Övergångsvägledning 27001:2013/2017->27001:2022

1 Checklista för GAP-analys

Nr	Kontrollfråga	Verksamhetens beskrivning	Status	Ansvarig
1	Har verksamheten jämfört identifierade nödvändiga säkerhetsåtgärder med 27001:2022 Bilaga A?			
2	Har verksamheten tagit fram ett uttalande om tillämplighet utifrån 27001:2022 Bilaga A?			
3	Hur har verksamheten beaktat följande säkerhetsåtgärdsområden:			
3.1	*5.7 Hotunderrättelser*			
3.2	*5.23 Informationssäkerhet för användning av molntjänster*			
3.3	*5.30 Kontinuitetsberedskap inom IKT*			
3.4	*7.4 Fysisk säkerhetsövervakning*			
3.5	*8.9 Konfigurationshantering*			
3.6	*8.10 Radering av information*			
3.7	*8.11 Datamaskning*			
3.8	*8.12 Förhindrande av dataläckage*			
3.9	*8.16 Övervakning*			
3.10	*8.23 Webbfiltrering*			
3.11	*8.28 Säker kodning*			
4	Vad har verksamheten för process/rutin vad gäller förändringar av ledningssystemet?			
5	Hur säkerställer verksamheten att de krav som identifierats uppfylls?			
6	Hur säkerställer verksamheten nödvändiga säkerhetsåtgärder implementeras?			
7	Har verksamheten genomfört riskanalysaktiviteter rörande övergång till 27001:2022?			
8	Har verksamheten uppdaterat och infört planen för behandling av informationssäkerhetsrisker?			
9	Finns tydlig dokumentation över nya samt förändrade säkerhetsåtgärder?			
10	Har verksamheten säkerställt implementering av nya och/eller förändrade säkerhetsåtgärder?			
11	Har verksamheten anpassat internrevisionsprogrammet?			

2 Referenser och vägledning

2.1 Kontrollfråga 1

Har verksamheten jämfört identifierade nödvändiga säkerhetsåtgärder med 27001:2022 Bilaga A?

2.1.1 Referens

6.1.3 Behandling av informationssäkerhetsrisker
Organisationen ska fastställa och tillämpa en behandlingsprocess för informationssäkerhetsrisker för att
c) jämföra säkerhetsåtgärderna i 6.1.3 b) ovan med säkerhetsåtgärderna i bilaga A och verifiera att inga nödvändiga säkerhetsåtgärder har utelämnats,

2.1.2 Förslag

Om verksamheten vid genomläsning av 27001:2022 Bilaga A tar stöd av 27002:2022 och identifierar säkerhetsåtgärder vilka förefaller nödvändiga eller rimliga, då bör det undersökas om identifierade risker relaterade till dessa säkerhetsåtgärder finns eller ej i riskkatalogen. Om risker saknas och åtgärdsområdet ej kan anses vara nödvändigt utifrån intressentkrav, då bör riskkatalogen kompletteras.

2.2 Kontrollfråga 2 och 3

Har verksamheten tagit fram ett uttalande om tillämplighet utifrån 27001:2022 Bilaga A?

2.2.1 Referens

6.1.3 Behandling av informationssäkerhetsrisker
Organisationen ska fastställa och tillämpa en behandlingsprocess för informationssäkerhetsrisker för att
d) ta fram ett uttalande om tillämplighet som innehåller
– nödvändiga säkerhetsåtgärder (se 6.1.3 b) och c)),
– motivering för att de ska inkluderas,
– information om huruvida nödvändiga säkerhetsåtgärder har införts eller ej,
– motivering för att exkludera någon av säkerhetsåtgärderna i bilaga A.

2.2.2 Förslag

Motivering för inkludering samt beskrivning av tillämpning bör kunna hämtas ur befintligt uttalande om tillämplighet för huvuddelen av säkerhetsåtgärdsområden i det uttalande om tillämplighet vilket tas fram utifrån 27001:2022. Stöd kan hämtas i 27002:2022 Bilaga B vilken omfattar korsreferensförteckningar, dock kommer flertalet av beskrivningarna behöva omformuleras och 27002:2022 bör konsulteras för att förstå vad som avses med säkerhetsåtgärdsområdet i den nya utgåvan av standarden.

Följande poster i 27001:2022 Bilaga A saknar tydlig motsvarighet i 27001:2013/2017 och för dessa behöver beskrivning av tillämpning eventuellt härledas ur andra rutiner eller arbetssätt:

5.7 Hotunderrättelser
5.23 Informationssäkerhet för användning av molntjänster
5.30 Kontinuitetsberedskap inom IKT

7.4 Fysisk säkerhetsövervakning
8.9 Konfigurationshantering
8.10 Radering av information
8.11 Datamaskning
8.12 Förhindrande av dataläckage
8.16 Övervakning
8.23 Webbfiltrering
8.28 Säker kodning

2.3 Kontrollfråga 4

Vad har verksamheten för process/rutin vad gäller förändringar av ledningssystemet?

2.3.1 Referens

6.3 Planering av förändring
När organisationen fastställer att ledningssystemet för informationssäkerhet behöver förändras, ska ändringarna genomföras på ett planerat sätt.

2.3.2 Förslag

Förändringar av ledningssystemet bör beakta verksamhetens ändringshanteringsprocess i allmänhet och särskilt bör kriterier för under vilka förutsättningar processen ur för att identifiera, bedöma och behandla risker beaktas; i.e. “Är förändringen så omfattande att en riskanalysaktivitet bör genomföras?”

2.4 Kontrollfråga 5 och 6

Hur säkerställer verksamheten att de krav som identifierats uppfylls?
Hur säkerställer verksamheten nödvändiga säkerhetsåtgärder implementeras?

2.4.1 Referens

8.1 Planering och styrning av verksamheten
Organisationen ska planera, implementera och styra de processer som behövs för att uppfylla kraven, och implementera de åtgärder som anges i avsnitt 6 genom att
– fastställa kriterier för processerna,
– införa styrning av processerna enligt kriterierna.

2.4.2 Förslag

Verksamheten bör säkerställa att det finns en etablerad process för att följa upp identifierade intressentkrav utifrån såväl avtal som författning samt en etablerad rutin för att identifiera tillkommande intressentkrav. Denna process bör övervakas för att säkerställa tillämpning.

Verksamheten bör ha en tydlig rutin för hur riskbehandlingsplaner formuleras samt en rutin för att genom stickprov följa upp att redan implementerade säkerhetsåtgärder tillämpas. Forum för uppföljning kan vara bland annat interna revisioner men också annan periodisk egenkontroll.

2.5 Kontrollfråga 7

Har verksamheten genomfört riskanalysaktiviteter med anledning av den förändring som övergång till 27001:2022 innebär?

2.5.1 Referens

8.2 Bedömning av informationssäkerhetsrisker
Organisationen ska utföra bedömningar av informationssäkerhetsrisker vid planerade intervall eller när betydande ändringar föreslås eller sker, med beaktande av kriterierna i 6.1.2 a).

2.5.2 Förslag

Verksamheten bör genomföra en dedikerad riskanalysaktivitet med anledning av övergången till 27001:2022. Riskanalysaktiviteten bör följa verksamhetens process för att identifiera, bedöma och behandla risker. Aktiviteten bör genomföras uppdelat i takt med att övergångsarbetet fortskrider.

2.6 Kontrollfråga 8 och 9

Har verksamheten uppdaterat och infört (eller påbörjat införandet av) planen för behandling av informationssäkerhetsrisker?
Finns tydlig dokumentation över nya samt förändrade säkerhetsåtgärder?

2.6.1 Referens

8.3 Behandling av informationssäkerhetsrisker
Organisationen ska införa planen för behandling av informationssäkerhetsrisker.
Organisationen ska bevara dokumenterad information om resultaten av riskbehandlingen inom informationssäkerhet.

2.6.2 Förslag

Verksamheten bör säkerställa att erforderlig dokumentation finns över eventuella nyinförda säkerhetsåtgärder samt över eventuella förändrade säkerhetsåtgärder.

2.7 Kontrollfråga 10 och 11

Har verksamheten genomfört en avgränsad kontrollaktivitet för att säkerställa implementering av nya och/eller förändrade säkerhetsåtgärder, exempelvis inom ramen för interna revisioner?
Har verksamheten anpassat internrevisionsprogrammet för att säkerställa att säkerhetsåtgärder utifrån verksamhetens nya uttalande om tillämplighet beaktas och följs upp inom ramen för interna revisioner?

2.7.1 Referens

9.2.1 Allmänt
Organisationen ska med planerade intervall genomföra interna revisioner för att inhämta information om ledningssystemet för informationssäkerhet:
b) har implementerats och underhållits på ett verkningsfullt sätt.

9.2.2 Internt revisionsprogram
Organisationen ska planera, införa, genomföra och underhålla ett eller flera revisionsprogram, vilket innefattar

frekvens, metoder, ansvar, planeringskrav och rapportering.
När interna revisionsprogram införs ska organisationen ta hänsyn till de berörda processernas betydelse samt resultat av tidigare revisioner.

2.7.2 Förslag

Verksamheten bör genomföra en avgränsad internrevisionsaktivitet inför externrevision mot 27001:2022. Syftet med internrevisionsaktiviteten är dels att säkerställa att erforderlig GAP-analys har genomförts, att relevanta riskbedömningar har genomförts samt att verksamheten har tagit fram ett relevant och rättvisande uttalande om tillämplighet och uppdaterat samt implementerat sin riskbehandlingsplan.