KONFERENSEN

INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

14–15 SEPTEMBER 2016

Myndigheten för samhällsskydd och beredskap

Kontinuitetshantering i samhällsviktig verksamhet

Spår 1: Informationssäkerhet i kommuner
15 september 2016

Omar Harrami

Myndigheten för samhällsskydd och beredskap

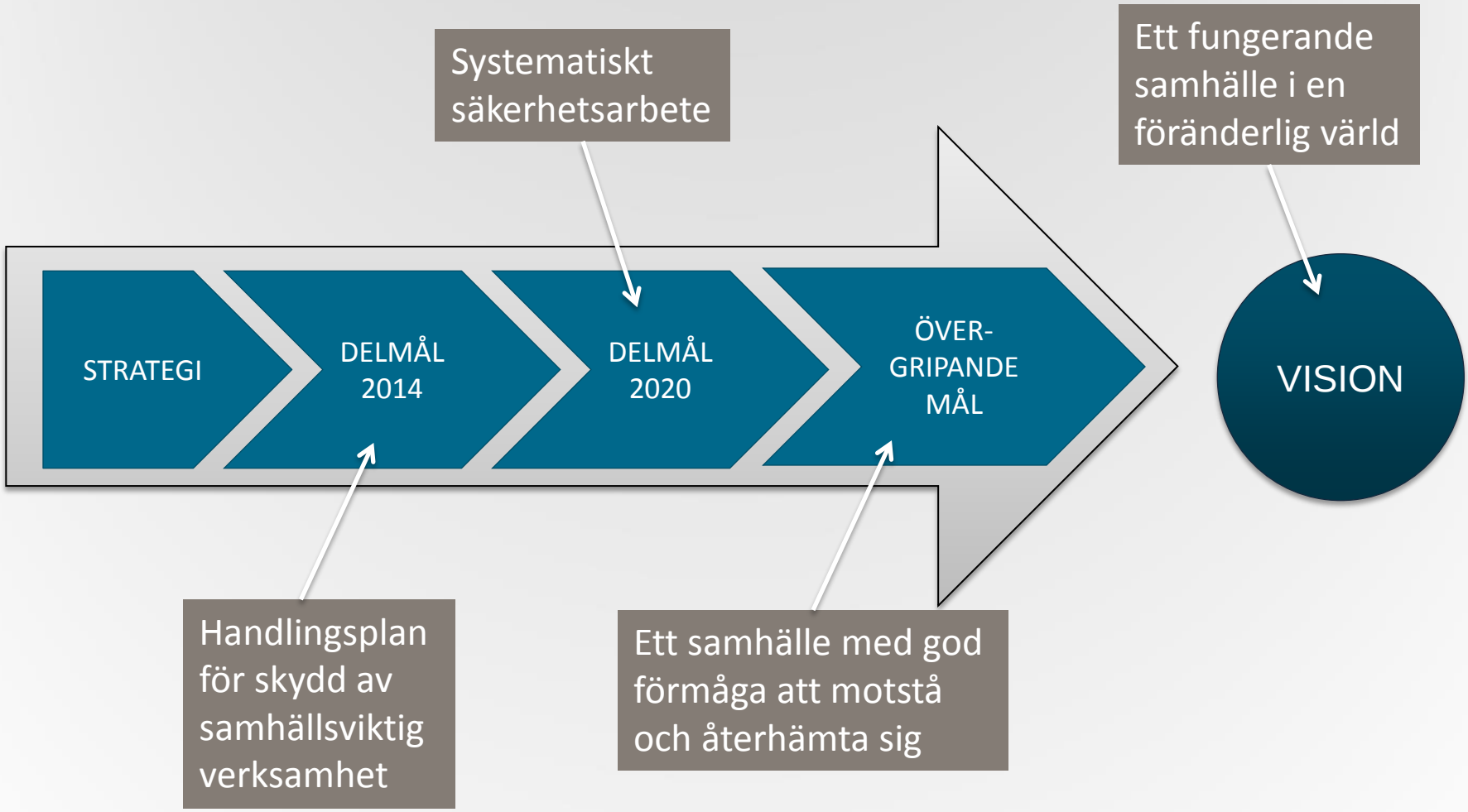
Innehåll

- Strategi och handlingsplan Skydd av samhällsviktig verksamhet
- Stöd för Systematisk säkerhetsarbete
- **Vägledning Kontinuitetshantering**

Myndigheten för samhällsskydd och beredskap

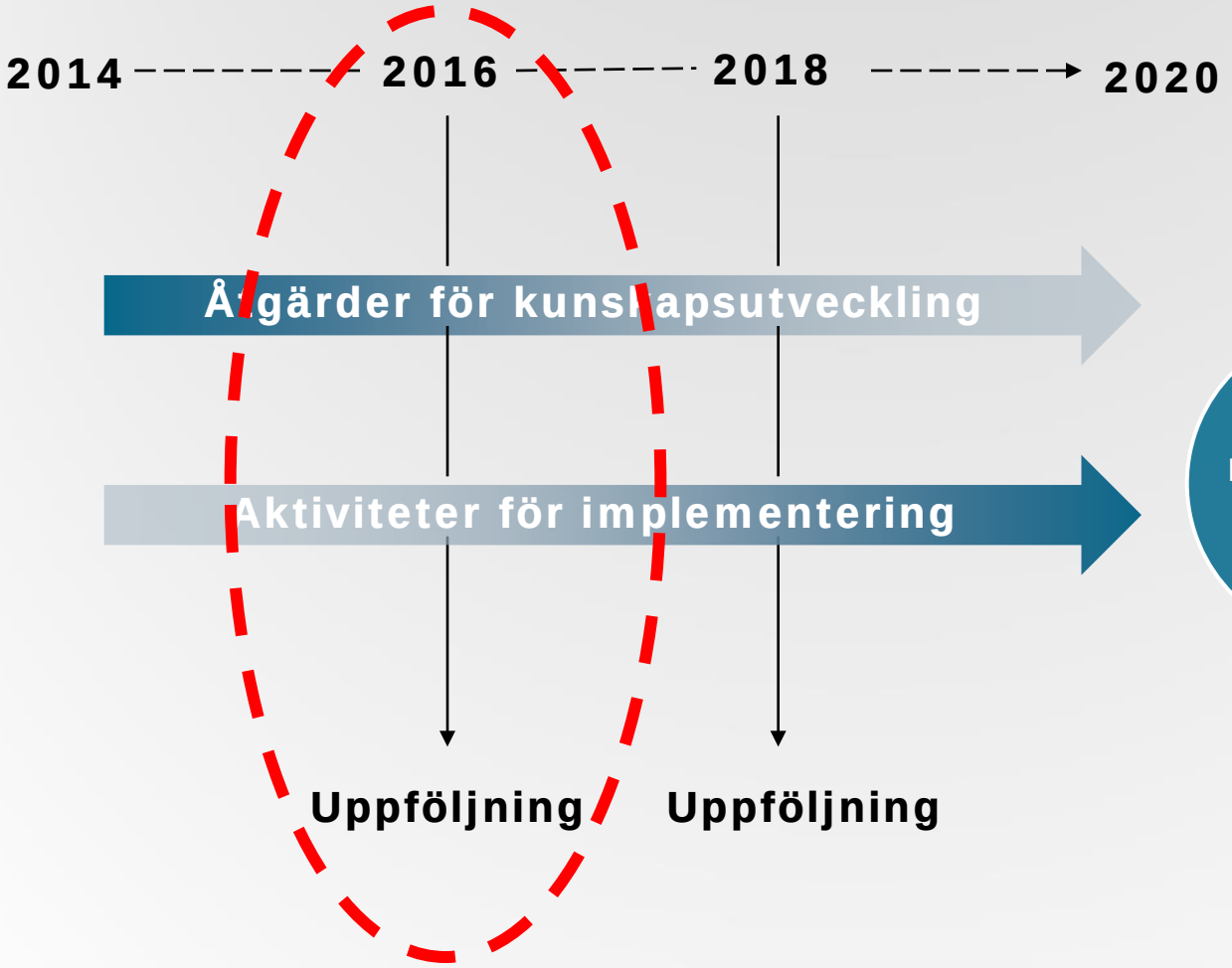
Strategi och handlingsplan för skydd av samhällsviktig verksamhet

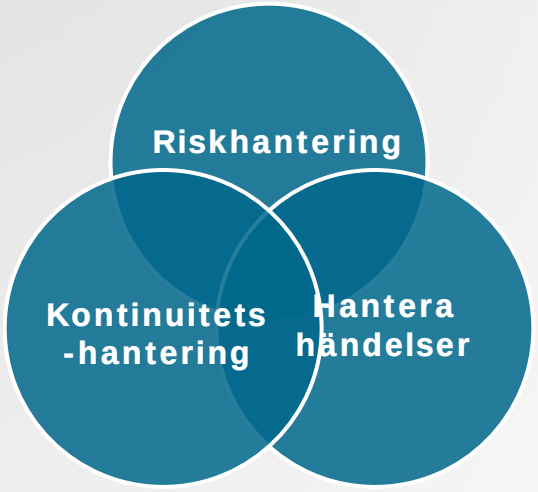
Myndigheten för samhällsskydd och beredskap



Myndigheten för samhällsskydd och beredskap

Uppföljning av handlingsplanen 2016

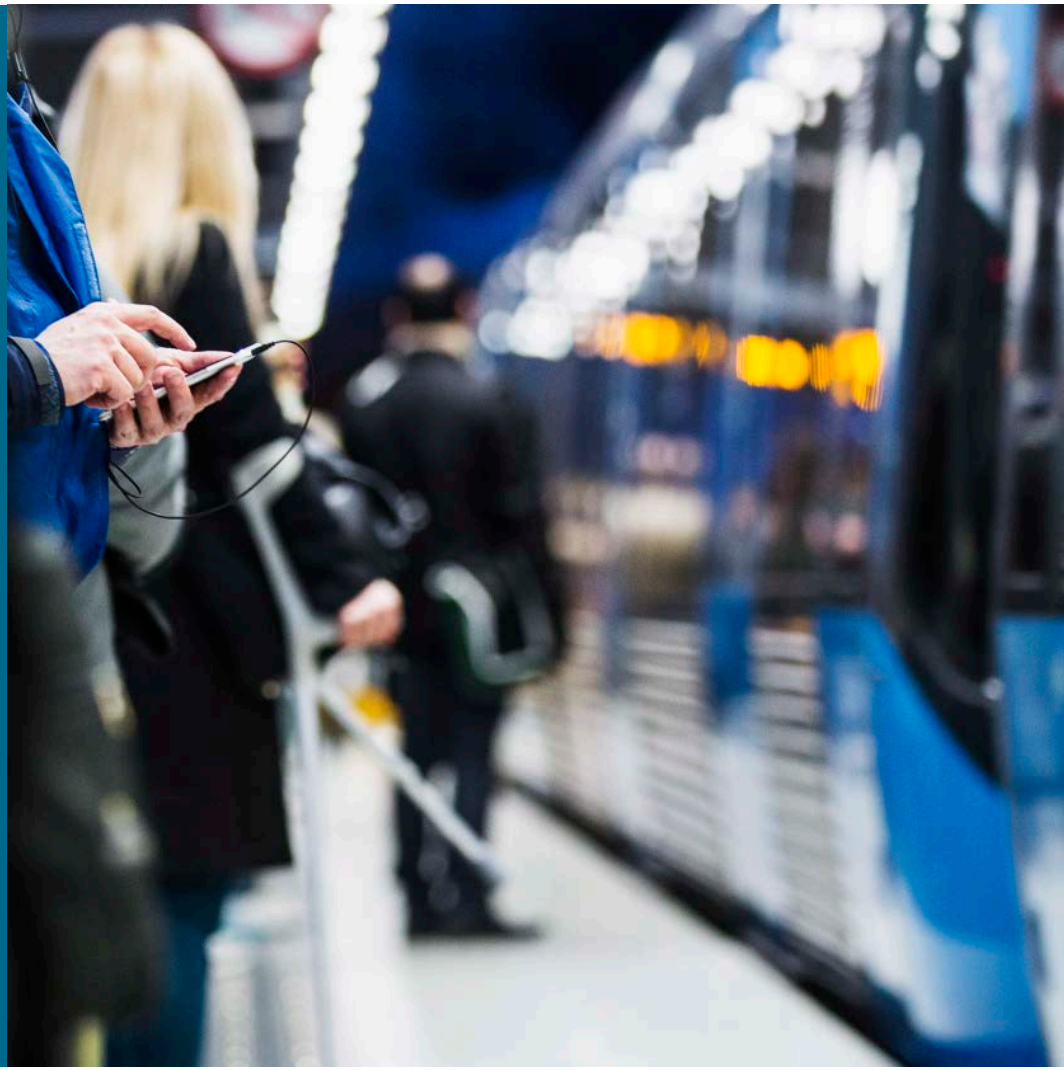




Myndigheten för samhällsskydd och beredskap

Systematiskt arbete med skydd av samhällsviktig verksamhet

Stöd för arbete med riskhantering, kontinuitetshantering och hantera händelser



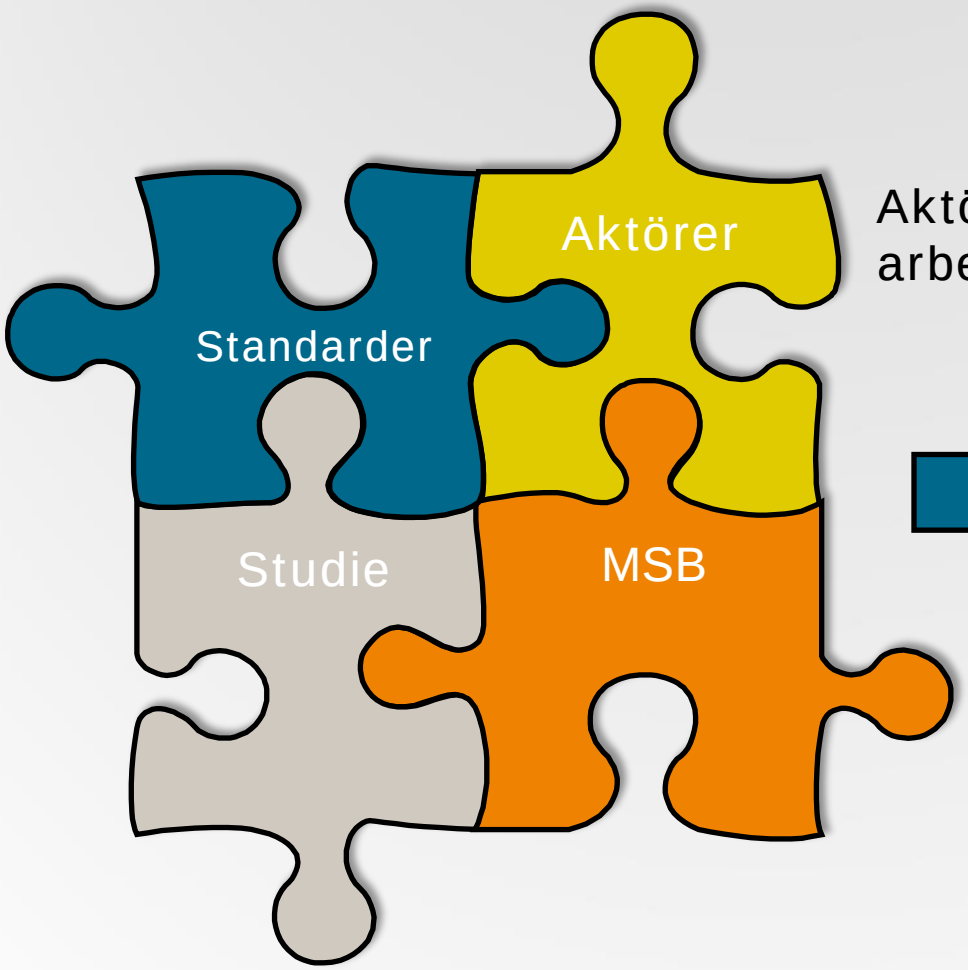
Myndigheten för samhällsskydd och beredskap

Stödet

- Konkretiserar vad som kan ingå i arbetet med riskhantering, kontinuitetshantering och att hantera händelser.
- Kan stödja aktörerna att nå handlingsplanens mål; **att all samhällsviktig verksamhet har integrerat ett systematiskt arbete i sin verksamhet på lokal, regional och nationell nivå senast 2020**.
- Vänder sig till privata och offentliga aktörer.

Myndigheten för samhällsskydd och beredskap

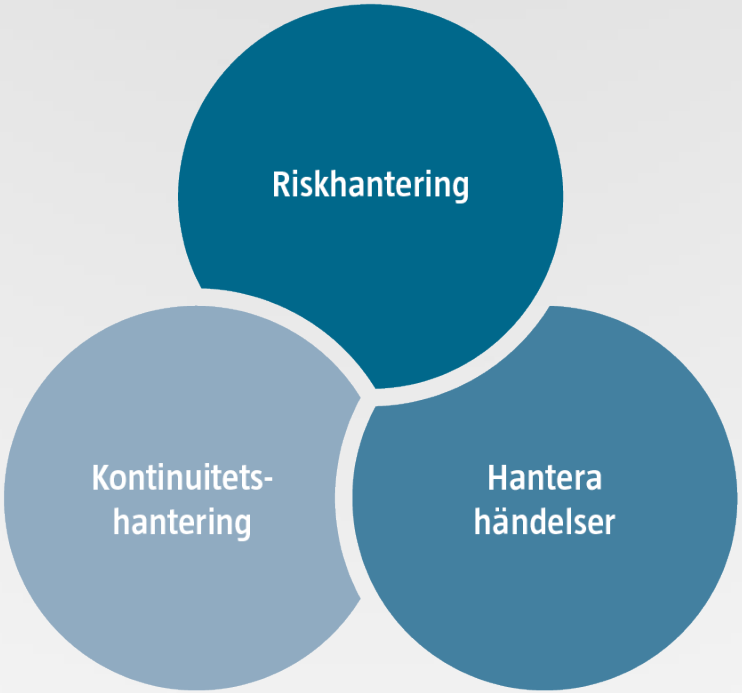
Hur stödet växt fram



Aktörerna har styrt arbetet

Myndigheten för samhällsskydd och beredskap

Systematiskt arbete med skydd av samhällsviktig verksamhet



Myndigheten för samhällsskydd och beredskap

Systematiskt arbete

Övergripande komponenter

Styrande dokument	
1	Förutsättningar och utgångspunkter
2	Innehåll i styrande dokument
3	Interna och externa aktörer
Utbildning och övning	
4	Utbildning och övning av relevant personal
Information och kommunikation	
5	Etablerade metoder

Myndigheten för samhällsskydd och beredskap

Riskhantering	
1	Roller och ansvar
2	Resurser för arbetet
3	Strategiska arbetet
4	Dagliga arbetet
5	Riskacceptans
6	Bedömning av risker och sårbarheter i verksamheten
7	Åtgärdsplan
8	Följa upp och utvärdera

Myndigheten för samhällsskydd och beredskap

Kontinuitetshantering	
1	Roller och ansvar
2	Strategiska arbetet
3	Dagliga arbetet
4	Konsekvensanalys
5	Bedömning av risker som kan störa
6	Hantering av störningar
7	Kontinuitetsplan
8	Följa upp och utvärdera
9	Omhändertagande av erfarenheter

Myndigheten för samhällsskydd och beredskap

Hantera händelser	
1	Metoder, former, ansvar och roller
2	Kontakter, nätverk eller forum
3	Kontaktpunkt
4	Omvärldsbevakning
5	Lägesbild
6	Tekniska system och utrustning
7	Dokumentation
8	Planer för hantering
9	Psykiskt och socialt omhändertagande
10	Uppföljning och utvärdering
11	Omhändertagande av erfarenheter

Myndigheten för samhällsskydd och beredskap

Bilaga – Från standard till komponent

TYP	REFERENS	ÅR
Riskhantering		
Standard	**ISO 31000 Riskhantering** – Principer och riktlinjer innehåller principer och generella riktlinjer för riskhantering och kan användas av offentliga, privata eller kommunala verksamheter, organisationer, grupper eller individer.	2009
Vägledning	**COSO Enterprise Risk Management Framework** är framtaget som hjälp att sortera och strukturera organisationens risker.	-
Kontinuitetshantering		
Standard	**ASIS/BSI BCM.01** – Business Continuity Management Systems ger kontrollerbara kriterier med tillhörande vägledning för att utveckla och implementera ett ledningssystem för kontinuitet som förbättrar en organisations förmåga att förbereda sig för, hantera och återhämta sig från störningar.	2010
Standard	**BSI-Standard 100-4** – Business Continuity Management presenterar en metod för att på ett systematiskt sätt att utveckla, upprätta och underhålla ett internt verksamhetsomfattande ledningssystem för kontinuitet.	-
Standard (EU)	**BSI ISO 22313** – Societal security – Business Continuity Management Systems – Guidance ger vägledning för att planera, upprätta, genomföra, driva, övervaka, granska, underhålla och ständigt förbättra ett dokumenterat ledningssystem som gör det möjligt för organisationer att förbereda sig för, svara på och återhämta sig från störningar i verksamheten.	2012
Vägledning	**FSPOS Vägledning för kontinuitetshantering** baseras på standarden SS-ISO 22301:2012 – Samhällssäkerhet – Ledningssystem för kontinuitet och beskriver processen för kontinuitetshantering. Som ytterligare stöd inkluderar vägledningen mallar och exempel för arbetet med kontinuitetshantering.	2014
Standard	**NFPA 1600** – Standard on Disaster/Emergency Management and Business Continuity Programs fastställer gemensamma kriterier för att utveckla, genomföra, utvärdera och upprätthålla program för katastrof-/krishantering och kontinuitetshantering.	2013
Standard	**ISO 22301** – Samhällssäkerhet – Ledningssystem för kontinuitet – Krav anger krav för att planera, upprätta, införa, tillämpa, övervaka, underhålla och ständigt förbättra ett dokumenterat ledningssystem för att skydda mot, minska sannolikheten och förbereda för, agera på och återställa efter avbrott, när de inträffar.	2012
Standard	**SS 22304** – Samhällssäkerhet – Ledningssystem för kontinuitet – Vägledning till SS-ISO 22301 kompletterar ISO 22301 med mer praktisk vägledning om hur organisationer arbetar med kontinuitetshantering.	2014
Hantering av händelser		
Standard	**BSI BS 11200** – Crisis Management – Guidance and good practice ger vägledning för att bygga en krishanteringsförmåga, och omfattar även aspekter såsom krisledarskap, beslutsfattande, kriskommunikation och utbildning och träning.	2014
Standard (EU)	**ISO 22320** – Krishantering – Krav för Samverkan beskriver hur organisationer kan etablera ledning och samverkan och dela information vid kriser och andra stora incidenter.	2011
Vägledning	**Gemensamma grunder för samverkan och ledning vid samhällsstörningar** (MSB777 – december 2014) ska ge vägledning till aktörer i förhållningssätt och arbetssätt som underlättar aktörsgemensam inriktning och samordning.	2014

Myndigheten för samhällsskydd och beredskap

Övergripande komponenter

	KOMPONENT	HJÄLPTEXT	HÄNVISNING TILL STANDARD ELLER VÄGLEDNING	KOPPLING TILL FÖRFATTNINGAR
Styrande dokument				
1	Organisationens ledning har i styrande dokument fastställt och dokumenterat förutsättningar och utgångspunkter för hur riskhantering, kontinuitetshantering och planering för hantering av händelser ska hanteras utifrån organisationens förutsättningar.		**ISO 31000** avsnitt 3g, 4.2 och 4.3.1. **ISO 22301** avsnitt 4.1. **COSO** sida 20. **BS1120:2014** avsnitt 4.4.	-
2	I organisationens styrandedokument, kan följande framgå: • Grunder och utgångspunkter för att skydda organisationens samhällsviktiga verksamheter (t ex acceptabel risk*). • Mål och syfte för organisationens arbete med skydd av samhällsviktig verksamhet. • Roller, ansvar, befogenheter och resurstilldelning för att skydda organisationens samhällsviktiga verksamheter. • Sättet på vilket resultatet ska mätas och rapporteras. • Hur efterlevnaden av det styrande dokumentet ska granskas. • Rutiner för hur information och kommunikation ska ske till berörd personal. • Rutiner för regelbunden utbildning och övning. • Hur aktiviteter, implementering, uppföljning och förbättring (policy, analyser, bedömningar, planer) ska genomföras.	* Risk definieras som osäkerheternas effekt för att nå verksamhetens mål/ En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.	**ISO 31000** avsnitt 3k, 4.3.2, 4.3.3, 4.3.5, 4.5, 4.6 och 5.6. **ISO 22301** avsnitt 5.3 och 6.2. **ISO 22320** avsnitt 4.2.2. **SS22304** avsnitt 5.3. **BS1120:2014** avsnitt 4.2.	Förordning (2006:942) om krisberedskap och höjd beredskap 9 §.
3	Organisationen bör identifiera viktiga interna och externa aktörer för att skydda de samhällsviktiga verksamheterna.			

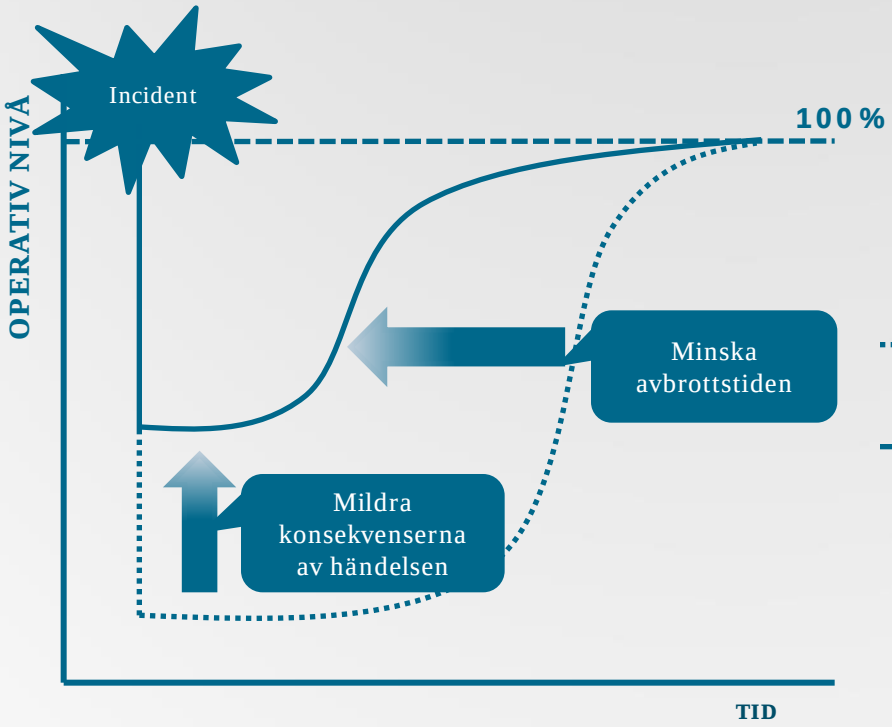
Myndigheten för samhällsskydd och beredskap

Vad är kontinuitetshantering?

- Process för att skapa robusthet i organisationen
  - Minskar sårbarheten
  - Ökar motståndskraft
- Utgångpunkt i kritiska verksamhetsprocesser, dess beroenden och konsekvenserna av ett avbrott

Myndigheten för samhällsskydd och beredskap

Hur fungerar kontinuitetshantering?

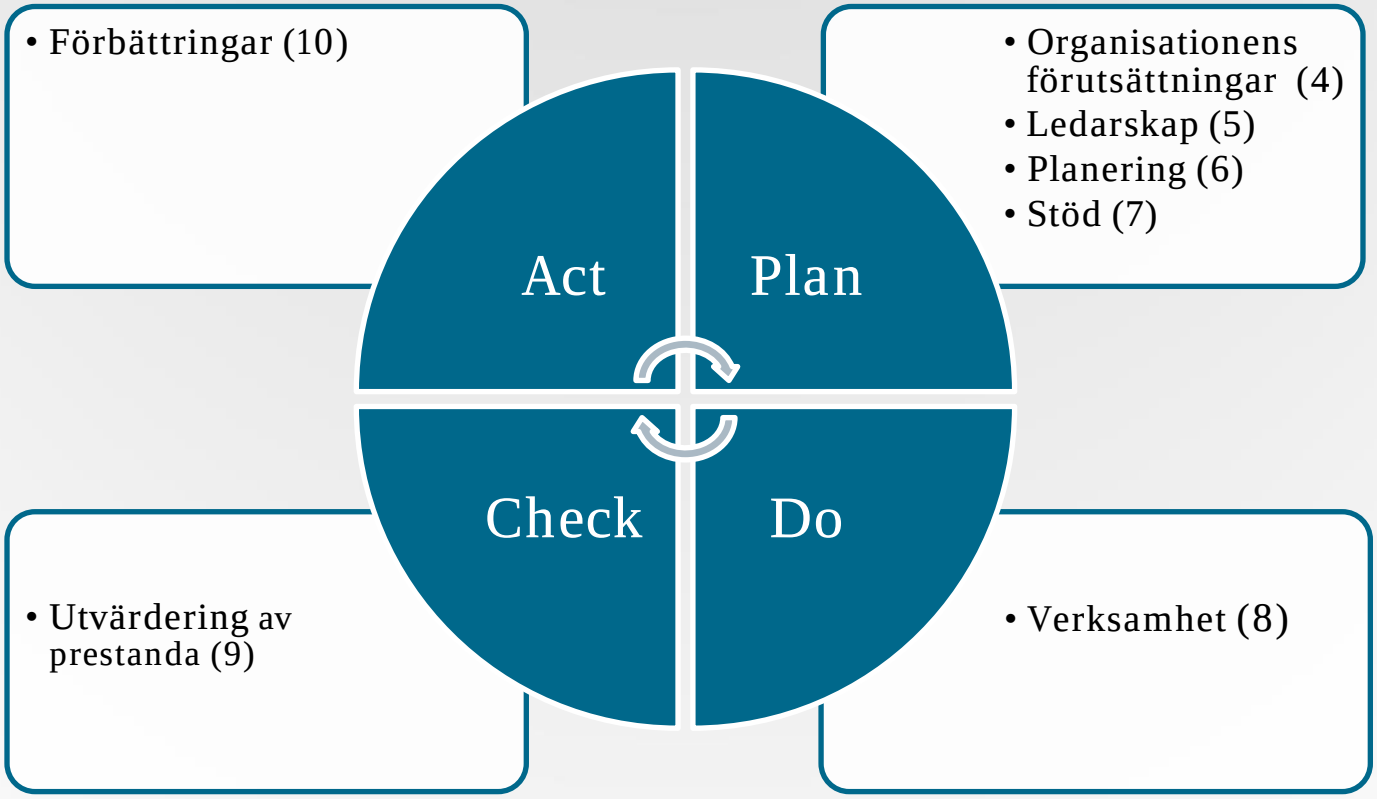


Före introduktion av ett program för kontinuitetshantering

Efter introduktion av ett program för kontinuitetshantering

Myndigheten för samhällsskydd och beredskap

PDCA-modellen tillämpad på processen för kontinuitetshantering

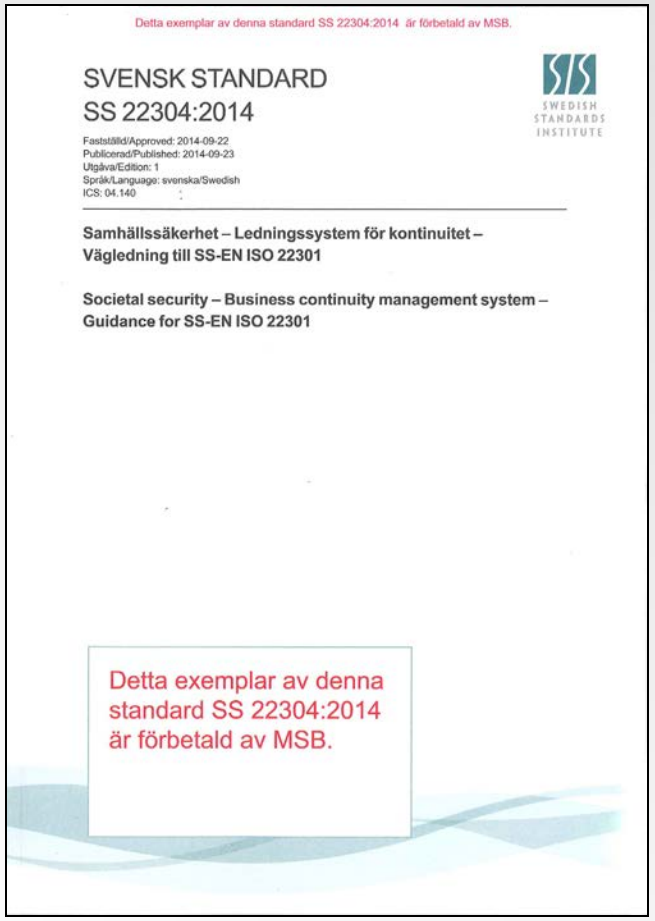


Myndigheten för samhällsskydd och beredskap

Samhällssäkerhet – Ledningssystem för kontinuitet – Vägledning till SS-EN ISO 22301 (SS 22304:2014)

Myndigheten för samhällsskydd och beredskap

Vägledning kontinuitetshantering



- Framtagen av SIS i samverkan med privata och offentliga aktörer
- Ett led i MSB:s handlingsplan för skydd av samhällsviktig verksamhet
- MSB sprider den kostnadsfritt till offentliga aktörer

Myndigheten för samhällsskydd och beredskap

Syftet med vägledningen

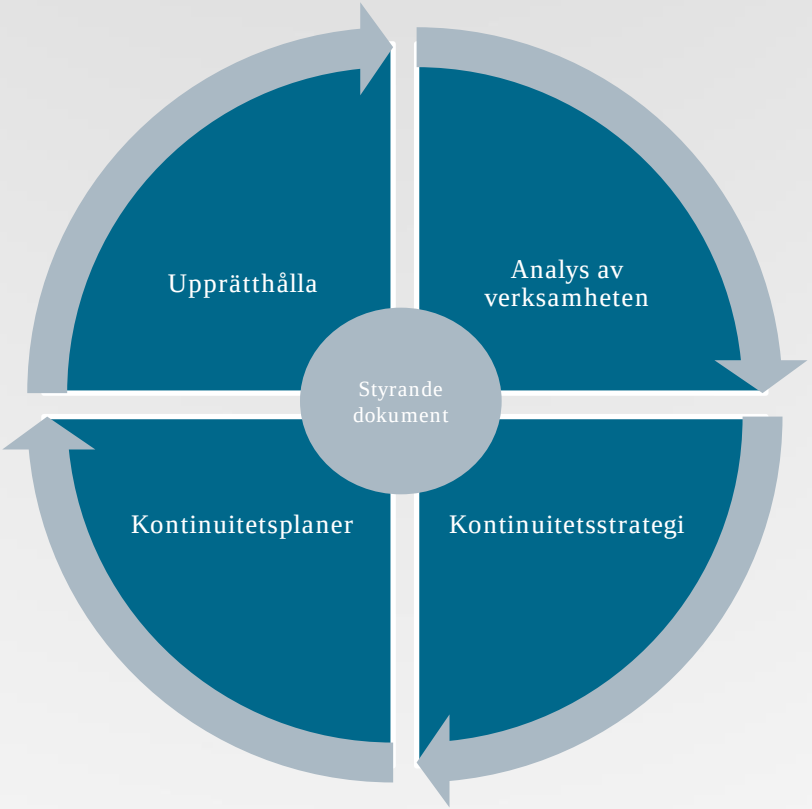
- En grundförståelse för kontinuitetshantering
- Praktiska tips som knyter ihop hela kedjan från vad kontinuitetshantering är till varför man ska arbeta med det och hur det kan göras.

Myndigheten för samhällsskydd och beredskap

Vägledningens upplägg

- Kraven från 22301 med vägledande text
- Mål och förväntat resultat
- *Tänk på att…*
- Exempel på tillämpning av kraven

Övergripande steg



Bildkälla: FSPOS Vägledning för kontinuitetshantering (2013)

Bildkälla: FSPOS Vägledning för kontinuitetshantering (2013)

Myndigheten för samhällsskydd och beredskap

Styrande dokument

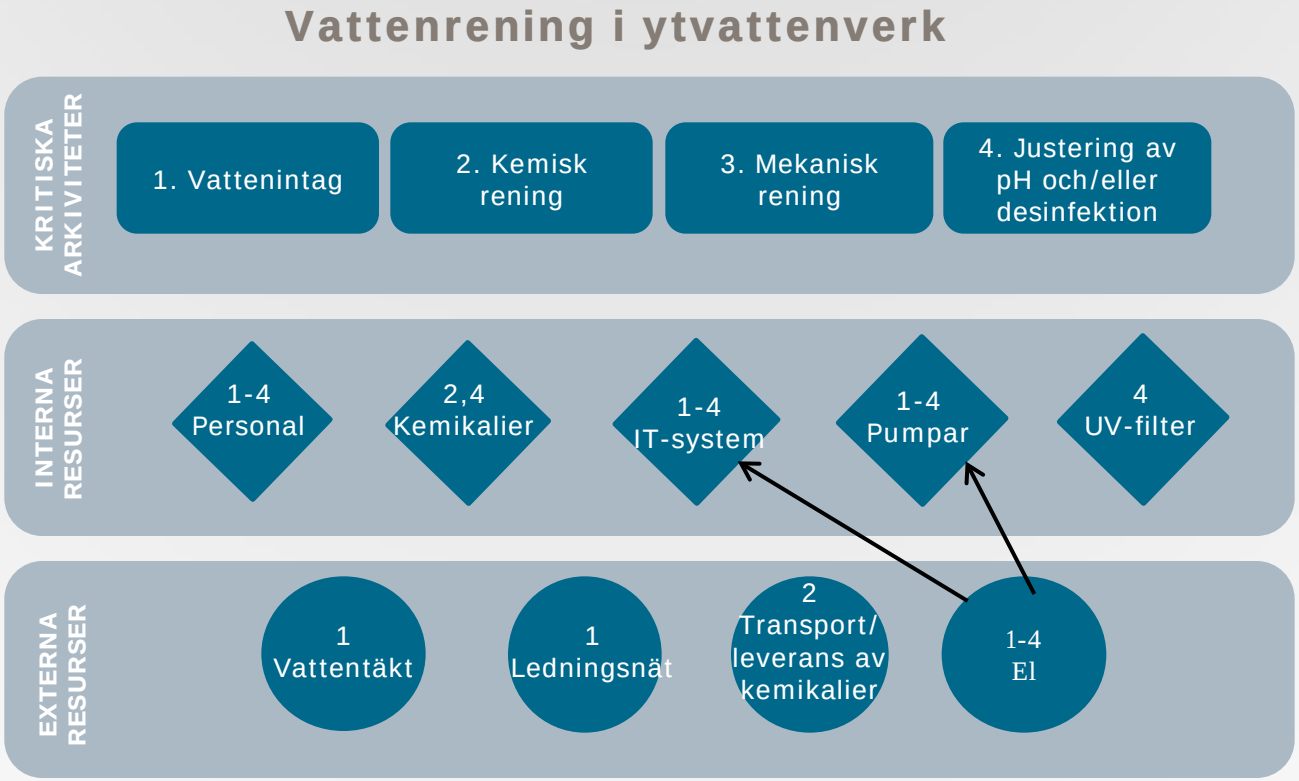
- Policy
  - Mål
  - Avgränsning och omfattning
  - Roller och ansvar
  - Metoder och rutiner
  - kriteriemodell

Styrande dokument - kriteriemodell

KRITERIEMODELL			
	Obetydlig	Märkbar	Allvarlig
Ekonomi	Förlust < 500 000	Förlust < 5 000 000	Förlust > 5 000 000
Förtroende	Ingen förlust av kunder	Förlust av låg andel kunder	Förlust av stor andel kunder
Leverans-förmåga	Ingen påverkan på leverans-förmågan	Låg påverkan på leverans-förmågan	Stor påverkan på leverans-förmågan

Bildkälla: FSPOS Vägledning för kontinuitetshantering (2013)

Analys av verksamheten - Konsekvensanalys



Layout: FSPOS Vägledning för kontinuitetshantering (2013)

Analys av verksamheten - Riskbedömning

Kritisk resurs (mål för återställningstid)	Händelser som kan påverka resursens tillgänglighet	Befintlig redundans	Sannolikhet att avbrott överstiger mål för återställningstid			Prio	Kommentar
			LÅG	MEDEL	HÖG		
IT-system (2 h)	Elavbrott	Det finns reservkraft samt diesel för 3 dagars drift	X			3	Viktigt med löpande test av reservkraft (ansvar: kontorschef)
	Kabelfel	Ingen redundans finns			X	1	Utred möjliga redundanslösningar (ansvar: IT-chef, klart: innan årsskiftet)
	Skadlig kod	Virusprogram finns, oklart om tillräckligt		X		2	Se över befintlig redundanslösning (ansvar: IT-chef, klart: innan årsskiftet)

Bildkälla: FSPOS Vägledning för kontinuitetshantering (2013)

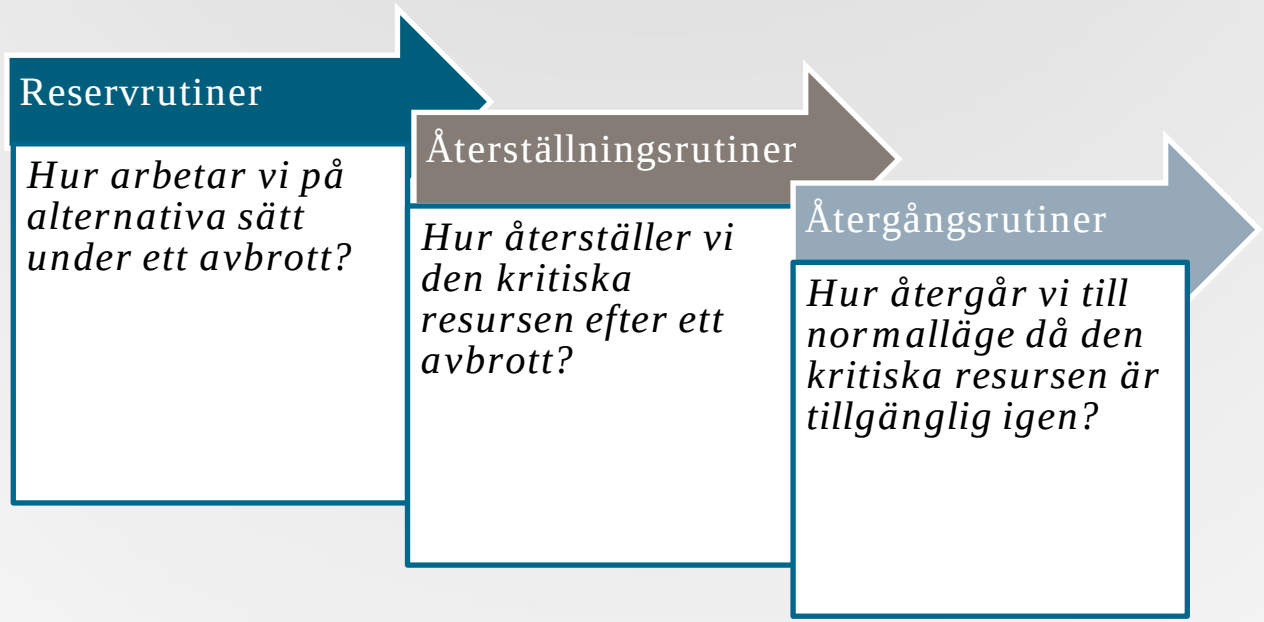
Bildkälla: FSPOS Vägledning för kontinuitetshantering (2013)

Myndigheten för samhällsskydd och beredskap

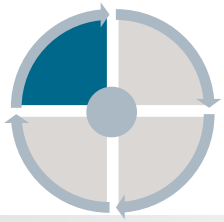
Kontinuitetsstrategi

Myndigheten för samhällsskydd och beredskap

Kontinuitetsplan



Myndigheten för samhällsskydd och beredskap



Upprätthålla

- Granskning och revidering
- Test, övning och utbildning

Myndigheten för samhällsskydd och beredskap

Tack för uppmärksamheten!

www.msb.se/samhallsviktigverksamhet

omar.harrami@msb.se