GAP-analys av 27001

Efterlevnad av standarden

Innehållsförteckning

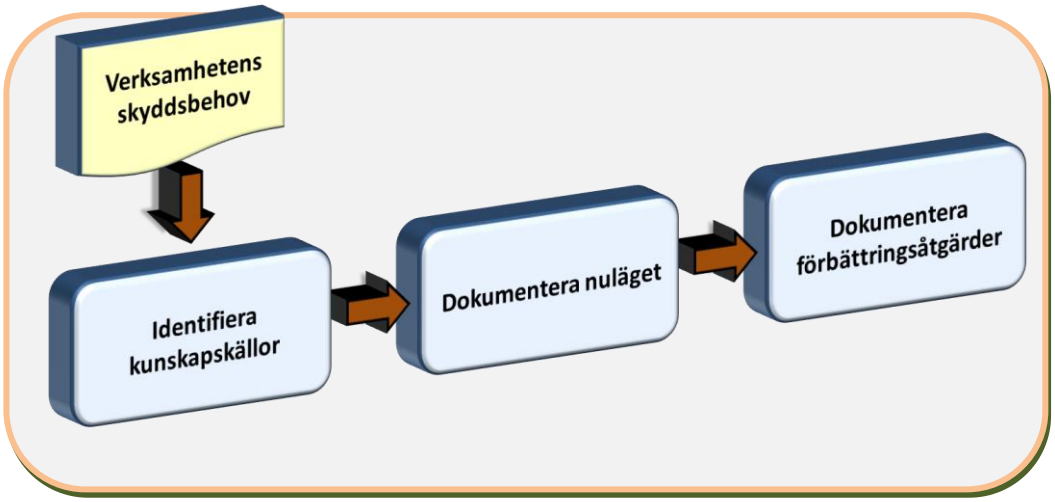
1. Introduktion

1.1 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 bra sätt som möjligt. Huvudsyftet är att stödja, så att organisationens mål uppfylls. Verksamhetens information måste skyddas så att den alltid är *konfidentiell*, *tillgänglig* och *riktighet*, och därför inför man ett ledningssystem och *administrativa*, *organisatoriska*, *fysiska* och *logiska* skydd.

Det finns därför ett stort behov att tidigt utvärdera på vilken nivå en verksamhets informationssäkerhetsarbete befinner sig i. Genom att värdera sitt skydd kan verksamheten få ett bra kvitto på hur sårbar den är för olika risker som kan uppträda, och det skapar också en trygghet i organisationen att veta hur man mår. Vi har därför tagit fram denna metod för gap-analys, som gör det möjligt att snabbt skapa sig en bild av nuläget för informationssäkerheten. Gap-analysen utförs efter att behov, krav och risker har kartlagts genom verksamhetsanalys och riskanalys. Uttrycket syftar på gapet mellan det som standarden beskriver som bästa praxis och den rådande säkerhetsnivån i verksamheten. Arbetsuppgifterna för gap-analysen illustreras i figuren nedan.

Figur 1. Arbetsuppgifterna under gap-analysen



1.2 Mål och syfte

Målet med denna metod är att vara ett underlag för kontroll av verksamhetens införande av ett ledningssystem (LIS). Metoden ger vägledning för hur denna kontroll går till och skapar ett underlag för att planerat arbeta vidare med de brister som finns.

Syftet med att utföra gap-analysen är att få:

- bevis på hur effektivt ni infört ledningssystem och nivån på ert skydd
- en uppfattning om kvaliteten på informationssäkerhetsarbetet och er säkerhetsprocess
- ett underlag för resten av arbetet med att införa ledningssystemet

1.3 Målgrupp

Den här metoden för gap-analys 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.

1.4 När ska metoden användas?

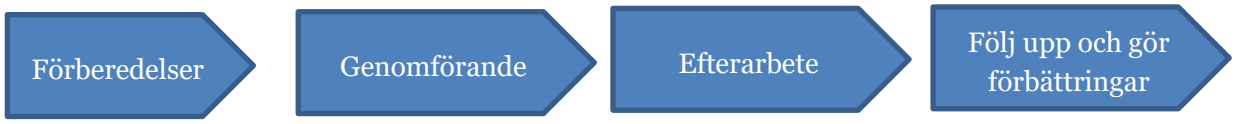
Metoden ska användas för att få fram gapet mellan den existerande och den önskade säkerhetsnivån, innan organisationen inför ett LIS. Metoden är generisk och fungerar på de flesta verksamheter, även om den troligtvis behöver anpassas något. En viktig del i säkerhetsarbetet är att årligen följa upp säkerhetsnivåns status och verktyget passar bra även för det ändamålet.

2. Metod

2.1 Arbetsflöde vid gap-analys

I detta avsnitt beskrivs stegen för att utföra gap-analysen översiktligt. Det finns ett antal steg som analysledaren bör gå igenom före, under och efter analysen, och en del saker att tänka på. I figuren nedan anges schematiskt stegen för genomförande.

Figur 2. Övergripande process för att göra en gap-analys:



Det första steget i arbetet med gap-analysen utgörs alltså av förberedelser. Det innefattar bland annat att identifiera kunskapskällor, det vill säga kartlägga vilka områdesansvariga man behöver information från, att skicka ut analysunderlag till dem, och att bestämma en agenda för analysarbetet.

I genomförandesteget utförs sedan själva analysen. Förslagsvis utför man en rundvandring och analys av den fysiska miljön, för att sedan gå över i intervjuer med berörda parter. Intervjuerna utgår från underlaget som presenteras i nästa kapitel. Observationer och intervjusvar används sedan för en dokumentation av nuläget genom att sammanställa säkerhetsnivåer för de olika områdena i underlaget, och sammanfatta de brister som framkommit.

När analysarbetet är genomfört bör resultaten sammanställas i en nivå- och bristrapport som skickas till alla medverkande för avstämning, varpå en åtgärdsplan utformas och slutrapport skrivs. Slutrapporten kan sedan användas som underlag för förbättringar i organisationens informationssäkerhetsarbete.

2.2 Intervjuteknik

Eftersom detta är en subjektiv och kvalitativ metod är det viktigt att man får en god kontakt med intervjupersonerna. Det är lämpligt att skapa ett bra rum att vara i och låta de som ska intervjuas komma till analysledaren. Ett annat tips är att ge alla som intervjuas en egen kopia av underlaget att titta i. Analysledaren ställer frågor och de intervjuade svarar ja eller nej med kommentarer. Om analysledaren inte kan området i detalj kan man ställa frågan och låta de intervjuade tolka och analysera den. Be alla som intervjuas vara ärliga då detta är hjälp till självhjälp.

2.3 Bedömning av säkerhetsnivåer

Analysledaren ska efter intervjuer och observationer analysera materialet och ange vilka värden som de olika delområdena i underlaget bör få. Värdebedömningar görs enligt skalan nedan.

Nivåskala 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.

2.4 Att tänka på

När åtgärderna ska granskas är det viktigt att tänka i flera dimensioner för att få reda på om åtgärden är effektiv och ändamålsenlig:

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

2.5 Efter gap-analysen

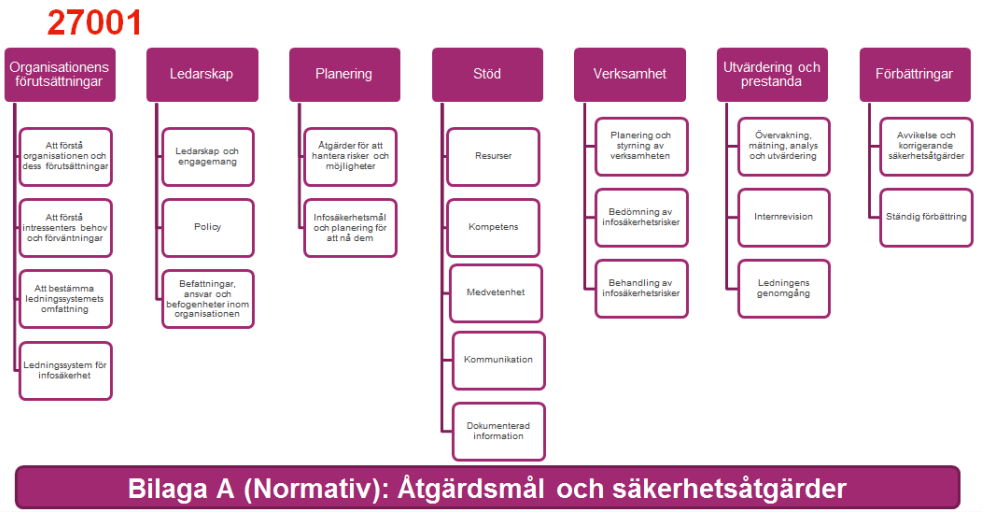
När analysen har genomförts har organisationen en bra dokumentation över alla informationstillgångar, risker och sårbarheter. Med denna kunskap går det att utforma ett lämpligt sätt att styra och leda ledningssystemet för informationssäkerhet.

Hänvisa till MSB metodstöd.

3. Vad ska analyseras?

De områden som ska analyseras är de områden ni ser i bilden enligt nedan:

- Organisationens förutsättningar
- Ledarskap
- Planering
- Stöd
- Verksamhet
- Utvärdering och prestanda
- Förbättringar



3 Organisationens förutsättningar

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
4	**Organisationens förutsättningar**	
4.1	Att förstå organisationen och dess förutsättningar	
4.2	Att förstå intressenters behov och förväntningar	
4.3	Bestämma ledningssystemets omfattning	
4.4	Ledningssystem för informationssäkerhet	

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

3.1 Att förstå organisationen och dess förutsättningar

Organisationen ska avgöra vilka externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda resultaten med sitt ledningssystem för informationssäkerhet. *ANM. Fastställandet av dessa frågor avser upprättande av organisationens externa och interna kontext vilka beaktas i avsnitt 5.3 i SS-ISO 31000:2009* Delar som ingår: 1. Idéer om hur ledningssystemet ska struktureras 2. Innehållet ska vara dokumenterat 3. Innehållet ska kommuniceras 4. Ledningssystemet ska kunna uppdateras/revideras 5. Organisationen ska känna till sina risker och dessa ska kunna kommuniceras.	**Nivå**

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

Kommentarer:

3.2 Att förstå intressenters behov och förväntningar

	Nivå

Organisationen ska bestämma vilka intressenter som är relevanta för ledningssystemet för informationssäkerhet och dessa intressenters krav (rättsliga, regelmässiga, avtal) som är relevanta för informationssäkerhet. Delar som ingår: 1. Intressenternas krav ska fastställas 2. Tillfredställelsen av informationssäkerhetsnivån ska förbättras	

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

Kommentarer:

3.3 Att bestämma ledningssystemets omfattning

Organisationen ska bestämma avgränsningar och tillämpligheten av ledningssystemet för informationssäkerhet för att fastställa systemets omfattning. Delar som ingår: 1. Både interna och externa frågor ska beaktas i skapandet av ledningssystemet 2. Organisationens behov ska speglas i ledningssystemet 3. Omfattningen av ledningssystemet ska vara dokumenterad 4. Högsta ledningen ska godkänna omfattningen 5. Organisationen ska ha uppnått ställda mål 6. Ledningssystemet ska fungera vid förändringar	**Nivå**

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

Kommentarer:

3.4 Ledningssystem för informationssäkerhet

	Nivå

Organisationen ska upprätta, införa, underhålla och ständigt förbättra ett ledningssystem för informationssäkerhet, inklusive nödvändiga processer och deras samverkan, enligt kraven i 27001. Delar som ska ingå: 1. Ledningssystemet ska vara upprättat, underhållas och fungera under ständig förbättring. 2. Följande processer ska finnas: a. Riskhantering b. Incidenthantering c. Kontinuitetshantering d. Ledningsgenomgång e. Ändringshantering	

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

Kommentarer:

4 Ledarskap

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
5	**Ledarskap**	
5.1	Ledarskap och engagemang	
5.2	Policy	
5.3	Befattningar, ansvar och befogenheter inom organisationen	

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

4.1 Ledarskap och engagemang

Högsta ledningen ska tydligt visa ledarskap och åtagande i fråga om ledningssystemet för informationssäkerhet.	**Nivå**
Delar som ska ingå: 1. Högsta ledningen ska aktivt visa sitt engagemang och ledarskap i frågan 2. Det ska finnas tillräckligt med resurser 3. Betydelsen för informationssäkerhet ska kommuniceras 4. Det ska finnas ”bevis” på ledningens engagemang 5. Kund- och författningskrav ska vara analyserade 6. Ledningen ska genomföra en genomgång av ledningssystemet.	

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

Kommentarer:

4.2 Policy

Högsta ledningen ska upprätta en informationssäkerhetspolicy som efterlever formkraven på en policy enligt LIS.	**Nivå**
Delar som ska ingå: 1. Det ska finnas en informationssäkerhetspolicy som uppfyller standardens krav. 2. Policyn ska vara kommunicerad 3. Policyn ska i tillämplig utsträckning vara tillgänglig för intressenter 4. Policyn ska vara aktuell	

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

Kommentarer:

4.3 Befattningar, ansvar och befogenheter inom organisationen

Högsta ledningen ska säkerställa att relevanta befattningar har tilldelats ansvar och befogenheter och att dessa är kommunicerade inom organisationen. Delar som ska ingå: 1. Ledningens representant för ledningssystemet ska vara medlem i ledningen 2. Denna representant ska säkerställa ledningssystemet 3. Ansvar och befogenheter ska vara tilldelade 4. Relevanta befattningar ska vara utsedda	**Nivå**

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

Kommentarer:

5 Planering

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
6	**Planering**	
6.1	Åtgärder för att hantera risker och möjligheter	
6.2	Informationssäkerhetsmål och planering för att uppnå dem	

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

5.1 Åtgärder för att hantera risker och möjligheter

Organisationen ska ha vidtagit åtgärder för att hantera risker och möjligheter.	**Nivå**

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

Kommentarer:

5.1.1 Allmänt

När organisationen planerar ledningssystemet för informationssäkerhet ska den beakta frågor om organisationen och dess förutsättningar, intressenternas behov och förväntningar samt avgöra vilka risker och möjligheter som behöver hanteras. Delar som ska ingå: 1. Det ska finnas en planeringsprocess för informationssäkerhetsarbetet 2. Det ska finnas en säkring så att ledningssystemet får avsedd effekt 3. Åtgärder för att hantera risk ska vara införda 4. Det ska finnas en process för ständig förbättring	**Nivå**

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

Kommentarer:

5.1.2 Bedömning av informationssäkerhetsrisker

Organisationen ska fastställa och tillämpa en process för bedömning av informationssäkerhetsrisker. Delar som ska ingå: 1. Det ska finnas kriterier för riskacceptans och bedömning av risker 2. Det ska finnas en process för att bedöma och hantera risker 3. Risker ska dokumenteras	**Nivå**

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

Kommentarer:

5.1.3 Behandling av informationssäkerhetsrisker

Organisationen ska fastställa och tillämpa en process för behandling av informationssäkerhetsrisker. Delar som ska ingå: 1. Det ska finnas process för hantering av risker 2. Risker ska dokumenteras	**Nivå**

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

Kommentarer:

5.2 Informationssäkerhetsmål och planering för att uppnå dem

Organisationen ska upprätta informationssäkerhetsmål för relevanta funktioner och nivåer. Delar som ska ingå: 1. Högsta ledningen ska styra målhanteringen 2. Målen ska beskrivas som SMARTA mål 3. Målen ska vara kommuniceras 4. Målen ska vara dokumenteras	**Nivå**

Nivå: 0=Oacceptabel risk (Ingen efterlevnad), 1=Risk (Bristfällig efterlevnad), 2=Liten risk (Acceptabel efterlevnad), 3=Mycket liten risk (stor efterlevnad)

Kommentarer:

6 Stöd

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
7	**Stöd**	
7.1	Resurser	
7.2	Kompetens	
7.3	Medvetenhet	
7.4	Kommunikation	
7.5	Dokumenterad information	

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

6.1 Resurser

Organisationen ska fastställa vilka resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra sitt ledningssystem för informationssäkerhet. Delar som ska ingå: 1. Resursbehovet ska vara fastställt	**Nivå**

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

Kommentarer:

6.2 Kompetens

Säkerställa att organisationen har erforderlig kompetens. Delar som ska ingå: 1. Kompetenskartläggning ska vara genomförd 2. Plan för kompetensförstärkning ska finnas 3. Kompetensbehovet ska vara dokumenterat	**Nivå**

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

Kommentarer:

6.3 Medvetenhet

Personer som arbetar inom eller åt organisationen ska vara medvetna om informationssäkerhetspolicyn och dess roll i informationssäkerhetsarbetet.	**Nivå**

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

Kommentarer:

6.4 Kommunikation

Organisationen ska avgöra behovet av intern och extern kommunikation som är relevant i fråga om ledningssystemet för informationssäkerhet. Delar som ska ingå: 1. Vilka delar av ledningssystemet som ska kommuniceras och hur. 2. En kommunikationsplan. Vem som kommunicerar till vem, och hur.	**Nivå**

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

Kommentarer:

6.5 Dokumenterad information

6.5.1 Allmänt

Ledningssystemet ska innehålla dokumenterad information som krävs enligt standarden. Delar som ska ingå: 1. Dokumenterad information enligt denna standard ska finnas på plats. Se bilaga 1. 2. Det ska finnas relevant informationsklassificering. 3. Dokumentationen ska vara reviderad enligt fastställda perioder. 4. Dokumentationen ska vara riktad mot respektive målgrupp.	**Nivå**

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

Kommentarer:

6.5.2 Skapande och uppdatering

När dokumenterad information skapas och uppdateras ska organisationen säkerställa lämplig utformning enligt denna standard. Delar som ska ingå: 1. Den dokumenterade informationen ska vara styrd. 2. Den ska vara i lämplig form. 3. Det ska finnas en granskande och godkännande process kring informationen.	**Nivå**

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

Kommentarer:

6.5.3 Styrning av dokumenterad information

Dokumenterad information som krävs av ledningssystemet för informationssäkerhet och av denna standard ska styras. Delar som ska ingå: 1. Dokumenterad information ska vara styrd, tillgänglig och lämplig för användning där och när den behövs. 2. Den dokumenterade informationen ska vara skyddad.	**Nivå**

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

Kommentarer:

7 Verksamhet

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
8	**Verksamhet**	
8.1	Planering och styrning av verksamheten	
8.2	Bedömning av informationssäkerhetsrisker	
8.3	Behandling av informationssäkerhetsrisker	

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

7.1 Planering och styrning av verksamheten

Organisationen ska planera, införa och styra de processer som krävs för att uppfylla informationssäkerhetskraven, och införa åtgärderna som fastställs. Delar som ska ingå: 1. Processer för att planera, införa och styra ska finnas. 2. Information som upprättas i processer ska i nödvändig mån bevaras. 3. Outsourcade processer ska vara fastställda och styrda.	**Nivå**

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

Kommentarer:

7.2 Bedömning av informationssäkerhetsrisker

Organisationen ska genomföra bedömningar av informationssäkerhetsrisker med planerade intervall eller när betydande förändringar föreslås eller uppstår, med hänsyn till de kriterier organisationen fastställt. Delar som ska ingå: 1. Riskerna i verksamheten ska vara under kontroll. 2. Riskerna ska dokumenteras.	**Nivå**

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

Kommentarer:

7.3 Behandling av informationssäkerhetsrisker

Organisationen ska införa planer för behandling av informationssäkerhetsrisker. Delar som ska ingå: 1. Det ska finnas planer för att behandla risker. 2. Dessa planer ska vara dokumenterade.	**Nivå**

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

Kommentarer:

8 Utvärdering av prestanda

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
9	**Utvärdering av prestanda**	
9.1	Övervakning, mätning, analys och utvärdering	
9.2	Internrevision	
9.3	Ledningens genomgång	

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

8.1 Övervakning, mätning, analys och utvärdering

Organisationen ska utvärdera informationssäkerheten och verkan av ledningssystemet för informationssäkerhet. Delar som ska ingå: 1. Den ska finnas en plan (när, av vem, hur) för vad som ska övervakas, mätas. 2. Det ska finnas beskrivet vilken/vilka metoder som ska användas. 3. Det ska även finnas en beskrivning av hur och av vem resultatet ska analyseras. 4. Detta ska vara dokumenterat.	**Nivå**

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

Kommentarer:

8.2 Internrevision

	Nivå

Organisationen ska genomföra interna revisioner med planerade intervall för att få information om huruvida ledningssystemet för informationssäkerhet fungerar. Detta ska ingå: 1. Interna revisioner ska vara genomförda för att fastställa ledningssystemet och kraven i standarden. 2. Det ska vara tydligt för vilket ändamål revisionen utförs. 3. Revisioner ska utföras på ett sådant sätt att resultatet inte kan ifrågasättas gällande oberoende och objektivitet. 4. Resultatet från revisionen ska nå relevanta intressenter. 5. Revisioner ska vara dokumenterade.	

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

Kommentarer:

8.3Ledningens genomgång

	Nivå

Högsta ledningen ska ha en genomgång av organisationens ledningssystem för informationssäkerhet med planerade intervall för att säkerställa systemets fortsatta lämplighet, tillräcklighet och verkan. Delar som ska ingå: 1. Högsta ledningen ska ha genomfört en genomgång av systemet. 2. Resultat från tidigare genomgångar ska presenteras. 3. Vid ledningens genomgång ska intern och extern påverkan beaktas. 4. Ledningens genomgång ska beakta de krav som standarden ställer. 5. Resultat från riskbedömningar och behandlingsplaner ska beaktas vid genomgången. 6. Möjligheten till ständigt förbättring bör beaktas. 7. Ledningens genomgång ska vara dokumenterad.	

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

Kommentarer:

9 Förbättringar

Bedömning av risk/efterlevnadsnivån

#	Område	Nivå
10	**Förbättringar**	
10.1	Avvikelse och korrigerande åtgärder	
10.2	Ständig förbättring	

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

9.1 Avvikelse och korrigerande åtgärd

Organisationen ska ha en process för avvikelse och korrigerande åtgärder. Delar som ska ingå: 1. Verksamheten ska agera på avvikelser och vidta åtgärder för att styra och korrigera dem samt hantera deras konsekvenser. 2. Det ska finnas en process för att hantera orsaken till avvikelsen. 3. Avvikelsehanteringen ska vara dokumenterad.	**Nivå**

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

Kommentarer:

9.2 Ständig förbättring

Organisationen ska ständigt förbättra lämpligheten, tillräckligheten och verkan av ledningssystemet för informationssäkerhet. Delar som ska ingå: 1. Det ska finnas processer som ger ständig förbättring. 2. Verksamheten ska kunna visa hur ständiga förbättringar genomförs.	**Nivå**

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

Kommentarer:

10 Bilaga 1: Krav på styrande dokument i ledningssystemet

Följande dokumentation bör finnas enligt denna standard för att man ska ha ett ledningssystem.

Pkt i 27001	Krav
4.3	Beskrivning av ledningssystemets omfattning
5.2	Informationssäkerhetspolicy
6.1.2	Beskrivning av processen för bedömning av informationssäkerhetsrisker
6.1.3	Beskrivning av processen för behandling av informationssäkerhetsrisker
6.1.3 d)	Uttalande om tillämplighet (SoA) innehållande nödvändiga säkerhetsåtgärder samt motiv för inkludering ev. uteslutning av säkerhetsåtgärder
6.2	Beskrivning av informationssäkerhetsmålen
7.2	Belägg för hur kompetens upprätthålls
8.2	Resultatet från bedömning av informationssäkerhetsrisker
8.3	Resultatet från behandling av informationssäkerhetsrisker
9.1	Resultatet från övervakning och mätning
9.2	Beskrivning av genomförande av revisionsprogram och revisionsresultat
9.3	Resultatet från ledningens genomgång
10.1	Dokumenterad information som visar arten av avvikelser och åtgärder som vidtagits.
10.1	Resultatet av korrigerande åtgärder