Enheten strategi och samordning (ST)
Johan Turell
010-240 4155
Johan.Turell@msb.se

Modellens uttolkning av föreskriftens krav

Inledning

Nedan följer en genomgång av hur modellens frågor används för att indikera i vilken utsträckning en organisation efterlever kraven i MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Det kan dock inte uteslutas att det finns andra sätt att uppfylla krav i föreskrifterna än de som testas för i modellen. Modellens frågor och svarsalternativ är så långt möjligt anpassade till föreskrifternas krav men i vissa fall har, av enkättekniska skäl, en fullständig överenstämmelse inte gått att uppnå. Det finns ytterligare skiljelinjer. Modellen har till syfte att mäta centrala arbetssätt och processer i det systematiska informationssäkerhetsarbetet medan föreskrifterna även innehåller krav som ligger utanför detta, exempelvis krav på fysisk säkerhet. Detta innebär att efterlevnaden av vissa föreskriftskrav inte mäts. Det bör också noteras att de svarsalternativ som nedan kopplas till föreskrifternas krav i några fall även innebär en konkretisering i förhållande till i hur kravet formuleras i föreskrifterna. Som exempel kan nämnas att kravet att ”*analysera risker för sin information*” i föreskrifternas 6 § 2 p där nedan utpekade svarsalternativ inte bara innebär att analys genomförs utan även ger inriktning rörande vilken möjlig skadeverkan, såsom påverkan på människors liv och hälsa, som bör analyseras.

”Säker bedömning (dokumenterat underlag finns)” krävs på alla frågor där minst ett poänggivande svarsalternativ måste vara ikryssat för att nå föreskriftskravet. Genom detta omhändertas föreskrifternas krav på att olika aktiviteter ska vara dokumenterade.

Genomgång av föreskriftskrav

Inledningsvis redovisas respektive föreskriftsparagraf. Därefter följer en redogörelse för vilka frågor respektive svarsalternativ som har bedömts motsvara. I vissa fall ges ytterligare bakgrundsinformation till valet i form av en kommentar.

4 § Myndigheten ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande.

Krav		
1.	Minst nivå 3 i modellen	
2.	Svarsalternativ 5 i fråga 1	**Har ledningen styrt organisationens informationssäkerhetsarbete de senaste 2 åren?** Ja, under perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om… Att arbetet ska bedrivas med stöd av standarderna ISO/IEC 27001 respektive ISO/IEC 27002 eller motsvarande
Kommentar		
Det generella kravet på att uppnå minst nivå 3 i modellen för att uppfylla 4 § motiveras av att denna nivå ger en indikation på att organisationen bedriver ett systematiskt informationssäkerhetsarbete med både bredd och kvalitet.		

5 § Informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation.

När myndigheten utformar informationssäkerhetsarbetet ska den

1. *säkerställa att det finns en informationssäkerhetspolicy där ledningens målsättning med och inriktning för informationssäkerhetsarbetet framgår,*
2. *tydliggöra myndighetsledningens och den övriga organisationens ansvar, inklusive den eller de som utses att leda och samordna informationssäkerhetsarbetet, och ge dessa befattningar de befogenheter som behövs,*
3. *säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser,*
4. *upprätta de interna regler, arbetssätt och stöd som behövs, och*
5. *säkerställa att innehållet i myndighetens interna regler, arbetssätt och stöd utvärderas samt vid behov anpassas.*

Utformningen av informationssäkerhetsarbetet ska dokumenteras.

5 § Informationssäkerhetsarbetet ska utformas utifrån de risker och behov myndigheten identifierar. Det ska omfatta all behandling av information som myndigheten ansvarar för och integreras med myndighetens befintliga sätt att leda och styra sin organisation.

Krav		
1.	Svarsalternativ 1 i fråga 3	**Har organisationen någon gång under de senaste två åren inventerat sina informationsmängder och informationssystem, inklusive nätverk?**

		Ja, och under perioden har organisationen inventerat (eller sett över tidigare inventering av) både informationsmängder och informationssystem, inklusive nätverk i… Alla organisationens verksamheter
2.	Svarsalternativ 1 i fråga 21	**Har organisationen, de senaste två åren, analyserat sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker?** Ja, och under perioden har organisationen (minst en gång) använt arbetssättet och analyserat informationssäkerhetsrisker inom… Alla organisationens verksamheter
3.	Svarsalternativ 1 i fråga 23	**De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?** Ja, under perioden har organisationen fattat beslut om säkerhetsåtgärder med anledning av genomförd analys av informationssäkerhetsrisker inom… Alla organisationens verksamheter
4.	Svarsalternativ 1 i fråga 25	**Har organisationen, de senaste två åren, infört de säkerhetsåtgärder som beslutats?** Ja, under perioden har organisationen infört… Alla de beslutade säkerhetsåtgärderna
5.	Svarsalternativ 5 i fråga 40	**De senaste två åren, har organisationens ledning arbetat för att säkerställa ständiga förbättringar i det systematiska informationssäkerhetsarbetet?** Ja, under perioden har organisationens ledning minst en gång följt upp, och vid behov beslutat om, organisationens arbete med att… Integrera informationssäkerhetsarbetet med befintliga sätt att leda och styra organisationen
6.	Uppfyllande av alla de punkter som hör till paragrafen	

1. säkerställa att det finns en informationssäkerhetspolicy där ledningens målsättning med och inriktning för informationssäkerhetsarbetet framgår,

Krav		
1.	Svarsalternativ 2 och 3 i fråga 2	**Har organisationen haft en informationssäkerhetspolicy de senaste två åren?** Ja, och under hela perioden har informationssäkerhetspolicyn (eller motsvarande dokument) innehållit… Ledningens målsättningar för informationssäkerhetsarbetet (vad som ska uppnås) Ledningens inriktning för informationssäkerhetsarbetet (hur det ska uppnås)

2. tydliggöra myndighetsledningens och den övriga organisationens ansvar, inklusive den eller de som utses att leda och samordna informationssäkerhetsarbetet, och ge dessa befattningar de befogenheter som behövs,

Krav		
1.	Svarsalternativ 2 i fråga 1	**Har ledningen styrt organisationens informationssäkerhetsarbete de senaste två åren?** Ja, under perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om… Ansvar och befogenheter för informationssäkerhetsarbetet inom organisationen, inklusive den roll eller funktion som ska leda och samordna informationssäkerhetsarbetet

3. säkerställa att informationssäkerhetsarbetet tilldelas nödvändiga resurser,

Krav		
1.	Svarsalternativ 3 i fråga 1	**Har ledningen styrt organisationens informationssäkerhetsarbete de senaste två åren?** Ja, under perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om… Resurser som informationssäkerhetsarbetet kräver

4. upprätta de interna regler, arbetssätt och stöd som behövs, och

Krav		
1.	Svarsalternativ 4 i fråga 1	**Har ledningen styrt organisationens informationssäkerhetsarbete de senaste två åren?** Ja, under perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om… Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
2.	Svarsalternativ 1, och 4 i fråga 7	**Har organisationen haft ett arbetssätt för informationsklassning de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
3.	Svarsalternativ 1 och 4 i fråga 8	**Har organisationen haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
4.	Svarsalternativ 1 och 4 i fråga 9	**Har organisationen haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser de senaste två åren?** Ja, och under perioden har arbetssättet…

		Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
5.	Svarsalternativ 1 och 4 i fråga 10	**Har organisationen haft ett arbetssätt för kontinuitetshantering de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
6.	Svarsalternativ 1 och 4 i fråga 11	**Har organisationen haft ett arbetssätt för omvärldsbevakning avseende informationssäkerhet de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
7.	Svarsalternativ 1 och 4 i fråga 12	**Har organisationen haft ett arbetssätt för utbildning i informationssäkerhet de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
8.	Svarsalternativ 1 och 4 i fråga 13	**Har organisationen haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen Varit beskrivet i stöd och vägledning för medarbetarna
5. säkerställa att innehållet i myndighetens interna regler, arbetssätt och stöd utvärderas samt vid behov anpassas.		
Krav		
1.	Svarsalternativ 4 i fråga 1	**Har ledningen styrt organisationens informationssäkerhetsarbete de senaste två åren?** Ja, och under perioden har organisationens ledning minst en gång beslutat om eller sett över tidigare beslut om… Regler för informationssäkerhetsarbetet, alternativt delegerat ansvaret för beslut eller översyn
2.	Svarsalternativ 1 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?**

		Ja, och under perioden har organisationen minst en gång per år följt upp, genom att sammanställa och analysera… Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete

6 § Myndigheten ska säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att

1. *klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),*
2. *identifiera, analysera och värdera risker för sin information (riskbedömning),*
3. *utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och*
4. *utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.*

Krav	
1.	Uppfyllande av alla de punkter som hör till paragrafen

1. klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning),

Krav		
1.	Svarsalternativ 1 i fråga 6	**Har organisationen de senaste två åren haft tillgång till särskilda kompetenser som behövs i ett systematiskt informationssäkerhetsarbete?** Ja, under perioden har organisationen haft tillgång till särskild kompetens inom… Informationsklassning samt analys och hantering av informationssäkerhetsrisker
2.	Svarsalternativ 1 i fråga 7	**Har organisationen haft ett arbetssätt för informationsklassning de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
3.	Svarsalternativ 1 i fråga 20	**Har organisationen, de senaste två åren, klassat sin information enligt sitt arbetssätt för informationsklassning?** Ja, under perioden har organisationen minst en gång använt arbetssättet för att värdera och klassa informationstillgångar inom… Alla organisationens verksamheter
4.	Svarsalternativ 1, 2 och 3 i fråga 32	**De senaste två åren, har organisationens arbetssätt för informationsklassning omfattat följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att informationsklassningen ska…

		Utgå ifrån organisationens inventering av informationsmängder, informationssystem och nätverk Beakta tillämplig lagstiftning, inklusive offentlighets- och sekretesslagen, dataskyddsförordningen, säkerhetsskyddslagen, arkivlagen, samt krisberedskapsförordningen eller lagen om extraordinära händelser Utgå ifrån krav på tillgänglighet, riktighet och konfidentialitet

Kommentar

Angående kravet på poäng för fråga 32 svarsalternativ 1: Det bör noteras att även om föreskriftskravet på informationsklassning inte uttryckligen innefattar krav på föregående inventering av informationsmängder, informationssystem och nätverk så ses det inom ramen för modellen som en förutsättning för att kunna genomföra informationsklassning på ett systematiskt sätt.

2. identifiera, analysera och värdera risker för sin information (riskbedömning),

Krav

1.	Svarsalternativ 1 i fråga 6	**Har organisationen de senaste två åren haft tillgång till särskilda kompetenser som behövs i ett systematiskt informationssäkerhetsarbete?** Ja, under hela perioden har organisationen haft tillgång till särskild kompetens inom… Informationsklassning samt analys och hantering av informationssäkerhetsrisker
2.	Svarsalternativ 1 i fråga 8	**Har organisationen haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
3.	Svarsalternativ 1 i fråga 21	**De senaste två åren, har organisationen analyserat sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker?** Ja, och under perioden har organisationen minst en gång använt arbetssättet för att analysera informationssäkerhetsrisker inom… Alla organisationens verksamheter
4.	Svarsalternativ 1 och 3 i fråga 33	**De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att analysen av informationssäkerhetsrisker ska … Utgå ifrån organisationens informationsklassning av berörda informationsmängder, informationssystem och nätverk

		Utvärdera riskers påverkan på informationsmängders, informationssystems och nätverks tillgänglighet, riktighet och konfidentialitet
5.	Svarsalternativ 1 och minst två av de övriga poänggivande svarsalternativen i fråga 34	**De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat bedömning av följande centrala typer av skadeverkan och grad av skadeverkan?** Ja, under perioden har arbetssättet omfattat bedömning av riskers grad av potentiell skadeverkan på … Informationsmängder, informationssystem och nätverk (den egna organisationens och andras) OCH Människors liv och hälsa (de egna medarbetarnas och andras) ELLER Finansiella tillgångar och övrig egendom (den egna organisationens och andra människors eller organisationers) ELLER Tillhandahållande av tjänster (den egna organisationens och andra organisationers) ELLER Förtroende (allmänhetens eller andras, för organisationen eller andra organisationer, för egna eller andras tjänster)
6.	Minst ett av de poänggivande svarsalternativen, eller Nej, men-svarsalternativet, i fråga 35	**De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala typer av sannolikhetsbedömning?** Ja, under perioden har arbetssättet omfattat sannolikhetsbedömningar såsom … Hur ofta risken kan väntas inträffa givet de rådande omständigheterna När risken tidigast, senast och troligast kan väntas inträffa givet de rådande omständigheterna Hur ofta risken kan väntas inträffa om föreslagna säkerhetsåtgärder genomförs

		När risken tidigast, senast och troligast kan väntas inträffa om föreslagna säkerhetsåtgärder genomförs Hur säker man kan vara på sannolikhetsbedömningarna givet vad man vet och de antaganden man har gjort ELLER Nej, men arbetssättet har omfattat andra centrala typer av sannolikhetsbedömningar

3. utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder, och

Krav		
1.	Svarsalternativ 1 i fråga 8	**Har organisationen haft ett arbetssätt för analys och hantering av informationssäkerhetsrisker de senaste två åren?** Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1 i fråga 21	**De senaste två åren, har organisationen analyserat sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker?** Ja, och under perioden har organisationen minst en gång använt arbetssättet för att analysera informationssäkerhetsrisker inom… Alla organisationens verksamheter
3.	Svarsalternativ 1 i fråga 23	**De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?** Ja, under perioden har organisationen fattat beslut om säkerhetsåtgärder med anledning av genomförd analys av informationssäkerhetsrisker inom… Alla organisationens verksamheter
4.	Svarsalternativ 1 i fråga 25	**Har organisationen, de senaste två åren, infört de säkerhetsåtgärder som beslutats?** Ja, under perioden har organisationen infört… Alla de beslutade åtgärderna
5.	Svarsalternativ 1 i fråga 33	**De senaste två åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att analysen av informationssäkerhetsrisker ska…

		Utgå ifrån organisationens informationsklassning av berörda informationsmängder, informationssystem och nätverk
6.	Svarsalternativ 2 i fråga 36	**De två senaste åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat riskhantering med följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att… Organisationen har ett ramverk för riskacceptans som definierar vilka informationssäkerhetsrisker som måste åtgärdas och vilka informationssäkerhetsrisker som kan accepteras utan åtgärd

4. utvärdera säkerhetsåtgärderna och vid behov anpassa skyddet av informationen. I arbetet ingår att genomföra en gapanalys.

Krav		
1.	Svarsalternativ 5 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?** Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet
2.	Svarsalternativ 1 i fråga 23	**De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?** Ja, under perioden har organisationen fattat beslut om säkerhetsåtgärder med anledning av genomförd analys av informationssäkerhetsrisker inom… Alla organisationens verksamheter
3.	Svarsalternativ 1 i fråga 26	**Har organisationen, de senaste två åren, utvärderat om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga?** Ja, under perioden har införda säkerhetsåtgärder utvärderats för... Alla organisationens verksamheter
4.	Svarsalternativ 3-5 i fråga 36	**De två senaste åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat riskhantering med följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att… Analys av enskilda informationssäkerhetsrisker uppdateras efter att beslutade säkerhetsåtgärder har införts

		Inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker Status för informationssäkerhetsrisker följs upp utifrån definierade intervall

7 § I de fall myndigheten överlåter åt en annan statlig myndighet att fullgöra uppgifter som regleras i dessa föreskrifter ska myndigheterna komma överens om och dokumentera vad respektive myndighet ansvarar för samt hantera de risker överlåtelsen innebär.

Krav
-
Kommentar
Modellen kan inte ge någon indikation om paragrafen uppfylls eftersom den inte innehåller någon fråga och svarsalternativ som rör utkontraktering mellan statliga myndigheter. Frågor om utkontraktering på en mer generell nivå omhändertas i 8 §.

8 § Myndigheten ska, innan den låter en extern aktör behandla information, utifrån informationsklassning och riskbedömning, hantera de risker en sådan behandling innebär. Myndigheten ska i avtal ställa krav på vilka säkerhetsåtgärder den externa aktören ska vidta och hur myndigheten följer upp dessa krav.

Krav		
1.	Svarsalternativ 1 i fråga 13	**Har organisationen haft ett arbetssätt för att säkerställa informationssäkerhet vid upphandling de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1 i fråga 28	**Har organisationen, de senaste två åren, genomfört upphandling enligt sitt arbetssätt för att säkerställa informationssäkerhet?** Ja, under perioden har organisationen använt arbetssättet för att säkerställa informationssäkerhet vid upphandling i samband med… All upphandlingar
3.	Svarsalternativ 1, 2, 3, 4 och 5 i fråga 37	**De senaste två åren, har organisationens arbetssätt för att säkerställa informationssäkerhet vid upphandling omfattat följande centrala delar?** Ja, och under perioden har organisationens arbetssätt omfattat att … Klassa information och analysera informationssäkerhetsrisker för det som ska utkontrakteras/anskaffas

		Bedöma behovet av åtgärder med anledning av informationsklassningens och riskanalysens resultat, samt att identifiera säkerhetsåtgärder Införa de säkerhetsåtgärder som organisationen har beslutat om utifrån informationsklassningens och riskanalysens resultat och som kan utföras av organisationen själv Ställa krav på den kontrakterade parten utifrån informationsklassningens och riskanalysens resultat Följa upp om de ställda kraven var ändamålsenliga och tillräckliga, samt om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats

9 § Myndigheten ska

1. *anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till,*
2. *hålla egen och inhyrd personal informerad om relevanta interna regler, arbetssätt och stöd,*
3. *utvärdera att interna regler, arbetssätt och stöd används på avsett sätt,*
4. *säkerställa att egen och inhyrd personal med utpekade roller i informationssäkerhetsarbetet har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter, och*
5. *utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning.*

Krav	
1.	Uppfyllande av alla de punkter som hör till paragrafen
Kommentar	
Modellen kan inte ge en fullständig indikation om paragrafen uppfylls eftersom den inte mäter om organisationen uppfyller punkt 1 i 9 §. Föreskriftsåterkopplingen indikerar endast kravuppfyllnad gällande punkt 2 – 5.	
1. anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till,	
Krav	
-	
Kommentar	
Modellen mäter inte punkt 1 i 9 §.	
2. hålla egen och inhyrd personal informerad om relevanta interna regler, arbetssätt och stöd,	
Krav	
1.	Svarsalternativ 1 i fråga 16	**De senaste två åren, har organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning?** Ja, under perioden har organisationen minst en gång, enligt arbetssättet, utbildat… Alla medarbetare
2.	Svarsalternativ 1 och 4 i fråga 31	**De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?**

		Ja, under perioden har utbildningen varit utformad utifrån… Medarbetarnas roller, uppgifter, ansvar och behov Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet

Kommentar

Det bör noteras att föreskrifternas krav i p. 2 även kan mötas av informationsinsatser.
Med medarbetare avses anställda och annan personal som har arbetat i organisationen i minst sex månader. Begreppet medarbetare motsvarar i stort föreskrifternas begrepp ”egen och inhyrd personal”.

3. utvärdera att interna regler, arbetssätt och stöd används på avsett sätt,

Krav

1.	Svarsalternativ 1 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?** Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
2.	Svarsalternativ 1 i fråga 17	**Har organisationen, de senaste två åren, undersökt i vilken utsträckning medarbetarna efter genomförd utbildning i informationssäkerhet vet hur de ska arbeta på ett informationssäkert sätt?** Ja, under perioden har organisationen undersökt detta minst en gång hos… Alla de som genomgått utbildning i informationssäkerhet
3.	Svarsalternativ 1 i fråga 18	**De senaste två åren, har organisationen undersökt om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet?** Ja, under perioden har organisationen undersökt detta minst en gång hos… Alla de som hade genomgått utbildning i informationssäkerhet
4.	Svarsalternativ 4 i fråga 31	**De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?** Ja, under perioden har utbildningen varit utformad utifrån… Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet

4. säkerställa att egen och inhyrd personal med utpekade roller i informationssäkerhetsarbetet har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter, och

Krav

1.	Svarsalternativ 1, 2, 3, 4 och 5 i fråga 6	**Har organisationen de senaste två åren haft tillgång till särskilda kompetenser som behövs i ett systematiskt informationssäkerhetsarbete?** Ja, under hela perioden har organisationen haft tillgång till särskild kompetens inom… Informationsklassning samt analys och hantering av informationssäkerhetsrisker Utbildning i informationssäkerhet Uppföljning av informationssäkerhetsarbetet Arbete med it-säkerhet Säkerställande av informationssäkerhet vid upphandling
2.	Svarsalternativ 1, 2, 3, 4 och 5 i fråga 31	**De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?** Ja, under perioden har utbildningen varit utformad utifrån… Medarbetarnas roller, uppgifter, ansvar och behov Medarbetarnas kunskapsnivå Ledningens målsättningar för det systematiska informationssäkerhetsarbetet Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter
Kommentar		
Det bör noteras att föreskrifternas krav i p. 4 även kan mötas av informationsinsatser.		
5. utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning.		
Krav		
1.	Svarsalternativ 1 i fråga 5	**Har organisationen de senaste två åren undersökt medarbetarnas kunskaper om informationssäkerhet?** Ja, under perioden har organisationen, vid minst ett tillfälle, undersökt kunskaperna hos… Alla medarbetare
2.	Svarsalternativ 1 i fråga 12	**Har organisationen haft ett arbetssätt för utbildning i informationssäkerhet de senaste två åren?** Ja, och under hela perioden har arbetssättet…

		Varit beslutat eller på annat sätt medvetet valt av organisationen
3.	Svarsalternativ 1 i fråga 16	**De senaste två åren, har organisationen utbildat sina medarbetare inom informationssäkerhet enligt sitt arbetssätt för utbildning?**
		Ja, under perioden har organisationen minst en gång, enligt arbetssättet, utbildat… Alla medarbetare
4.	Svarsalternativ 1 i fråga 27	**Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?**
		Ja, och under perioden har organisationen övat kontinuitet inom… Alla organisationens verksamheter
5.	Svarsalternativ 1, 2, 3, 4 och 5 i fråga 31	**De senaste två åren, har organisationens utbildning i informationssäkerhet varit utformad utifrån följande centrala aspekter?**
		Ja, under perioden har utbildningen varit utformad utifrån… Medarbetarnas roller, uppgifter, ansvar och behov Medarbetarnas kunskapsnivå Ledningens målsättningar för det systematiska informationssäkerhetsarbetet Organisationens regelverk samt olika arbetssätt och stöd för informationssäkerhetsarbetet Organisationens identifierade risker eller inträffade incidenter, samt dess identifierade hot och sårbarheter

Kommentar
Det bör noteras att föreskrifternas krav i p. 5 även kan mötas av informationsinsatser.

10 § Myndigheten ska identifiera och hantera behovet av

1. *skalskydd och tillträdesbegränsning för sina lokaler,*
2. *tekniska system för att larma vid obehörigt tillträde till sina lokaler, och*
3. *att dela in sina lokaler i fysiskt separerade zoner.*

Krav
-
Kommentar
Modellen mäter inte efterlevnaden av detta föreskriftskrav.

11 § Myndigheten ska ha förmåga att

1. *skyndsamt upptäcka och bedöma incidenter och avvikelser,*

2. *återställa manipulerad eller förlorad information, och*
3. *bedöma om inträffad incident ska rapporteras externt.*

Krav		
Uppfyllande av alla de punkter som hör till paragrafen		
1. skyndsamt upptäcka och bedöma incidenter och avvikelser,		
Krav		
1.	Svarsalternativ 1 i fråga 9	**Har organisationen haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1, 2, 3 och 5 i fråga 29	**De senaste två åren, har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat följande centrala delar?** Ja, under perioden har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat… En funktion för att hantera informationssäkerhetsincidenter och -avvikelser med dedikerad personal som har särskild kompetens Kanaler som medarbetare inom organisationen kan använda för att nå funktionen och rapportera incidenter och avvikelser Kanaler som funktionen kan använda för att nå andra organisationer och rapportera om incidenter, få rapporter om incidenter eller dela information, samt rutiner för deras användning Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete
2. återställa manipulerad eller förlorad information, och		
Krav		
-		
Kommentar		
Modellen mäter inte efterlevnaden av detta föreskriftskrav.		
3. bedöma om inträffad incident ska rapporteras externt.		
Krav		
1.	Svarsalternativ 1 i fråga 9	**Har organisationen haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser de senaste två åren?** Ja, och under hela perioden har arbetssättet…

		Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1, 3, 4 och 5 i fråga 29	**De senaste två åren, har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat följande centrala delar?** Ja, under perioden har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat… En funktion för att hantera informationssäkerhetsincidenter och -avvikelser med dedikerad personal som har särskild kompetens Kanaler som funktionen kan använda för att nå andra organisationer och rapportera om incidenter, få rapporter om incidenter eller dela information, samt rutiner för deras användning En eskaleringsrutin för att hantera stora och allvarliga incidenter, inklusive extern rapportering vid behov Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete

12 § Om en incident eller avvikelse inträffat ska myndigheten identifiera grundorsaker till incidenten eller avvikelsen och vidta åtgärder för att motverka att liknande incidenter och avvikelser inträffar på nytt.

Krav		
1.	Svarsalternativ 1 i fråga 9	**Har organisationen haft ett arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1 i fråga 23	**De senaste två åren, har organisationen fattat beslut om att införa – eller att inte införa – säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker?** Ja, under perioden har organisationen fattat beslut om säkerhetsåtgärder med anledning av genomförd analys av informationssäkerhetsrisker inom… Alla organisationens verksamheter
3.	Svarsalternativ 5 i fråga 29	**De senaste två åren, har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat följande centrala delar?**

		Ja, under hela perioden har organisationens arbetssätt för hantering av informationssäkerhetsincidenter och -avvikelser omfattat... Analys av inträffade incidenter, deras grundorsaker och hantering, samt erfarenhetsåterföring till förebyggande arbete
4.	Svarsalternativ 4 i fråga 36	**De två senaste åren, har organisationens arbetssätt för analys och hantering av informationssäkerhetsrisker omfattat riskhantering med följande centrala delar?** Ja, under perioden har organisationens arbetssätt omfattat att… Inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker

13 § Myndigheten ska,

1. *identifiera och hantera behovet av kontinuitet för behandling av information, och*
2. *öva förmåga att upprätthålla identifierat behov av kontinuitet.*

Krav		
Uppfyllande av alla de punkter som hör till paragrafen		
1. identifiera och hantera behovet av kontinuitet för behandling av information, och		
Krav		
1.	Svarsalternativ 1 i fråga 3	**Har organisationen någon gång under de senaste två åren inventerat sina informationsmängder och informationssystem, inklusive nätverk?** Ja, och under perioden har organisationen inventerat (eller sett över tidigare inventering av) både informationsmängder och informationssystem, inklusive nätverk i… Alla organisationens verksamheter
2.	Svarsalternativ 1 i fråga 7	**Har organisationen haft ett arbetssätt för informationsklassning de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
3.	Svarsalternativ 1 i fråga 10	**Har organisationen haft ett arbetssätt för kontinuitetshantering de senaste två åren?** Ja, och under hela perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
4.	Svarsalternativ 4 i fråga 38	**De senaste två åren, har organisationen undersökt och hanterat sina behov av att bygga beredskap för kriser och höjd beredskap?** Ja, under perioden har organisationen minst en gång undersökt …

		Eventuellt behov av kontinuitetshantering för att skydda sin information vid kris eller höjd beredskap, samt vid behov säkerställt att påkallad förmåga finns
2. öva förmåga att upprätthålla identifierat behov av kontinuitet.		
Krav		
1.	Svarsalternativ 1 i fråga 10	**Har organisationen haft ett arbetssätt för kontinuitetshantering de senaste två åren?**
		Ja, och under perioden har arbetssättet… Varit beslutat eller på annat sätt medvetet valt av organisationen
2.	Svarsalternativ 1 i fråga 27	**Har organisationen, de senaste två åren, övat kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering?**
		Ja, och under perioden har organisationen övat kontinuitet inom… Alla organisationens verksamheter

14 § Myndigheten ska minst en gång per år följa upp att informationssäkerhetsarbetet svarar mot myndighetsledningens målsättning och inriktning, genom att sammanställa och analysera resultatet av genomförda

1. *utvärderingar av interna regler, arbetssätt och stöd enligt 5 § p. 5,*
2. *informationsklassningar enligt 6 § p. 1,*
3. *riskbedömningar enligt 6 § p. 2,*
4. *utvärderingar av säkerhetsåtgärder enligt 6 § p. 4, och*
5. *utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt enligt 9 § p. 3.*

Krav		
Uppfyllande av alla de punkter som hör till paragrafen		
1. utvärderingar av interna regler, arbetssätt och stöd enligt 5 § p. 5,		
Krav		
1.	Svarsalternativ 1 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?**
		Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda utvärderingar av organisationens interna regler, arbetssätt och stöd för informationssäkerhetsarbete
2. informationsklassningar enligt 6 § p. 1,		
Krav		
1.	Svarsalternativ 4 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?**
		Ja, och under perioden har organisationen minst en gång följt upp…

		Resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker
3. riskbedömningar enligt 6 § p. 2,		
Krav		
1.	Svarsalternativ 4 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste 2 åren?**
		Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda informationsklassningar och analyser av informationssäkerhetsrisker
4. utvärderingar av säkerhetsåtgärder enligt 6 § p. 4, och		
Krav		
1.	Svarsalternativ 5 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste två åren?**
		Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda utvärderingar av säkerhetsåtgärders ändamålsenlighet och tillräcklighet
5. utvärderingar av att interna regler, arbetssätt och stöd används på avsett sätt enligt 9 § p. 3.		
Krav		
1.	Svarsalternativ 2 i fråga 14	**Har organisationen följt upp resultatet av sitt systematiska informationssäkerhetsarbete de senaste 2 åren?**
		Ja, och under perioden har organisationen minst en gång följt upp… Resultat av genomförda utvärderingar av om medarbetarna tillämpar interna regler, arbetssätt och stöd för informationssäkerhetsarbete på avsett sätt

15 § Myndighetsledningen ska informera sig om

1. *i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov,*
2. *allvarliga risker som inte åtgärdats, och*
3. *övriga hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet.*

Krav		
Uppfyllande av alla de punkter som hör till paragrafen		
1. i vilken utsträckning införda säkerhetsåtgärder motsvarar myndighetens behov,		
Krav		
1.	Svarsalternativ 3 i fråga 15	**Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?**
		Ja, under perioden har organisationens ledning minst en gång informerat sig om…

		I vilken utsträckning införda säkerhetsåtgärder är ändamålsenliga och tillräckliga (svarar mot identifierat behov)
2. allvarliga risker som inte åtgärdats, och		
Krav		
1.	Svarsalternativ 4 i fråga 15	**Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?** Ja, under perioden har organisationens ledning minst en gång informerat sig om… Eventuella allvarligare risker i organisationens informationsbehandling som inte har åtgärdats
3. övriga hinder för att uppnå ledningens målsättning med och inriktning för informationssäkerhetsarbetet.		
Krav		
1.	Svarsalternativ 5 i fråga 15	**Har organisationens ledning informerat sig om status på organisationens systematiska informationssäkerhetsarbete de senaste två åren?** Ja, under perioden har organisationens ledning minst en gång informerat sig om… Eventuella identifierade hinder för att uppnå ledningens målsättning med informationssäkerhetsarbetet