar också åtgärder för att säkra att ledningen får relevant information från organisationen.

Det bör finnas en **process** för systematisk och återkommande information och utbildning beträffande informationssäkerhet till **berörda personalgrupper**[38]. Den bör innefatta de anställdas ansvar för informationssäkerheten samt de väsentliga hot och risker som ska beaktas i deras arbete. Syftet med informations- och utbildningsåtgärderna bör vara att ge all berörd personal förutsättningar att hantera sådana informationssäkerhetshändelser som kan uppkomma. För cheferna ska det vidare finnas välfungerande **informations och rapporteringsrutiner** som ger erforderligt underlag för ledningsarbetet som avser informationskvalitet.

6.2 Iakttagelser

SjöV har tagit fram omfattande dokumentation som riktar sig till SjöV:s personalgrupper i skilda informationssäkerhetsfrågor: regelverk i form av bl.a. IT-säkerhetshandbok, IT-handbok och handbok för dokumenthantering, ett kortare informationsavsnitt i introduktionsutbildningen för nyanställda samt viss information om säkerhet i samband med att en anställd ges tillgång till specifik IT-tjänst eller IT-system. Det finns emellertid ingen systematisk **process** för utbildning av olika **personalgrupper**, inklusive chefer. Detta har även SjöV påpekat i svaret på webbenkäten. Av intervjuer med chefer inom SjöV framkommer ett uttalat behov av någon form av vidareutbildning och/eller återkommande information för chefer. Det framkom bl.a. i intervjuerna att systemägare inte varit fullt medvetna om vilka uppdateringar som gjorts av reglerna inom säkerhetsområdet och innebörden av dessa för systemägarens ansvar. Problematiskt är också att regelverket, som också

[38] Personal med ansvar för säkerhet, nyanställda, myndighetsledning, övriga chefer och övriga medarbetare.

beskrivits i avsnitt 5:2, blivit svåröverblickbart genom sin omfattning och genom att det spritts i många dokument. Intervjuerna visar också på att detta medfört svårigheter för personalen att ta till sig budskapet och följa reglerna.

Hur det förhåller sig med kunskaperna har inte närmare undersökts av SjöV. En kompetensinventering som omfattat hälften av personalen har dock gjorts, och den har delvis berört informationssäkerhetskunnandet.

När personal begär att få tillgång till ett visst IT-system sker vidare ingen kontroll från systemägarnas sida om personen i fråga kan[39] de regler som gäller för detta.

Som nämnts i avsnitt 3.2 finns brister i **rapporteringsrutinerna** som har till uppgift att göra att delegationsgivare och delegationstagare uppmärksamma på problem, möjligheter och behov av åtgärder beträffande LIS eller informationssäkerheten. Någon dokumenterad rutin för rapportering till verksledningen, IT-rådet och avdelningscheferna finns inte heller.

6.3 Bedömning

Riksrevisionen bedömer att SjöV i alltför stor utsträckning utgår från att personalen, inklusive cheferna, är förtrogen med informationssäkerhetsfrågorna och att de följer regelverket för informationssäkerhet. Det finns ingen systematisk process för utbildning av olika personalgrupper, inklusive chefer. Bland annat saknas en återkommande och systematisk uppföljning av personalens kunskaper om informationssäkerhet och av regelefterlevnaden. Ledningen har alltså inte infört tillräckliga funktioner för att försäkra sig om att personalen får tillräckliga kunskaper om informationssäkerhet och följer de regler som finns. Detta ökar risken för brister i LIS funktion och därmed i informationssäkerheten.

[39] Exempelvis genomgått relevant utbildning.

7 Uppföljning och förvaltning

7.1 Bedömningskriterier

Den snabba förändringstakten i omvärlden och i de egna verksamheterna kräver kontinuerlig omvärdering av processer och system för intern styrning och kontroll. Ledningens uppföljning av den interna styrningens och kontrollens utformning och effektivitet är vidare det kanske viktigaste underlaget för förbättring av myndighetens LIS.

Uppföljningen bör ske **systematiskt och regelbundet**.

Den bör vara **dokumenterad**.

Verksledningen bör också följa upp beslutade **delegationer**.

Uppföljningen bör ge svar på om följande **väsentliga delar** av LIS fungerar som avsett:

- riskanalysprocessen
- åtgärdsplanering och genomförande av planerna
- incidentrapporteringen
- kontinuitetsplaneringen
- den interna kontrollen beträffande information och utbildning angående informationssäkerhet
- den interna kontrollen av utveckling och förändringar i IT-miljö, IT-system och bemanning
- den interna kontrollen av tekniska skyddsåtgärders funktion (behörighetskontrollsystem, virusskydd, brandväggar m.m.)
- den interna kontrollen av efterlevnaden av det regelverk för upprätthållande av informationssäkerhet som grundas på informationssäkerhetspolicy, Internetpolicy, e-postpolicy, distansarbetspolicy m.fl.
- den faktiskt uppnådda informationssäkerheten prövas systematiskt och uppfyller säkerhetskraven.

Resultaten från denna uppföljning och kontroll utgör underlag för förvaltning och utveckling av myndighetens LIS. Ledningen bör ha infört en dokumenterad process för **förvaltning och utveckling** av sitt LIS.

7.2 Iakttagelser

Ledningens ansvar för informationssäkerheten har delegerats och decentraliserats inom organisationen. Frågor som rör informationssäkerhetens betydelse för verksamheterna finns, som nämnts i avsnitt 3.2, inte på verksledningens mötesagenda som en återkommande rapporteringspunkt. Dessa frågor har delegerats till avdelningschefer i linjen, ekonomichefen, IT-rådet, Paraplygruppen[40], IT-chefen och IT-säkerhetscontrollern. Frågor om informationssäkerhet hanteras sällan i respektive avdelningschefs egen ledningsgrupp. Verksledningens bedömning av hur LIS fungerar bygger till stor del på de frågor som kommer upp i IT-rådet och Paraplygruppen. Ledningen har som nämnts i tidigare avsnitt dock inte dokumenterat rapporteringsrutinerna till och från IT-rådet och inte heller följt upp att IT-rådet fungerar bra som informationskanal i frågor som rör informationssäkerheten. Riksrevisionen har inte presenterats någon **systematisk och regelbunden** uppföljning av LIS som helhet eller av enskilda **delar.** Särskilda analyser av frågor som rör informationssäkerhet har dock genomförts i projektform, t.ex. digitala signaturer (PKI-projektet). Ledningen har inte heller genom externa eller internt genomförda test låtit genomföra någon utvärdering av den faktiskt uppnådda informationssäkerheten.

Beträffande uppföljning av beslutade **delegationer** uttrycker ledningen att man förutsätter att arbetet med informationssäkerheten fungerar enligt beslutat regelverk och delegationer. IT-säkerhetscontrollern har att stödja informationssäkerhetsarbetet men har inte som uppgift att stödja verksledningens uppföljning av systemägarnas och andra delegationsmottagares ansvarstagande för att IT-säkerheten fungerar inom respektive ansvarsområde.

Frånvaron av systematisk och regelbunden uppföljning av LIS medför att underlag saknas för förvaltning och utveckling av LIS. Riksrevisionen har inte heller funnit någon tydlig och dokumenterad process för **förvaltning och utveckling** av myndighetens LIS.

7.3 Bedömning

Ett ändamålsenligt LIS består av en kedja av samverkande delar. De brister i systematik i uppföljningen av väsentliga delars funktionssätt som påpekats ovan försämrar verksledningens möjligheter till överblick av säkerhetsarbetets ändamålsenlighet och försämrar möjligheterna att förvalta och utveckla myndighetens LIS. Konsekvenserna av bristande uppföljning blir

[40] Har som främsta uppgift att samordna IT-baserad verksamhetsutveckling. Har dock i mindre utsträckning, enligt protokollen, hittills ägnat sig åt informationssäkerhetsfrågor. Enligt SjöV kommer gruppen att mera uppmärksamma dessa frågor framöver.

därigenom många och komplexa. Bristande uppföljning av exempelvis personalens kunskaper om regelverket för informationssäkerhet och dess tillämpning innebär förhöjd risk för brister i informationssäkerheten eftersom kunskapsbristen inte kommer att beaktas i myndighetens riskanalyser. Riskanalysen (delen sårbarhetsanalys) utgår därmed inte från en samlad bild av det faktiska sårbarhetsläget, och ledningens bild av det säkerhetsläget blir osäker.

Riksrevisionen bedömer att SjöV har brister i uppföljningen av det LIS som vuxit fram samt att det inte finns någon tydlig och dokumenterad process för förvaltning och utveckling av myndighetens LIS.

Riksrevisionens slutsats är att bristerna i uppföljning minskar ledningens möjligheter till rationella beslut om förbättringar i säkerheten och om utvecklingen av LIS.

8 Slutsatser och rekommendationer

8.1 Inledande lägesbeskrivning

Granskningen av SjöV:s ledningssystem för informationssäkerhet visar att myndigheten infört flera av de delar av ledningssystemet som bör finnas enligt standarden SS-ISO/IEC 17799[41]. Bland dessa finns exempelvis behörighetssystem, eget skalskydd och fristående nätverk för särskilt känsliga data, säkerhetskopiering etc. Myndigheten har också utarbetat policyer samt riktlinjer för organisering av arbetet med informationssäkerheten.

Riksrevisionen konstaterar att SjöV under senare tid inte har haft – eller inte upptäckt[42] – några allvarliga incidenter. Samtidigt har myndighetens utveckling av e-tjänster lett till en ökad exponering för risker både internt vid myndigheten och för andra aktörer och myndigheter som är beroende av den information som förmedlas via de nya e-tjänsterna.

8.2 Bedömning och slutsatser

Granskningen har till syfte att besvara följande fråga:

Arbetar Sjöfartsverket, utifrån gängse normer, systematiskt med sin informationssäkerhet?

Granskningen visar på följande huvudsakliga brister.

Brister i informationssäkerhetsarbetets rapporteringsrutiner

Det finns brister i rapporteringsrutinerna som har till uppgift att göra delegationsgivare och delegationstagare uppmärksamma på problem, möjligheter och behov av åtgärder beträffande LIS eller informationssäkerheten. Någon dokumenterad rutin för rapportering till verksledningen, IT-rådet och avdelningscheferna finns inte. Vilken information – exempelvis vilka typer av incidenter som ska rapporteras vidare från verksamheterna – som ska nå dessa mottagare är inte beskrivet. Andra brister i rapporteringen tas upp nedan i riskanalysavsnittet.

[41] SS-ISO/IEC 17799 är den väletablerade internationella standards som Riksrevisionen granskat mot.

[42] Enligt Riksrevisionen är ”inget hänt” inte ett kriterium på god säkerhet.

Brister i SjöV:s styrande dokument
Informationssäkerhetspolicyn och vart och ett av de övriga styrande dokumenten och handböckerna uttrycker kraven på informationssäkerhet inom de områden de avser på ett rimligt tydligt sätt. Deras styrande verkan som helhet kan dock ifrågasättas genom att de uppfattas som svåra att överblicka för personalen.

Brister i riskanalysen
Det finns flera brister i SjöV:s riskanalysprocess och i förutsättningarna för processen. Det genomförs inte en systematisk och metodisk riskanalys som fokuserar informationssäkerhetsriskerna i verksamheterna och som omfattar de viktigaste IT-systemen.

Det saknas också beslut om val av och utbildning beträffande användning av specifika metoder och verktyg för riskanalysen. Den riskanalys som sker av tekniska system, IT-stöd och IT-infrastruktur i februari varje år utgår från förordningen om myndigheternas riskhantering[43] och har därför fokus på ekonomiska risker för staten.

Riskanalysen, som utförs av systemägarna, är inte kopplad till någon mer systematisk omvärldsbevakning. Den gjorda analysen presenteras inte för avdelningscheferna utan skickas direkt från systemägarna till ekonomiavdelningen.

Behovet av säkerhetsåtgärder tas fram för enskilda system och hanteras sedan i beslutsprocessen för respektive systems förvaltning. Åtgärdsplaner finns alltså endast i meningen systemförvaltningsplaner. Insprängt i dessa planer, vid sidan av planerade förändringar i systemens funktionalitet, finns informationssäkerhetsinriktade åtgärder. Någon samlad bild av risker, beslutade informationssäkerhetsåtgärder samt genomförandeläget beträffande dessa finns inte och förmedlas alltså inte heller till ledningen.

Brister i möjligheterna till överblick i informationssäkerhetsarbetet
Att skapa, upprätthålla och utveckla god informationssäkerhet är en svår uppgift i det alltmer komplexa hot- och riskpanorama som alla myndigheter möter. En väsentlig del av svårigheten ligger i behovet av att överblicka och hantera en stor mängd företeelser varav många förändras över tiden. SjöV:s informationssäkerhetsarbete kräver överblick bl.a. över

- vilka informationstillgångar som ska skyddas,
- vilka hot som ska prioriteras och avvärjas med skyddsåtgärder,
- vilka risker man får leva med och nöja sig med att lindra effekterna av,

[43] Förordningen (1995:1300) om myndigheternas riskhantering.

- vilka skyddsåtgärder som redan införts och vilka svagheter (sårbarhet) som uppstått hos dem till följd av tillkommande hot,
- vilka tekniska förändringar i IT-miljö och rutiner som skett och som skapar ny sårbarhet.

För SjöV:s del motsvaras de uppräknade faktorerna av tusentals företeelser som behöver överblickas i skilda delar av informationssäkerhetsarbetet. Det är på grund av sådana komplex av tillgångar, beslut, åtgärder och hot som LIS-standarden efterlyser stöd för att överblicka arbetsfältet. Det bör i en informationsbehandlande verksamhet av SjöV:s omfattning och komplexitet finnas en databas som registrerar alla skyddsvärda informationstillgångar, vilka individuella krav på skydd som gäller för dem, vilka skyddsåtgärder som vidtagits för var och en av dem, vilka som ansvarar för tillgångarna, vilka beroendeförhållanden som finns tillgångarna emellan m.m. SjöV har separata listor över vissa tillgångar men saknar en sammanställning som gör det möjligt att överblicka SjöV:s informationstillgångar och där även säkerhetsklassning, dokumentation av system och driftprocesser, licenser m.m. ingår.

En klassificering av informationstillgångarna påbörjades, men slutfördes inte. Det finns heller inget formellt beslutat regelverk för klassificering av informationstillgångar.

På samma sätt behövs en övergripande plan över alla beslutade nya skyddsåtgärder (säkerhetsinvesteringarna), vilka som ansvarar för deras införande och korrekta funktion samt när de ska vara operativa.

Inget av dessa behov av hjälpmedel för överblick finns väl tillgodose. Behovet accentueras av de ovan beskrivna bristerna i rapportering i en komplex säkerhetsorganisation.

Brister i uppföljning och förvaltning av LIS

SjöV saknar en systematisk och regelbunden uppföljning av LIS som helhet liksom av enskilda delar. Särskilda analyser av frågor som rör informationssäkerhet har dock genomförts i projektform, t.ex. PKI-projektet. Ledningen har inte heller genom externa eller internt genomförda test låtit genomföra någon utvärdering av den faktiskt uppnådda informationssäkerheten.

Rapportering av säkerhetsincidenter har flera funktioner, bl.a. som uppföljning av vidtagna säkerhetsåtgärders effektivitet. Styrning av incidentrapporteringen är relativt otydlig och ofullständigt systematiserad. Varje systemägare bedömer vad som ska betraktas som en rapporteringsvärd incident. Det sker inte heller någon systematisk erfarenhetsåterföringen beträffande incidenterna.

Frånvaron av systematisk och regelbunden uppföljning av LIS medför att underlag saknas för förvaltning och utveckling av LIS.

Det saknas viktiga delar i SjöV:s LIS

Till bristerna i möjligheterna till överblick, i riskanalysen och i utbildningsprocessen kan läggas att en myndighetsövergripande kontinuitetsplan saknas liksom regler för hur de partiella kontinuitetsplanerna ska utformas och övas.

Det finns ingen systematisk process för utbildning av olika personalgrupper, inkl. chefer, i informationssäkerhet vid sidan av introduktionsutbildningen. Insatser för att underhålla personalens kunskaper om informationssäkerhet sker inte regelmässigt.

SjöV:s LIS saknar därmed viktiga komponenter som tas upp i LIS-standarden.

Sammanfattande bedömning

SjöV har flera av de delar som enligt standarden tillsammans utgör ett LIS. Som framgått ovan är dock vissa delar av LIS mindre väl utvecklade – funktioner som skapar överblick, rapportering, riskanalys, utbildning samt uppföljning och förvaltning av LIS. Dessa brister medför att SjöV:s LIS inte utgör en fullt ut lämpligt utformad och fungerande helhet. Vissa länkar i den kedja som ledningssystemets komponenter bildar saknas eller är för svaga. I praktiska termer innebär detta att bl.a. bristerna i rapportering i informationssäkerhetsarbetet, bristande överblick och brister i uppföljning av LIS minskar SjöV:s möjligheter att registrera de erfarenheter som gör ett systematiskt förvaltningsarbete möjligt. Med förvaltningsarbete avses här det styrda förbättringsarbete som syftar till att stegvis förbättra LIS.

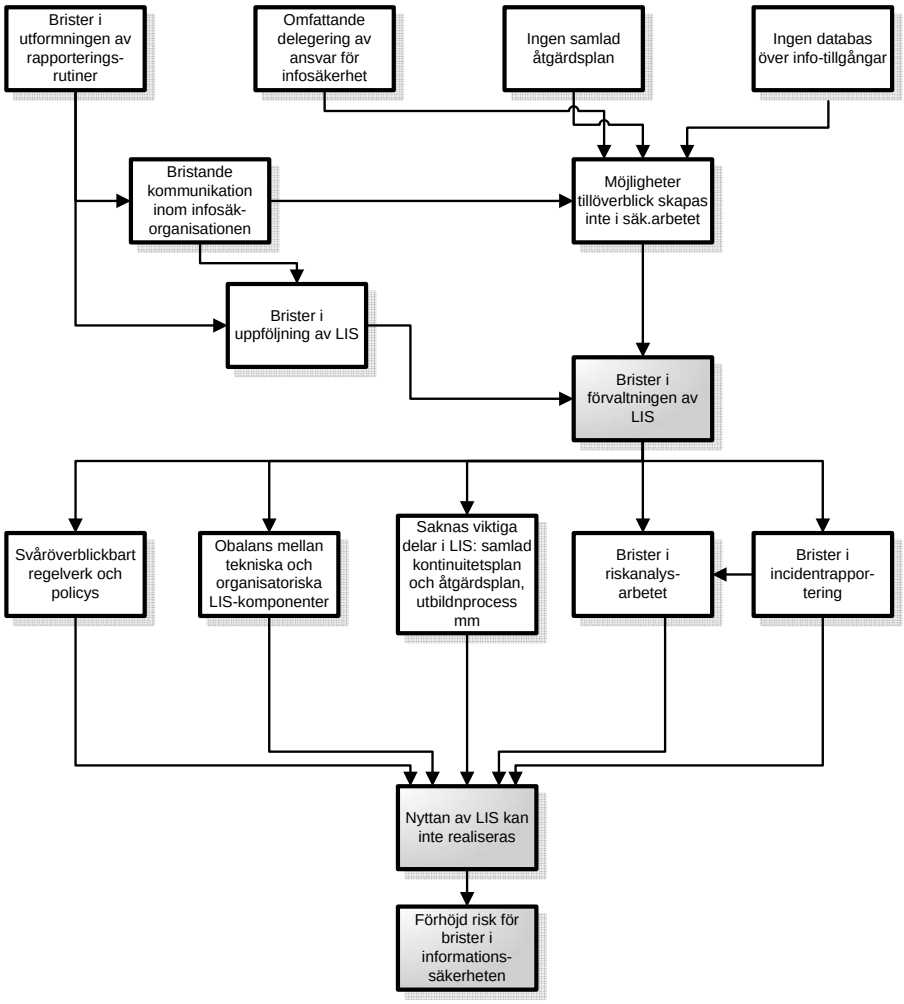
Enligt Riksrevisionens bedömning har SjöV kommit att prioritera tekniska skyddsåtgärder, medan organisatoriska, beteendepåverkande åtgärder såsom uppföljnings- och rapporteringsrutiner, erfarenhetsåterföring samt utbildning i informationssäkerhet inte fått tillräcklig uppmärksamhet. Att en sådan prioritering skett har inte framstått tydligt för verksledningen på grund av de påpekade bristerna i uppföljning och förvaltning av LIS.

Vidare finns brister i den kanske mest grundläggande delprocessen i ledningssystemet för informationssäkerhet – riskanalysen. SjöV har inte skaffat sig de förutsättningar och rutiner som behövs för att kunna överblicka informationstillgångarna, säkerhetsåtgärderna – både redan vidtagna och beslutade men inte genomförda – och de kostnader som säkerhetsarbetet medför. De brister som framkommit beträffande fokus och metodik i myndighetens riskanalys bedömer Riksrevisionen medföra svårigheter att bedriva en effektiv riskanalys och riskhantering. Svårigheterna ökar eftersom stöd för en samlad överblick över informationstillgångarna m.m. inte utvecklats, som tidigare påpekats. Ett tecken på sådana svårigheter är att de interna hoten (misstag, regelbrott och eventuella oegentligheter från personalens sida) ges liten uppmärksamhet i analyserna.

Kunskapsläget beträffande risker i verksamheterna torde vidare ha försämrats under de senaste två åren under vilka säkerhetscontrollern på grund av sjukdom inte fullt ut kunnat sköta sin informationsinhämtning och vidarerapportering. I det läget hade det enligt Riksrevisionens bedömning varit motiverat att göra en extern genomgång både av LIS ändamålsenlighet och nivån på myndighetens faktiskt uppnådda informationssäkerhet så att eventuellta nödvändiga säkerhetsåtgärder snabbt kunnat vidtas, men någon sådan har inte genomförts. Detta förhållande bedöms bidra till att det finns olika uppfattningar inom SjöV om informationssäkerheten är god eller oklar. Å ena sidan hävdas från chefer att säkerheten är god med tanke på frånvaron av grava incidenter och vidtagna tekniska säkerhetsåtgärder i IT-miljön. Å andra sidan framkommer under intervjuerna sådant[44] som pekar på att informationssäkerhetsnivån är oklar.

[44] Bl.a. att information och utbildning för personalen, inte minst för chefer, inte är tillräcklig samt att systemägare inte kontrollerar hur väl säkerhetsåtgärderna faktiskt fungerar.

Figur 2. Sambandsschema.



Bristerna i LIS påverkar i sin tur möjligheterna att uppnå och vidmakthålla eftersträvad informationssäkerhet.

Svaret på den fråga som granskningen syftat till att besvara är därmed att SjöV inte fullt ut arbetar systematiskt med sin informationssäkerhet utifrån gängse normer.

En schematisk illustration av hur de ovan beskrivna bristerna i LIS påverkar SjöV:s nytta av ledningssystemet framgår av figur 2. De faktorer som enligt Riksrevisionens bedömning medverkar till ”Brister i förvaltningen av LIS” återfinns i den övre delen av schemat. Av den nedre delen av schemat framgår att ”Brister i förvaltningen av LIS” medför att brister i SjöV:s LIS inte upptäcks eller åtgärdas. Bristerna i LIS får som konsekvens

att nyttan av ledningssystemet blir nedsatt, vilket i sin tur medför förhöjd risk för brister i den faktiska informationssäkerheten.

8.3 Rekommendationer

SjöV:s ledning bör genomföra åtgärder för att komplettera sitt LIS i syfte att öka nyttan för myndigheten. En del av bristerna i LIS avser de funktioner – uppföljning och kontroll av LIS funktionssätt – som möjliggör ett systematiskt lärande beträffande LIS. Detta behövs för att SjöV stegvis ska kunna förbättra sitt LIS. Riksrevisionen rekommenderar därför att

- ledningen kombinerar sin omfattande delegering av ansvaret för informationssäkerheten till systemägare med en systematisk uppföljning av att systemägarna tar sitt ansvar. Ledningens behov av stöd och metoder för denna uppföljning bör samtidigt ses över.
- avdelningarna och deras systemägare följer på ett mer systematiskt sätt upp kontinuiteten i verksamhetens nyckelprocesser, personalens kompetens i informationssäkerhetsfrågor och efterlevnaden av regelverket för informationssäkerhet. Behovet av stöd och metoder ör denna uppföljning bör samtidigt ses över.
- riskanalysen utvecklas med avseende på metodik, fokus och stöd. Med stöd avses att systemägarna kan behöva få en mer handfast hjälp med bl.a. informationsklassificering samt upplägg och genomförande av riskanalyser.
- alla noteringar i systemförvaltningsplaner, IT-planen och andra dokument som avser beslutade säkerhetsåtgärder sammanställs årligen till en tydlig plan över beslutade åtgärder (åtgärdsplan) som används för genomförandet men också för återkommande uppföljning av vad som genomförts. Den bör ge en samlad bild av risker, beslutade informationssäkerhetsåtgärder samt beräknade kostnader för dessa. Planens genomförande bör följas upp. Planen och dess uppföljning utgör ett viktigt underlag för ledningens styrning av arbetet med informationssäkerhet.
- myndigheten utvecklar sin incidentrapportering. Det bör undersökas om det ledningssystem (ISO-systemet) med tillhörande webbaserade rapporteringssystem som utvecklas även skulle kunna omfatta incidentrapportering som avser IT-säkerheten. I samband med detta bör tydligt definieras vilka typer av incidenter som ska rapporteras och hur rapporteringen ska gå till.

- ledningen initierar en systematisk och återkommande utbildning och informationsförmedling inom området informationssäkerhet för olika personalkategorier. En särskild fråga är hur sådan utbildning ska utformas för dem med lång anställningstid, direktionen samt systemägarna.
- den faktiskt uppnådda informationssäkerheten följs upp och prövas när hotbilden, IT-miljön eller andra för informationssäkerheten väsentliga faktorer förändrats. Är förändringarna väsentliga eller svåra att bedöma bör insats av extern expertis övervägas.
- de förstärkningar av myndighetens LIS som föreslås ovan dokumenteras i de styrande nyckeldokumenten. Det kan i samband därmed finnas anledning att se över regelverket som beskrivs i dessa dokument i syfte att göra det mera överblickbart för personalen.

Bilaga 1 SjöV:s IT-system[45]

System	Beskrivning
Adressregister	Receptionens adressregister
Aecdis	Elektroniskt navigationsstöd. Inkl. inspelning av AIS-data
AMOS M&P	Underhåll fartyg
BearbSYS	Bearbetning djupdata
BehörighetsSystemet - SYB	Sjömansbehörigheter
Beklädnadssystemet	
Bibliotekssystem (Polydoc)	
Bilregister	
BSC-verktyg	ProDacapo - stödsystem för Balanced Score Card.
DGPS	Referensstationer för GPS.
DISCO-SAR	Sjöräddningssystem
EasIT	HelpDesk-system
ECDIS Transas	Navigationsystem
Ekonomisystemet	RAINDANCE
EU-ärendelista	
FAREG	Farledsunderhållssytem
Fargos	Farligt gods-databas som KBV rapporterar in till.
Farled	Tidrapportering, och lotsadministration och lön
Faster	Inrapportering och hantering av förbättringsförslag, noterade fel och avvikelser.
Fordonsregistret	
Foxtrot	Farledsdeklarationer
FRS	Fartygsrapportering, förhandsanmälningar
Fyren	Extern hemsida
Förarintygsregister	
Geodesi/Vattenstånd	

[45] Kursiverad text markerar de system som av myndigheten betecknas som verksamhetskritiska.

IB-NET		Operativ isbrytningsledning
Insjö		Incidentrapportering för sjöfarten
Landlord		Fastighetsunderhåll
NAPA		Stabilitets-beräkningssystem
Nauticus Hull		Beräkning av skrovstyrka
PACT		Diarieföring
PA-system (TPHR)		
Pensionsregister		
Personaliz		Personaladministration isbrytare
Personuppgiftsregister	PUL	
PROFS		Produktframställning sjökort och publ. (inkl. Barco)
PS Lön Travel		Reseräkningar
ROS		Administrerar rättelser i djupdata och sjökort
Simulator Arkö		Bryggsimulator för utbildning
Sirenac 2000		Registrering av hamnstatskontroller i databas i Frankrike.
SITS		Fartygstillsynssystem
SJKBAS		Sjökortsdatabas
Sjöfartsregistret		Skeppsregister
SJÖMIS		Vrakregister
Sjömätningssystem	Ombordsystem	
SJÖSAG		Incidentrapportering för fritidsbåtssektorn.
SMR inkl. SYB, Behörighetsguiden.		Sjömansregister och Sjömäns behörigheter
SOS		Sjöolyckssystem
Telefonboken		
Ventilen		Intranät
Vattenstånd (Nivel, VM 2B, Linjäritetsberäkning)		
VIVA		Vind och vatten
Trafikövervakning		På VTS:er
Ärenderegister		

Nya eller förbättrade informationssystem

Under 2004 har verket utvecklat ett IT-baserat fartygsrapporteringssystem (FRS) som en följd av EU-direktiv, enligt vilka medlemsländerna ska föra över nationell information till ett centralt informationssystem inom EU (Safe Sea Net). Rapporteringen görs elektroniskt via verkets webbplats på Internet och togs i drift den 1 januari 2005.

Utgivningen av sjökort och nautiska publikationer ingår som en del för att nå målen att säkerställa en hög transportkvalitet och en säker sjöfart. Produktionen av elektroniska sjökort som täcker Helcom-farlederna har prioriterats under 2004 och beräknas slutföras under 2005. Samtliga svenska farvatten ska år 2006 vara täckta av Electronical Navigation Chart (ENC) och rutiner för rättelseverksamhet av dessa ska ha införts.

Kvaliteten i de satellitbilder som isbrytarna får har förbättrats.

Förstudien Nationell Strand Linje (NSL) har genomförts i samarbete med Lantmäteriet. Uppbyggnaden av en gemensam databas har startat. Databasen ska innehålla strandlinjedata med hög upplösning för kartproduktion.

Projektet DIS II har slutförts och nya funktioner har implementerats och driftsatts i Djup Informations Systemet (DIS). Laddning av data fortgår enligt plan.

Centralerna för Vessel Traffic Services (VTS) i Göteborg och Marstrand samlokaliserades i nya lokaler i Göteborg. I samband med detta investerades i nya radaranläggningar och större persondatorer för att personalen ska kunna följa sjötrafiken.

Arbetet med att utveckla olika tekniska stödsystem för att underlätta och effektivisera lotsens arbete har intensifierats. Det gäller bl.a. förbättrade informationssystem mellan lotsen och lotsplatsen.

Inom sjöfartsinspektionen pågick ett arbete med att utveckla ett nytt IT-baserat tillsynssystem som innebär en modernisering av befintligt tillsynssystem. Fartygsinspektörer får en bärbar datorutrustning.

Arbetet med att ta fram ett nytt IT-system för sjöfartsregister startades under 2004. Arbetet med implementeringen av olycksrapporteringssystemet för fritidsbåtar fortsätter under 2005.

Under 2004 infördes SjöV:s system för rapportering och hantering av avvikelserapporter och förbättringsförslag.

E-tjänster införs successivt på verkets webbplats. En tjänst är att kunna lämna elektroniska underlag för debitering av farledsavgifter. Under år 2005 införs elektroniska lotsbeställningar och elektronisk rapportering av farligt gods och fartygsgenererat avfall.

Bilaga 2 Komponenter i LIS

I tabellen nedan sammanfattas SjöV komponenter för informationssäkerhet och IT-säkerhet. Komponenterna är sorterade efter rubrikerna i COSO-modellen och Riksrevisionens program för granskning av myndigheternas ledningssystem för informationssäkerhet (LIS).

Kontrollmiljö
SjöV har på förfrågan år 2004 informerat sin styrelse om IT-relaterade frågor (styrning inom IT-området samt utvecklingsarbete).
SjöV:s verksledning (direktion) behandlar ibland ärenden som rör IT-säkerhet efter beredning i IT-rådet.
Organisation av IT-säkerhetsfrågor: GD, verksledning (direktion), IT-råd, ekonomichefen, som har personligt ansvar för att samordna IT-säkerhetsfrågor och därför är ordförande i IT-rådet, ekonomichefen har en säkerhetscontroller ansvarig för IT-säkerhetssamordning, verksamhetschefer, har ansvar för sina IT-system. Vidare finns säkerhetsskyddschef samt IT-chef med ansvar för IT-infrastrukturen.
IT-rådet fångar upp frågeställningar som rör IT-säkerhet, bl.a. genom incidentrapporter, och tar vid behov upp ärenden, t.ex. förslag till regelverk och förändringar i dessa, i verksledningen, ställer krav på säkerheten i IT-infrastrukturen samt ger vid behov systemägarna och stöd.
Precisering av ansvar för säkerheten av informationstillgångar: Avdelningschef (linjechef) är ansvarig för informationssäkerheten. Ansvaret är delegerat till verksamhetschefer (inom sakverksamhet, administration och IT-verksamhet) som tillika är systemägare[46]. Systemägaren svarar för beställning av utveckling av IT-stöd eller IT-infrastruktur, genomför årliga riskanalyser samt dokumenterar, fastställer och inför rutiner för handhavande.
GD-beslut (1999) om vilka verksamheter och system som är samhällskritiska och/eller verksamhetskritiska, som direktiv för prioritering och för beredskapsplanering.
Styrande dokument: IT-säkerhetshandbok med bl.a. IT-säkerhetspolicy, IT-handboken, systemförvaltningsmodell, Dokument och ärendehanteringshandbok samt Säkerhetsskyddsbestämmelser för SjöV.

[46] Rollbeskrivning finns i IT-handboken, systemförvaltningsmodellen och i Dokument- och ärendehanteringshandboken.

GD får särskilda rapporter från IT-säkerhetscontrollern och av ekonomidirektören (i egenskap av ordförande i IT-rådet).
IT-säkerhetscontroller. Rollen innebär att vara ledningens organ för framtagning av regler för IT-säkerheten. Vidare att bistå med råd inom IT-säkerhetsområdet till systemägarna, att sprida information internt inom SjöV om IT-säkerhet genom bl.a. intranätet Ventilen och interna utbildningar. I rollen ligger inte att ansvara för IT-säkerheten vid SjöV eller att följa upp systemägarnas säkerhetsarbete. IT-säkerheten är en del av det normala chefsansvaret och ligger i linjeorganisationen. Samverkan i säkerhetsfrågor sker med Sjöv:s säkerhetsskyddschef.
Riskanalyser, informationsklassificering, skyddsnivå och åtgärdsplaner
IT-enheten för ett register över informationssystem (applikationer och databaser), vilka som är ägare till dem samt var systemen finns. Säkerhetsklassificering beskrivs i IT-säkerhetshandboken och i ett särskilt, dock ej fastställt, dokument.
SjöV genomförde en riskanalys av hela sin verksamhet år 2001 enligt förordningen [1995:1300] om myndigheters riskhantering. Den innehåller en övergripande beskrivning av risk- och skadehantering i SjöV. Därvid berörs tekniska system, IT-stödet, skalskydd, säkerhetskopiering, systemförvaltningsavtal, tillbud på fartyg och utslagning av datahall. Som underlag för den årliga riskanalysen finns en särskild blankett som verksamhetsansvariga besvarar (personal, information, skepp/fartyg, maskiner/inventarier, byggnader/anläggningar, mark). Riskerna värderas och konsekvenserna bedöms.
Resultatet av analysen från 2001 hålls levande genom årliga revisioner, men fortfarande med utgångspunkt i förordningen om riskhantering (avser ekonomiska risker). Systemägarna skickar resultaten av revisionerna till ekonomiavdelningen. Analyserna tas sedan upp i IT-rådet. Resultatet av analysen är främst försäkringar som SjöV tecknar.
Riskanalys är en stående punkt på IT-rådets dagordning. Underlag är bl.a. den årliga riskanalysen (ekonomiska risker) samt incidentrapportering.
Analys av SjöV:s behov av åtkomstkontroll genom PKI-lösningar utfördes 2004.
Årlig IT-plan utarbetas som del av budgetarbetet. IT-säkerhetsrelaterade aktiviteter återfinns under budgetens/årsplanens flikar ”Förvaltning infrastruktur” och ”Projekt infrastruktur”.
En del säkerhetsåtgärder ligger som komponenter i andra projekt som bl.a. avser nytt IT-stöd.

Förändringar i verksamhetskrav som påverkar IT-system och IT-infrastruktur rapporteras från systemägarna till IT-chefen.
Djupdatabasen vid sjökarteenheten innehåller hemlig information och registerverksamheten har ett eget nätverk och eget skalskydd, utan koppling till SjöV:s ordinarie nätverk.
Strävan är att öka standardiseringen av IT-utrustning och basprogramvara (plattformar) för att minska verkets sårbarhet när det gäller enskilda händelser.

LIS, kontrollfunktioner, skyddsåtgärder

Fysisk säkerhet: Den fysiska åtkomsten till lokaler och datahall hanteras av SjöV:s säkerhetsskyddschef och administreras i receptionen efter begäran till och godkännande från IT-enheten.
Fysisk säkerhet: Den nya datahallen i Norrköping uppfyller Säpos krav när det gäller inbrottsskydd, brandsäkerhet och tillgänglighet. För externa företag som utför service på plats i SjöV:s lokaler finns särskilda regler och rutiner för övervakningen av detta arbete.
Personal: Viss personal är särskilt säkerhetsklassad (djupdatahanteringen samt IT-enhetens personal).
IT-infrastruktur: Med IT-infrastruktur avser SjöV det gemensamma generella tekniska IT-stöd, i form av program- och maskinvaror, som verksamheten ges tillgång till. På infrastrukturen körs de allmänna och verksamhetsspecifika informationssystemen och applikationer som respektive ansvarig chef beslutar om. Komponenter i IT-infrastrukturen som rör informationssäkerhet och IT-säkerhet är: Anti-virus, Helpdesk, brandväggar, säkerhetskopiering, digital arkivering/långtidslagring, datorhall, kontinuitetsplaner, övervakning, kryptering, behörighetssystem (administration av rättigheter i SjöV nätverk, tilldelning av rättigheter och lösenord).
Informationssystem: Med IT-arkitektur avser Sjöv ett ramverk som på olika nivåer (koncept, information, informationssystem, teknik) styr hur systemen ska byggas för att kunna tillgodose myndighetens krav. Några principer som rör informationssäkerhetsområdet är följande: – Direkt kommunikation mellan system ska undvikas. – Informationsutbyte ska gå via standardiserade anrop mot en gemensam integrationsmotor extern kommunikation ska gå genom portallösning. – Information som är gemensam för flera verksamheter eller informationssystem ska förvaltas på ett ställe. Där så är lämpligt byggs gemensamma databaser.

SjöV har flera olika tekniska miljöer men strävar numera efter en enhetlig plattform.
Informationssystem: Varje systemägare svarar för att systemet är dokumenterat och har de fastställda rutiner som just den verksamheten kräver.
Informationssystem: Rutin finns för utveckling/förändringar i IT-miljö, IT-system och bemanning (styrning av IT-projekt).
Informationssystem: Säkerheten i nyutvecklade system testas av särskild certifierad testpersonal.
Informationssystem: Alla informationssystem i nätverket auktoriseras innan driftsättning sker. Ett driftsättningsbeslut skrivs under av beställaren och den som ansvarar för driften. Som bilagor ska bl.a. finnas risk- och sårbarhetsanalys, kontinuitetsplan samt system- och driftdokumentation.
Informationssystem: Alla system ska omfattas av ett förvaltningsavtal, bl.a. med regler om backup, mellan systemägare och IT-enheten. Systemägaren svarar för att det finns en förvaltningsplan för systemet.
Informationssystem: Kontinuiteten i VTS har testats vid övning.
Behörighet till IS/IT: Systemägaren har ansvaret för att utfärda regler och rutiner för tilldelning av behörigheter till sina system samt för att utforma dokument och rutiner för hur nyanställda ska begära och få tillgång till dessa system. Helpdesk biträder systemägaren med blanketter[47]. IT-enheten får uppgifter om personalförändringar.
Behörighet till IS/IT: För externa företag som från extern plats utför IT-service finns särskilda regler och rutiner som styr deras temporära behörigheter till SjöV:s nätverk, IT-system eller maskinvara.
Dataskydd: Vissa data som samlas in från verksamheterna kvalitetskontrolleras innan de får användas.
Dataskydd: Hantering av sekretessbelagda uppgifter: regler och rutiner för åtkomst till sekretessbelagda uppgifter regleras i ett separat, ännu ej fastställt dokument.
Dataskydd: Rutin för säkerhetskopiering enligt IT-säkerhetshandboken och blanketen Backuphantering.
Dataskydd: Regler och rutiner finns för utplåning av information från medier som varit bärare av sekretessbelagd information.
Etik: Regler finns för e-post. Internetpolicy finns.
Incidenter: Rutin och IT-stöd för incidentrapportering finns.
Incidenter: Rapporter över virusangrepp (månadsvis) tas fram.

[47] Bl.a. Ny användare Sjovnet, Lokala administratörsrättigheter – ansökan, Fjärruppkoppling RAS och VPN anslutning ansökan.

Incidenter: Viss form av penetrationstest från Internet sker återkommande med hjälp av standardprogramvara.

Information och utbildning
Genomgång av säkerhetsfrågor sker i samband med introduktionsutbildning.
Särskild genomgång av säkerhetsfrågor sker inför användning av vissa system och andra IT-tillgångar.

Uppföljning, utvärdering och förvaltning av LIS
Säkerhetsanalys av SjöV:s nätverk gjordes år 2000.
Visst arbete pågår med att utvärdera myndighetens informationssäkerhet.

Källförteckning

Lagstiftning

Tryckfrihetsförordning (1949:105)

Arkivlagen (1990:782)

Personuppgiftslagen (1998:204)

Sekretesslagen (1980:100)

Skyddslagen (1990:217)

Lag (2003:389) om elektronisk kommunikation

Förordningar

Arkivförordningen (1991:446)

Förordning (1995:1300) om myndigheters riskhantering.

Förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap.

Säkerhetsskyddsförordning (1996:633, 2000:888).

Datainspektionens allmänna råd: Säkerhet för personuppgifter (december 1999).

Personuppgiftsförordning (1998:1191)

Verksförordningen (1995:1322).

Rikspolisstyrelsens föreskrifter om säkerhetsskydd (RPS FS 1996:9 FAP 244-1)

Texter från Internet

Mörkertalsundersökningen. Hämtat från http://www.pts.se/Archive/Documents/SE/Morkertalsundersokningen_2005.pdf

National Institute of Standards and Technology (NIST), special publications (SP):

Draft Special Publication 800-40 Version 2 - Creating a Patch and Vulnerability Management Program

Draft NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling

NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form

Control Objectives for Information and related Technology (COBIT). Hämtat från ISACA http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Övrigt material

SS-ISO/IEC 17799, SS 627799. Ledningssystem för informationssäkerhet.

Krisberedskapsmyndigheten 2003. Krisberedskapsmyndighetens rekommendation 2003:2 Basnivå för IT-säkerhet (BITS).

National Institute of Standards and Technology (NIST), special publications (SP):

SP800-26	Security Self-Assessment Guide for Information Technology Systems,
SP800-27 Rev. A	Engineering Principles for Information Technology Security
SP800-30	Risk Management Guide for Information Technology Systems,
SP800-31	Intrusion Detection Systems (IDS),
SP800-33	Underlying Technical Models for Information Technology Security,
SP800-34	Contingency Planning Guide for Information Technology Systems,
SP800-35	Guide to Information Technology Security Services,
SP800-40	Procedures for Handling Security Patches,
SP800-41	Guidelines on Firewalls and Firewall Policy,
SP800-42	Guideline on Network Security Testing,
SP800-44	Guidelines on Securing Public Web Servers,
SP800-45	Guidelines on Electronic Mail Security,
SP800-46	Security for Telecommuting and Broadband communications,
SP800-47	Security Guide for Interconnecting Information Technology Systems,
SP800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices,
SP800-50	Building an Information Technology Security Awareness and Training Program,
SP800-55	Security Metrics Guide for Information Technology Systems,
SP800-60	Guide for Mapping Types of Information and Information Systems to Security Categories,
SP800-61	Computer Security Incident Handling Guide,
SP800-64	Security Considerations in the Information System Development Life Cycle,
SP800-65	Integrating Security into the Capital Planning and Investment Control Process,

Kommunikation avseende erfarenheter från andra nationella revisionsorgan, bl.a. GAO i USA, OAG i Canada. samt erfarenheter från den svenska bank- och försäkringssektorn.

Committee of Sponsoring Organizations of the Treadway Commission. Framework for assessing and developing an internal control structure (COSO)