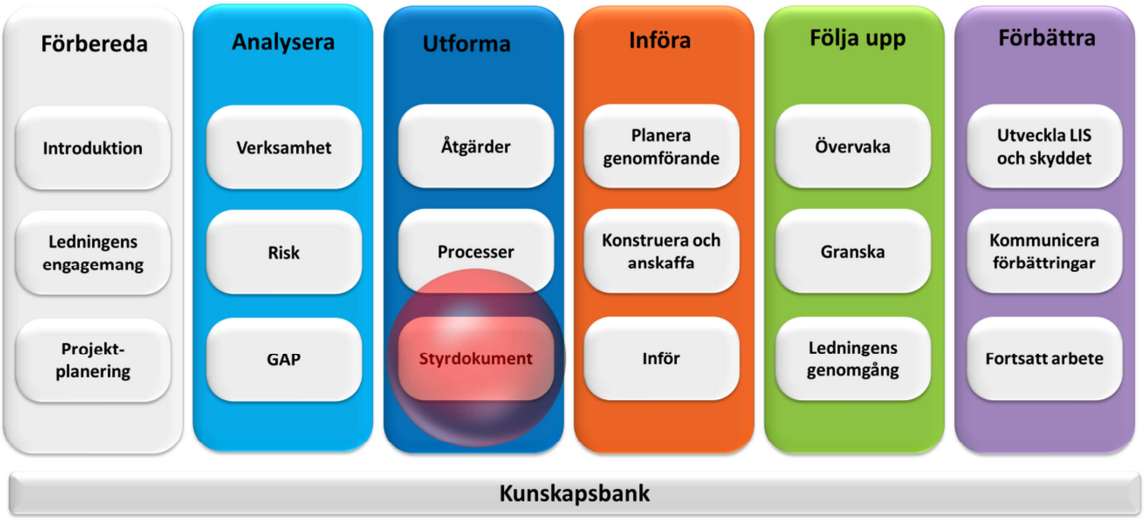
Myndigheten för samhällsskydd och beredskap

Utforma policy och styrdokument



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Upphovsrätt
Tillåtelse ges att kopiera, distribuera, överföra samt skapa egna bearbetningar av detta dokument, även för kommersiellt bruk. Upphovsmannen måste alltid anges som ”MSB, www.informationssäkerhet.se”. Vid egna bearbetningar får det inte antydas att MSB godkänt eller rekommenderar bearbetningen eller användningen av det bearbetade verket. Dessa villkor följer licensen ”Erkännande 2.5 Sverige (CC BY 2.5)” från Creative Commons. För fullständiga villkor, se http://creativecommons.org/licenses/by/2.5/se/legalcode.

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

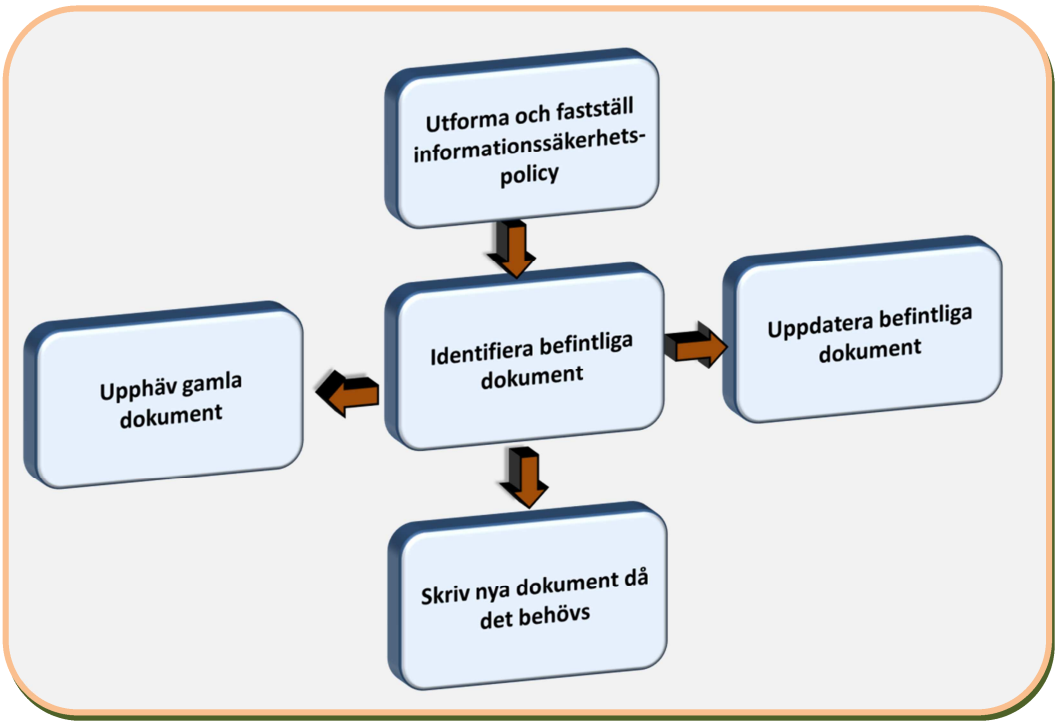
1. Inledning

De tidigare momenten har lett till fastställda säkerhetsåtgärder och ett antal nya eller förändrade processer. Om inte den övergripande policyn redan är skriven så behövs nu den och ett antal styrdokument för att förändringarna ska få en djup förankring i verksamheten. Dessa dokument är grunden för att säkerhetsarbetet genomförs på ett strukturerat sätt. De är också viktiga att ha för att kunna granska informationssäkerhetsarbetet.

Styrdokumenten ska följa en intern struktur som bör gälla för alla styrdokument inom organisationen. De beteckningar på olika styrdokument som används här är desamma som i exemplet på styrdokumentshierarki som finns i bilaga D till dokumentet Introduktion till metodstödet.

Figur 1 visar de olika arbetsuppgifterna som kan genomföras parallellt eller i den ordning som passar organisationen bäst, beroende på utgångsläget. Rekommendationen är dock att tidigt ta fram en övergripande policy eftersom den är ett viktigt verktyg när ledningen ska förtydliga och föra ut sin intention på informationssäkerhetsområdet. Den ger därmed viktiga signaler om att arbetet med informationssäkerhet är viktigt och högt prioriterat.

Figur 1. Aktivitetens arbetsuppgifter



1.1 Exempel på styrdokumentshierarki

Interna styrdokument kan ha olika benämningar. Det viktiga är dock inte vad dokumenten kallas utan att organisationen har en gemensam terminologi för styrdokumenten och att de följer en given hierarki så att läsaren känner igen sig och förstår vilken vikt de olika dokumenten har, eller vilken grad av styrning de anger.

Här följer en kort summering av diskussionen i ”Introduktion till metodstödet” om de olika dokumenttyper som kan ingå i en dokumenthierarki. Detta är dock bara förslag på dokumenttyper.

Figur 2. Exempel på styrdokumentshierarki

2. Arbetsuppgifter

2.1 Förberedelser

De som ska utforma policyn och framför allt de övriga styrdokumenten måste känna till processen för att ta fram och fastställa styrdokument i organisationen. De flesta organisationer har någon sorts formaliserad process med till exempel en fastställd styrdokumentshierarki, interna beredningar och remisser samt fastställda mallar för hur styrdokument ska se ut. Organisationens juridiska kompetens bör vara med om att ta fram dokumenten.

Det första steget är att läsa igenom bilaga D till dokumentet Introduktion till metodstödet och relatera innehållet till den egna organisationen. Det är viktigt att fundera på vilken styreffekt man vill uppnå för att därmed välja den typ av styrdokument som passar bäst. Ett viktigt led i förberedelserna är att hitta de personer som ska vara med i arbetet. Vem är ansvarig för det som ska regleras? Vem är beställare eller uppdragsgivare för arbetet? Förutom juridisk kompetens bör arbetsgruppen förstås inkludera de personer som är experter inom det område som ska regleras.

Styrdokumenten bör inte nämna teknik – särskilt inte dokumenten högt upp i hierarkin. Utvecklingen inom informationssäkerhet går fort och tekniska detaljer blir snabbt inaktuella. I stället är det bättre att fokusera på vilket skydd man vill uppnå utan att nämna de tekniska lösningar som finns i dag. Detta gäller dock inte rutinbeskrivningar eller instruktioner där man ofta måste relatera innehållet till befintlig teknik. Det innebär att dessa styrdokument måste ses över ganska ofta.

2.2 Planering

Arbetsupplägget måste anpassas till verksamheten. Policyn bör dock tas fram i ett tidigt skede, före eller samtidigt som aktiviteterna fastställa säkerhetsåtgärder och utforma säkerhetsprocesser. Policyn är inte detaljreglerande och därmed inte beroende av att ledningssystemet i övrigt är klart. Den kan i stället ge skjuts åt det övriga arbetet i och med att ledningen sätter ned foten och formulerar sin viljeinriktning på informationssäkerhetsområdet.

Det är viktigt att identifiera alla befintliga styrdokument för att veta vilket material man har att utgå ifrån. Detta ger en bild av vilken arbetsinsats som krävs för att utarbeta de styrdokument som behövs samt för att få ordning och reda bland styrdokumenten. Arbetsgruppen kan sedan uppdatera och skriva styrdokumenten i den ordning som passar resultatet från verksamhetsanalysen, riskanalysen och gapanalysen samt resultatet från inventeringen av befintliga styrdokument. Ett generellt tips är att först reglera

skyddet av den känsligaste informationen inom de områden där riskerna är störst.

2.3 Utforma och fastställa informationssäkerhetspolicy

Informationssäkerhetspolicyn (eller säkerhetspolicyn) är det främsta av de dokument som ledningen riktar till organisationen. Har organisationen redan en struktur för och rutiner kring vilka policyer som ska finnas och hur dessa ska tas fram ska man förstås ta hänsyn till detta. Vad man väljer att kalla policyn – till exempel verksamhetspolicy (som förmodligen innehåller även annat än säkerhetsrelaterad information), säkerhetspolicy (som förmodligen tar ett större grepp över säkerhetsfrågor) eller informationssäkerhetspolicy är upp till varje organisation. Det viktiga är att ledningen ger uttryck för sin viljeinriktning avseende informationssäkerhet. I metodstödet hanteras förstås enbart informationssäkerhet och här finns rekommendationer för det som bör tas upp i policyn för informationssäkerhet.

Policyn ska inte innehålla några konkreta förhållningsregler utan uttrycka ledningens viljeinriktning och på så sätt ”rama in” de övriga styrdokumenten. En policy bör vara kortfattad och därmed lättillgänglig för alla. Mer information och förklarande texter kan presenteras på något annat sätt, till exempel på den interna webben.

En informationssäkerhetspolicy bör innehålla:

- ledningens viljeinriktning – varför det är viktigt med informationssäkerhet
- en kort beskrivning av hur viljeinriktningen ska uppnås
- en kort beskrivning av ansvarsförhållandena inom informationssäkerheten
- en förklaring av viktiga begrepp
- en redogörelse för vem som ansvarar för policyn samt hur den ses över och revideras.

Ledningen ska aktivt vara med och utforma policyn. Det är trots allt ledningen som skickar budskapet och det är viktigt att den känner ansvar för policyn. I praktiken är det dock den som ansvarar för informationssäkerheten eller LIS-gruppens ledare som ansvarar för att policyn tas fram. Även om ledningen äger dokumentet bör experterna inom informationssäkerhet utforma den så att den stämmer överens med intentionerna i informationssäkerhetsarbetet.

När policyn är klar använder man etablerade processer för information och kunskapsspridning för att informera alla medarbetare om policyn och hur viktig den är för organisationen.

2.4 Identifiera befintliga dokument

Under arbetet med att fastställa säkerhetsåtgärderna utsåg man också ansvariga personer för varje säkerhetsåtgärd. För att finna alla befintliga styrdokument bör man först fråga dessa personer vilka sådana dokument som finns i dag. Det kan vara effektivt att samla alla ansvariga personer till ett möte för att gemensamt gå igenom vad som finns och vad som saknas. När alla befintliga styrdokument är identifierade och nerladdade (och eventuellt utskrivna) börjar arbetet med att matcha dem mot de nya säkerhetskraven.

Tänk på att det organisatoriska minnet inte alltid är så gott som det borde vara. Det kan finnas beslut som formellt sett gäller men som inte är kända och spridda. Ett beslut gäller dock fram till dess att det har upphävts. Tänk också på att allt kanske inte finns dokumenterat. En del kunskap om hur man hanterar olika säkerhetsfrågor kan överföras muntligt, och en del saker vet kanske bara den som i praktiken utför vissa säkerhetsåtgärder.

2.5 Uppdatera befintliga dokument

När de flesta styrdokument är identifierade ska de uppdateras. För att arbeta systematiskt kan man utgå från en matris där kolumnerna består av dokumenten och raderna av de säkerhetsåtgärder som ska införas. På så sätt blir det lätt att matcha alla nödvändiga åtgärder mot de dokument som i dag reglerar liknande åtgärder.

Börja med att lista de fastställda säkerhetsåtgärderna med tillhörande processer och försök att skapa kluster av åtgärder som hänger ihop. Skriv in respektive åtgärd i raderna, medan klustren kan beskrivas i ett separat dokument.

Skriv därefter in de identifierade dokumenten i kolumnerna och markera när dokumenten matchar någon fastställd säkerhetsåtgärd. Många åtgärder kräver ändringar i flera dokument, till exempel måste en vägledning ändras om den riktlinje den är en vägledning till förändras. Tack vare matrisen blir arbetet spårbart.

Tabell 1: Tabell för kontroll av och spårbarhet på förändringar i styrdokument

		Dokument		
		Dokument 1	Dokument 2	Dokument 3
Åtgärd	Åtgärd 1			
	Åtgärd 2			
	Åtgärd 3			
	Åtgärd 4			
	Åtgärd 5			

Den som är verksamhetsansvarig, eller motsvarande, måste avgöra vad som ska uppdateras och i vilken prioritetsordning, och bestämma det utifrån vilka risker som finns med att inte ha aktuella styrdokument för de olika områdena. Använd resultatet från den övergripande riskanalysen för att göra prioriteringar, och eventuellt också från övriga riskanalyser samt resultatet från verksamhetsanalysen och gapanalysen.

Självklart finns det inget egenvärde i att uppdatera dokument. De dokument som håller måttet behöver inte ändras men de bör granskas kritiskt innan beslut tas att inte uppdatera dem.

Ett generellt tips är att börja med dokument långt ner i hierarkin (exempelvis rutinbeskrivningar och instruktioner). Dessa dokument går fortare att uppdatera än dokument med högre styrningsgrad och ger snabbare effekt på informationssäkerheten. När de mer övergripande dokumenten är färdiga är det dock möjligt att en del rutinbeskrivningar och instruktioner måste skrivas om igen. Men det går ändå ganska fort.

Arbetet med att uppdatera styrdokument fortgår löpande. Det är viktigt att varje styrdokument versionshanteras och ägs av någon som ansvarar för att dokumentet är aktuellt.

För tips om genomförandet se kapitel 3.

2.6 Skriv nya styrdokument när det behövs

Det är möjligt att de befintliga dokumenten inte täcker allt utan att det måste skrivas nya styrdokument. Utgå från matrisen i tabell 1 och kontrollera om några åtgärder inte har ”checkats av” mot ett existerande dokument. I så fall behövs ett nytt styrdokument. Använd också bilaga B för att få förslag på vilka områden som kan behöva styrdokument.

Använd samma princip som ovan för att prioritera skrivandet av de nya dokumenten: genom att utgå från resultaten av de grundläggande analyserna

(verksamhetsanalys, riskanalys och gapanalys). Även nu bör man börja med dokument längre ner i hierarkin och jobba sig uppåt.

Även arbetet med att skriva nya styrdokument fortgår löpande. Den som ansvarar för en verksamhet ansvarar också för att det skrivs nya styrdokument när behov av sådana uppstår. För tips om genomförandet se kapitel 3.

2.7 Upphäv regler som inte längre gäller

Bland de dokument som identifierats finns säkert gamla dokument och delar i dokument som behöver upphävas. Exakt hur detta görs bör varje organisation ha rutiner för men generellt så bör ett upphävande tas i ett formellt beslut och dokumenteras som ett beslut.

3. Stöd för uppdatering och framtagning av nya styrdokument

3.1 Ordning på styrdokumenten

Den som ska ta fram nya styrdokument ska följa den praxis som finns i organisationen för detta. Om det inte finns någon sådan process eller en styrdokumentshierarki är det viktigt att lyfta frågan till ledningen. Bilaga D i dokumentet ”Introduktion till metodstödet” visar hur en styrdokuments-hierarki kan utformas, och antalet nivåer bör anpassas efter organisationens behov. Policyn bör dock vara ledningens dokument för en övergripande viljeinriktning. Dessutom bör man skilja på dokument som hanterar *bindande regler* och dokument som beskriver *hur* reglerna ska följas.

Glöm inte att versionshantera styrdokumenten. Det bör tydligt framgå när ett styrdokument är beslutat och vem (vilken befattning) som ansvarar för att det hålls aktuellt. Den som uppdaterar eller upprättar nya styrdokument bör också se till att de finns beskrivna i någon form av dokumentation som möjliggör ordning och reda, spårbarhet och kvalitet. Där anges dokumenttypen, beslutsdatumet och vem (vilken befattning) som ansvarar för att de olika dokumenten hålls aktuella.

Använd tabell 1 även fortsättningsvis som ett verktyg för att ha koll på vilka säkerhetsåtgärder som regleras i vilka styrdokument. Tabellen kan vidareutvecklas efter eget tycke så att den innehåller den information som organisationen har behov av.

3.2 Förankring

Det är viktigt att de som berörs av de nya styrdokumenten är med när dokumenten tas fram eftersom dokumenten då får större genomslag. Det är också bra med ett remissförfarande som ger olika delar av organisationen en chans att tycka till innan besluten fattas. Tänk på när i tiden en remiss skickas ut så att de som är berörda har tid och möjlighet att besvara remissen. Ge också tillräckligt lång svarstid. Det kan även vara bra att genomföra två remissrundor.

När styrdokumenten börjar gälla är det viktigt att ge medarbetarna riktad information eller utbildningar så att de förstår hur reglerna påverkar deras arbete.

3.3 Skrivtips

Den som skriver styrdokument måste ha tänkt igenom vad som behöver regleras, hur stark styreffekt som behövs (”ska-regler”, ”bör-regler” eller praxis)

och hur mycket stöd de som ska följa reglerna behöver. Börja gärna med att motivera säkerhetsåtgärden som ska regleras med hjälp av de noteringar som gjordes när säkerhetsåtgärden utformades. Beskriv därefter de säkerhetsprocesser som krävs för att åtgärden ska vara verksam. Dessa motiveringar och beskrivningar kan användas i styrdokument av typen vägledningar.

Identifiera målgruppen för styrdokumentet och anpassa i möjligaste mån språk och innehåll efter målgruppens behov och förutsättningar. Tänk igenom språket så att budskapet blir tydligt. I stället för *ska* kan man ibland skriva *är* för att tydliggöra texten.

Goda råd för att skriva tydliga styrdokument:

- Skriv enkelt i alla typer av styrdokument och använd inga komplicerade termer – det här är dokument som verkligen ska läsas och förstås.
- Använd exempel från konkreta fall i vägledningarna så innehållet blir tydligt för läsaren.
- Använd bilder i vägledningarna för att illustrera olika säkerhetsprocesser.

Bilaga A i detta dokument visar hur en policy kan utformas. I bilaga B finns en checklista för innehållet i en policy. Bilaga C ger förslag på vilka styrdokument en verksamhet kan behöva.

4. Nästa steg

När momenten i delprocessen Utforma är klara är ledningssystemet utformat på ”ritbordet” och färdigt att införas i verksamheten. Nästa steg är att trycka på startknappen – nu ska ledningssystemet sättas i rullning.

Bilaga A: Exempel på informationssäkerhetspolicy

Vi behöver skydda organisationens information på ett sätt som passar vår verksamhet. Det är nödvändigt för att vi ska uppnå verksamhetsmålen och för att kunder, uppdragsgivare, samarbetspartner, allmänhet och anställda ska känna förtroende för oss. Därför arbetar vi aktivt med informationssäkerhet så att all vår information alltid ska vara konfidentiell, riktig och tillgänglig.

Vi har valt ett gemensamt och strukturerat sätt att arbeta med informationssäkerhet som bygger på den svenska och internationella standarden LIS (ledningssystem för informationssäkerhet). Med stöd av LIS får vi rätt nivå på informationssäkerheten samtidigt som våra anställda får ett stöd i sitt dagliga arbete.

Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av vår verksamhet och alla de informationstillgångar som vi äger eller hanterar. Personalen ska få fortlöpande utbildning för att förstå hur informationssäkerhetsarbetet fungerar.

Alla har ett ansvar för att säkerheten fungerar. Den som upptäcker brister i informations-säkerheten måste uppmärksamma sin chef eller säkerhetsfunktionen på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker.

Ansvaret för informationssäkerhet följer verksamhetsansvaret.

Begreppsförklaringar (bygger på definitioner hämtade från ”Terminologi för informationssäkerhet, SIS HB550 utgåva 3, SIS förlag):

- Informationstillgångar är allt som innehåller information och allt som bär på information.
- Informationssäkerhet är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.
- Konfidentiell information får inte nås av eller avslöjas för någon obehörig. Oftast gäller det innehållet i en informationstillgång men ibland är även tillgångens existens hemlig.
- Riktig information innebär att informationen inte får obehörigen förändras, inte av misstag och inte på grund av en funktionsstörning.
- Tillgänglig information innebär att informationen går att utnyttja av behörig användare när det behövs och så mycket som det behövs.
- Ett ledningssystem för informationssäkerhet (LIS) är ett verktyg som hjälper oss att upprätta, införa, driva, övervaka, granska, underhålla och förbättra den önskade nivån på informationssäkerhet i vår organisation.

Varje år ska säkerhetschefen se över och eventuellt revidera informationssäkerhetspolicyn.

Bilaga B: Checklista för att kontrollera policyns fullständighet

Fråga	Ja	Delvis	Nej
Anger policyn ledningens viljeinriktning och stödjer informationssäkerhetsarbetet?			
Visar policyn målet med samt omfattningen och vikten av informationssäkerhet?			
Har ledningen fastställt policyn?			
Är ansvaret för informationssäkerhet definierat?			
Står det klart och tydligt vem som äger policyn?			
Är det beskrivet hur policyn ska underhållas?			
Finns det en definition av informationssäkerhetsbegreppet?			
Är policyn spridd i organisationen och finns det rutiner för detta?			

Bilaga C: Checklista och exempelsamling för övriga styrdokument

Kapitel i LIS 27002	Styrdokument
5. Säkerhetspolicy	5.1 Informationssäkerhetspolicy
6. Organisation av informationssäkerheten	6.1 Fastställande av organisation, ansvar och roller (arbetsordning, övergripande föreskrift e.d.) 6.2 Styrdokument för organisationens processer och styrning avseende informationssäkerhet 6.3 Styrdokument avseende ansvar och uppgifter inom informationssäkerhet
7. Hantering av tillgångar	7.1 Styrdokument för klassificering 7.2 Styrdokument för ansvar, ägarskap och förteckning av tillgångar 7.3 Styrdokument för hantering av tillgångar
8. Personalresurser och säkerhet	8.1 Styrdokument för kontroll av personal, före, under och efter anställning 8.2 Styrdokument för utbildning inom informationssäkerhet 8.3 Styrdokument för disciplinär process 8.4 Styrdokument för återlämnande av tillgångar och indragning av åtkomsträttigheter
9. Fysisk och miljö-relaterad säkerhet	9.1 Styrdokument för säkra utrymmen 9.2 Styrdokument för skydd av utrustning

10. Styrning av kommunikation och drift	10.1 Styrdokument för driften 10.2 Styrdokument för hantering av tredjepartsleverantör av tjänster 10.3 Styrdokument för systemplanering och systemgodkännande 10.4 Styrdokument för skydd mot skadlig och mobil kod 10.5 Styrdokument för säkerhetskopiering 10.6 Styrdokument för hantering av säkerhet i nätverk 10.7 Styrdokument för hantering av media 10.8 Styrdokument för utbyte av information 10.9 Styrdokument för tjänster för elektronisk handel 10.10 Styrdokument för övervakning
11. Styrning av åtkomst	11.1 Styrdokument för styrning av åtkomst 11.2 Styrdokument för användares ansvar 11.3 Styrdokument för mobil datoranvändning och distansarbete
12. Anskaffning, utveckling och underhåll av informationssäkerhet	12.1 Styrdokument för bearbetning i tillämpningar 12.2 Styrdokument för kryptering 12.3 Styrdokument för skydd av systemfiler 12.4 Styrdokument för utvecklings- och underhållsprocesser 12.5 Styrdokument för hantering av tekniska sårbarheter
13. Hantering av informationssäkerhetsincidenter	13.1 Styrdokument för rapportering och hantering av informationssäkerhetsincidenter
14. Kontinuitetsplanering för verksamheten	14.1 Styrdokument för kontinuitetsplanering (innefattande informationssäkerhetsaspekter)
15. Efterlevnad	15.1 Styrdokument för efterlevnad av rättsliga krav och interna riktlinjer
Övrigt	