Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

2 Säkerhet

TeliaSonera har under lång tid byggt upp stora värden i materiella och immateriella tillgångar. I syfte att säkra och underhålla dessa tillgångar arbetar TeliaSonera aktivt med program för riskhantering och säkerhet.

TeliaSoneras riskmiljö analyseras kontinuerligt och program för riskhantering är under ständig förbättring och utvärdering. I det löpande riskhanteringsarbetet finns utarbetat en definition av acceptabla grundskyddsnivåer baserade på strukturerat riskanalysarbete och väletablerade standarder, t.ex. SS-ISO/ IEC 27002: 2005.

Målet med riskhanteringsarbetet är att bl a minska riskkostnaderna, stärka företagets image och skydda företagets varumärke samt inte minst att minimera riskerna för störningar i nät och tjänster för TeliaSoneras kunder.

En viktig del av säkerhetsarbetet är inriktat på att skydda känslig information mot obehörig åtkomst och manipulation, för TeliaSonera såväl som för kunden.

TeliaSonera kan leverera och driva kommunikationstjänster även under extrema förhållanden, t.ex. som olika typer av kriser eller vid landsomfattande beredskapssituationer. För detta ändamål samarbetar TeliaSonera med olika myndigheter inom totalförsvaret i syfte att säkra tjänster som är samhällskritiska.

TeliaSoneras säkerhetspersonal är nationellt och internationellt känd för att vara mycket kunnig och kvalificerad. Hanteringen av risk- och säkerhetsärenden är fokuserad på att förebygga, upptäcka och korrigera säkerhetsbrister m m. TeliaSonera deltar vidare i ett flertal nationella och internationella organisationer för att driva och aktivt bidra till utvecklingen och därmed vara uppdaterad inom TeliaSoneras olika teknikområden.

TeliaSoneras **koncernsäkerhetspolicy** har följande struktur:

1. Roller och ansvarsområden
   - Corporate Security och säkerhetsorganisationen
   - Linjeorganisation, affärsområden och huvudkontorsenheter
2. Säkerhetsuppföljning och granskning
3. Informationssäkerhet och IT-säkerhet
4. Fysisk säkerhet
5. Personalsäkerhet
   - Skydda personalen
   - Skydda nyckelpersoner
   - Rekrytera nyckelpersoner
   - Resesäkerhet
6. Bedrägeri- och brottshantering
   - Hantering och rapportering av säkerhetsincidenter
   - Säkerhetsövervakning

- Bedrägerihantering
- Produktsäkerhet
- Penetrationstestning

7. Krishantering
   - Nationell säkerhet
   - Totalförsvar och civil beredskap
   - Telekommunikationskontroll

TeliaSoneras koncernpolicy för **informationssäkerhet** har följande struktur

1. Målsättning
2. Omfång
3. Definition av informationssäkerhet
4. Ansvar och skyldigheter
5. Säkerhetsmedvetenhet
6. Informationssäkerhetskontroller
   - Allmänna kontroller
   - IT-säkerhet
   - Nätverkssäkerhet
   - Personalsäkerhet
   - Lokalsäkerhet/Fysisk säkerhet

Formellt är policyn fastställd av koncernchefen efter godkännande av ansvariga enheter.

Koncernsäkerhetschefen ansvarar för kontroll och efterlevnad genom program för löpande säkerhetsuppföljning och förbättring. Avvikelser från gällande regelverk rapporteras till koncernledningen.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

TeliaSonera har organiserat säkerhetsstyrningen och tillhörande regelverk i enlighet med SS-ISO/IEC 27002:2005. TeliaSoneras säkerhetskrav täcker väl de områden som är beskrivna i BITS (KBM 2006:1).

TeliaSoneras säkerhetsstyrning fastställer en lägsta accepterad säkerhetsnivå (grundnivå) som måste uppfyllas i företagets tjänster, produkter och produktionsplattformar. Säkerhetskraven gäller samtliga telekommunikations-plattformar, IT-system och nät.

Säkerhetskraven återfinns i produktlivscykeln (PLC), dvs. förvaltning, underhåll och drift, liksom vid nyutveckling av TeliaSoneras tjänster, produkter och produktionsplattformar.

Säkerhetsstyrningen gäller för alla helägda dotterbolag inom TeliaSonera.

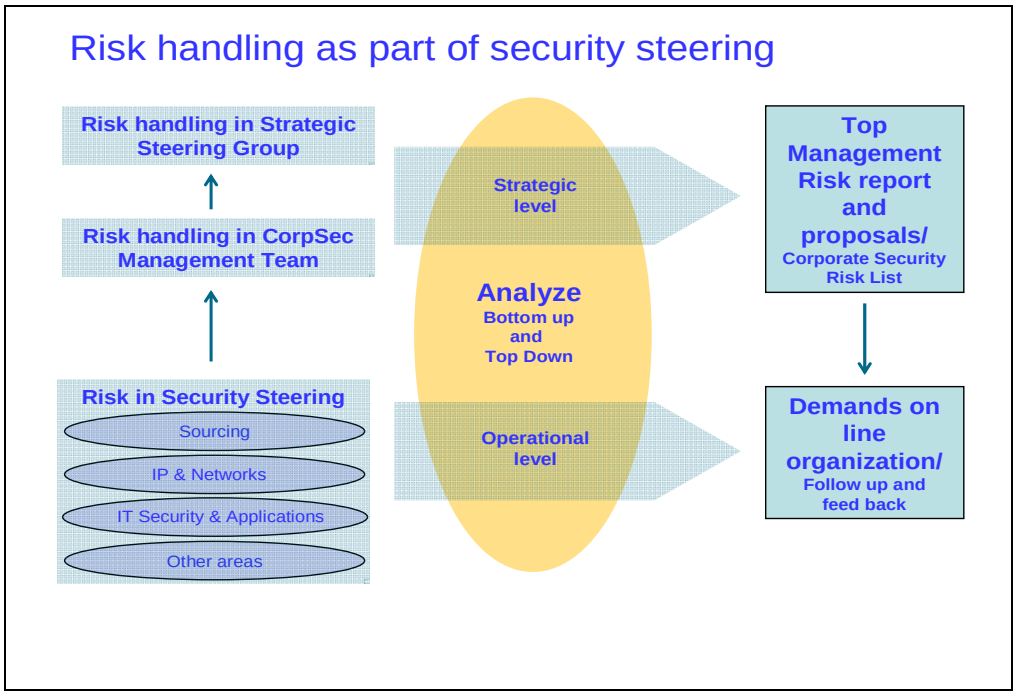
2.1.2 Uppföljning och kontroll – säkerhetsrevision

TeliaSonera erbjuder sina kunder möjlighet till uppföljning av avtalade säkerhetsnivåer med beaktande av kommersiella säkerhetskrav och lagstiftning inom området.

Inom TeliaSonera finns dessutom väl utarbetade rutiner för företagets egen kontroll och uppföljning av säkerhetsnivåer och efterlevnad av gällande säkerhetskrav.

2.1.3 Säkerhets- och sårbarhetsanalyser

TeliaSonera utför regelbundet säkerhets- och sårbarhetsanalyser såväl i samband med utveckling av nya produkter och produktionsplattformar som regelbundet för driftsatta sådana. TeliaSonera har rutiner hur dessa sårbarhetsanalyser skall utföras med hjälp av specialister som leder dessa. Inom TeliaSonera används ett antal metoder och tekniker för risk- och konsekvensanalyser beroende på tillämpningsområde.



Telia Soneras sårbarhetsanalys hjälper myndigheten att bli medveten om de risker som man är utsatt för och vilka konsekvenser en incident skulle kunna få. Dessutom kommer beställaren att se vilka möjligheter den har att eliminera och hantera riskerna. Sårbarhetsanalysen genomförs utifrån ett affärs- och verksamhetsperspektiv. Den hjälper myndigheten att säkerställa kontinuiteten i sina affärskritiska processer.

En sårbarhetsanalys genomförs i följande steg:
1. Kartläggning av nuläget
Några vanligt förekommande moment:
• Identifiering av de prioriterade processer som ska analyseras
• Beskrivning av den tekniska miljön
• Scenarier för olika krissituationer

2. Riskanalys
Analysen genomförs som en workshop där representanter från verksamheten deltar. Vi värderar olika scenarier och krissituationer.
Beslutspunkter:
• Vad är acceptabel risknivå
• Vilka risker är prioriterade och behöver hanteras

3. Framtagning av åtgärdsplan
Vi ställer samman en åtgärdsplan med prioriterade och analyserade åtgärder och rutiner.

2.1.4 Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

TeliaSoneras policies, processer, rutiner och strukturer avseende informations-säkerhet motsvarar SS-ISO/IEC 27002: 2005.

TeliaSoneras styrmodell och riktlinjer för säkerhet är uppbyggda i enlighet med SS-ISO/IEC 27002:2005, dessutom omfattar TeliaSoneras säkerhetsregelverk ytterligare områden som ej återfinns i nuvarande version av standarden – t ex bedrägerihan-tering.

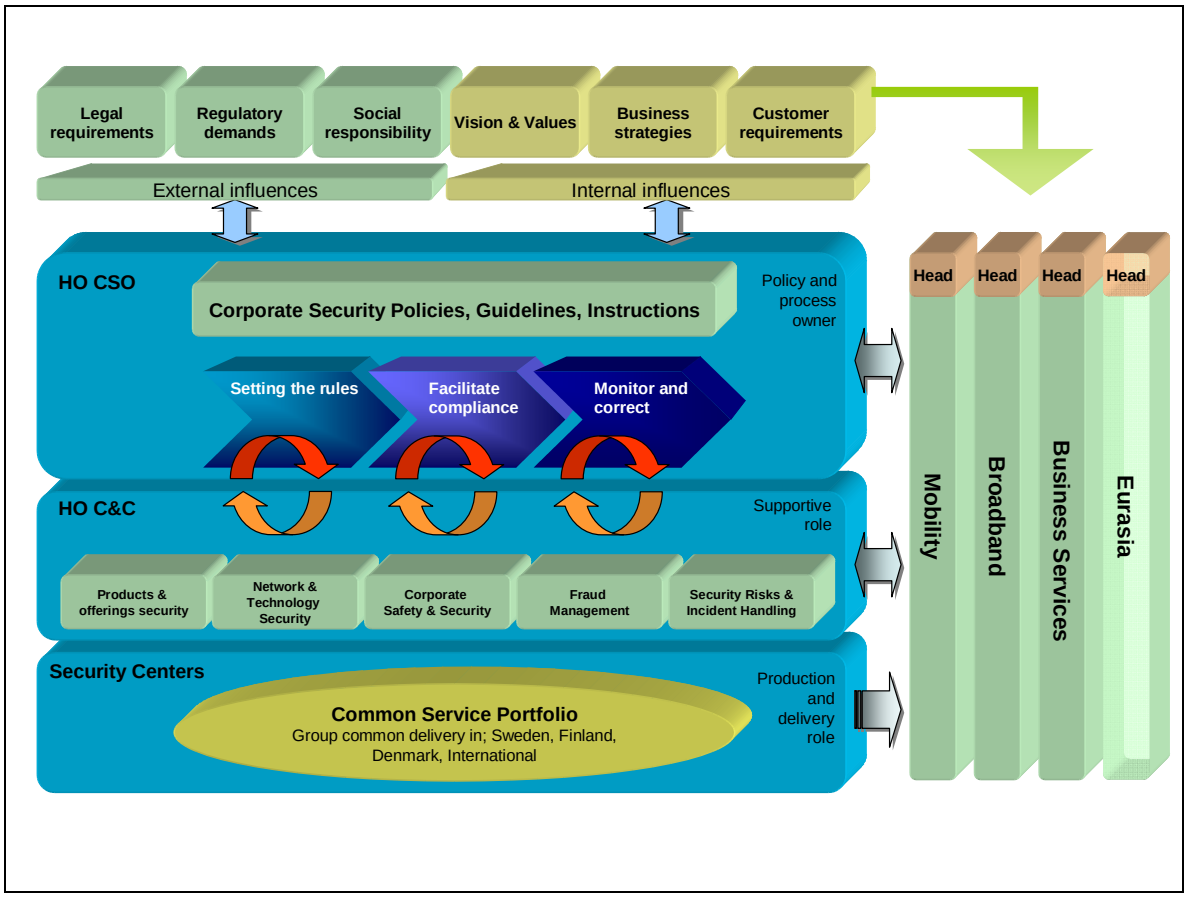
TeliaSoneras styrmodell och riktlinjer för säkerhet omfattar även grundskyddsnivå för interna stödsystem och tekniska produktionsplattformar.

2.1.5 Redogörelse av Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

TeliaSoneras säkerhetsstyrning bygger på allokerat säkerhetsansvar inom hela organisationen. Alla linjechefer och anställda har ett ansvar att efterleva och arbeta i enlighet med policies och riktlinjer för säkerhet. I syfte att säkerställa efterlevnaden av fastställda policies och riktlinjer har säkerhetskontroller utarbetats och delegerats i linjeorganisationen, som tydliggör och bemannar roller, uppgifter och ansvar inom säkerhetsområdet.

A. Ansvarsfördelning

Nedanstående styrmodell och efterföljande text beskriver hur säkerhetsstyrningen i TeliaSonera är definierad.



Not: HO= Head Office; C&C = Compliance & Control; CSO= Chief Security Officer

Corporate Security

Chief Security Officer - CSO

Ansvarar för att definiera det gemensamma säkerhetsregelverket för TeliaSonera Group, t.ex. företagets säkerhetsstrategi, företagets säkerhetspolicy, guidelines, instruktioner och anvisningar samt utformar specifika kontroller och mätpunkter (Key Performance Indicators – KPI)

CSO utser också en security governance process manager, som har det övergripande ansvaret för säkerhetsstyrningsprocessens utveckling, underhåll och effektivitet.

Security Governance Process Manager

Har ett övergripande ansvar för säkerhetsstyrningsprocessens utveckling och underhåll. Har också en total bild över säkerhetsstyrningsprocessens efterlevnad och effektivitet och ansvarar för att initiera åtgärder för att förbättra koncernens säkerhetsstyrning.

Compliance and Control Directors (C&C)

Agerar på mandat av CSO. Handhar kontroll av säkerhetsarbetet inom ett s.k. Practice Area och övervakar och granskar huruvida TeliaSoneras organisation uppfyller gällande säkerhetsregelverk. Practice Areas är

- Products and Offerings Security
- Network and Technology Security
- Corporate Safety and Security
- Fraud Management
- Security Risks and Incident Management

Ansvaret omfattar följande uppgifter:

- förbereda och underhålla säkerhetsstyrningsdokument på företagsnivå
- definiera säkerhetskontroller och mätvärden för säkerhet i produkter, tjänste och erbjudanden
- underlätta implementeringen av säkerhet i affärsområden och nyckelprocesser
- arbeta för att policies och riktlinjer efterlevs inom respektive område
- tillsammans med affärsområdena definiera accepterad risknivå
- följa upp säkerhetskontrollernas effektivitet
- ta fram (varje kvartal och år) rapporter över företagets säkerhet
- identifiera och hantera kritiska situationer och eskaleringar
- pådriva harmonisering, förbättringar och kostnadsbesparingar inom säkerhetsområdet inom respektive affärsområde.

Security Center Director

Hanterar de landsbaserade säkerhetscentren och bär ansvaret för tillhandahållandet av överenskomna säkerhetstjänster till affärsområdena. I länder där det inte finns något säkerhetscenter ansvarar affärsområdena för implementeringen av en säkerhetsorganisation för uppfyllandet av företagets säkerhetskrav.

Ansvaret omfattar följande uppgifter:

- utforma, utveckla och underhålla gruppgemensamma säkerhetstjänster
- säkerställa en konsekvent implementering av säkerhetsregelverket
- implementera och leverera gruppgemensamma säkerhetstjänster till affärsområden och ansvariga för nyckelprocesser i det aktuella landet (inklusive huvudkontorsenheter)
- säkerställa efterlevnaden av landsspecifika säkerhetsrelaterade lagar och bestämmelser, inklusive kraven om nationell säkerhet
- genomföra säkerhetsrevisioner och uppföljningar
- ta fram (varje kvartal och år) rapporter över företagets säkerhet
- stödja affärsområden med säkerhetsexpertis

- hantera tredjeparts leverantörer inom det aktuella landet.

Centers of Excellence

Centers Of Excellences (COE) kan etableras i syfte att samordna säkerhetskompetensområden inom TeliaSonera. COE Teliasonera CERT (Computer Emergency Response Team) ansvarar för samordningen och hanteringen av säkerhetsincidenter.

Linjeorganisation (affärsområden och huvudkontorsenheter)

Affärsområdeschefer

Affärsområdescheferna ansvarar för att upprätta en fungerande delegeringsordning för säkerhetskontroller inom affärsområdet. Delegeringsordningen beskrivs och godkänns av Corporate Security. Delegeringsordningen fastställs på affärsområdesnivå samt roller, uppgifter och ansvar kommuniceras till linjeorganisationen.

Linjechefer

Linjecheferna för affärsområdena och huvudkontorsenheterna ansvarar för att agera och följa företagets säkerhetspolicies och - riktlinjer.

De har också ett delegerat ansvar att äga, implementera och följa upp överenskomna säkerhetskontroller inom sina ansvarsområden. Linjechefer i affärsområden som har ett säkerhetsansvar ska, i samverkan med Corporate Security, komma överens om tjänstenivån för tjänster som tillhandahålls av Security Centers.

I länder där inget Security Center har etablerats ansvarar Compliance and Control Directors för att styra och följa upp linjeorganisationernas säkerhet inom sina respektive områden.

Medarbetare

Medarbetare ansvarar för säkerhetsfrågor i sin omedelbara närhet och är skyldiga att följa givna säkerhetsanvisningar, samt att rapportera säkerhetsincidenter till närmaste chef och till säkerhetsorganisationen.

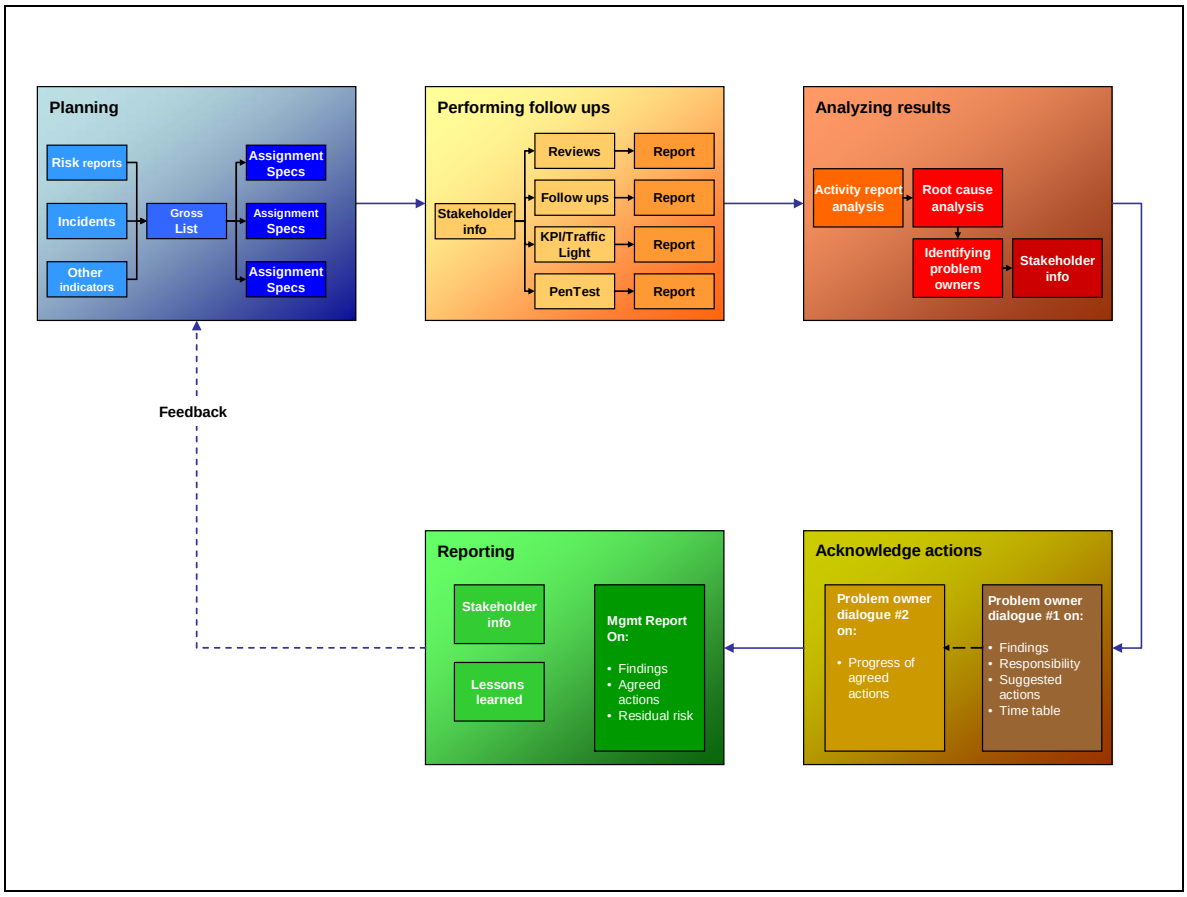
Säkerhetsuppföljning

Uppföljningar, i syfte att säkerställa att säkerhetskontrollerna motsvarar uppsatta mål, genomförs regelbundet.

Säkerhetsriskerna sammanställs av Corporate Security och rapporteras till koncernledningen. Corporate Security genomför särskilda säkerhetsuppföljningar inom hela eller delar av TeliaSonera-gruppen. Följande huvudområden ingår uppföljningen:

- efterlevnad av policies, riktlinjer och övriga interna styrdokument inom säkerhetsområdet
- efterlevnad av lagar, författningar och myndighetsdirektiv inom säkerhetsområdet
- säkerhetsstatus för system och plattformar avseende teknisk säkerhet, processer och rutiner.
- Förutsättningar för effektiv säkerhetsstyrning – organisation, budget, definierade roller och ansvar.

Processillustrationen nedan beskriver översiktligt TeliaSoneras gemensamma arbetssätt.



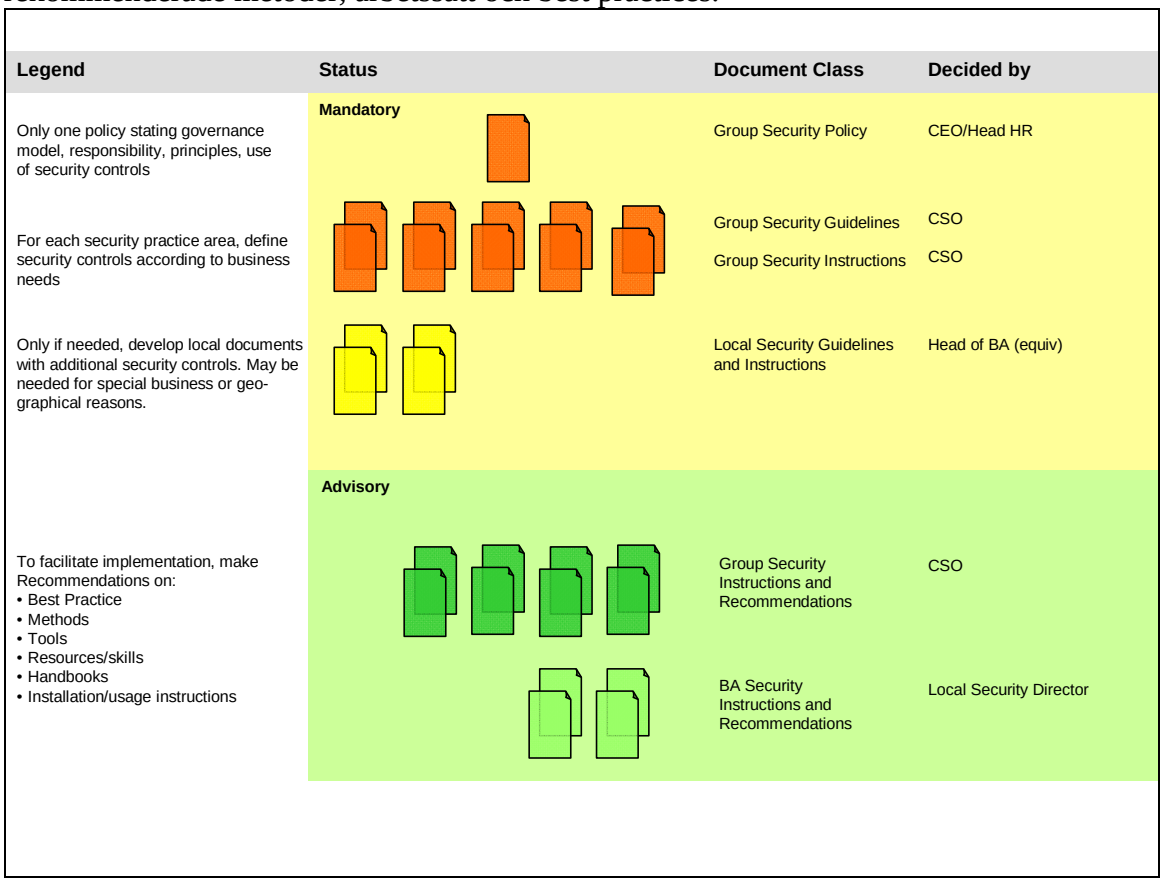
B. Regelverksstruktur

TeliaSoneras regelverk för säkerhet består av policies, guidelines och instruktioner enligt strukturen i bild nedan.

Styrningen sker inom tidigare nämnda security practice areas under ledning av en Compliance & Control Director på mandat från Chief Security Officer . Följande security practice areas finns:

- Products and Offerings Security
- Network and Technology Security
- Corporate Safety and Security
- Fraud Management
- Security Risks and Incident Management

Inom samtliga dessa practice areas finns styrande regelverk och anvisningar samt rekommenderade metoder, arbetssätt och best practices.



2.2 Allmänna tekniska säkerhetskrav

2.2.1 Fysisk infrastruktur

TeliaSonera kan efter begäran från kunden redogöra för den, för tjänsten relevanta, nationella fysiska infrastruktur och eget kommunikationsnät inklusive placering av noder och framföringsvägar. Redogörelsen sker alltid med hänsyn till kundavtal, nationella säkerhetsföreskrifter, lagstiftning och parternas säkerhetsrutiner. Uppbyggnaden av TeliaSoneras nät är att betrakta som företagshemlig information.

TeliaSonera har vidare tecknat säkerhetsskyddsavtal med berörda kunder, myndigheter, enligt gällande lagstiftning rörande rikets säkerhet och har enligt dessa avtal en säkerhetsskyddsorganisation för detta specifika ändamål. Upphandlingar enligt SUA hanteras av särskild enhet inom TeliaSonera AB, vars nätinformation inte kan göras tillgänglig utan de aktuella kundernas medgivande.

2.2.2 Uthållighet

PTS krav på ”uthållighet” i produkter och tjänster (enligt PTSFS 2007:2) uppfylls genom att bl a alla incidenter rapporteras till PTS enligt utarbetad rutin.

2.2.3 Skydd av tjänst

TeliaSoneras skydd av erbjudna tjänster har ett såväl förebyggande, detekterande som korrigerande syfte.

Det förebyggande säkerhetsarbetet utgår från löpande riskanalyser med beaktande av kontraktsmässiga säkerhetskrav, fastställande av skyddskrav, enhetliga processer för utveckling och förvaltning/drift av erbjudna tjänster där säkerhet är en integrerad del samt tydligt dokumenterad ansvarsfördelning, utbildning, övning och uppföljning av säkerhetsnivåer.

Det förebyggande säkerhetsarbetet innefattar även tekniska lösningar för konfidentialitet, tillgänglighet, integritet och spårbarhet. Det förebyggande säkerhetsarbetet är som tidigare nämnts strukturerat i enlighet med SS-ISO/IEC 27002:2005.

Det detekterande och korrigerande säkerhetsarbetet består dels av tekniska lösningar för att upptäcka och avvärja angrepp mot infrastruktur, tjänster och arbetsprocesser dels av TeliaSoneras organisation för krishantering.

En viktig del av TeliaSoneras detekterande och korrigerande skydd av erbjudna tjänster är TeliaSonera CERT (Computer Emergency Response Team – TS-CERT). Nedan följer beskrivning av dess huvuduppgift och verksamhet.

Roll och syfte
TS-CERTs huvuduppdrag består i att hantera hot och attacker mot datorer och datornätverk som behövs för TeliaSoneras affärsverksamhet och informationstillgångar. Syftet är att minimera skadan och avbrotten som orsakas av IT-säkerhetsincidenter.

TS-CERT är ett samordningscenter för hantering av IT-säkerhetsincidenter. Uppdraget omfattar uppföljning av IT-säkerheten inom TeliaSonera-gruppen genom genomförandet av sårbarhetsbedömningar, penetrationstester och implementering av tillämpliga principer.

TS-CERT representerar TeliaSonera i internationella Forum of Incident Response and Security Teams (FIRST), European Task Force CollaboratonSecurity Incident Response Teams (TF-CSIRT) och Trusted Introducer (TI). TeliaSonera är en fullvärdig medlem i FIRST och en auktoriserad medlem i TF-CSIRT/TI. Dessa medlemskap ger TeliaSonera tillgång till korrekt, tidig och tillförlitlig information om nya hot och sårbarheter i datornätverk.

Uppgifter

TS-CERTs uppgifter kan delas in i följande fyra huvudkategorier:

- Incidenthantering
- Uppföljning
- Informationsbevakning och -distribution
- Råd och vägledning

I tabellen nedan visas tjänsterna inom dessa fyra kategorier:

Incidenthantering	**Uppföljning**	**Informations-insamling och distribution**	**Råd och vägledning**
• Identifiera och agera på IT-säkerhetsinciden ter • Övervakning och hantering av intrångsidentifie ringssystem • Incidentunder-sökning och -analys (datortekniska undersökningar)	• Kontinuerligt följa upp IT-säkerheten i TeliaSonera-gruppen • Detta omfattar sårbarhetsbedöm ningar och penetrations-tester • Följa upp tillämpningen och	• IT-säkerhetsinform ation och nyhetsbevakning • Få ut aviseringar och varningar • Förse gruppen med allmän information om IT-säkerhets-området	• Ge råd och support till system- och nätverksadminist ratörer i gruppen • Kontrollistor för IT-säkerhet för vanliga operativsystem och program • Stödja externa affärs-uppgörelser

• Samordna åtgärder mot IT-säkerhetsinciden ter som påverkar TeliaSonera-gruppen • Stödja system och nätverksadminis tratörer med incidentsupport • Utveckla Telia-Soneras inci-denthanterings-process • Tillhandahålla verktyg och metoder	efterlevnaden av företagets principer för informationssäk erhet och IT-säkerhet		

Incidenthanteringsorganisation
TS-CERT är en del av Corporate Security. TeliaSoneras incidenthanteringsorganisation är distribuerad. Teamen kallas för sub-CERTs. TS-CERT CC är den centrala och samverkande incidenthanteringsenheten och kontaktpunkt för gruppen. Därigenom skapas:

- möjlighet att snabbt och effektivt reagera på IT-säkerhetsincidenter
- den personal som är insatt i den berörda IT-miljön och affärsoperationerna i fråga hanterar incidenterna
- täcker en stor organisation med verksamhet i olika länder
- responsen på företagsomfattande incidenter är samordnad
- ger det centrala CERT-teamet en översikt över incidenter som inträffat i olika delar av organisationen, och därmed möjligheten att identifiera trender och mönster
- incidenthanteringsprocedurerna är enhetliga och konsekventa i hela organisationen.

Kontaktinformation för incidenthanteringsenheterna

Domän	**Enhet**	**Beskrivning**
telia.com	Telia Internet Abuse	Hanterar missbruk av Telias Internettjänster
telia.net	Telia Internet IRT	Incidenter som har sitt ursprung i eller som påverkar Telias nätverk (Telia Net)

homerun.telia.com	Telia Mobile Abuse	Hanterar missbruk av tjänsten Telia Homerun WLAN
sonera.com/net/fi	CSIRT TSF	Incidenter som har sitt ursprung i eller som påverkar Soneras nätverk (SONERA-INET)
TSF-säkerhetsprodukter	Secure-CERT	brandväggar, VPN, certifikatutfärdare, IDS o.s.v.
netcom.no	Netcom IRT	Internetkunder och Netcoms interna nätverk
telia.dk	CSIRT-TSDK	Interna nätverk
stofanet.dk/stofa.dk	Telia Stofa A/S	Internetkunder
telia.se	CSIRT-TSS	Incidenter som påverkar TeliaSoneras interna nätverk
Alla andra incidenter med anknytning till TeliaSonera	TS-CERT CC	Kontaktpunkt för TeliaSonera-gruppen

2.2.4 Rapportering

Telia erbjuder en Service Management funktion som fortlöpande följer upp och rapporterar driftsavvikelser i kundens avtalade tjänst. Vid regelbundna driftmöten följs avtalade tjänster upp avseende de parametrar som finns i kundavtalet.

Telias företagswebb, www.telia.se/foretag, är en samlad webbplats för information, köp, självbetjäning och administration av Telias produkter och tjänster. Kunden kommer dit genom att gå direkt till www.telia.se/foretag eller genom att gå in på www.telia.se och sedan klicka på Företag. Här redovisas driftsinformation för Fast och Mobil telefoni.

Mina Sidor på Arbetet
Den lösenordsskyddade delen av företagswebben är Mina Sidor på Arbetet. För att få tillgång till MSpA måste kunden först registrera sig på den öppna delen av företagswebben. Kunder som loggar in på MSpA har givetvis också tillgång till all den information som finns på den öppna delen av företagswebben.

Via Mina Sidor på Arbetet kan kunden dygnet runt gå in och hämta rapporter och statistik.

Följande funktioner finns bland annat att få via webbgränssnitt:

Driftsstatistik
Driftstatistik (SLA-rapporter) inklusive statistik över tillgänglighet kan också ses i förekommande fall via webbgränssnittet.

Historik för Statistik
All statistik kan sparas i 15 månader och plockas fram när som helst via webbgränssnittet.