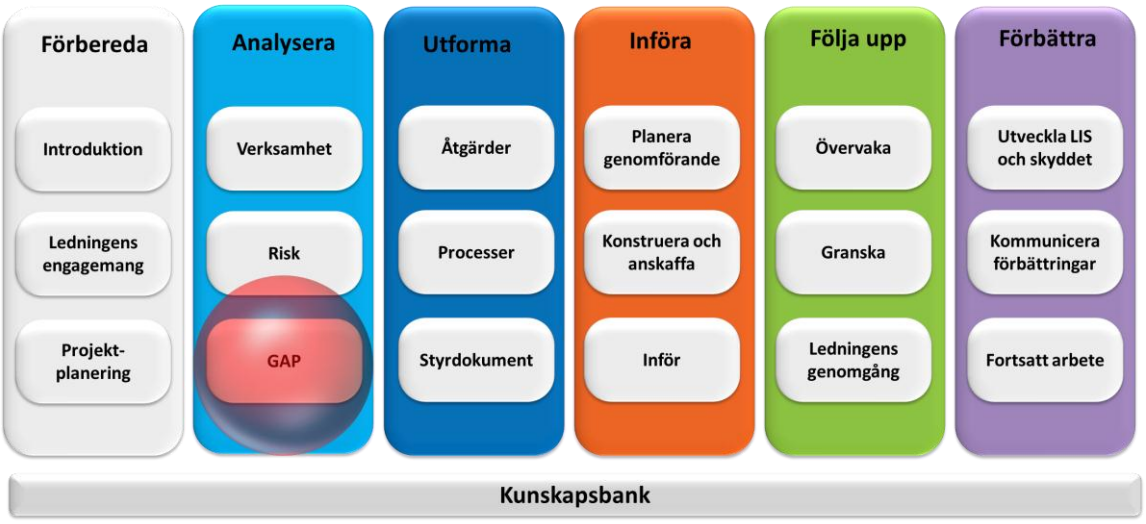
Myndigheten för samhällsskydd och beredskap

Gapanalys



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

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

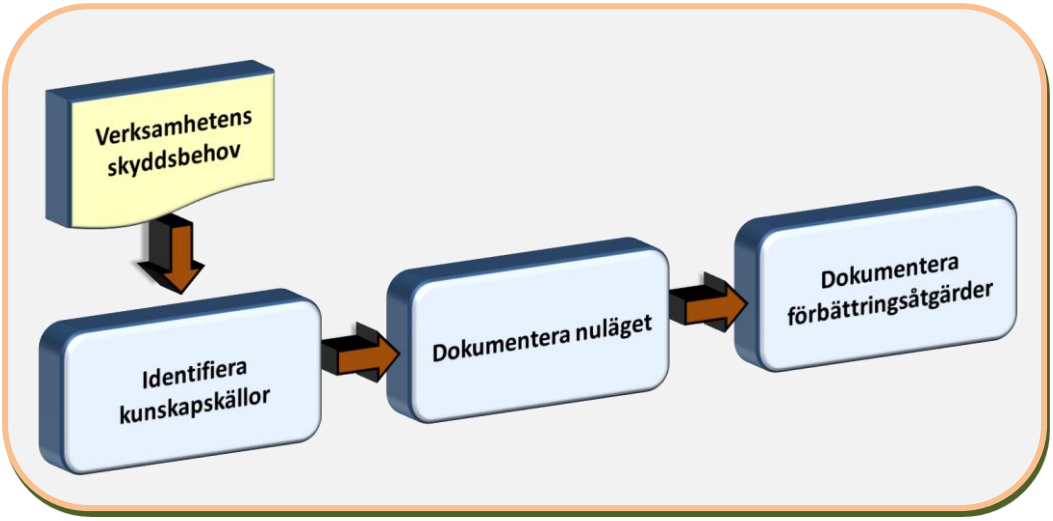
Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning

Efter verksamhetsanalysen och riskanalysen är behoven, kraven och riskerna kartlagda. Nu är det dags för en analys av nuläget när det gäller informationssäkerheten – en gapanalys. Uttrycket syftar på gapet mellan det som standarden beskriver som bästa praxis och den rådande säkerhetsnivån i verksamheten. Arbetsuppgifterna för gapanalysen illustreras i figuren nedan.

Figur 1. Arbetsuppgifterna under gapanalysen



1.1 Syfte med aktiviteten

Gapanalysen ska ge

- bekräftelse på att skyddet är infört i tillräcklig omfattning
- en uppfattning om kvaliteten på säkerhetsarbetet
- information om styrkor och svagheter i skyddet
- ett underlag för resten av arbetet med att införa ledningssystemet.

1.2 Ingångsvärden

För att kunna göra en gapanalys av informationssäkerheten behöver du som analysledare information och kunskap:

- **Behov och krav.** Det är nödvändigt att känna till verksamhetens behov och krav, enligt resultaten från verksamhetsanalysen och riskanalysen.
- **Säkerhetsdokument.** Analysledaren måste studera vad existerande policydokument och riktlinjer säger om informationssäkerhet.
- **Standard och norm.** Gapanalysen utgår från en norm, det vill säga en lista med krav eller säkerhetsåtgärder. I den här metoden används kraven i 27001 och 27002.

Det kan också vara användbart att leta rätt på eventuella tidigare revisionsrapporter som gäller informationssäkerheten.

Checklistan

Den så kallade *checklistan* finns som en separat bilaga på www.informationssakerhet.se och går att ladda ner därifrån. Listan är en summering av krav och vägledningar från 27002 där man under arbetet med gapanalysen kan ange i vilken grad olika säkerhetsåtgärder är uppfyllda. Checklistan har gjorts tillgänglig med tillstånd av SIS Förlag.

1.3 Beskrivning av aktiviteten

Med hjälp av ingångsvärdena ovan ska analysledaren sammanställa material och kunskap. Standarden 27001 innehåller 133 olika krav på säkerhetsåtgärder, och analysledaren ska gå igenom dem för att se vilka av dessa säkerhetsåtgärder som:

1. redan finns och fungerar tillfredsställande (utifrån verksamhetens specifika behov)
2. fungerar tillfredsställande tack vare kompenserande åtgärder
3. inte existerar eller inte fungerar tillfredsställande
4. inte behövs (motivera).

Analysen dokumenteras sedan genom att beskriva nuläget och eventuella förbättringsåtgärder för varje krav i standarden.

1.4 Resultat

Rapporten från gapanalysen bör inkludera

- en översiktlig beskrivning av analysprocessen och hur arbetet är genomfört
- information om vad som har legat till grund för analysen (dokumenten i avsnitt 1.2 om ingångsvärden ovan)
- dokumentation av själva analysen
- sammanfattande slutsatser kring verksamhetens nuvarande informationssäkerhetsnivå.

Om gapanalysen görs som en del av ett LIS-införande ska projektledaren för LIS-införandet föra in resultatet i beslutsunderlaget (Beslut 2a) för det fortsatta arbetet. I bilaga C finns ett exempel på hur en rapport från gapanalysen kan vara utformad. Tänk på att resultatet av gapanalysen kan vara känsligt och att det bör hanteras därefter.

1.5 Rättighet

2. Vägledning

2.1 Inledning

De flesta verksamheter i dag är väldigt komplexa med en blandning av teknologier, processer och medarbetare som alla samverkar för att hantera verksamhetens information på ett så sätt som möjligt. Huvudsyftet är att stödja så att organisationens mål uppfylls. Verksamhetens information måste skyddas så att den alltid är *konfidentiell, tillgänglig* och *riktig*, och därför inför man *administrativa*, *organisatoriska*, *fysiska* och *logiska* skydd.

När skyddsåtgärderna ska granskas är det viktigt att tänka i flera dimensioner:

- Är skyddsåtgärden dokumenterad?
- Är skyddsåtgärden verkligen på plats och används den?
- Fungerar skyddsåtgärden som det är tänkt?
- Underhålls skyddsåtgärden?

Genom att värdera skyddet med hjälp av en gapanalys får verksamheten ett bra kvitto på hur sårbar den är för de risker som finns. Det skapar en trygghet om organisationen känner till den aktuella nivån av informationssäkerhet och analysen blir ett bra underlag för resten av LIS-införandet.

2.2 Mål

Metoden som beskrivs i det här dokumentet ska vara till hjälp för att kontrollera hur verksamhetens informationssäkerhet står sig i förhållande till de uppsatta målen. Finns det inga sådana mål kan man använda checklistan (separat bilaga på www.informationssäkerhet.se) i sin helhet. Analysen blir ett underlag för att planera arbetet med de brister som finns.

2.3 Målgrupp

Den här metoden för gapanalys är användbar för flera grupper av användare:

- projekt som ska införa ett ledningssystem för informationssäkerhet
- personer som är ansvariga för att mäta eller verifiera nivån på säkerhetsskyddet
- verksamhetschefer som vill ställa krav på sin skyddsnivå, till exempel systemägare
- säkerhets- eller informationssäkerhetsansvariga som ska mäta effektiviteten i skyddet.

2.4 Hur ska metoden användas?

Metoden ska användas för att få fram gapet mellan den existerande och den önskade säkerhetsnivån, innan organisationen inför ett LIS. Metoden är generisk och fungerar på de flesta verksamheter, även om den troligtvis behöver anpassas något.

En viktig del i säkerhetsarbetet är att årligen följa upp säkerhetsnivåns status och verktyget passar bra även för det ändamålet. Vi kommer senare i ramverket att beskriva hur detta går till.

2.5 Kritisk säkerhetsåtgärd

Av de totalt 133 säkerhetsåtgärderna i checklistan bedöms 62 säkerhetsåtgärder som kritiska. De kritiska säkerhetsåtgärderna bör varje organisation införa som basnivå för att skydda sin information, och dessa åtgärder är nödvändiga för att organisationen ska känna förtroende för informationshanteringen. Denna bedömning bygger på många års erfarenhet av vilka risker en verksamhet måste skydda sig mot.

2.6 Arbetsflöde vid gapanalys

Innan analysen börjar är det viktigt med noggrann planering för att kunna arbeta så effektivt som möjligt. Det finns ett antal steg som analysledaren bör gå igenom före, under och efter analysen, och en del saker att tänka på. I rutan nedan anges översiktligt det som ska genomföras.

Inför analysen

1. Avsätt tid för gapanalysen (normalt två till tre hela dagar).
2. Skicka analysunderlag och förslag på agenda till olika områdesansvariga som ska fylla i och returnera dem. Be om förslag på deltagare (se tabell 1 Förslag på ansvariga för respektive område).
3. Egna förberedelser:
    a. Läs det inkomna underlaget.
    b. Stäm av agendan och deltagarna med områdesansvariga.

Under analysen

På plats – dag 1:

1. Inledning:
    a. Stäm av agendan.
    b. Be ansvarig för IT-verksamten presentera IT-miljön.
2. Rundvandring och analys av
    a. datorrum
    b. placeringen av kylsystemets värmeavgivning
    c. övrig viktig IT-utrustning på andra platser
    d. förvaring av säkerhetskopior
    e. kablage
    f. korskopplingsskåp.
3. Intervjuer enligt agendan med hjälp av frågepaketet från bilagan A Gapanalys checklistan.
4. Inför dag 2 – sammanställ säkerhetsnivåer och sammanfatta brister.

På plats – dag 2:

1. Fortsätt intervjuerna enligt agendan med hjälp av frågepaketet.
2. Sammanställ resterande säkerhetsnivåer och sammanfatta brister.
3. Rapportering för de intressenter som medverkat i analysen – presentera analysnivåerna och kortfattat även funna brister.

På plats – dag 3:

1. Fortsätt intervjuerna enligt agendan med hjälp av frågepaketet.
2. Sammanställ resterande säkerhetsnivåer och sammanfatta brister.
3. Rapportering för projektet och ev. de intressenter som medverkat i analysen – presentera analysnivåerna och kortfattat även funna brister.

Efter analysen

1. Sammanställ en nivå- och bristrapport och ge den till de medverkande för avstämning.
2. Sammanställ en åtgärdsplan och foton till en slutlig rapport.

3. Gapanalysens arbetsuppgifter

En gapanalys består i huvudsak av tre arbetsuppgifter som illustreras i figur 1. Det här kapitlet innehåller en närmare beskrivning av dessa arbetsuppgifter.

3.1 Identifiera kunskapskällor

Gör ett schema för analysdagarna i god tid före en gapanalys. Skicka dessutom frågeformuläret (se bilaga A) till de personer som är ansvariga för de elva olika områdena som standarden (27002) omfattar. Till exempel bör den ansvarige för område 6 – ”Organisation av informationssäkerheten” vara säkerhetschefen eller informationssäkerhetschefen. Tabell 1 nedan innehåller förslag på ansvariga personer för samtliga elva områden. Det är dock inte den ansvariga för området som ska besvara frågorna, utan han eller hon ska välja lämpliga personer till analysgruppen. Under kolumnen område (enligt 27002) har vi tagit med de kapitel som innehåller säkerhetsåtgärder. Ett tips är att inkludera en jurist som troligtvis kan jobba inom flera områden.

Tabell 1. Förslag på ansvariga för respektive område

Område (enligt 27002)	**Förslag till ansvarig**
5. Säkerhetspolicy	Säkerhetschef eller informationssäkerhetschef
6. Organisation av informationssäkerheten	Säkerhetschef eller informationssäkerhetschef
7. Hantering av tillgångar	Säkerhetschef/Informationssäkerhetschef
8. Personalresurser och säkerhet	Säkerhetschef, informationssäkerhetschef eller personalchef
9. Fysisk och miljörelaterad säkerhet	Säkerhetschef eller informationssäkerhetschef
10. Styrning av kommunikation och drift	IT-chef
11. Styrning av åtkomst	IT-chef
12. Anskaffning, utveckling och underhåll av informationssystem	IT-chef eller utvecklingsansvarig

Område (enligt 27002)	Förslag till ansvarig
13. Hantering av informationssäkerhets-incidenter	Säkerhetschef, informationssäkerhetschef eller IT-chef
14. Kontinuitetsplanering för verksamheten	Säkerhetschef eller informationssäkerhetschef
15. Efterlevnad	Säkerhetschef, informationssäkerhetschef eller IT-chef

Senast en vecka innan gapanalysen börjar ska de ansvariga för respektive område lämna tillbaka dokumenten med förslag på deltagare. De namngivna personerna ska vara de inom organisationen är bäst lämpade att besvara frågorna för varje delområde. Den som ansvarar för gapanalysen ska sedan se till att dessa personer är bokade och att det finns ett rum där intervjuerna kan hållas under analysdagarna.

3.2 Dokumentera nuläget

När kunskapskällorna för varje delområde är identifierade och schemat är framtaget är det dags att genomföra själva gapanalysen. Figur 2 visar ett lämpligt schema för gapanalysen, med ungefärliga tidsangivelser. Schemat kommer från en av författarna som har en lång erfarenhet av många gapanalyser, och det bör följas med så små ändringar som möjligt. En oerfaren analysledare kan dock behöva lägga på en halvtimme på alla delmoment. En mer ingående beskrivning av de olika momenten finns i bilaga B.

Under intervjuerna ska analysledaren ställa frågor och ”experterna” från respektive områden svarar ja eller nej med kommentarer. Ibland kan det gälla ett område som analysledaren inte känner till i detalj, och då kan deltagarna själva få tolka och analysera frågan. Be alla deltagare att vara ärliga eftersom de själva tjänar på det i längden.

Tänk på att de nivåstyrande frågorna ska besvaras med ja, nej eller vet ej (se figur 3 för ett utdrag). Det går också att kommentera svaret och ge en mer fullständig beskrivning. På så sätt tar analysen mycket längre tid men i senare steg kan det vara bra för andra att veta på vilket sätt frågorna är införda i verksamheten. Den ordning som de olika kapitlen i standarden genomgås kommer från erfarenhet i vilken ordning de bör genomgås.

Figur 2. Förslag till tidsschema för gapanalysen

Dag 1

07:45–09:30	Egen kontroll av kringmiljön och lokaler
09:30–10:20	Presentation av verksamheten och IT-miljön
10:30–11:30	Rundvandring i ”datorlokalerna”
11:30–12:30	Lunch
12:30–13:30	**Område 9**. Fysisk och miljörelaterad säkerhet
13:45–14:45	**Område 5**. Säkerhetspolicy
15:00–16:00	**Område 6.** Organisation av informationssäkerheten
16:00–17:00	**Område 7**. Hantering av tillgångar
17:00–17:30	Analysledarens enskilda summering av dagen
17:30–17:45	Komplettering av analysunderlag

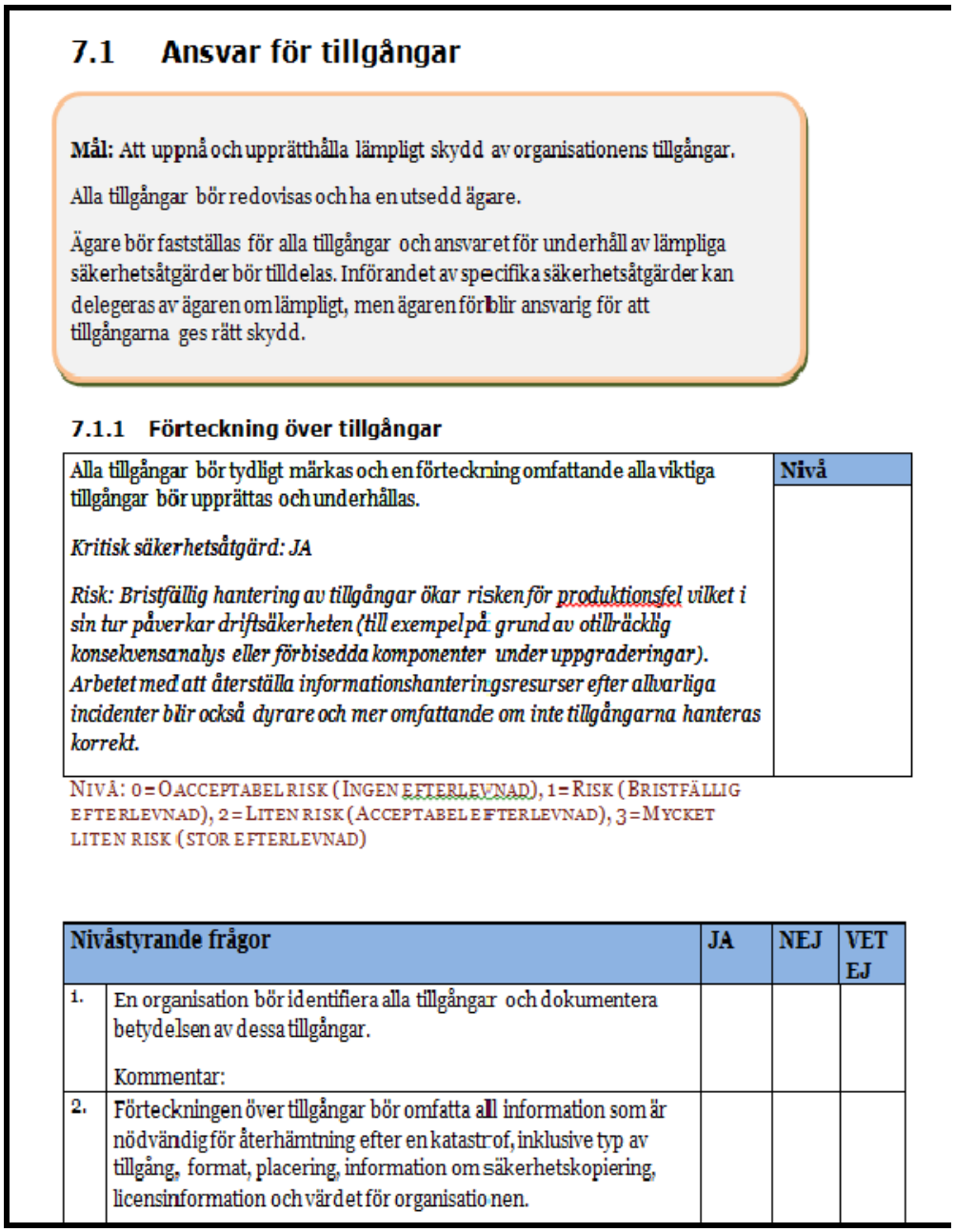
Dag 2

08:30–09:00	Presentation och synpunkter från gårdagen
09:00–10:00	**Område 8.** Personalresurser och säkerhet
10:15–11:30	**Område 10.** Styrning av kommunikation och drift
11:30–12:30	Lunch
12:30–14:00	**Område 11.** Styrning av åtkomst
14:00–15:00	**Område 12**. Anskaffning, utveckling och underhåll av informationssystem
15:00–16:00	**Område 13**. Hantering av informationssäkerhetsincidenter
16:00–16:30	Analysledarens enskilda summering av dagen
16:30–16:45	Komplettering av analysunderlag

Dag 3

08:30–09:00	Presentation och synpunkter från gårdagen
09:00–10:15	**Område 14.** Kontinuitetsplanering för verksamheten
10:30–11:30	**Område 15**. Efterlevnad
11:30–12:30	Lunch
12:30–13:30	Reservtid
13:30–15:00	Analysledarens enskilda summering
15:00–16:00	Presentation av synpunkter

Figur 3. Utdrag från bilaga A för att visa vilka uppgifter som ska matas in vid analysen



7.1 Ansvar för tillgångar

Mål: Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

Alla tillgångar bör redovisas och ha en utsedd ägare.

Ägare bör fastställas för alla tillgångar och ansvaret för underhåll av lämpliga säkerhetsåtgärder bör tilldelas. Införandet av specifika säkerhetsåtgärder kan delegeras av ägaren om lämpligt, men ägaren förblir ansvarig för att tillgångarna ges rätt skydd.

7.1.1 Förteckning över tillgångar

Alla tillgångar bör tydligt märkas och en förteckning omfattande alla viktiga tillgångar bör upprättas och underhållas. *Kritisk säkerhetsåtgärd: JA* *Risk: Bristfällig hantering av tillgångar ökar risken för produktionsfel vilket i sin tur påverkar driftsäkerheten (till exempel på grund av otillräcklig konsekvensanalys eller förbisedda komponenter under uppgraderingar). Arbetet med att återställa informationshanteringsresurser efter allvarliga incidenter blir också dyrare och mer omfattande om inte tillgångarna hanteras korrekt.*	**Nivå**

NIVÅ: 0 = OACCEPTABEL RISK (INGEN EFTERLEVNAD), 1 = RISK (BRISTFÄLLIG EFTERLEVNAD), 2 = LITEN RISK (ACCEPTABEL EFTERLEVNAD), 3 = MYCKET LITEN RISK (STOR EFTERLEVNAD)

Nivåstyrande frågor		**JA**	**NEJ**	**VET EJ**
1.	En organisation bör identifiera alla tillgångar och dokumentera betydelsen av dessa tillgångar. Kommentar:			
2.	Förteckningen över tillgångar bör omfatta all information som är nödvändig för återhämtning efter en katastrof, inklusive typ av tillgång, format, placering, information om säkerhetskopiering, licensinformation och värdet för organisationen.			

3.3 Dokumentera förbättringsåtgärder

Efter de tre dagarnas arbete är det dags att analysera svaren. Analysledaren ska analysera materialet och ange vilka gapanalysnivåer som de olika delfrågorna bör få. Detta kan göras med hjälp av checklistan och bilaga B.

Nivåskalan för bedömningar:

0 = Oacceptabelt (ingen efterlevnad)
0,5
1 = Risk (bristfällig efterlevnad)
1,5
2 = Liten risk (acceptabel efterlevnad)
2,5
3 = Mycket liten risk (stor efterlevnad)

För att bestämma en huvudfrågas nivå måste man göra en sammantagen bedömning av frågesvaren och sina egna observationer på plats samt använda sin erfarenhet. Olika analysledare brukar göra i stort sett samma bedömningar av samma material – sällan skiljer det mer än 0,5 poäng per fråga.

Den som är ansvarig för en aktivitet (se tabell 1) ska få en lista över de aktuella bristerna, och sedan ska den ansvariga tillsammans med intervjupersonerna kontrollera och intyga att de brister som anges på listan är korrekta. Om det finns relevanta invändningar mot bristerna ska analysledaren komplettera eller ändra listan..

När bristlistan har godkänts är det dags att börja rapportskrivningen, gärna med stöd från den rapportmall som finns i bilaga B. Analysledaren ska också göra en åtgärdslista och bifoga den till rapporten. Rapporten bör alltid skickas rekommenderat (e-posta aldrig om inte krypteringsskyddet är pålitligt).

Underlaget från gapanalysen kan även användas för att definiera var verksamheten befinner sig på enligt en mognadstrappa. Vi ger i denna metodik inga ytterligare anvisningar på hur detta görs.

4. Nästa steg

Gapanalysen var sista aktiviteten i processteget ”Grundläggande analys” och nu har organisationen en bra dokumentation över alla informationstillgångar, risker och sårbarheter. Med denna kunskap går det att utforma ett lämpligt sätt att styra och leda ledningssystemet för informationssäkerhet.

Bilaga A: Detaljerat schema för gapanalysen

DAG 1

	**Aktivitet**
07:45	Egen kontroll av kringmiljön och lokaler Analysledaren bör vara på plats vid analysobjektet i god tid innan kl. 09:30 då gapanalysen enligt schemat ska börjas, för att i lugn och ro kunna vandra runt i lokalerna och undersöka kringmiljön. Finns det vägar och järnvägar i anläggningens omedelbara närhet? Vilka "grannar" har organisationen, och kan de tänkas förvara farligt gods inom sitt område? Hur ser tillträdesskyddet ut? Finns det uppenbara "hål" eller liknande? Allt detta återkommer sedan under analysen och med denna yttre granskning kan analysledaren ställa sina egna observationer mot de svar som ges under intervjuerna.
09:30–10:20	Presentation av verksamheten och IT-miljön Uppdragsgivaren eller en utsedd person presenterar verksamheten och IT-miljön. Analysledaren kan då få klarhet i hur man inom organisationen ser på sin verksamhet och hur man upplever att IT-miljön ser ut samt borde fungera.
10:30–11:30	Rundvandring i ”datorlokalerna” Denna timme bör utnyttjas så effektivt som möjligt. Utgå ifrån systembeskrivningen och be den ansvarige från organisationen peka ut alla de komponenter som finns angivna där. Lägg noga på minnet vilka komponenter som inte har pekats ut och utred vad de är. Rita in dessa på systembeskrivningen med relevanta kopplingar. När analysledaren känner sig klar över vad som finns i datorhallen är det dags att undersöka det fysiska skyddet. Kontrollera tillträdesskyddet: • Finns något inbrottslarm? • Finns galler för fönstren? • Är dörrar och väggar svårforcerade? Kontrollera brandsektioneringen runt datorhallen: • Är dörrar och väggar brandklassade (på dörrar står som regel brandklassen på dörrens inre kortsida)? • Är ytskiktet på dörrar och väggar i ett brandfarligt material?

	**Aktivitet**
	• Finns det datamedieskåp i eller vid en datorhall? I så fall ska detta lägst vara klassat enligt S60D, eller S60DIS om disketter förvaras i skåpet. • Är kabel- och rörgenomföringar brandtätade? • Finns både skum- och kolsyresläckare i omedelbar anslutning till datorhallen? • Är utrymmet under golvet och i undertaket rent och utan otäta genomföringar (lyft plattorna till ett eventuellt undergolv och undertak och kontrollera utrymmet)? • Är alla genomföringar brandtätade? Finns det slarvigt dragna kablar eller avloppsrör eller vattenrör som inte ingår i den fasta brandsläckningsutrustningen? Kontrollera klimatanläggningen: • Är klimatanläggningen dubblerad? • Är även försörjningen av den dubblerad (kyla, vatten)? • Är värmeavgivaren placerad på en skyddad plats (oftast finns den på väggen utanför och är sällan skyddad)? Kontrollera strömförsörjningen: • Hur ser strömförsörjningen ut? • Är den dubblerad? • Använder man femledarkabel? • Hur ansluts strömmen till maskinerna? • Finns en UPS, och i sådana fall var står den? • Var finns huvudströmbrytaren (bör finnas vid dörren till datorhallen)? Notera även det allmänna intrycket av lokalen: • Verkar där vara god ordning? • Finns det tecken på att personal röker i lokalen? • Hur är brandbelastningen (mängden brännbart material)? Be även att få se korskopplingsrum, switchar, någon del av kabeldragningen i huset samt telefonväxeln.
11:30–12:30	Lunch
12.30–13.30	Fysisk och miljörelaterad säkerhet Här gäller det hur verksamheten förhindrar obehörig från att komma in i lokalerna samt vilka skador och störningar som finns i organisationens lokaler och information. Detta kapitel omfattar områdena säkra utrymmen och skydd av utrustning.

	**Aktivitet**
13:45–14:45	Säkerhetspolicy Genomgången ska visa ledningens viljeinriktning och stöd för informationssäkerheten i enlighet med verksamhetskrav och relevanta lagar och föreskrifter. Kapitlet omfattar informationssäkerhetspolicy.
15:00–16:00	Organisation av informationssäkerheten Här är frågan om informationssäkerheten styrs i organisationen. Kapitlet omfattar både intern organisation och utomstående parter.
13:30–14:00	Hantering av tillgångar Diskussionen ska visa om verksamheten kan uppnå och upprätthålla ett lämpligt skydd av tillgångarna. Kapitlet omfattar ansvaret för tillgångar och klassificeringen av information.
16:00–16.30	Analysledarens enskilda summering av dagen Vid dagens slut ska analysledaren mycket övergripande redovisa för uppdragsgivaren sina intryck under dagen. Både positiva och negativa åsikter ska nämnas.
16:30–16:45	Komplettering av analysunderlag Intervjupersonerna hänvisar ibland till andra personer i organisationen när det gäller specifika frågor. Analysledaren bör försöka få kontakt med dem innan de går hem för dagen.

DAG 2

	**Aktivitet**
08:30–09:00	Presentation av synpunkter från gårdagen
09:00–10:00	Personalresurser och säkerhet Denna del av analysen kontrollerar att anställda, uppdragstagare och tredjepartsanvändare förstår sitt ansvar och är lämpliga för sina roller och för att minska risken för stöld, bedrägeri eller missbruk av resurser. Det handlar om hur verksamheten ska stödja säkerhetspolicyn för att minska risken för mänskliga fel och hur man hanterar ändrade arbetsförhållanden. Kapitlet omfattar före anställningen, under anställningen och när anställningen har upphört eller ändrats.
10:15–11:30	Styrning av kommunikation och drift Detta moment går ut på att se om organisationen har en korrekt och säker drift av sina informationsbehandlingsresurser. Det gäller även hur man inför och bibehåller en lämplig nivå på informationssäkerheten och hur utförandet av tjänster sker i enligt med överenskommelser med tredje part. Uppföljningen ska även visa hur verksamheten har minimerat risken för systemfel. Kapitlet omfattar driftrutiner och ansvar, hantering av tjänsteleverantörer (tredjepart), systemplanering och systemgodkännande, skydd mot skadlig och mobil kod, säkerhetskopiering, hantering av säkerhet i nätverk, hantering av medier, utbyte av information, tjänster för elektronisk handel och övervakning.
11:30–12:30	Lunch
12:30–14:00	Styrning av åtkomst Här gäller det att följa upp hur verksamheten styr vem informationen går till och hur användarna får åtkomst till information, nätverk och operativsystem. Momentet gäller även hur informationssäkerheten är ordnad vid mobil datoranvändning och distansarbete. Kapitlet omfattar verksamhetskrav på styrning av åtkomst, styrning av användarens åtkomst, användarens ansvar, styrning av åtkomst

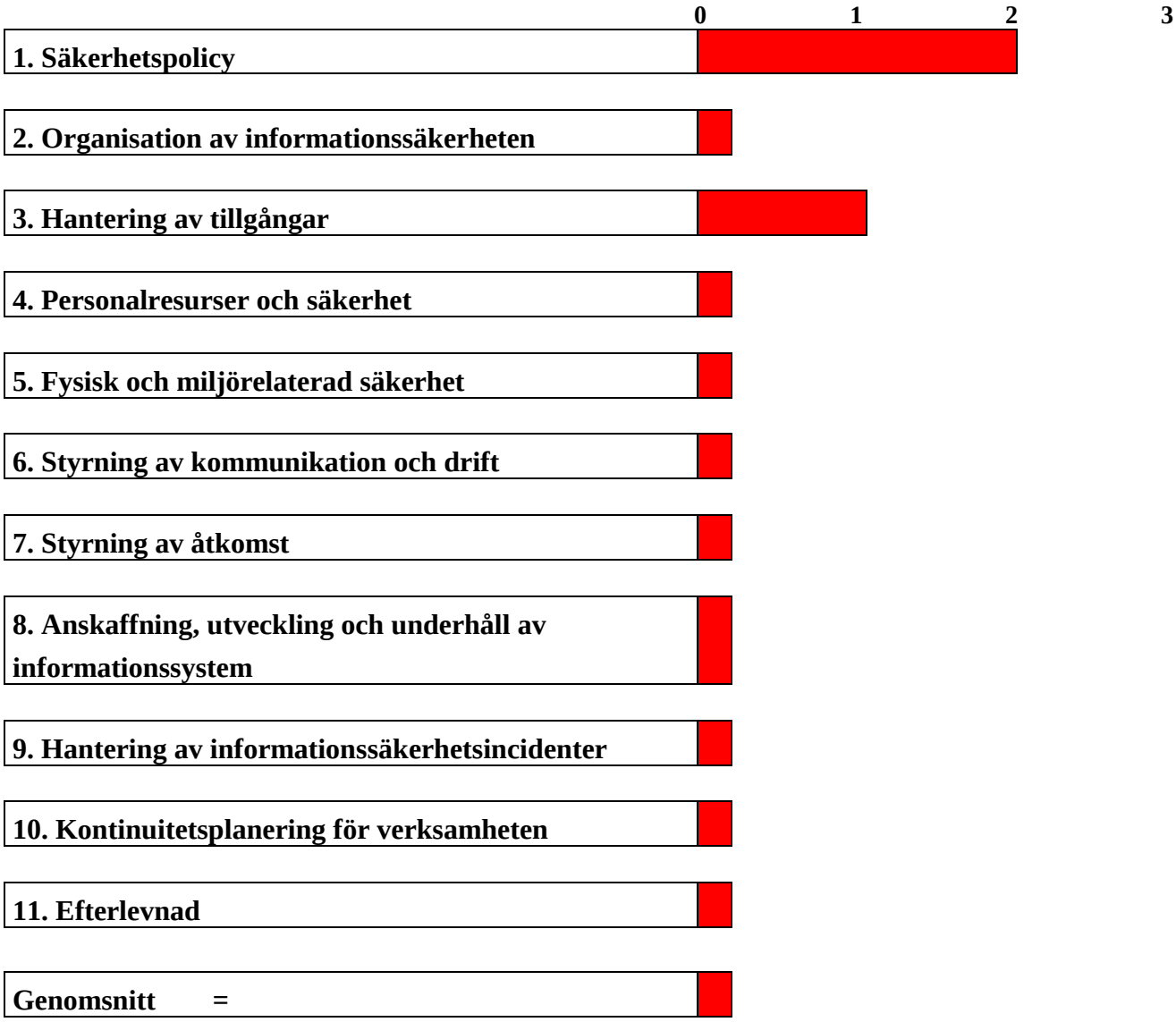
	**Aktivitet**
	till nätverk, styrning av åtkomst till operativsystem, styrning av åtkomst till information och tillämpningar samt mobil datoranvändning och distansarbete.
14:00–15:00	Anskaffning, utveckling och underhåll av informationssystem Frågorna rör organisationens systemutveckling om den har en egen sådan. Finns det klara regler för hur utvecklingen ska gå till och tar de hänsyn till säkerhetsaspekter? Hur testas nya system och vilken dokumentation krävs? Finns det regler för hur nya system driftsätts? Kapitlet omfattar säkerhetskrav på informationssystem, korrekt bearbetning i tillämpningar, kryptering, skydd av systemfiler, säkerhet i utvecklings- och underhållsprocesser och hantering av tekniska sårbarheter.
15:00–16:00	Hantering av informationssäkerhetsincidenter Granskningen gäller om verksamheten har rutiner och metoder för att kunna hantera informationssäkerhetsincidenter – från rapportering till en konsekvent och effektiv hantering.
16:00–16:30	Analysledarens enskilda summering av dagen Vid dagens slut ska analysledaren mycket övergripande redovisa sina intryck under dagen. Både positiva och negativa åsikter ska nämnas.
16:30–16:45	Komplettering av analysunderlag Intervjupersoner hänvisar ibland till andra personer i organisationen när det gäller specifika frågor. Analysledaren bör försöka få kontakt med dem innan de går hem för dagen.

DAG 3

	**Aktivitet**
08:30– 09:00	Presentation av synpunkter från gårdagen
09:00–10:15	Kontinuitetsplanering för verksamheten Ett effektivt skydd bygger på att kontinuerligt kunna hantera avbrott, förluster och störningar i verksamheten. Granskningen gäller på vilket sätt informationssäkerheten ingår i kontinuitetsprocessen och åtgärderna för att kunna hantera en kris. Kapitlet omfattar informationssäkerhetsaspekter på kontinuitetsplanering för verksamheten.
10:30–11:30	Efterlevnad Målet är en ständig förbättring och då är det viktigt att följa upp hur verksamheten lever upp till de krav som ställs. Kapitlet 15 i standarden omfattar efterlevnad av rättsliga krav, efterlevnad av säkerhetspolicyer, -standarder och teknisk efterlevnad samt överväganden vid revision av informationssystem.
11:30–12:30	Lunch
12:30–13:30	Reservtid
13:30–15:00	Analysledarens enskilda summering Denna tid är avsatt för att förbereda summeringen. Använd gärna ett bildspel i Power Point eller liknande för att tydligare åskådliggöra resultatet och slutsatserna.
15:00–16:00	Presentation av synpunkter
16:00	SLUT

Bilaga B: Mall för sammanställning av säkerhetsnivån

Ange säkerhetsnivån i tabellens högra del. Nivån beräknas från tabellen ”Säkerhetsnivåer” nedan.



Säkerhetsnivåer

0 = Oacceptabel risk, 1 = Risk, 2 = Liten risk, 3 = Mycket liten risk

*/ = 0 poäng på någon av frågorna.

Ange värdet per delavsnitt och avsnitt. Beräkna därefter genomsnittet för hela kapitlet. Ange även viktiga kommentarer till kapitlet. Observera att det bara är de vita fälten som ska fyllas i.

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
5	Säkerhetspolicy				
5.1	Informationssäkerhetspolicy				
5.1.1	Policydokument för informationssäkerhet				
5.1.2	Granskning av informationssäkerhetspolicyn				
6	Organisation av informationssäkerheten				
6.1	Intern organisation				
6.1.1	Ledningens engagemang för informationssäkerhet				
6.1.2	Samordning av informationssäkerhetsarbetet				
6.1.3	Tilldelning av ansvar för informationssäkerhet				
6.1.4	Godkännandeprocess för informationsbehandlingsresurser				
6.1.5	Konfidentialitetsavtal				
6.1.6	Myndighetskontakt				
6.1.7	Kontakt med särskilda intressegrupper				
6.1.8	Oberoende granskning av informationssäkerhet				
6.2	Utomstående parter				
6.2.1	Identifiering av risker med utomstående parter				
6.2.2	Hantering av säkerhet vid kundkontakter				
6.2.3	Hantering av säkerhet i tredjepartsavtal				
7	Hantering av tillgångar				
7.1	Ansvar för tillgångar				
7.1.1	Förteckning över tillgångar				
7.1.2	Ägarskap för tillgångar				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
7.1.3	Godtagbar användning av tillgångar				
7.2	Klassificering av information				
7.2.1	Riktlinjer för klassificering				
7.2.2	Märkning och hantering av information				
8	Personalresurser och säkerhet				
8.1	Före anställning				
8.1.1	Roller och ansvar				
8.1.2	Kontroll av personal				
8.1.3	Anställningsvillkor				
8.2	Under anställning				
8.2.1	Ledningens ansvar				
8.2.2	Informationssäkerhetsmed-vetande, utbildning och övning				
8.2.3	Disciplinär process				
8.3	Upphörande eller ändring av anställning				
8.3.1	Ansvar vid upphörande av anställning				
8.3.2	Återlämnande av tillgångar				
8.3.3	Indragning av åtkomsträttigheter				
9	Fysisk och miljörelaterad säkerhet				
9.1	Säkra utrymmen				
9.1.1	Skalskydd				
9.1.2	Tillträdeskontroll				
9.1.3	Skydd av kontor, rum och faciliteter				
9.1.4	Skydd mot externa hot och miljöhot				
9.1.5	Arbete i säkra utrymmen				
9.1.6	Allmänna tillträdes-, leverans- och lastutrymmen				
9.2	Skydd av utrustning				
9.2.1	Placering och skydd av utrustning				
9.2.2	Tekniska försörjningssystem				
9.2.3	Kablageskydd				
9.2.4	Underhåll av utrustning				
9.2.5	Säkerhet för utrustning utanför egna lokaler				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
9.2.6	Säker avveckling eller återanvändning av utrustning				
9.2.7	Avlägsnande av egendom				
10	Styrning av kommunikation och drift				
10.1	Driftsrutiner och driftansvar				
10.1.1	Dokumenterade driftsrutiner				
10.1.2	Ändringshantering				
10.1.3	Uppdelning av arbetsuppgifter				
10.1.4	Uppdelning av resurser för utvecklingstest och drift				
10.2	Hantering av tredjeparts tjänsteleverantörer				
10.2.1	Tjänsteleverans				
10.2.2	Övervakning och granskning av tjänster från tredje part				
10.2.3	Ändringshantering för tjänster från tredje part				
10.3	Systemplanering och systemgodkännande				
10.3.1	Kapacitetsplanering				
10.3.2	Systemgodkännande				
10.4	Skydd mot skadlig och mobil kod				
10.4.1	Säkerhetsåtgärder mot skadlig kod				
10.4.2	Säkerhetsåtgärder mot mobil kod				
10.5	Säkerhetskopiering				
10.5.1	Säkerhetskopiering av information				
10.6	Hantering av säkerhet i nätverk				
10.6.1	Säkerhetsåtgärder för nätverk				
10.6.2	Säkerhet i nätverkstjänster				
10.7	Hantering av medier				
10.7.1	Hantering av flyttbara datamedier				
10.7.2	Avveckling av medier				
10.7.3	Rutiner för informationshantering				
10.7.4	Säkerhet för systemdokumentation				
10.8	Utbyte av information				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
10.8.1	Policyer och rutiner för informationsutbyte				
10.8.2	Överenskommelser om utbyte				
10.8.3	Fysiska medier under transport				
10.8.4	Elektroniska meddelanden				
10.8.5	Verksamhetsrelaterade informationssystem				
10.9	Tjänster för elektronisk handel				
10.9.1	Elektronisk handel				
10.9.2	Direktanslutna transaktioner				
10.9.3	Offentligt tillgänglig information				
10.10	Övervakning				
10.10.1	Revisionsloggning				
10.10.2	Övervakning av systemanvändning				
10.10.3	Skydd av logginformation				
10.10.4	Administratörs- och operatörsloggar				
10.10.5	Loggning av fel				
10.10.6	Klocksynkronisering				
11	Styrning av åtkomst				
11.1	Verksamhetskrav på styrning av åtkomst				
11.1.1	Åtkomstpolicy				
11.2	Styrning av användares åtkomst				
11.2.1	Användarregistrering				
11.2.2	Hantering av särskilda rättigheter				
11.2.3	Lösenordshantering				
11.2.4	Granskning av användares åtkomsträttigheter				
11.3	Användares ansvar				
11.3.1	Användning av lösenord				
11.3.2	Obevakad användarutrustning				
11.3.3	Policy för renstädat skrivbord och tom bildskärm				
11.4	Styrning av åtkomst till nätverk				
11.4.1	Policy för användning av nätverkstjänster				
11.4.2	Autentisering av användare vid extern anslutning				
11.4.3	Identifiering av utrustning i				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
	nätverk				
11.4.4	Skydd av extern diagnos- och konfigurationsport				
11.4.5	Nätverkssegmentering				
11.4.6	Styrning av nätverksanslutning				
11.4.7	Styrning av routning				
11.5	Styrning av åtkomst till operativsystem				
11.5.1	Säker påloggningsrutin				
11.5.2	Identifiering och autentisering av användare				
11.5.3	Lösenordsrutin				
11.5.4	Användning av systemverktyg				
11.5.5	Tidsfördröjd nedkoppling				
11.5.6	Begränsning av uppkopplingstid				
11.6	Styrning av åtkomst till information och tillämpningar				
11.6.1	Begränsning av åtkomst till information				
11.6.2	Isolering av känsliga system				
11.7	Mobil datoranvändning och distansarbete				
11.7.1	Mobil datoranvändning och kommunikation				
11.7.2	Distansarbete				
12	Anskaffning, utveckling och underhåll av informationssystem				
12.1	Säkerhetskrav på informationssystem				
12.1.1	Analys och specifikation av säkerhetskrav				
12.2	Korrekt bearbetning i tillämpningar				
12.2.1	Validering av indata				
12.2.2	Styrning av intern bearbetning				
12.2.3	Meddelandeintegritet				
12.2.4	Validering av utdata				
12.3	Kryptering				
12.3.1	Krypteringspolicy				
12.3.2	Nyckelhantering				
12.4	Skydd av systemfiler				
12.4.1	Styrning av programvara i drift				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
12.4.2	Skydd av testdata				
12.4.3	Styrning av åtkomst till källprogramkod				
12.5	Säkerhet i utvecklings- och underhållsprocesser				
12.5.1	Rutiner för ändringshantering				
12.5.2	Teknisk granskning av tillämpningar efter ändringar i operativsystem				
12.5.3	Restriktioner mot ändringar i programvarupaket				
12.5.4	Informationsläckor				
12.5.5	Utlagd programvaruutveckling				
12.6	Hantering av tekniska sårbarheter				
12.6.1	Skydd för tekniska sårbarheter				
13	Hantering av informationssäkerhetsincidenter				
13.1	Rapportering av informationssäkerhetshändelser och svagheter				
13.1.1	Rapportering av informationssäkerhetshändelser				
13.1.2	Rapportering av säkerhetsbrister				
13.2	Hantering av informationssäkerhetsincidenter och förbättringar				
13.2.1	Ansvar och rutiner				
13.2.2	Att lära av informationssäkerhetsincidenter				
13.2.3	Insamling av bevis				
14	Kontinuitetsplanering för verksamheten				
14.1	Informationssäkerhetsaspekter på kontinuitetsplanering för verksamheten				
14.1.1	Att inkludera informationssäkerhet i verksamhetens kontinuitetsplaneringsprocess				
14.1.2	Kontinuerlig verksamhet och riskbedömning				
14.1.3	Utveckling och införande av kontinuitetsplaner innefattande				

Kapitel nr. enligt ISO/IEC 27002:2005	Kapitel	Bedömt värde på kapitlet	Bedömt värde på avsnitt	Bedömt värde på delavsnitt värde 0–3	Kommentar
	informationssäkerhet				
14.1.4	Ramverk för kontinuitetsplanering i verksamheten				
14.1.5	Test, underhåll och omprövning av kontinuitetsplaner				
15	Efterlevnad				
15.1	Efterlevnad av rättsliga krav				
15.1.1	Identifiering av tillämplig lagstiftning				
15.1.2	Immaterialrätt				
15.1.3	Skydd av organisationens register och andra redovisande dokument				
15.1.4	Skydd av personuppgifter				
15.1.5	Förhindrande av missbruk av informationsbehandlingsresurser				
15.1.6	Reglering av kryptering				
15.2	Efterlevnad av säkerhetspolicyer, -standarder och teknisk efterlevnad				
15.2.1	Efterlevnad av säkerhetspolicyer och -standarder				
15.2.2	Kontroll av teknisk efterlevnad				
15.3	Överväganden vid revision av informationssystem				
15.3.1	Säkerhetsåtgärder för revision av informationssystem				
15.3.2	Skydd av verktyg för granskning av informationssystem				

Bilaga C: Exempel på rapport från gapanalys

Hemlig information

Gapanalys

Informationssäkerhetsnivån för

XX IT-verksamhet

2010

Dokumentstyrning

Dok.id.:	Version*:* **1**	Ersätter:
Dok.status:	Rev.datum:	
Gäller fr.o.m.:	Gäller t.o.m.:*:*	
Upprättat av:	Datum:	
Godkänt av: :	Datum:	
Filnamn och plats på nätverket:		
Distribution*:*		

BAKGRUND

Inledning

Syftet med gapanalysen var att tillsammans med XX bedöma hur informationssäkerheten fungerar i XXs verksamhet samt ange de brister som finns.

Genomgången av analysområdena har utförts genom rundvandring i lokalerna, besiktning av lokaliteter samt intervjuer. Observera att detta är en översiktlig analys och inte en analys av informationssäkerheten i detalj. Därför har vi bara granskat några av de efterfrågade dokumenten och kvaliteten i dem.

Sammantaget bedöms XXs informationssäkerhet ha stora brister och nivån blev 1,4 på en fyrgradig skala (0–3, där 3 är det bästa värdet). XX behöver förbättra arbetet inom alla de områden som gapanalysen omfattade.

I den bifogade åtgärdsrapporten finns samtliga brister fördelade på de olika plattformarna. De brister som är prioriterade med siffran 1 behöver åtgärdas omgående eftersom de har stor betydelse för den totala säkerheten. XX får själva bedöma hur viktiga de andra bristerna är.

Vi kan även se att säkerhetsnivån inte har förbättrats över tiden. Vi har analyserat verksmaheten vid tre tillfällen med följande resultat:

- År XX: Genomsnittsvärde 1,1 poäng.
- År XX: Genomsnittsvärde 1,3 poäng.

Analysledare

< Här anges vilka som gjorde analysen>

Tidsåtgång

Vi har totalt ägnat cirka XX dagar åt denna analys.

Genomförande

Arbetet har genomförts genom intervjuer, rundvandring och analys.

Intervjuade personer

Följande personer har intervjuats:

- XX

Analysmetod

Vi har valt samma metod som vid de tidigare analyserna för att få en möjlighet att jämföra resultatet. Den täcker områdena

1. säkerhetspolicy
2. organisation av informationssäkerheten
3. hantering av tillgångar
4. personalresurser och säkerhet
5. fysisk och miljörelaterad säkerhet
6. styrning av kommunikation och drift
7. styrning av åtkomst
8. anskaffning, utveckling och underhåll av informationssystem
9. hantering av informationssäkerhetsincidenter
10. kontinuitetsplanering för verksamheten
11. efterlevnad.

Resultat av gapanalysen

Bedömningen är graderad i fyra nivåer:

0 = Oacceptabel risk

1 = Risk

2 = Liten risk

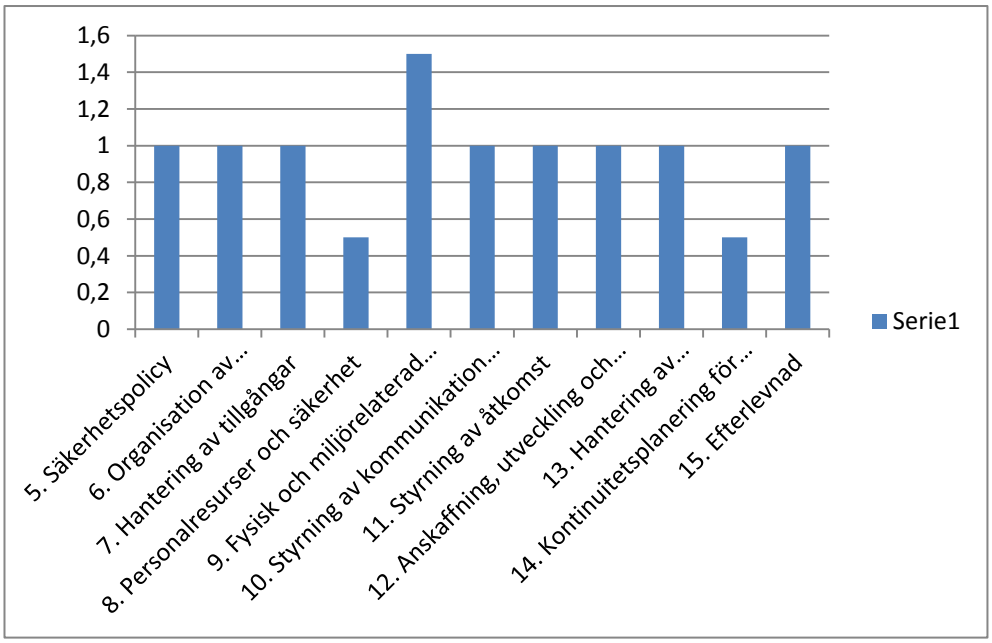
3 = Mycket liten risk

Maxvärde: 3

Normvärde: 2

Genomsnitt: 1

X procent av de X frågorna visar att det finns brister i verksamheten.



För varje analysområde redovisar vi vilka delar som ingår under varje avsnitt, de sammanfattade bristerna och resultatet för varje del. Resultatet redovisas som tre staplar: en röd som visar ert faktiska värde, en grön som visar det värde ni bör ha för varje avsnitt och ett blått som beskriver ert genomsnittsvärde för alla områden.

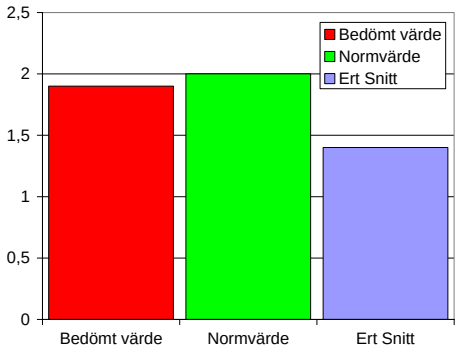
<Vi visar ett exempel från ett av kapitlen i standarden. Ni får själva skapa motsvarade för varje del>

5. Brister: Säkerhetspolicy

Bedömt värde: X,X procent av frågorna inom området visar att det finns en brist i vår verksamhet.

Analyserade områden:

- Informationssäkerhetspolicy
    - <Beskriv kortfattat cirka fem brister inom varje analysområde>



Åtgärdsplan

Utifrån dessa resultat har vi tagit fram en åtgärdsplan som täcker huvuddelen av de redovisade bristerna. Vi föreslår även en prioritering av de saker som vi anser att ni måste åtgärda på en gång

Bilagor

Denna rapport har följande bilagor:

- Analysresultat med en grafisk bild
    - Windows-miljön
    - UNIX-miljön
    - stordator-miljön
- Förslag till åtgärdsplan
    - Windows-miljön
    - UNIX-miljön
    - stordator-miljön
- Foton från datorutrymmena

Bilaga D: Handlingsplan

Upprätta en handlingsplan för att kunna hantera de brister som upptäckts vid gapanalysen. Använd gärna denna mall.

Löp-nr.	Prioritet 1–3	Åtgärd och eventuella förslag	Kostnad	Ansvarig	Mottaget	Färdig tidpunkt
1.					☐	
2.					☐	
3.					☐	
4.					☐	
5.					☐	
6.					☐	
7.					☐	
8.					☐	
9.					☐	
10.					☐	
11.					☐	
12.					☐	
13.					☐	
14.					☐	
15.					☐	
16.					☐	