Myndigheten för samhällsskydd och beredskap

Skydd av samhällsviktig verksamhet

Ökad motståndskraft genom arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser

Skydd av samhällsviktig verksamhet – Ökad motståndskraft genom arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser

Enhet: Inriktning av civil beredskap

Foto omslag: Mikael Svensson/Johnér
Produktion: Advant

Publikationsnummer: MSB2401 – augusti 2024
ISBN: 978-91-7927-530-3
Tidigare utgiven: MSB932 – april 2018
ISBN: 978-91-7383-823-8

Innehåll

Inledning

Inledning

Det förändrade omvärldsläget och den säkerhetspolitiska utvecklingen ställer ökade krav på samhällets aktörer att kunna upprätthålla viktiga samhällsfunktioner. För att viktiga samhällsfunktioner ska kunna upprätthållas behöver samhällsviktiga verksamheter ha som målsättning att, så långt det är möjligt, fungera i vardagen, under en fredstida krissituation, vid krigsfara och ytterst i krig.

För att Sverige ska kunna fungera och försvaras i krig behöver alla aktörer, såväl offentliga som privata, ta ansvar för att stärka samhällets motståndskraft och att ha förmågan att fortsätta bedriva sin samhällsviktiga verksamhet även under kris och ytterst i krig.[1] De som tillhandahåller en samhällsviktig verksamhet behöver skapa en motståndskraft i verksamheten då detta utgör en grundförutsättning för Sveriges beredskap. Det kan handla om att minska sannolikheten för att risker inträffar eller säkerställa tillgången till resurser i form av personal, varor, tjänster och information.

Behovet av att arbeta med motståndskraft hos samhällsviktig verksamhet har ökat de senaste åren, inte minst som en del av uppbyggnaden av den civila beredskapen. Även inom ramen för EU-samarbetet har arbetet med att stärka motståndskraften i samhällsviktig verksamhet accelererat. Medlemsländerna ska implementera två EU-direktiv, CER[2] och NIS2[3], som innebär en tydligare reglering på området. De båda direktiven riktar sig till de aktörer som tillhandahåller samhällsviktiga verksamheter och ställer krav på ökad motståndskraft.

1. Regeringens proposition 2020/21:30 Totalförsvaret 2021–2025.

2. **Europaparlamentets och rådets direktiv** (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

3. **Europaparlamentets och rådets direktiv** (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Faktaruta om CER och NIS2

CER-direktivet: direktivet om kritiska entiteters (tillhandahållare av samhällsviktig verksamhet) motståndskraft. Enligt CER-direktivet ska medlemsstaterna säkerställa förmågan hos samhällsviktig verksamhet att förebygga, motstå och hantera störningar eller avbrott i verksamheten.

NIS2-direktivet: direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen. Enligt NIS2-direktivet ska medlemsstaterna genom att skydda nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster och säkerställa kontinuiteten i sådana tjänster när de utsätts för incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

Stödet kommer att uppdateras när CER- och NIS2-direktiven är implementerade i svensk lagstiftning.

Grundläggande områden att arbeta med för att skapa motståndskraft är riskhantering, kontinuitetshantering, informations- och cybersäkerhet och att hantera oönskade händelser. Dessa områden går in i varandra, har kompletterande perspektiv och utgör en basplatta för en organisations beredskaps- och säkerhetsarbete. Arbetet bidrar inte bara till en mer robust organisation utan också till att stärka hela samhällets motståndskraft.

Syfte

Syftet med detta stödjande dokument är att närmare beskriva vad aktörer som tillhandahåller samhällsviktig verksamhet, som minst, behöver arbeta med för att öka motståndskraften och vad som ingår i detta arbete.

Målgrupp

Stödet vänder sig till alla privata och offentliga aktörer som tillhandahåller samhällsviktig verksamhet, men kan användas av alla som vill skapa förutsättningar för att fortsätta att bedriva sin verksamhet under kriser och krig.

Så är stödet tänkt att användas

Stödet består av checklistor som bygger på nationella och internationella standarder och områdesspecifika vägledningar inom riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser. De är tänkt att utgöra stöd i vad en aktör som tillhandahåller samhällsviktig verksamhet, som minst behöver arbeta med för att skapa förutsättningar att kunna upprätthålla verksamheten. Stödet är generiskt för att kunna användas av alla typer av organisationer.

Stödet är också tänkt att användas för att bättre kunna samordna arbetet med de olika områdena.

I bilagan finns en korshänvisning till de standarder och områdesspecifika vägledningar som ligger till grund för checklistorna samt koppling till relevanta författningar.

Stödet beskriver inte hur arbetet kan genomföras utan vägleder i vad som behöver ingå för att skapa en motståndskraft i samhällsviktig verksamhet. Stödet innehåller inga dimensioneringar eller förmågekrav för den samhällsviktiga verksamheten.

Stöd för utvecklingen av motståndskraften kan fås i publikationen *Planeringsinriktning för civil beredskap – Ett underlag till stöd för fortsatt planering (MSB2194).*

Begreppslista

Samhällsviktig verksamhet
Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet.[4] I detta sammanhang ska verksamhet förstås som ett vidare begrepp. Verksamhet, tjänst eller infrastruktur inkluderar exempelvis även anläggningar, processer, system och noder.

Viktig samhällsfunktion
Med viktig samhällsfunktion avses samhällsfunktion som är nödvändig för samhällets grundläggande behov, värden eller säkerhet[5], till exempel tillsyn av barn och elever, betalningsförmedling och landtransporter. Dessa upprätthålls och säkerställs av samhällsviktiga verksamheter.

Motståndskraft
Förmågan att förebygga, stå emot, lindra, absorbera, anpassa sig till och återhämta sig från en incident som stör eller skulle kunna störa verksamheten.[6]

4. Förordning (2022:524) om statliga myndigheters beredskap.

5. Identifiering av samhällsviktig verksamhet: lista med viktiga samhällsfunktioner (MSB1844 – oktober 2021).

6. **Europaparlamentets och rådets direktiv** (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Motståndskraft i samhällsviktig verksamhet

Motståndskraft i samhälls-viktig verksamhet

För att skapa en basplatta och för att ge ett kompletterande perspektiv för en organisations säkerhets- och beredskapsarbete krävs det att arbeta med riskhantering, kontinuitetshantering, informations- och cybersäkerhet samt hantera oönskade händelser. Ett systematiskt arbete är centralt för att kunna skapa motståndskraft i samhällsviktig verksamhet.

Genom att arbeta systematiskt skapas förutsättningar för att kunna förebygga, förbereda, motstå och hantera oönskade händelser. Arbetet med:

- Riskhantering tar sin utgångspunkt i att hantera de risker som kan påverka verksamheten. Genom att systematiskt identifiera, analysera, utvärdera och behandla risker kan organisationen hantera osäkerheter i sin omgivning.[7] Arbetet bidrar till att minimerade ekonomiska-, personella-, funktionella- eller informationsförluster, och till en mer effektiv återhämtning när någon oönskad händelse inträffat.
- Kontinuitetshantering tar sin utgångspunkt i vad som ska levereras och de resurser som behövs för det. Arbetet fokuserar på att planera för att kunna upprätthålla verksamhet på en acceptabel nivå, oavsett vilken typ av störning som en organisation utsätts för. Genom att arbeta med kontinuitetshantering kan organisationer snabbare återhämta sig från och minska konsekvenserna av en inträffad oönskad händelse. Arbetet bidrar också till ett mindre sårbart samhälle.[8]
- Informations- och cybersäkerhet tar sin utgångspunkt i att skydda information och de informationssystem som behövs för att verksamheten ska fungera, och genomsyrar allt beredskapsarbete. Alla verksamheter är beroende av att korrekt och fullständig information finns tillgänglig för behöriga användare vid rätt tidpunkt för att verksamheten ska fungera. Ett systematiskt informationssäkerhetsarbete innebär att organisationen behöver identifiera vilken information som den samhällsviktiga verksamheten är beroende av och var den behandlas för att kunna säkerställa ett väl anpassat skydd för informationen och dess konfidentialitet, riktighet och tillgänglighet.[9]

7. ISO 31000:2018 – Riskhantering – Vägledning.

8. ftSS22304:2023 – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Handbok för kontinuitetshantering enligt SS EN ISO 22301.

9. ISO 27000: 2020 – Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi.

- Hantera oönskade händelser inkluderar incident- och krishantering samt samverkan och ledning vid samhällsstörningar. Det tar sin utgångspunkt i att organisationer behöver ha en beredskap för att hantera oönskade händelser av olika allvarlighetsgrad när dom inträffar. Genom att planera för olika oönskade händelser skapas förutsättningar för att en händelse effektivt ska kunna hanteras, för att konsekvenserna begränsas och för att den samhällsviktiga verksamheten kan upprätthållas.

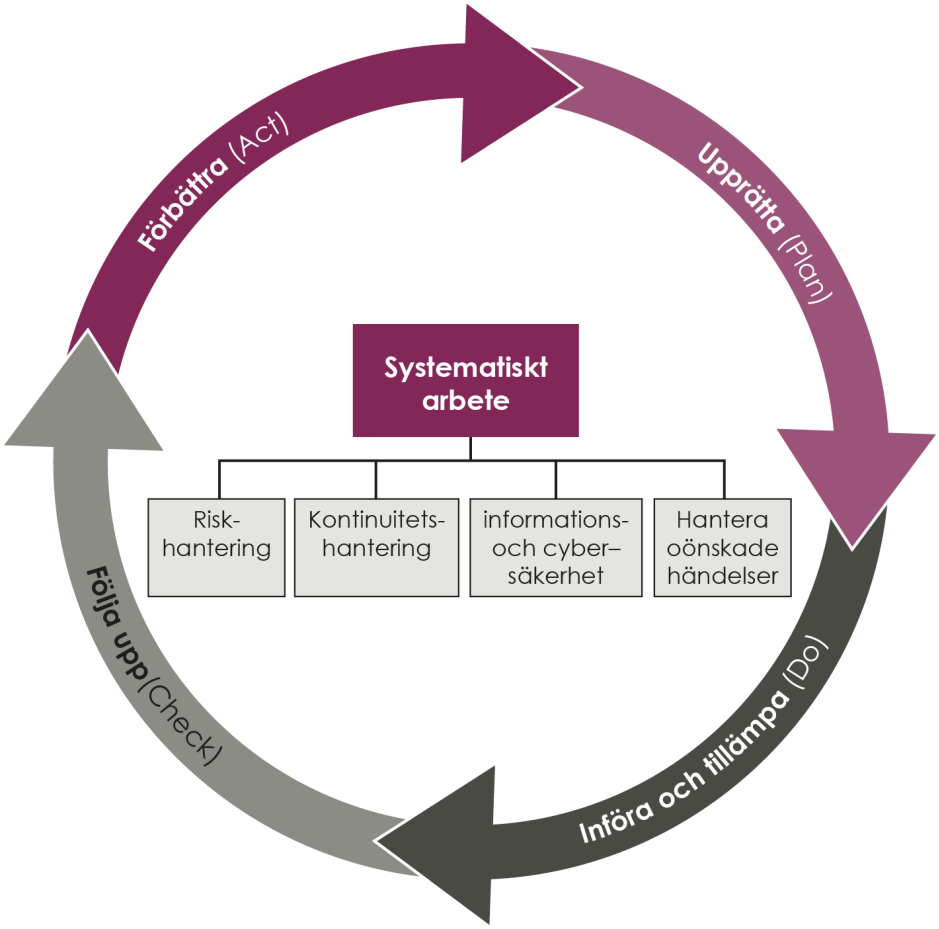
Arbetet behöver ske systematiskt, integreras i verksamhetens befintliga arbetssätt och genomsyra hela organisationen, till exempel inom ramen för organisationens ledningssystem. Det finns stora fördelar att samordna detta för ett mer effektivt arbete. Bland annat innehåller de alla moment av analys och bedömningar utifrån verksamheten och potentiella risker men utifrån olika perspektiv. Arbetet kommer också att generera behov av åtgärder som behöver samordnas för att skapa bästa effekt inom organisationen. Att inte se detta arbete som isolerade processer minskar också risken för dubbelarbete.

Nedan ges exempel på kopplingar mellan de olika arbetssätten:

- Arbetet med riskhantering ger bland annat kunskap om vilka risker som organisationen och dess verksamhet kan utsättas för. Underlaget kan vara ett stöd i den riskbedömning av resurser som görs i kontinuitetshanteringen och kan även användas för att bedöma risker mot information och därmed lämpliga åtgärder inom ramen för informations- och cybersäkerhetsarbetet.
- Arbetet med kontinuitetshantering ger t ex underlag om vilka resurser som behövs för att upprätthålla den samhällsviktiga verksamheten. Det ger bland annat kunskap om vilken information och informationssystem som verksamheten är beroende av och är ett underlag för vilka krav på skydd av informationen som verksamheten har.
- Åtgärder som är identifierade för att ge skydd inom ramen för riskhanteringsarbetet eller informations- och cybersäkerhetsarbetet kan vara desamma inom samtliga områden.
- Erfarenhetsåterföring från att hantera oönskade händelser, särskilt arbetet med incident- och krishantering, är viktiga ingångsvärden för förbättringsarbetet inom samtliga områden.

Nästkommande avsnitt beskriver r*iskhantering, kontinuitetshantering, informations- och cybersäkerhet* och *hantera oönskade händelse* med tillhörande checklistor. Det finns även en checklista som heter *systematiskt arbete* som beskriver gemensamma arbetssätt.

Figur 1. Systematiskt arbete med motståndskraft i samhällsviktig verksamhet



Systematiskt arbete

Checklistan syftar till att skapa en systematik för arbetet med motståndskraft i samhällsviktig verksamhet. Den innehåller delar om styrande dokument, omvärldsbevakning, utbildning och övning, information och kommunikation, uppföljning och förbättring samt erfarenhetsåterföring.

Tabell 1. Checklista – Systematiskt arbete

Nummer	Beskrivning
S1	Organisationens ledning har i styrande dokument fastställt övergripande förutsättningar och mål för hur arbetet med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och planering för hantering av oönskade händelser ska genomföras utifrån organisationens förutsättningar. *Målen ska vara baserade på ställda krav mot organisationen, mätbara, kommunicerade och uppdaterade*.
S2	Organisationen har i styrande dokument och arbetssätt dokumenterat det som behövs för att planera, implementera, använda, följa upp och förbättra organisationens arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och planering för hantering av oönskade händelser för samhällsviktig verksamhet.
S3	Organisationen arbetar med omvärldsbevakning för att identifiera händelser som påverkar den samhällsviktiga verksamheten för att kunna fatta effektiva beslut om prioriteringar för riskhantering, kontinuitetshantering, informations- och cybersäkerhet och vid hantering av händelser.
S4	Organisationen utbildar och övar personal som berörs av arbetet med samhällsviktig verksamhet.
S5	Organisationen har etablerade metoder och planer för intern och extern kommunikation och rapportering för riskhantering, kontinuitetshantering, informations- och cybersäkerhet och vid hantering av händelser.
S6	Organisationen har etablerade arbetssätt för att följa upp och utvärdera arbetet med riskhantering, kontinuitetshantering, informations- och cybersäkerhet samt hantering av oönskade händelser. *Det inkluderar arbetssätt för att utvärdera inträffade händelser och övningar och att följa upp efterlevnaden av interna och externa krav*.
S7	Organisationen tar till vara erfarenheter från uppföljningar och revisioner av arbetet med riskhantering, kontinuitetshantering och informations- och cybersäkerhet, inträffade händelser och övningar.

Riskhantering

Arbetssättet för riskhantering kan se ut på olika sätt men kan i stora drag sammanfattas i nedan checklista.

Tabell 2. Checklista – Riskhantering

Nummer	Beskrivning
R1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande riskhantering.
R2	Det finns framtagna mål för arbetet och organisationen arbetar med riskhanteringen i det strategiska arbetet. *Att arbeta med riskhantering i det strategiska arbetet kan exempelvis ske genom att det ingår i organisationens styrande processer så som planerings- och budgetprocess och att det finns som en återkommande punkt på ledningens agenda*.
R3	Organisationen har tillräckliga resurser för att uppfylla målen gällande riskhantering enligt styrande dokument. *Exempelvis kundkrav och lagkrav. Dessa resurser kan även avsättas till personal, teknik, metod och verktyg, finansiering och information för att hantera sårbarheter och möjliggöra anpassning till förändrade omständigheter*.
R4	Organisationen arbetar med riskhanteringen i det dagliga arbetet. *Exempelvis genom att riskhantering implementeras i redan befintliga processer i organisationen och att alla inom organisationen ansvarar för att hantera risker.*
R5	Organisationen har beslutat och kommunicerat verksamhetens nivå för riskacceptans, vilket används som utgångspunkt vid hantering av riskerna (se även K5 och IC5). *Organisationens nivå för riskacceptans, kallas ibland även risktolerans och är de nivåer som organisationen/ ledningen har beslutat ska gälla för att kunna acceptera en risk dvs. behålla risken utan att vidta någon ytterligare åtgärd. Notera att även accepterade risker fortlöpande måste bevakas*.
R6	Organisationen genomför regelbundet bedömningar av risker och sårbarheter (se även K6 och IC7) i verksamheten och dessa innehåller bland annat: • Identifiering av verksamhetens risker, sårbarheter och förmågor. • Sannolikhet för och konsekvens av att riskerna inträffar. • Värdering och prioritering av riskerna i relation till verksamhetens mål/krav. • Åtgärdsplan för hantering av riskerna. *Bedömningarna avser att skaffa organisationen en tillräckligt bra bild över vilka interna och externa risker som finns kopplat till verksamheten. Dessa bedömningar kan genomföras inom en rad olika områden bl.a. riskanalys för intern styrning och kontroll, försäkringsmässiga riskanalyser samt risk- och sårbarhetsanalyser*.
R7	Organisationen beslutar och genomför åtgärder enligt beslutad åtgärdsplan för riskerna.
R8	Organisationen följer upp och utvärderar genomförda åtgärder för att säkerställa att de minskat riskerna som förväntat.

Kontinuitetshantering

Arbetssättet för kontinuitetshantering kan se ut på olika sätt men kan i stora drag sammanfattas i nedan checklista.
Se www.msb.se/kontinuitetshantering för mer stöd i arbetet.

Tabell 3. Checklista – Kontinuitetshantering

Nummer	Beskrivning
K1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande kontinuitetshantering.
K2	Det finns framtagna mål för arbetet och organisationen arbetar med kontinuitetshantering i det strategiska arbetet. *Exempelvis genom att det är en integrerad del av organisationens övergripande ledningssystem och att det finns som en återkommande punkt på ledningens agenda*.
K3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande kontinuitetshantering enligt styrande dokument.
K4	Organisationen arbetar med kontinuitetshantering i det dagliga arbetet. *Det kan ske genom att kontinuitetshantering implementeras i redan befintliga processer i organisationen.*
K5	Organisationen har genomfört och dokumenterat en konsekvensanalys om störningar inträffar i organisationens leveranser av viktiga/kritiska produkter och tjänster som kan innehålla: • En kriteriemodell (eller motsvarande) för att bedöma konsekvenser av avbrott (se även R5 och IC5). • Vilka aktiviteter som behövs för att leverera produkter och tjänster. • Vilka konsekvenser ett avbrott i dessa aktiviteter har för organisationen genom bedömning med hjälp av kriteriemodellen. • Definition av hur länge aktiviteten kan ligga nere utan att konsekvenserna blir oacceptabla för verksamheten (acceptabel avbrottstid). • Identifierade prioriterade aktiviteter • Fastställda resurser (beroenden) inklusive partners och leverantörer som behövs för att utföra de prioriterade aktiviteterna. • Identifierade återställningstider för resurserna.
K6	Organisationen har genomfört och dokumenterat en riskbedömning över vilka risker som kan störa viktiga/kritiska produkter och tjänster (se även R6 och IC7). Riskbedömningen kan innehålla en identifiering och bedömning av: • Risker som kan leda till ett avbrott i resurser eller prioriterade aktiviteter • Befintlig redundans eller andra skyddsåtgärder • Sannolikheten för att mål för återställningstid överskrids om risken inträffar • Vilka risker som behöver åtgärdas *Riskbedömningen kan göras på prioriterade aktiviteter eller de resurser de är beroende av*.
K7	Organisationen har en eller flera beslutade åtgärdsplaner med åtgärdsförslag.
K8	Organisationen har valt och dokumenterat kontinuitetslösningar dvs. hur de ska hantera störningar i verksamheten, före, under och efter en händelse. *Kontinuitetslösningar kan exempelvis vara att anställa ny personal, teckna avtal med flera leverantörer, omfördela personal och möjliggöra lagerhållning av insatsvaror och reservdelar.*

Nummer	Beskrivning
K9	Organisationen har upprättat och dokumenterat en eller flera kontinuitsplaner som kan innehålla: • Dokumentägare • Syfte och mål • Omfattning • Ansvar och roller • Befogenheter • Aktiveringsrutiner • Reservrutin • Återställningsrutin • Återgångsrutin • Nödvändiga kontaktuppgifter • Övning och utbildning • Rutin för revidering av planen Kontinuitetsplanen är tillgänglig och förankrad i organisationen. *En kontinuitetsplan innehåller dokumenterad information som vägleder en organisation att hantera en störning och återuppta, återställa, och återupprätta leveransen av produkter och tjänster i överenskommelse med dess mål för kontinuitetshantering.*
K10	Organisationen följer upp och utvärderar genomförda åtgärder och kontinuitetslösningar för att säkerställa att de har fått avsedd effekt.

Informations- och cybersäkerhet

Arbetssätt för informations- och cybersäkerhet kan se ut på olika sätt då det behöver integreras med organisationens sätt att leda och styra sin verksamhet men kan i stora drag sammanfattas i nedan checklista.

Se www.msb.se/informationssakerhet för mer stöd i arbetet med att utforma informations- och cybersäkerhetsarbetet i din organisation.

Tabell 4. Checklista – Informations-och cybersäkerhet

Nummer	Beskrivning
IC1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande informations- och cybersäkerhetsarbetet.
IC2	Det finns framtagna mål för arbetet och organisationen arbetar med informations- och cybersäkerhet i det strategiska arbetet. *Det innebär att arbeta systematiskt med att planera, implementera, upprätthålla och förbättra informations- och cybersäkerhet i verksamheten. Exempelvis genom att det är en integrerad del av organisationens övergripande ledningssystem och att det finns som en återkommande punkt på ledningens agenda*.
IC3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande informations- och cybersäkerhet enligt styrande dokument.
IC4	Organisationen arbetar med informations- och cybersäkerhet i det dagliga arbetet utifrån styrande dokument och arbetssätt. *Det kan ske genom att informations- och cybersäkerhet implementeras i redan befintliga processer i organisationen*.
IC5	Organisationen har beslutat och kommunicerat verksamhetens nivå för riskacceptans, vilket används som utgångspunkt vid hantering av riskerna (se även R5 och K5). *Organisationens nivå för riskacceptans, kallas ibland även risktolerans och är de nivåer som organisationen/ ledningen har beslutat ska gälla för att kunna acceptera en risk dvs. behålla risken utan att vidta någon ytterligare åtgärd. Notera att även accepterade risker fortlöpande måste bevakas*.

Nummer	Beskrivning
IC6	Organisationen genomför och dokumenterar informationsklassningar. Detta innebär att informationen värderas utifrån konfidentialitet, riktighet och tillgänglighet. *Här identifieras vilka konsekvenser som uppstår om inte informationen är tillgänglig, riktig eller om den blir röjd till obehörig*.
IC7	Organisationen genomför och dokumenterar riskbedömningar genom att identifiera och analysera risker för informationsbehandlingen, exempelvis utifrån var den bearbetas, förvaras eller kommuniceras (se även R6 och K6). *Riskbedömningen är det arbetssätt som innefattar riskidentifiering, riskanalys och riskutvärdering*.
IC8	Organisationen väljer vilka säkerhetsåtgärder som behöver vidtas för att skydda informationen utifrån resultatet av informationsklassningen och riskbedömningen. Arbetet med att införa åtgärderna inkluderar att ta fram en åtgärdsplan som beskriver: • Vem som ska införa säkerhetsåtgärden. • När den ska vara införd. • Hur organisationen kontrollerar att åtgärden är införd och ger det skydd som behövs. *Säkerhetsåtgärderna kan vara av olika slag tex organisatoriska, personalrelaterade, tekniska eller fysiska*.
IC9	Organisationen har infört tillräckliga säkerhetsåtgärder för att skydda informationen genom att ställa krav på resurser som hanterar information vid informationshantering. *Exempelvis genom att ställa krav på personalens hantering, det fysiska skyddet samt tekniska åtgärder*.
IC10	Organisationen arbetar för att säkerställa kontinuitet för sin information och sina informationssystem, se checklista för kontinuitetshantering. *Se särskilt K5-K9*.
IC11	Organisationen har i styrande dokument för hur informations- och cybersäkerhetsincidenter ska anmälas och arbetssätt för incidenthantering. Detta inkluderar att kommunicera fastställda arbetssätt, roller och ansvarsområden för hantering av informationssäkerhetsincidenter.
IC12	Organisationen följer upp och utvärderar genomförda åtgärder för att säkerställa att de har fått avsedd effekt.

Hantera oönskade händelser

Arbetet med att hantera oönskade händelser kan se ut på olika sätt men kan i stora drag sammanfattas i nedan checklista. Checklistan nedan gäller för alla typer av händelser och kan anpassas därefter.

Se www.msb.se/samverkanledning för mer stöd i arbetet.

Tabell 5. Checklista – Hantera oönskade händelser

Nummer	Beskrivning
H1	En policy gällande incidenthantering och krishantering är upprättad och känd i organisationen.
H2	Det finns framtagna mål för organisationens arbete med att hantera oönskade händelser.
H3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande organisationens hantering av oönskade händelser.

Nummer	Beskrivning
H4	Organisationen har etablerade och dokumenterade arbetssätt för hur en oönskad händelse ska hanteras, inklusive tydliggjorda roller och ansvar: • Internt inom den egna organisationen. • I samverkan med andra aktörer.
H5	Organisationen har etablerade kontakter, nätverk, eller forum med berörda aktörer.
H6	Organisationen har en kontaktpunkt för: • Larmning och samordning internt inom organisationen. • Att samverka med andra aktörer. *Exempelvis TiB, jourhavande befäl, ansvarig chef, inriktnings- och samordningskontakt eller motsvarande*.
H7	Organisationen genomför omvärldsbevakning i syfte att stärka sin hanteringsförmåga. *Omvärldsbevakning genomförs för att aktivt samla in, analysera, värdera och förmedla information som hjälper organisationer att skapa en kunskap om omvärlden som stöd för bättre beslutsfattande i en händelse/kris*.
H8	Organisationen har metoder för att upprätta och kommunicera lägesbilder internt och externt. *En lägesbild är urval av information som sammanställs i form av beskrivningar eller bedömningar av läget. Syftet är att ge överblick, förståelse eller underlag för beslut och åtgärder.*
H9	Organisationen har lämpliga tekniska system och utrustning för att kunna hantera en oönskad händelse som kan påverka samhällsviktiga verksamheter.
H10	Organisationen har rutiner för att dokumentera hanteringen, analyser och beslut före, under och efter en inträffad oönskad händelse.
H11	Organisationen har upprättat en eller flera planer för hantering av oönskade händelser. Planerna kan innehålla följande: • Roller, ansvar och mandat. • Ägare och förvaltare av plan. • Mål och syfte. • Rutin för larmning och aktivering av plan. • Kontaktuppgifter, både internt och till andra aktörer. • Metoder och former för hur oönskade händelser ska hanteras internt samt i samverkan med andra aktörer. • Rutiner för att dela information och skapa lägesbilder. • Rutiner för intern och extern kommunikation. • Rutiner för kriskommunikation. • Rutiner för omvärldsbevakning. • Lokaler och teknisk utrustning. • Rutiner för erfarenhetsåterföring. • Rutiner för utbildning och övning av plan. • Plan för återställande. *Planer kan bestå av en eller flera rutiner, checklistor etc. De används vid när det finns ett behov av att upprätta en krishanteringsorganisation för att hantera den uppkomna händelsen. Dessa planer kan benämnas beredskapsplaner, krishanteringsplaner etc*.
H12	Organisationen har planerat för att kunna genomföra psykiskt och socialt omhändertagande av egen personal.

Bilaga

Bilaga – Standarder och vägledningar

Tabell 6. Standarder och vägledningar

Typ	Referens	År
Systematiskt arbete		
Standard	**ISO 22301** – Samhällssäkerhet – Ledningssystem för kontinuitet – Krav	2019
Standard	**SS 22304** – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Handbok för kontinuitetshantering enligt SS EN ISO 22301	2023
Standard	**ISO 22313** – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för implementering av ISO 22301	2020
Standard	**ISO 22316** – Säkerhet och resiliens – Organisatorisk resiliens - Principer	2020
Standard	**ISO 22318** – Ledningssystem för kontinuitet – Vägledning för kontinuitet i försörjningskedjan (ISO/TS 22318:2021, IDT)	2022
Standard	**ISO 22320** – Krishantering – Krav för Samverkan	2019
Standard	**ISO 22331** – Ledningssystem för kontinuitet – Vägledning för att välja strategi för kontinuitet	2018
Standard	**ISO 22332** – Ledningssystem för kontinuitetshantering – Vägledning för framtagning av planer och processer (ISO/TS 22332:2021)	2021
Standard	**ISO 27000** – Informationsteknik, säkerhetstekniker-ledningssystem för informationssäkerhet – översikt och terminologi	2020
Standard	**ISO 27001** – Informationssäkerhet – Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav	2022
Standard	**ISO 27002** – Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet	2022
Standard	**ISO 27003** – Informationsteknik – Säkerhetstekniker - Vägledning för införande av ledningssystem för informationssäkerhet	2018
Standard	**ISO 27005** – Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning om riskhantering inom informationssäkerhet	2022
Standard	**ISO 31000** – Riskhantering – Vägledning	2018
Standard	**BSI-Standard 100-4** – Business Continuity Management	2009
Standard	**NFPA 1600** – Standard on Disaster/Emergency Management and Business Continuity Programs	2013
Vägledning	**COSO Compliance Risk Management, Applying the Coso ERM Framework**	2020

Typ	Referens	År
Vägledning	**FSPOS Vägledning för kontinuitetshantering** (baseras på standarden SS-ISO 22301:2012 – Samhällssäkerhet – Ledningssystem för kontinuitet)	2024
Vägledning	**FSPOS Vägledning för Krishantering**	2017
Vägledning	**MSB 30128** – Säkerhetsåtgärder i informationssystem	2022
Vägledning	**MSB 1447** – Utvärdering av hantering av inträffade händelser	2019
Riskhantering		
Standard	**ISO 31000** Riskhantering – Vägledning	2018
Standard	**ISO 22316** Säkerhet och resiliens – Organisatorisk resiliens – Principer	2020
Standard	**ISO 27001** – Informationssäkerhet, Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav	2022
Standard	**ISO 27003** – Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet	2018
Standard	**ISO 27005** – Riskhantering för Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning	2022
Vägledning	**COSO Compliance Risk Management, Applying the Coso ERM Framework**	2020
Vägledning	**FSPOS Vägledning för kontinuitetshantering** (Tar bland annat upp hur organisationer kan arbeta med riskbedömning och riskhantering)	2024
Kontinuitetshantering		
Standard	**ISO 22301** – Samhällssäkerhet – Ledningssystem för kontinuitet – Krav	2019
Standard	**SS 22304** – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Handbok för kontinuitetshantering enligt SS EN ISO 22301	2023
Standard	**ISO 22313** – Säkerhet och resiliens – Ledningssystem för kontinuitetshantering – Vägledning för implementering av ISO 22301	2020
Standard	**ISO 22316** – Säkerhet och resiliens – Organisatorisk resiliens – Principer	2020
Standard	**ISO 22317** – Ledningssystem för kontinuitet – Vägledning för konsekvensanalys (ISO/TS 22317:2021, IDT)	2022
Standard	**ISO 22318** – Ledningssystem för kontinuitet – Vägledning för kontinuitet i försörjningskedjan (ISO/TS 22318:2021, IDT)	2022
Standard	**ISO 22331** – Ledningssystem för kontinuitet – Vägledning för att välja strategi för kontinuitet	2018

Typ	Referens	År
Standard	**ISO 22332** – Ledningssystem för kontinuitetshantering – Vägledning för framtagning av planer och processer (ISO/TS 22332:2021)	2021
Standard	**ISO 27002** – Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet	2022
Standard	**BSI-Standard 100-4** – Business Continuity Management	2009
Standard	**NFPA 1600** – Standard on Disaster/Emergency Management and Business Continuity Programs	2013
Vägledning	**FSPOS Vägledning för kontinuitetshantering** (baseras på standarden SS-ISO 22301:2012 – Samhällssäkerhet – Ledningssystem för kontinuitet)	2024
Informations- och cybersäkerhet		
Standard	**ISO 27000** – Informationsteknik, säkerhetstekniker-ledningssystem för informationssäkerhet - översikt och terminologi	2020
Standard	**ISO 27001** – Informationssäkerhet- Cybersäkerhet och integritetsskydd – Ledningssystem för informationssäkerhet – Krav	2022
Standard	**ISO 27002** – Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet	2022
Standard	**ISO 27003** – Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet	2018
Standard	**ISO 27005** – Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning om riskhantering inom informationssäkerhet	2022
Standard	**ISO 22316** – Säkerhet och resiliens – Organisatorisk resiliens – Principer	2020
Standard	**SS-EN IEC 62443-3-2** – IT-säkerhet i industriella automationssystem – Del 3–2: Riskbedömning och systemkonstruktion	2020
Standard	**SS-EN IEC 62443-3-3** – IT-säkerhet i industriella automationssystem – Del 3–3: IT-säkerhet i nät och system – Fordringar på systemets säkerhet och på säkerhetsnivåer	2019
Vägledning	**MSB 30128** – Säkerhetsåtgärder i informationssystem	2022
Hantera oönskade händelser		
Standard	**ISO 22320** – Krishantering – Krav för Samverkan	2019
Standard	**ISO 22316:2020** Säkerhet och resiliens – Organisatorisk resiliens – Principer	2020
Vägledning	**FSPOS Vägledning för Krishantering**	2024
Vägledning	**Gemensamma grunder** – ramverk för samverkan och ledning	2024

Systematiskt arbete

Tabell 7. Checklista – Systematiskt arbete

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
S1	Organisationens ledning har i styrande dokument fastställt övergripande förutsättningar och mål för hur arbetet med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och planering för hantering av oönskade händelser ska genomföras utifrån organisationens förutsättningar.	Målen ska vara baserade på ställda krav mot organisationen, mätbara, kommunicerade och uppdaterade.	**ISO 22301:2019** avsnitt 5.2. **SS 22304:2023** avsnitt 5.2. **ISO 22313:2020** avsnitt 5.2. **ISO 22316:2020** avsnitt 4.1, 4.2. **ISO 22318:2022** avsnitt 5.2.1. **ISO 22320:2019** avsnitt 5.2.1 och 5.3.1. **ISO 27000:2020** avsnitt 3.75, 4.2.1 och 4.6. **ISO 27001:2022** avsnitt 4.4, 5.1–5.2, 6.2, 8.1, 9.3 och 10. **ISO 27002:2022** avsnitt 0.1–0.2, 5.1–5.2, 5.4 och 5.36. **ISO 27003:2018** avsnitt 4.4, 5.1–5.2, 6.2, 8.1, 9.3 och 10. **ISO 31000:2018** avsnitt 5.2 och 5.4.2. **MSB 30128** avsnitt 2.1.3. **COSO** sida 11 och 14. **BSI-Standard-100-4** avsnitt 3.2. **FSPOS vägledning för kontinuitetshantering** avsnitt 3.1.	6§ **i Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**
S2	Organisationen har i styrande dokument och arbetssätt dokumenterat det som behövs för att planera, implementera, använda, följa upp och förbättra organisationens arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och planering för hantering av oönskade händelser för samhällsviktig verksamhet.		**ISO 22301:2019** avsnitt 5.2. **SS 22304:2023** avsnitt 5.2. **ISO 22313:2020** avsnitt 5.2. **ISO 22320:2019** avsnitt 5.3. **ISO 22316:2020** avsnitt 4.1 och 4.2. **ISO 27000:2020** avsnitt 4.6. **ISO 27001:2022** avsnitt 5.1 och 5.2. **ISO 27003:2018** avsnitt 5.3, 6.1 och 6.2. **ISO 31000: 2018** avsnitt 6.3.2, 5.2, 5.4.2, 5.4.3, 5.4.5, 6.2 och 6.5.3.	6§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter**.

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
S3	Organisationen arbetar med omvärldsbevakning för att identifiera händelser som påverkar den samhällsviktiga verksamheten för att kunna fatta effektiva beslut om prioriteringar för riskhantering, kontinuitetshantering, informations- och cybersäkerhet och vid hantering av händelser.		**SS 22304:2023** avsnitt 8.2.1. **ISO 22316:2020** avsnitt 5.3. **ISO 27001:2022** avsnitt, 4.1 och 4.3. **ISO 27003:2018** avsnitt 4.1. **ISO 27005:2022** avsnitt 7.2.1. **ISO 22316:2020** avsnitt 3.4, 4.1, 5.3, 5.10, 6.3.2 och 6.4. **ISO 27005:2022** avsnitt 5.2. **ISO 31000:2018** avsnitt 5.7.1. **COSO** sidan 11. **MSB 30128** avsnitt 2.2.	5 § punkt 4 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 2 kap. 2 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.**
S4	Organisationen utbildar och övar personal som berörs av arbetet med samhällsviktig verksamhet.		**ISO 22301:2019** avsnitt 7.2 och 8.5. **SS 22304:2023** avsnitt 7.2 och 8.5. **ISO 22313:2020** avsnitt 7.2 och 8.5. **ISO 22320:2019** avsnitt 6.3.1. **ISO 27001:2022** avsnitt 7.2b. **ISO 27002:2022** avsnitt 6.3. **ISO 31000:** 2018 avsnitt 5.4.4. **COSO** sidan 33. **MSB 30128** avsnitt 2.1.6. **FSPOS vägledning för kontinuitetshantering** avsnitt E.2 och E.3. **FSPOS vägledning för krishantering** avsnitt 3.4.	9 § punkt 5 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 2 kap. 4 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.** 2 kap. 8 § i **Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.** 8 § och 20 § punkt 11 i **Förordning (2022:524) om statliga myndigheters beredskap.** 5 kap. 1 § i **Säkerhetsskyddsförordning (2021:955).**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
S5	Organisationen har etablerade metoder och planer för intern och extern kommunikation och rapportering för riskhantering, kontinuitetshantering, informations- och cybersäkerhet och vid hantering av händelser.		**ISO 22301:2019** avsnitt 7.4, 8.4.3 och 9.2. **SS 22304:2023** avsnitt 8.4.2 och 9.2. **ISO 22313:2020** avsnitt 7.4, 8.4.3 och 9.2. **ISO 22320:2019** avsnitt 6.2:4. **ISO 27001:2022** avsnitt, 7.4. **ISO 27002:2022** avsnitt 6.8. **ISO 27003:2018** avsnitt 7.4. **ISO 31000:2018** avsnitt 5.4.5, 6.2, 6.4 och 6.5. **FSPOS vägledning för krishantering** avsnitt 3.4.	8 § och 9 § i **Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.** 19 § och 22 § i **Förordning (2022:524) om statliga myndigheters beredskap.**
S6	Organisationen har etablerade arbetssätt för att följa upp och utvärdera arbetet med riskhantering, kontinuitetshantering, informations- och cybersäkerhet samt hantering av oönskade händelser.	Det inkluderar arbetssätt för att utvärdera inträffade händelser och övningar och att följa upp efterlevnaden av interna och externa krav.	**ISO 22301:2019** avsnitt 8.6 och 9. **SS 22304:2023** avsnitt 8.6 och 9. **ISO 22313:2020** avsnitt 9.1.1 och 9.3.3. **ISO 22316:2020** avsnitt 5.9, 6.2.2, 6.3.1 och 6.6. **ISO 22318:2022** avsnitt 6.5 och Bilaga B4. **ISO 22331:2018** avsnitt 7.1 och 7.2. **ISO27000:2020** avsnitt 4.5.6 och 4.5.7. **ISO27001:2022** avsnitt 4.4, 5.2d, 9.1 och 10. **ISO 27003:2018** avsnitt 9.1 och 10.2. **ISO 27005:2022** avsnitt 10.5–6. **ISO 31000:2018** avsnitt 5.6 och 6.6. **BSI-Standard-100-4** kap. 8. **NFPA 1600** kap. 8. **FSPOS vägledning för kontinuitetshantering** avsnitt 3. **FSPOS vägledning för krishantering** avsnitt 3.2–3.3. **MSB1447** Utvärdering av hantering av inträffade händelser.	

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
S7	Organisationen tar till vara erfarenheter från uppföljningar och revisioner av arbetet med riskhantering, kontinuitetshantering och informations- och cybersäkerhet, inträffade händelser och övningar.		**ISO 22301:2019** avsnitt 9.2 och 10. **SS 22304:2023** avsnitt 9.2 och 10. **ISO 22313:2020** avsnitt 9.2-9.3 och 10. **ISO 22316:2020** avsnitt 5.6 och 5.9. **ISO 22318:2022** Bilaga B4. **ISO 22332:2021** avsnitt 12. **ISO 27005:2022** avsnitt 10.6–10.8. **ISO 31000:2018** avsnitt 5.7.2 och 6.1. **COSO** sidan 22–26. **BSI-Standard-100-4** kap. 9. **NFPA 1600** kap. 9. **FSPOS vägledning för krishantering** avsnitt 3.3. **MSB1447** Utvärdering av hantering av inträffade händelser.	

Riskhantering

Tabell 8. Checklista – Riskhantering

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
R1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande riskhantering.		**ISO 27005:2022** avsnitt 6.1. **ISO 31000:2018** avsnitt 5.3, 5.4.2, 5.4.3.	
R2	Det finns framtagna mål för arbetet och organisationen arbetar med riskhanteringen i det strategiska arbetet.	Att arbeta med riskhantering i det strategiska arbetet kan exempelvis ske genom att det ingår i organisationens styrande processer så som planerings- och budgetprocess och att det finns som en återkommande punkt på ledningens agenda.	**ISO 27003:2018** avsnitt 6.3, 8. **ISO 31000:2018** avsnitt 4, 5.1–5.3 och 6.1. **COSO** sidan 11.	7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap.**
R3	Organisationen har tillräckliga resurser för att uppfylla målen gällande riskhantering enligt styrande dokument.	Exempelvis kundkrav och lagkrav. Dessa resurser kan även avsättas till personal, teknik, metod och verktyg, finansiering och information för att hantera sårbarheter och möjliggöra anpassning till förändrade omständigheter.	**ISO 22316:2020** avsnitt 4.2, 5.2, 5.5 och 5.7–5.8. **ISO 27005:2022** avsnitt 6.1. **ISO 31000:2018** avsnitt 5.4.2 och 5.4.4. **COSO** sidan 8.	
R4	Organisationen arbetar med riskhanteringen i det dagliga arbetet.	Exempelvis genom att riskhantering implementeras i redan befintliga processer i organisationen och att alla inom organisationen ansvarar för att hantera risker.	**ISO 27001:2022** avsnitt 8. **ISO 27003:2018** avsnitt 6.3. **ISO 31000:2018** avsnitt 4, 5.1–5.3 och 6.1.	

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
R5	Organisationen har beslutat och kommunicerat verksamhetens nivå för riskacceptans, vilket används som utgångspunkt vid hantering av riskerna (se även K5 och IC5).	Organisationens nivå för riskacceptans, kallas ibland även risktolerans och är de nivåer som organisationen/ ledningen har beslutat ska gälla för att kunna acceptera en risk dvs. behålla risken utan att vidta någon ytterligare åtgärd. Notera att även accepterade risker fortlöpande måste bevakas.	**ISO 27005:2022** avsnitt 6.4.2. **ISO 31000:2018** avsnitt 6.3.4. **FSPOS vägledning kontinuitetshantering** avsnitt 2.4.2.	
R6	Organisationen genomför regelbundet bedömningar av risker och sårbarheter i verksamheten och dessa innehåller bland annat: • Identifiering av verksamhetens risker, sårbarheter och förmågor. • Sannolikhet för och konsekvens av att riskerna inträffar. • Värdering och prioritering av riskerna i relation till verksamhetens mål/krav. • Åtgärdsplan för hantering av riskerna.	Bedömningarna avser att skaffa organisationen en tillräckligt bra bild över vilka interna och externa risker som finns kopplat till verksamheten. Dessa bedömningar kan genomföras inom en rad olika områden bl.a. riskanalys för intern styrning och kontroll, försäkringsmässiga riskanalyser samt risk- och sårbarhetsanalyser.	**ISO 27005:2022** avsnitt 7. **ISO 31000:2018** avsnitt 6.4.2–6.4.4 och 6.5. **COSO** sidan 15–25.	7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap.** 3 § i **Förordning (2018:1343) om intern styrning och kontroll.**
R7	Organisationen beslutar och genomför åtgärder enligt beslutad åtgärdsplan för riskerna.		**ISO 27005:2022** avsnitt 8.6. **ISO 31000:2018** avsnitt 6.5.3. **COSO** sidan 22–26.	
R8	Organisationen följer upp och utvärderar genomförda åtgärder för att säkerställa att de minskat riskerna som förväntat.		**ISO 22316:2020** avsnitt 6.3.1, 6.2.2. **ISO 27005:2022** avsnitt 10.5. **ISO 31000:2018** avsnitt 5.6, 6.6. **COSO** sidan 22–26.	

Kontinuitetshantering

Tabell 9. Checklista – Kontinuitetshantering

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
K1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande kontinuitetshantering.		**ISO 22301:2019** avsnitt 5.2–5.3, 7.3, 8.4.2 och 8.4.4. **SS 22304:2023** avsnitt 5.2–5.3, 7.3, 8.4.2 och 8.4.4. **ISO 22313:2020** avsnitt 5.2–5.3, 7.1.2, 7.3, 7.5 och Tabell 3. **ISO 22317:2022** 4.3.1. **ISO 22318:2022** 5.2.1 och 5.2.3. **ISO 22331:2018** 4.4.1. **BSI-Standard-100-4** avsnitt 3.2, 4.5 och 4.6. **FSPOS Vägledning för kontinuitetshantering** avsnitt 3.1 och appendix A.	
K2	Det finns framtagna mål för arbetet och organisationen arbetar med kontinuitetshantering i det strategiska arbetet.	Exempelvis genom att det är en integrerad del av organisationens övergripande ledningssystem och att det finns som en återkommande punkt på ledningens agenda.	**ISO 22301:2019** avsnitt 6.2 och 7.3. **SS 22304:2023** avsnitt 6.2 och 7.3. **ISO 22313:2020** avsnitt 6.2.2.och 7.3. **ISO 22316:2020** avsnitt 5.2. **ISO 22331:2018** avsnitt 4.4.2–4.4.4, 4.5 och 5.6.4. **BSI-Standard-100-4** avsnitt 4.6. **FSPOS Vägledning för kontinuitetshantering** avsnitt 3.1 och Appendix A.	10 § och 19–20 §§ i **Förordning (2022:524) om statliga myndigheters beredskap.**
K3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande kontinuitetshantering enligt styrande dokument.		**ISO 22301:2019** avsnitt 5.1, 6.2.2 och 7.1. **SS 22304** avsnitt 5.1, 5.3, 6.2.2 och 7.1. **ISO 22316:2020** avsnitt 4.2, 5.5 och 5.7. **ISO 22318:2022** avsnitt 5.2.2.	
K4	Organisationen arbetar med kontinuitetshantering i det dagliga arbetet.	Det kan ske genom att kontinuitetshantering implementeras i redan befintliga processer i organisationen.	**ISO 22301:2019** avsnitt 7.2–7.3. **SS 22304:2023** avsnitt 7.2–7.3. **ISO 22313:2020** avsnitt 5.1.3, 7.2 och 7.3. **ISO 22316:2020** avsnitt 5.8. **ISO 22318:2022** avsnitt 4.2.2. **NFPA 1600** avsnitt 8.1.1. **BSI-Standard-100-4** avsnitt 4.6.	10 § och 19–20 §§ i **Förordning (2022:524) om statliga myndigheters beredskap.** 13 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter MSBFS 2020:6.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
K5	Organisationen har genomfört och dokumenterat en konsekvensanalys om störningar inträffar i organisationens leveranser av viktiga/kritiska produkter och tjänster som kan innehålla: • En kriteriemodell (eller motsvarande) för att bedöma konsekvenser av avbrott (se även R5 och IC5). • Vilka aktiviteter som behövs för att leverera produkter och tjänster. • Vilka konsekvenser ett avbrott i dessa aktiviteter har för organisationen genom bedömning med hjälp av kriteriemodellen. • Definition av hur länge aktiviteten kan ligga nere utan att konsekvenserna blir oacceptabla för verksamheten (acceptabel avbrottstid). • Identifierade prioriterade aktiviteter. • Fastställda resurser (beroenden) inklusive partners och leverantörer som behövs för att utföra de prioriterade aktiviteterna. • Identifierade återställningstider för resurserna.		**ISO 22301:2019** avsnitt 4.3.2 och 8.2.2. **SS 22304:2023** avsnitt 4.3.2 och 8.2.2. **ISO 22313:2020** avsnitt 4.3.2 och 8.2.2. **ISO 22317:2022** Tabell 3, 5.5–5.6 och Bilaga D. **ISO 22318:2022** avsnitt 5.4.2. **ISO 22331:2018** avsnitt 5.2 och 4.7. **ISO 27002:2022** avsnitt 5.30. **FSPOS Vägledning för kontinuitetshantering** Appendix B och B.1–2.	7 § punkt 1 och 3 i **Förordning (2022:524) om statliga myndigheters beredskap.**
K6	Organisationen har genomfört och dokumenterat en riskbedömning över vilka risker som kan störa viktiga/kritiska produkter och tjänster (se även R6 och IC7). Riskbedömningen kan innehålla en identifiering och bedömning av: • Risker som kan leda till ett avbrott i resurser eller prioriterade aktiviteter. • Befintlig redundans eller andra skyddsåtgärder. • Sannolikheten för att mål för återställningstid överskrids om risken inträffar. • Vilka risker som behöver åtgärdas.	Riskbedömningen kan göras på prioriterade aktiviteter eller de resurser de är beroende av.	**ISO 22301:2019** avsnitt 8.2.3. **SS 22304:2023** avsnitt 8.2.3. **ISO 22313:2020** avsnitt 8.2.3. **FSPOS Vägledning för kontinuitetshantering** Appendix B och B3-4.	7 § punkt 2 i **Förordning (2022:524) om statliga myndigheters beredskap.**
K7	Organisationen har en eller flera beslutade åtgärdsplaner med åtgärdsförslag.		**ISO 22301:2019** avsnitt 8.3. **SS 22304:2023** avsnitt 8.3. **ISO 22313:2020** avsnitt 8.3.	

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
K8	Organisationen har valt och dokumenterat kontinuitetslösningar dvs. hur de ska hantera störningar i verksamheten, före, under och efter en händelse.	Kontinuitetslösningar kan exempelvis vara att anställa ny personal, teckna avtal med flera leverantörer, omfördela personal och möjliggöra lagerhållning av insatsvaror och reservdelar.	**ISO 22301:2019** avsnitt 4.4, 8.3.2 och 8.4.4–8.4.5. **SS 22304:2023** avsnitt 4.4, 8.3 och 8.4.4–8.4.5. **ISO 22313:2020** avsnitt 8.3.2. **ISO 22331:2018** avsnitt 5.2, 5.5.4 och 5.6. **NFPA 1600** avsnitt 6.7.1.	
K9	Organisationen har upprättat och dokumenterat en eller flera kontinuitsplaner som kan innehålla: • Dokumentägare. • Syfte och mål. • Omfattning. • Ansvar och roller. • Befogenheter. • Aktiveringsrutiner. • Reservrutin. • Återställningsrutin. • Återgångsrutin. • Nödvändiga kontaktuppgifter. • Övning och utbildning. • Rutin för revidering av planen. Kontinuitetsplanen är tillgänglig och förankrad i organisationen.	En kontinuitetsplan innehåller dokumenterad information som vägleder en organisation att hantera en störning och återuppta, återställa, och återupprätta leveransen av produkter och tjänster i överenskommelse med dess mål för kontinuitetshantering.	I**SO 22301:2019** avsnitt 8.4.3–8.4.5. **SS 22304:2023** avsnitt 8.4.3–8.4.5. **ISO 22313:2020** avsnitt 8.4.4.3. **ISO 22332:2021** avsnitt 9,10 och 11. **NFPA 1600** avsnitt 6.1.1 och 6.7.1. **BSI-Standard-100-4** avsnitt 7.4.4, 7.4.5 och Bilaga A. **FSPOS Vägledning för kontinuitetshantering** avsnitt 3.4, Appendix D och H.	
K10	Organisationen följer upp och utvärderar genomförda åtgärder och kontinuitetslösningar för att säkerställa att de har fått avsedd effekt.		**ISO 22301:2019** avsnitt 8.5, 8.6. **SS 22304:2023** avsnitt 8.5, 8.6. **ISO 22313:2020** avsnitt 8.5, 8.6. **FSPOS Vägledning för kontinuitetshantering** Appendix H.	

Informations- och cybersäkerhet

Tabell 10. Checklista – Informations- och cybersäkerhet

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
IC1	En policy är upprättad och organisationen har implementerade och dokumenterade beskrivningar för roller och ansvar gällande informations- och cybersäkerhetsarbetet.		**ISO 27000:2020** avsnitt 4.2.1. **ISO 27001:2022** avsnitt 5.1h, 5.2–5.3, 7.2 och 7.3a. **ISO 27002:2022** avsnitt 5.2–5.3, 5.4d, 5.12 och 6.1. **ISO 27003:2018** avsnitt 5.3, 7.2 och Bilaga A. **ISO 27005:2022** avsnitt 10.2. **MSB 30128** avsnitt 2.1.3–2.1.4 och 2.1.6.	2 kap. 2 § och 5 kap. i **Säkerhetsskyddsförordning (2021:955).** 4–6 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 2 kap. 1 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.**
IC2	Det finns framtagna mål för arbetet och organisationen arbetar med informations- och cybersäkerhet i det strategiska arbetet.	Det innebär att arbeta systematiskt med att planera, implementera, upprätthålla och förbättra informations- och cybersäkerhet i verksamheten. Exempelvis genom att det är en integrerad del av organisationens övergripande ledningssystem och att det finns som en återkommande punkt på ledningens agenda.	**ISO 22316:2020** avsnitt 4.2, 5.2, 5.4–5.5 och 5.7–5.8. **ISO 27000:2020** avsnitt 3.75, 4.2.1 och 4.6. **ISO 27001:2022** avsnitt 4.4, 5.1–5.2, 6.2, 8.1, 9.3 och 10. **ISO 27002:2022** avsnitt 0.1–0.2, 5.1–5.2, 5.4. och 5.36. **ISO 27003:2018** avsnitt 4.4, 5.1–5.2, 6.2, 8.1, 9.3 och 10. **MSB 30128** avsnitt 2.1.3.	4–6 §§ och 14–15 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**
IC3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande informations- och cybersäkerhet enligt styrande dokument.		I**SO 27001:2022** avsnitt 5.1C. **ISO 27003:2018** avsnitt 7.1.	5 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
IC4	Organisationen arbetar med informations- och cybersäkerhet i det dagliga arbetet utifrån styrande dokument och arbetssätt.	Det kan ske genom att informations- och cybersäkerhet implementeras i redan befintliga processer i organisationen.	I**SO 27001:2022** avsnitt 8. **ISO 27005:2022** avsnitt 6.3.	8 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 6 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**
IC5	Organisationen har beslutat och kommunicerat verksamhetens nivå för riskacceptans, vilket används som utgångspunkt vid hantering av riskerna (se även R5 och K5).	Organisationens nivå för riskacceptans, kallas ibland även risktolerans och är de nivåer som organisationen/ledningen har beslutat ska gälla för att kunna acceptera en risk dvs. behålla risken utan att vidta någon ytterligare åtgärd. Notera att även accepterade risker fortlöpande måste bevakas.	**ISO 27000:2020** avsnitt 3.62, 4.5.4. **ISO 27001:2022** avsnitt 6.1.2a1. **ISO 27003:2018** avsnitt 6.1.2a1. **ISO 27005:2022** avsnitt 6.4.1–2.	
IC6	Organisationen genomför och dokumenterar informationsklassningar. Detta innebär att informationen värderas utifrån konfidentialitet, riktighet och tillgänglighet.	Här identifieras vilka konsekvenser som uppstår om inte informationen är tillgänglig, riktig eller om den blir röjd till obehörig.	**ISO 27002:2022** avsnitt 5.12.	8 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 6 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
IC7	Organisationen genomför och dokumenterar riskbedömningar genom att identifiera och analysera risker för informationsbehandlingen, exempelvis utifrån var den bearbetas, förvaras eller kommuniceras (se även R6 och K6).	Riskbedömningen är det arbetssätt som innefattar riskidentifiering, riskanalys och riskutvärdering.	**SS-EN IEC 62443-3-2:2020** avsnitt 4.3.1, 4.5.2, 4.6. **ISO27000:2020** avsnitt 3.64, 4.2.3 och 4.5.3. **ISO 27001:2022** avsnitt 6.1.1–6.1.2, 6.1.3, 7.5.2 och 8.2. **ISO 27002:2022** avsnitt 5.7, 5.9 och 5.12. **ISO 27003:2022** avsnitt 6.1.2. **ISO 27005:2022** avsnitt 6.3 och 7–9. **MSB 30128** avsnitt 2.3.	2 kap. 1 § i **Säkerhetsskyddsförordning (2021:955).** 7 § och 17 § i **Förordning (2022:524) om statliga myndigheters beredskap.** 8 § punkt 2 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 4–5 §§ och 6 § punkt 1 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 2 kap. 1 § och 3 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.**
IC8	Organisationen väljer vilka säkerhetsåtgärder som behöver vidtas för att skydda informationen utifrån resultatet av informationsklassningen och riskbedömningen. Arbetet med att införa åtgärderna inkluderar att ta fram en åtgärdsplan som beskriver: • Vem som ska införa säkerhetsåtgärden. • När den ska vara införd. • Hur organisationen kontrollerar att åtgärden är införd och ger det skydd som behövs.	Säkerhetsåtgärderna kan vara av olika slag tex organisatoriska, personalrelaterade, tekniska eller fysiska.	**ISO 27000:2020** avsnitt 4.5.4–4.5.5. **ISO 27001:2022** avsnitt 6.1.3 och 8.3. **ISO 27003:2018** avsnitt 6.1.3. **ISO 27005:2022** avsnitt 8.3–6. **MSB 30128** avsnitt 2.3.7.	8 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 6 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
IC9	Organisationen har infört tillräckliga säkerhetsåtgärder för att skydda informationen genom att ställa krav på resurser som hanterar information vid informationshantering.	Exempelvis genom att ställa krav på personalens hantering, det fysiska skyddet samt tekniska åtgärder.	**ISO 27001:2022** avsnitt 8.3. **ISO 27002:2022** avsnitt 5, 5.18–5.20, 5.30, 6.1, 7–7.9 och 8–8.28. **ISO 27003:2018** avsnitt 8.1. **ISO 27005:2022** avsnitt 9.2. **SS-EN IEC 62443-3-3** avsnitt 5–11. **MSB 30128** avsnitt 2.1–2.1.7, 4.1–4.6, 4.9–4.10,4.11, 4.13–4.14 och 5.1.	3–5 kap. i **Säkerhetsskyddsförordning (2021:955).** 8 § punk 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 6 § punkt 3 och 4 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 4 kap. 1 § och 22 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.**
IC10	Organisationen arbetar med förebyggande säkerhetsåtgärder för att säkerställa kontinuitet för sin information och sina informationssystem, se checklista för kontinuitetshantering.	Se särskilt K.5-K.9.	**ISO 27002:2022** avsnitt 5.29–5.30 och 8.13–8.14. **SS-EN IEC 62443-3-3** avsnitt 11. **MSB 30128** avsnitt 4.14.	12 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 13 § **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 4 kap. 22 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standard eller vägledning	Koppling till författningar
IC11	Organisationen har i styrande dokument för hur informations- och cybersäkerhetsincidenter ska anmälas och arbetssätt för incidenthantering. Detta inkluderar att kommunicera fastställa llda arbetssätt, roller och ansvarsområden för hantering av informationssäkerhetsincidenter.		**ISO 27002:2022** avsnitt 5.24-5.27 och 6.8.	14 § i **Förordning (2022:524) om statliga myndigheters beredskap.** 11 § i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 1–12 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.** 2–7 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:8) om rapportering av it-incidenter för statliga myndigheter.** 2 kap. 1–5 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:5) om rapportering av it-incidenter för leverantörer av samhällsviktiga tjänster.**
IC12	Organisationen följer upp och utvärderar genomförda åtgärder för att säkerställa att de har fått avsedd effekt.		**ISO 27001:2022** avsnitt 9 och 10.	6 § punkt 3, 8 § punkt 4 och 9 § punkt 3 i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.** 5 § punkt 5, 6 § punkt 4 och 14–15 §§ i **Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.**

Hantera oönskade händelser

Tabell 11. Checklista – Hantera oönskade händelser

Nummer	Beskrivning	Hjälptext	Hänvisning till standardeller vägledning	Koppling till författningar
H1	En policy gällande incidenthantering och krishantering är upprättad och känd i organisationen.		**ISO 22320:2019** avsnitt 4.	
H2	Det finns framtagna mål för organisationens arbete med att hantera oönskade händelser.		**ISO 22320:2019** avsnitt 5.2.1 och 5.3.1.	
H3	Organisationen har tillräckliga resurser för att uppfylla målen/kraven gällande organisationens hantering av oönskade händelser.		**ISO 22316:2020** avsnitt 4.2, 5.2, 5.5 och 5.7–5.8. **ISO 22320:2019** avsnitt 5.2.1f, 5.2.4b, 5.3.3.4, 5.3.4 och Bilaga B6.	15 § i **Förordning (2022:524) om statliga myndigheters beredskap.**
H4	Organisationen har etablerade och dokumenterade arbetssätt för hur en oönskad händelse ska hanteras, inklusive tydliggjorda roller och ansvar: • Internt inom den egna organisationen. • I samverkan med andra aktörer.		**ISO 22301:2019** avsnitt 8.4–8.4.3. **SS 22304:2023** avsnitt 8.4–8.4.3. **ISO 22313:2020** avsnitt 8.4–8.4.3. **ISO 22320:2019** avsnitt 5.3.1. **FSPOS vägledning för krishantering** avsnitt 3.1. **Gemensamma grunder** – ramverk för samverkan och ledning/arbetssätt/aktörsgemensam inriktning och samordning.	6 § i **Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.**
H5	Organisationen har etablerade kontakter, nätverk, eller forum med berörda aktörer.		**ISO 22301:2019** avsnitt 8.4–8.4.3. **SS 22304:2023** avsnitt 8.4–8.4.3. **ISO 22313:2020** avsnitt 8.4–8.4.3. **ISO 22320:2019** avsnitt 6.2.3–6.2.4 och Bilaga A3. **Gemensamma grunder** – ramverk för samverkan och ledning.	9 § i **Förordning (2022:524) om statliga myndigheters beredskap.** 6 § i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap.**

Nummer	Beskrivning	Hjälptext	Hänvisning till standardeller vägledning	Koppling till författningar
H6	Organisationen har en kontaktpunkt för: • Larmning och samordning internt inom organisationen. • Att samverka med andra aktörer.	Exempelvis TiB, jourhavande befäl, ansvarig chef, inriktnings- och samordningskontakt eller motsvarande.	**ISO 22320:2019** avsnitt C3. **Gemensamma grunder** – ramverk för samverkan och ledning.	2 § i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap.** 15 § i **Förordning (2022:524) om statliga myndigheters beredskap.**
H7	Organisationen genomför omvärldsbevakning i syfte att stärka sin hanteringsförmåga.	Omvärldsbevakning genomförs för att aktivt samla in, analysera, värdera och förmedla information som hjälper organisationer att skapa en kunskap om omvärlden som stöd för bättre beslutsfattande i en händelse/kris.	**ISO 22316:2020** avsnitt 5.3. **Gemensamma grunder** – ramverk för samverkan och ledning.	15 § i **Förordning (2022:524) om statliga myndigheters beredskap.**
H8	Organisationen har metoder för att upprätta och kommunicera lägesbilder internt och externt.	En lägesbild är urval av information som sammanställs i form av beskrivningar eller bedömningar av läget. Syftet är att ge överblick, förståelse eller underlag för beslut och åtgärder.	**ISO 22320:2019** avsnitt 5.2.1h och 5.3.3.1h. **FSPOS vägledning för krishantering** avsnitt 3.1.2 och 3.2.2. **Gemensamma grunder** – ramverk för samverkan och ledning/arbetssätt/lägesbild.	12 § i **Förordning (2022:524) om statliga myndigheters beredskap.** 4 § 1 punkten i **Förordning (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap.**
H9	Organisationen har lämpliga tekniska system och utrustning för att kunna hantera en oönskad händelse som kan påverka samhällsviktiga verksamheter.		**ISO 22320:2019** avsnitt 6.3.3.	
H10	Organisationen har rutiner för att dokumentera hanteringen, analyser och beslut före, under och efter en inträffad oönskad händelse.		**SS 22304:2023** avsnitt 8.4.2. **ISO 22320:2019** avsnitt 6.2.5.	

Nummer	Beskrivning	Hjälptext	Hänvisning till standardeller vägledning	Koppling till författningar
H11	Organisationen har upprättat en eller flera planer för hantering av oönskade händelser. Planerna kan innehålla följande: • Mål och syfte. • Rutin för larmning och aktivering av plan. • Kontaktuppgifter, både internt och till andra aktörer. • Metoder och former för hur oönskade händelser ska hanteras internt samt i samverkan med andra aktörer. • Rutiner för att dela information och skapa lägesbilder. • Rutiner för intern och extern kommunikation. • Rutiner för kriskommunikation. • Rutiner för omvärldsbevakning. • Lokaler och teknisk utrustning. • Rutiner för erfarenhetsåterföring. • Rutiner för utbildning och övning av plan. • Plan för återställande.	Planer kan bestå av en eller flera rutiner, checklistor etc. De används vid händelse där det finns ett behov av att upprätta en krishanteringsorganisation för att hantera den uppkomna händelsen. Dessa planer kan benämnas beredskapsplaner, krishanteringsplaner etc.	**ISO 22301:2019** avsnitt 8.4.2. **ISO 22320:2019** avsnitt 5.3.1–5.3.3. **FSPOS vägledning för krishantering** avsnitt 3.1.3 och 3.2.1.	2 kap. 1 § och 8 § **islag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap genom.**
H12	Organisationen har planerat för att kunna genomföra psykiskt och socialt omhändertagande av egen personal.		**ISO 22320** avsnitt 4.3.	

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2401 – augusti 2024 ISBN 978-91-7927-530-3