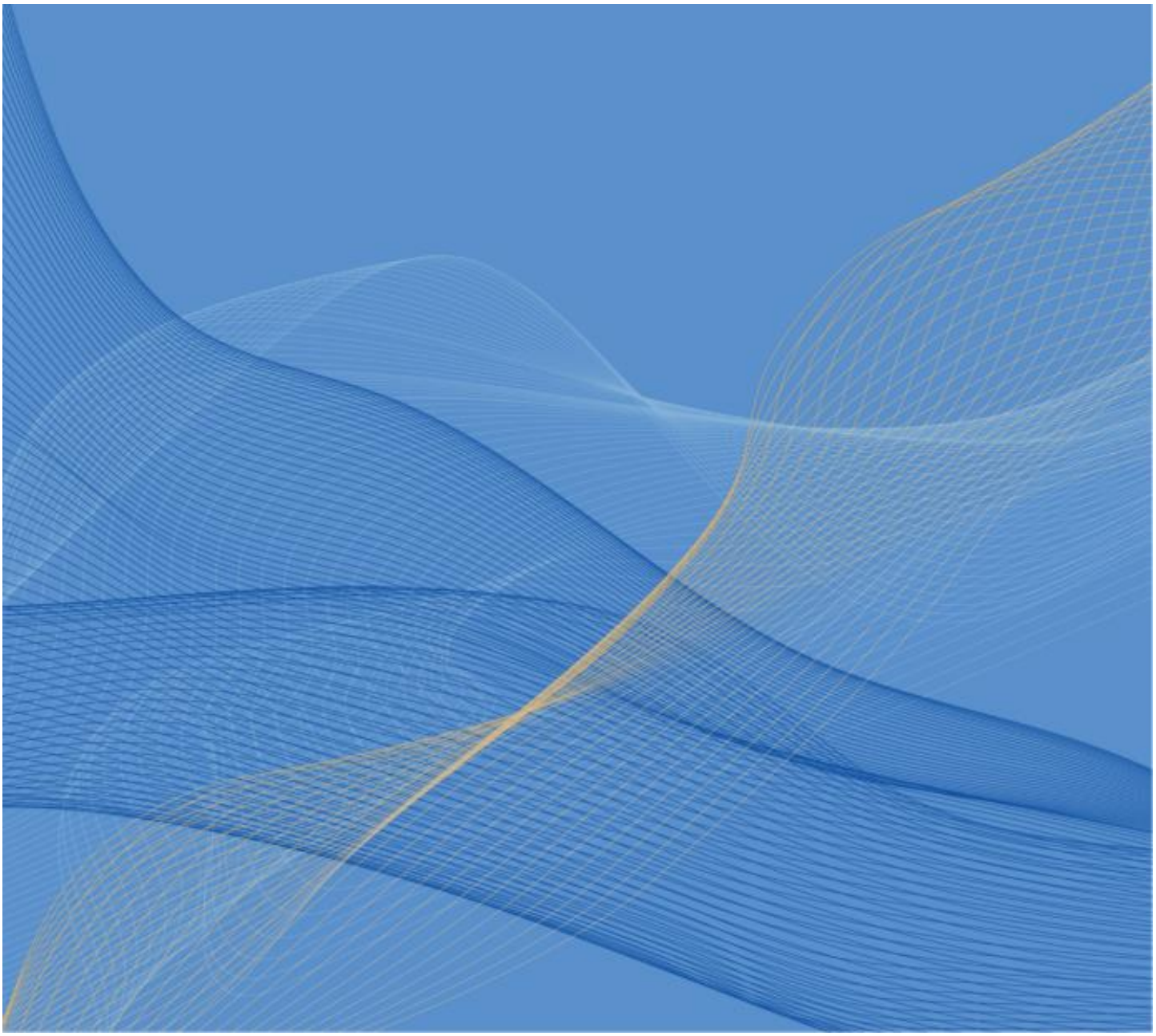
Vägledning
Civil beredskap för betalningar



SVERIGES RIKSBANK

Innehållsförteckning

1	Verksamheter av särskild betydelse för betalningar	3
1.1	Bankkonto	3
1.2	Betalningsinfrastruktur och tjänster för statliga myndigheters betalningar	3
1.3	Clearing och avveckling	3
1.4	Elektronisk identifiering och underskrift	3
1.5	Kontoöverföring	4
1.6	Kontanthantering	4
1.7	Kortbetalning	4
1.8	Kortinlösen	5
1.9	Säkerhetshantering och värdepappersavveckling	5
2	Fredstida kris och höjd beredskap	6
3	Totalförsvarets krav	7
3.1	Hotbild och typsituationer	7
3.2	Omställning och uthållighet	9
4	Avvägningar vid uppbyggnad av beredskap	10
5	Planering av krigsorganisation	11
5.1	Identifiering av uppgifter	12
5.2	Organisering och ledning	13
5.3	Personal och bemanning	14
5.4	Lokaler och anläggningar	16
5.5	Informationsförsörjning	18
5.6	Informationsteknik	19
5.7	Skydd och bevakning	21
5.8	Kritiska beroenden	23
5.9	Omlokalisering	25
6	Övning och utbildning	26
7	Planeringsstege	27

Betalningar måste fungera i kris och krig

Förmågan att upprätthålla samhällsviktiga funktioner vid kriser och ytterst vid krig är central för Sveriges totalförsvar och för Natos kollektiva försvarsförmåga.

Betalningsförmedling är en samhällsviktig funktion som behöver kunna stå emot störningar vid fredstida kriser och höjd beredskap.[1] Störningar i betalningssystemet kan snabbt få allvarliga konsekvenser. Människor kan exempelvis få svårt att köpa mat, läkemedel, drivmedel, betala räkningar eller ta emot sina löner. Samtidigt behöver företag som matvarubutiker och transportföretag kunna betala för tjänster och produkter för att kunna fortsätta sälja livsnödvändiga varor.

Företag av särskild betydelse för genomförande av betalningarna ska enligt 5 kap. 6 § lagen (2022:1568) om Sveriges riksbank (riksbankslagen) planera och förbereda för att kunna fortsätta verksamhet som avser betalningar under fredstida krissituationer och vid höjd beredskap. De företag som bedriver sådan verksamhet pekas ut i Riksbankens föreskrifter och allmänna råd (RBFS 2026:4) om företag av särskild betydelse för genomförandet av betalningar under fredstida krissituationer och vid höjd beredskap.

Denna vägledning syftar till att utgöra stöd för dessa företag i sin planering. Vägledningen fokuserar främst på att stödja företagens arbete med att planera och utforma en krigsorganisation.

Vägledningen är inte rättsligt bindande och företagen kan uppfylla föreskrifternas krav på andra sätt än vad som beskrivs i vägledningen. Den kan också med fördel användas av andra aktörer inom betalningsområdet som på något sätt deltar i det civila försvaret.

[1] Lista med de viktigaste samhällsfunktionerna – Utgångspunkt för att stärka samhället beredskap, Myndigheten för civilt försvar, MCF0018, februari 2026.

1 Verksamheter av särskild betydelse för betalningar

Nedan framgår verksamheter som Riksbanken bedömer är av särskild betydelse för genomförandet av betalningar.

1.1 Bankkonto

Som bankkonto räknas konton som används för betalningar i svenska kronor eller andra valutor, exempelvis betalkonton med grundläggande funktioner, samt sparkonton och klientmedelskonton. Bankkontoverksamhet omfattar möjligheten att öppna nya konton, göra och ta emot kontoöverföringar. Till verksamheten hör även att administrera konton, exempelvis genom att hämta information om saldo och genomförda betalningar via internetbank och fil, samt att avsluta konton.

1.2 Betalningsinfrastruktur och tjänster för statliga myndigheters betalningar

Verksamheten avser specifikt Riksgäldens avveckling gentemot ramavtalsbank av svenska kronor i betalningssystemet RIX samt laddningsbara kort och utbetalningsavier som används av statliga myndigheter för utbetalningar.

1.3 Clearing och avveckling

Clearing- och avveckling möjliggör betalningar och handel med finansiella instrument mellan olika parter. Verksamheten omfattar möjligheten att ansluta till, använda och avsluta deltagande i clearing- och avvecklingssystem. Clearing innebär att parternas ömsesidiga betalningsförpliktelser gentemot varandra sammanställs och redovisas innan betalning sker. Avveckling innebär att dessa förpliktelser slutligt regleras genom överföring av medel eller finansiella instrument. Avvecklingen kan ske via konton hos en centralbank eller hos en privat aktör, exempelvis en bank eller ett finansiellt infrastrukturföretag.

1.4 Elektronisk identifiering och underskrift

Med elektronisk identifiering och underskrift avses elektroniska tjänster som används för att kontrollera en betaltjänstanvändares identitet, dvs. identifiering, och behörighet, dvs. autentisering, samt för att signera en betalningsorder med en elektronisk underskrift. Verksamheten avser även möjligheten att ansluta till, använda och avsluta elektroniska identifierings- och underskriftstjänster.

1.5 Kontoöverföring

Kontoöverföring omfattar tjänster som gör det möjligt att skicka och ta emot betalningar mellan konton i Sverige och i utlandet. Kontoöverföringar kan genomföras genom att

- avsändaren i samband med betalningsuppdrag till banken anger mottagarens kontonummer eller IBAN vid utlandsbetalningar, exempelvis via internetbank eller på ett bankkontor
- avsändaren i samband med betalningsuppdrag till banken anger mottagarens alias i form av bank- eller plusgironummer, exempelvis via internetbank eller genom brevgiro
- avsändaren anger mottagarens alias, exempelvis i form av mobilnummer som är knutet till ett konto, genom tjänster för omedelbar betalning
- mottagaren och avsändaren har avtalat om att banken ska debitera avsändarens betalkonto, exempelvis autogiro och andra återkommande betalningar.

Verksamheten omfattar även möjligheten att göra flera kontoöverföringar samtidigt, exempelvis leverantörsbetalningar och filöverföringar. Den omfattar också registrering och avslutande av återkommande eller föranmälda kontoöverföringar samt hantering av kontoregister och register över alias som används för utbetalningar och betaltjänster.

1.6 Kontanthantering

Till kontanthantering räknas tjänster som möjliggör uttag av kontanter i uttagsautomat, i fysisk butik eller på ett bankkontor samt tillhandahålla växelkassetjänster. Verksamheten omfattar också tjänster som möjliggör insättning av kontanter, inklusive dagskassor, i insättningsautomat, serviceboxar, och på bankkontor eller genom upphämtning. Även förvaring, uppräkning, sortering, äkthetskontroll och transport av kontanter räknas som kontanthantering.

1.7 Kortbetalning

En kortbetalning är en betalning som genomförs med debet-, kredit- eller laddningsbart kort i fysisk butik eller via internet.[2] Det gäller både med fysiska och digitala kort. Även återkommande automatiska debiteringar kan räknas som kortbetalningar, som kan registreras och avslutas. Verksamheten omfattar även att möjliggöra ansökan om ett kort, att utfärda nya kort samt att spärra befintliga kort.

[2] Användningsområdet för vissa kort är begränsat, exempelvis kan vissa laddningsbara kort endast användas för att ta ut kontanter eller betala i en betalningsterminal.

1.8 Kortinlösen

Tjänsten kortinlösen, dvs. inlösen av transaktionsbelopp, innebär att kortbetalningsmottagare, normalt en näringsidkare, kan ta emot och behandla kortbetalningar. I tjänsten ingår att förmedla auktorisationen av kortbetalningar via ett kortnätverk till kortutgivaren. Kortinlösaren krediterar sedan betalningsmottagaren efter att kortutgivaren genomfört kontroll, avräkning och avveckling och överfört medel till inlösaren.

1.9 Säkerhetshantering och värdepappersavveckling

Verksamheten omfattar hantering av säkerheter som gör det möjligt för deltagare i betalningssystem att få tillgång till intradagskrediter för att genomföra och avveckla betalningar. Verksamheten omfattar även administration av konton som används för avveckling av värdepapperstransaktioner och därmed stödjer den finansiella infrastrukturen för betalningar och värdepappershandel.

2 Fredstida kris och höjd beredskap

Företagens planering och förberedelser ska syfta till att de ska kunna upprätthålla betalningsverksamheten under fredstida krissituationer och vid höjd beredskap.

Med fredstida krissituation avses en situation som avviker från det normala och drabbar många människor, stora delar av samhället eller hotar grundläggande värden. Situationen ska även innebära en allvarlig störning eller en överhängande risk för en allvarlig störning av viktiga samhällsfunktioner och kräva samordnade och skyndsamma åtgärder från flera aktörer.[3] Exempel på fredstida kriser är cyberangrepp, CBRNE-händelser[4], terrorism, pandemier, naturkatastrofer samt sabotage och andra störningar i kritisk infrastruktur. Att planera och förbereda inför fredstida kriser innebär att skapa förmåga att förebygga, stå emot och hantera kriser.

Är Sverige i krigsfara eller råder det sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara, får regeringen besluta om höjd beredskap.[5] Om Sverige är i krig råder det automatiskt högsta beredskap. Att en medlem i Nato anser sig vara i krig eller åberopar artikel 5 i nordatlantiska fördraget[6] betyder inte att Sverige automatiskt befinner sig i krig. Det kan dock innebära att det är krig utanför Sveriges gränser.

[3] Jämför med 6 § förordningen (2022:524) om statliga myndigheters beredskap.

[4] Händelser som involverar kemiska, biologiska, radiologiska, nukleära eller explosiva ämnen och som kan orsaka skador på människor, djur, egendom och miljö.

[5] 3 § lagen (1992:1403) om totalförsvar och höjd beredskap.

[6] Artikel 5 innehåller de ömsesidiga försvarsgarantier som utgör kärnan i Natos kollektiva försvar. Enligt artikeln ska ett väpnat angrepp mot en eller flera av parterna betraktas som ett angrepp mot samtliga parter.

3 Totalförsvarets krav

Företagen ska i sin planering och förberedelse inför höjd beredskap beakta totalförsvarets krav.

Det väpnade angreppet är dimensionerande för totalförsvaret. Det betyder att beredskapen behöver utformas för att kunna hantera de mycket allvarliga påfrestningar som ett sådant angrepp kan innebära. Genom att planera för krig stärks samtidigt förmågan att hantera fredstida kriser. Vid höjd beredskap och krig ska det civila försvaret stödja det militära försvaret och bidra till totalförsvarets samlade förmåga.[7]

*Det övergripande **målet för totalförsvaret** är att ha förmåga att försvara Sverige och Sveriges befolkning mot väpnat angrepp, hävda landets självständighet, suveränitet och territoriella integritet samt medverka till försvaret av allierade. Verksamhet inom totalförsvaret ska kunna bedrivas enskilt och tillsammans med andra, inom och utom landet och i enlighet med Sveriges åtaganden som medlem i Nato.*

***Målet för det civila försvaret** är att säkerställa de viktigaste samhällsfunktionerna, bidra till det militära försvarets förmåga inom ramen för Natos kollektiva försvar och uppgifter i övrigt, skydda civilbefolkningen samt upprätthålla försvarsviljan och samhällets motståndskraft mot externa påtryckningar.*

3.1 Hotbild och typsituationer

Planeringen behöver utgå från den aktuella säkerhetspolitiska situationen och från de sju typsituationer som Försvarsmakten och Myndigheten för civilt försvar har tagit fram för totalförsvaret 2025–2030[8]. Genom att totalförsvarets aktörer utgår från samma typsituationer, och därigenom har en gemensam bild av vilka störningar som kan uppstå och vilka förmågor som behövs, skapas bättre förutsättningar för en samordnad planering och hantering av oväntade händelseförlopp.

Vid en säkerhetspolitisk kris, konflikt eller krig kan Sverige utsättas för flera antagonistiska handlingar, som informationspåverkan, cyberangrepp, sabotage, terrorism, underrättelseinhämtning, störningar i samhällsviktig verksamhet och utnyttjandet av ekonomiska beroenden.[9] Det kan även förekomma militära angrepp mot civila mål och kritisk infrastruktur som elnät, drivmedelsdepåer, elektronisk kommunikation, datorhallar, sjukhus, tätbefolkade områden, hamnar, flygplatser, broar och industrier.[10]

[7] Regeringens proposition 2024/25:34 Totalförsvaret 2025–2030, s. 109.

[8] Utgångspunkter för totalförsvaret 2025–2030, FM2025-19772:2 och MSB 2025-08877.

[9] Prop. 2024/25:34 s. 15.

[10] Utgångspunkter för totalförsvaret 2025–2030, FM2025-19772:2 och MSB 2025-08877, s. 26.

Sju dimensionerande typsituationer

- Hybrida hot
- Värdlandsstöd
- Anfall mot norra Sverige
- Anfall mot Gotland
- Fjärrangrepp
- Förstärkning av alliansens norra flank
- Förstärkning av alliansen i Baltikumområdet



Läs mer i Försvarsmaktens och Myndigheten för civilt försvars **Utgångspunkter för totalförsvaret 2025–2030** för inriktning av Sveriges planering och utveckling av totalförsvaret under perioden 2025–2030.

Läs mer i Myndigheten för civilt försvars **Planeringsinriktning för krisberedskap och civilt försvar – Planering för att skapa och använda förmåga**, som anger lägsta acceptabla nivå för prioriterade förmågor.

Läs mer i Finansinspektionens **Planeringsinriktning för finansiella företag** för en bredare beskrivning av hur den finansiella sektorn kan påverkas av typsituationerna.

3.2 Omställning och uthållighet

Utgångspunkten för planeringen av det civila försvaret är att under minst **tre månader** kunna hantera konsekvenserna av ett krig i Europa som allvarligt påverkar samhällets funktionalitet.[11] Totalförsvarets aktörer ska därför kunna ställa om till krigsorganisation, prioritera verksamhet, omfördela resurser och anpassa försörjnings- och produktionslösningar.[12] På så sätt skapas förutsättningar att kunna hantera en längre period av allvarlig säkerhetspolitisk kris eller krig. Aktörer i totalförsvaret behöver samtidigt utgå från att ett läge av höjd beredskap kan pågå under längre tid än tre månader.

Det civila försvaret behöver även bygga upp en förmåga att under minst **två veckor** kunna upprätthålla viktiga samhällsfunktioner med främst egna resurser.[13] Det innebär att verksamheten behöver fungera trots exempelvis personalbortfall, störningar i elförsörjningen och elektroniska kommunikationer, avbrott i leveranskedjor eller brist på drivmedel. Planeringen bör därför omfatta alternativa arbetssätt, reservlösningar och möjligheten att prioritera eller tillfälligt stänga ner mindre kritiska delar av verksamheten.

Målsättningen ska ses utifrån det civila försvarets samlade förmåga där varje aktör förväntas uppnå en så hög förmåga som möjligt utifrån sina egna förutsättningar. Genom att samtliga aktörer identifierar och reducerar sina egna sårbarheter utifrån samma utgångspunkter minskar samhällets samlade sårbarhet och den totala motståndskraften höjs.

→ I avsnittet **Planering av krigsorganisationen** finns närmare vägledning om hur ovan utgångspunkter kan omsättas i praktiken vid utformningen av krigsorganisationen

[11] Prop. 2024/25:34 s. 109, och Gemensamma förutsättningar för utvecklingen av totalförsvaret 2025–2030, Fö24/02054 (delvis), 2024-01-19.

[12] Utgångspunkter för totalförsvaret 2025-2030, FM2025-19772:2 och MSB 2025-08877, s.13.

[13] Utgångspunkter för totalförsvaret 2025-2030, FM2025-19772:2 och MSB 2025-08877, s.13.

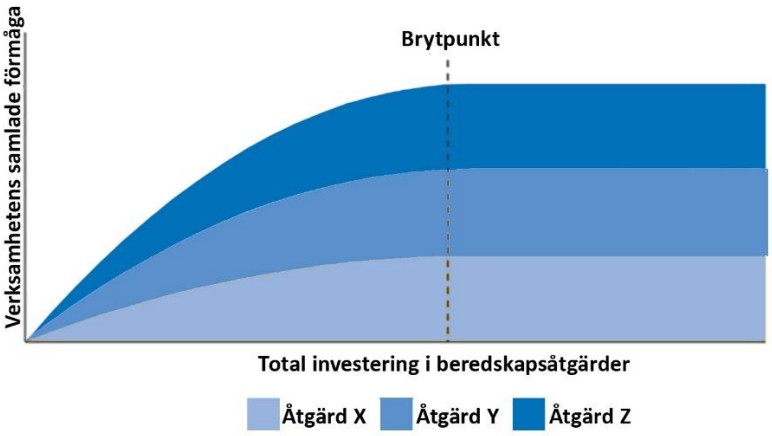
4 Avvägningar vid uppbyggnad av beredskap

I planeringen för att upprätthålla kritiska betalningsfunktioner behöver företagen göra avvägningar mellan olika beredskapsåtgärder. Utgångspunkten bör vara att investera i åtgärder som på ett effektivt sätt stärker verksamhetens förmåga att motstå störningar och upprätthålla prioriterade funktioner.

Planeringen ska utgå från konsekvenserna av ett väpnat angrepp mot Sverige. Företagen behöver därför inte bedöma sannolikheten för att ett sådant angrepp inträffar. Fokus bör i stället ligga på att analysera vilka konsekvenser krigsförhållanden kan få för den egna verksamheten och vilka förmågor som krävs för att kunna upprätthålla betalningsverksamheten under sådana förhållanden.

En viktig del av beredskapsplanering är att identifiera vilka åtgärder som bäst bidrar till att öka förmågan att upprätthålla betalningsverksamheten och när ytterligare investeringar i samma åtgärd inte längre ger bättre motståndskraft. Exempelvis kan kostsamma investeringar i en starkt skyddad anläggning vara mindre motiverade om området där verksamheten bedrivs bedöms kunna bli avskuret vid ett väpnat angrepp. I sådana fall kan resurserna i stället ge större effekt om de används för att säkerställa alternativa arbetssätt, omlokalisering eller samverkan med andra aktörer.

Investeringar i exempelvis reservkraft, redundanta kommunikationslösningar, alternativa leverantörer eller tekniska reservsystem kan öka förmågan betydligt. Men även satsningar på exempelvis personalförsörjning, transportmedel eller lokaler kan ge verksamheten ökad motståndskraft. Beredskapsförmågan behöver bygga på en kombination av olika typer av åtgärder.



Figur 1. Samlad förmåga från investeringar i beredskapsåtgärder
Figuren ovan illustrerar hur olika beredskapsåtgärder kan bidra till verksamhetens samlade förmåga. Efter en viss punkt ger ytterligare investeringar i samma typ av åtgärd successivt lägre effekt, vilket kan motivera andra lösningar för att hantera allvarliga störningar. Illustrationen är AI-genererad och bygger inte på empiriska data.

5 Planering av krigsorganisation

En krigsorganisation ska vara anpassad för krigsförhållanden och utformas för uppgifter som har betydelse för totalförsvaret.

Arbetet med att upprätta och utveckla en krigsorganisation handlar bland annat om att avgöra vilka verksamheter som behöver prioriteras och bedrivas under höjd beredskap. Det innefattar också att utveckla och implementera förmågor, rutiner och resurser för att stärka verksamhetens kontinuitet, uthållighet och motståndskraft. I planeringen ingår även att identifiera risker som behöver accepteras efter att relevanta åtgärder har vidtagits.

Arbetet med krigsorganisationen omfattar

- identifiering av uppgifter
- organisering och ledning
- personal och bemanning
- lokaler och anläggningar
- informationsförsörjning
- informationsteknik
- skydd och bevakning
- kritiska beroenden
- omlokalisering

Informationssäkerhet

I arbetet med att utforma en krigsorganisation behöver hänsyn tas till att planeringen kommer att innehålla skyddsvärda uppgifter. Det är viktigt att löpande informationsklassificera de uppgifter som hanteras i arbetet, för att de ska skyddas på rätt sätt. Om uppgifterna är säkerhetsskyddsklassificerade så behöver planeringen hanteras i enlighet med säkerhetsskyddslagstiftningen. Stöd i arbetet med informationssäkerhetsklassning och informationssäkerhetsarbete i övrigt finns i **Säkerhetspolisens vägledningar i säkerhetsskydd** och på **Nationellt cybersäkerhetscenters webbplats Om informationssäkerhet.**

5.1 Identifiering av uppgifter

Vid höjd beredskap kan företagen tvingas prioritera bland de verksamheter som är särskilt viktiga för genomförandet av betalningar. Företagen behöver därför analysera vilka delar av betalningsverksamheten som är mest kritisk att upprätthålla och vilka processer det kräver. Viss verksamhet behöver kunna bedrivas på ett robust sätt och under mycket svåra förhållanden, medan annan verksamhet kan bedrivas med lägre ambitionsnivå eller tillfälligt upphöra. Denna analys ligger sedan till grund för företagets krigsorganisation och beredskapsplanering och därmed även den gemensamma planeringen inom det samlade civila försvaret. Företagens kontinuitetsarbete kan vara ett stöd vid analysen av vilka uppgifter som måste upprätthållas eller kan tillkomma. Eftersom förutsättningarna snabbt kan förändras behöver planeringen vara flexibel och möjliggöra anpassningar över tid.

Det är också viktigt att företagen och övriga aktörer inom betalningsberedskap gemensamt kan prioritera uppgifter och agera på ett enhetligt sätt vid kris och krig. Det kan exempelvis ske med stöd av analyser som har tagits fram inom Riksbankens samverkansstruktur Civil beredskap betalningar. Inom ramen för samverkan kan även gemensamma reservrutiner och andra lösningar utvecklas för betalningsverksamhet som bedöms vara särskilt prioriterad.

Stödfrågor – identifiera uppgifter och prioritera verksamhet

- Vilka delar av betalningsverksamheten är prioriterad att bedriva under höjd beredskap, exempelvis för att möta kunders behov, upprätthålla samhällsviktiga funktioner och bidra till finansiell stabilitet?
- Vilka verksamheter förväntas under höjd beredskap få ökad belastning eller i övrigt vara i behov av att förstärkas med personal, materiella resurser, lokaler eller tekniskt stöd?
- Vilka tjänster eller processer kan bedrivas i begränsad omfattning, senareläggas eller tillfälligt upphöra vid höjd beredskap?
- Vilka uppgifter kan tillkomma vid höjd beredskap, exempelvis inom krisledning, samverkan, rapportering eller reservrutiner?



Läs mer i Myndigheten för civilt försvars **Vägledning Krigsuppgiftsförteckning**

5.2 Organisering och ledning

Företagen behöver ange former för hur de ska organisera och leda sin verksamhet vid höjd beredskap. Detta inkluderar exempelvis hur ansvar, arbetsuppgifter och beslutanderätt ska fördelas. Beskrivningen av hur det enskilda företaget ska organisera och leda betalningsverksamheten vid höjd beredskap är, liksom analysen av vilka uppgifter som ingår i företagets betalningsverksamhet, en grundläggande förutsättning för företagets krigsorganisation och beredskapsplanering i övrigt.

Företagets krigsorganisation behöver inte vara skild från den ordinarie organisationen. Om befintlig organisation och ledning bedöms fungera även vid höjd beredskap, med eventuella kompletteringar och anpassningar, kan det framgå av planeringen.

Stödfrågor – organisering och ledning

- Hur ska betalningsverksamheten vara organiserad vid höjd beredskap?
- Fungerar nuvarande struktur eller behöver den kompletteras?
- Vilka funktioner, roller och befattningar behöver finnas för att kunna bedriva betalningsverksamheten vid höjd beredskap?
- Behövs särskilda ledningsfunktioner eller stabsfunktioner?
- Vilka delar av den ordinarie styrningen behöver ändras, förstärkas eller ersättas?
- Hur ska samverkan mellan verksamhetsområden och funktioner bedrivas under höjd beredskap?
- Hur ska arbetsuppgifterna fördelas inom företaget?
- Hur förändras ansvar, befogenhet och beslutsmandat jämfört med fredstid?
- Behövs snabbare beslutsvägar eller förenklade rutiner?
- Vilka roller är kritiska och måste alltid vara bemannade?
- Hur säkerställs kontinuitet och uthållighet i ledning över tid?
- Vilka arbetsprocesser behöver anpassas eller ersättas?



Läs mer i Myndigheten för civilt försvars **Vägledning Krigsarbetsordning.**

5.3 Personal och bemanning

Arbetet med att bemanna krigsorganisationen innebär bland annat att identifiera vilken personal företaget behöver för sin betalningsverksamhet. Planeringen bör utgå från analysen av vilka uppgifter som ingår i företagets betalningsverksamhet och beakta vilket personalbortfall som kan uppstå. Planeringen bör även beakta möjligheten att omfördela personal från mindre tidskritiska verksamheter eller stödfunktioner till prioriterade delar av verksamheten. Om den egna personalen inte bedöms räcka till för att möta den ökade belastningen eller eventuella krav på skiftgång, kan det finnas behov av extern personalförstärkning.

Särskilt om allmän tjänsteplikt och krigsplacering

Enligt svensk arbetsrätt fortsätter anställningsavtal normalt att gälla vid höjd beredskap. Det innebär att den anställda har en arbetsrättslig skyldighet att fortsätta sitt arbete. Om regeringen föreskriver om allmän tjänsteplikt kan anställda som är totalförsvarspliktiga och arbetar i verksamhet som är av särskild vikt för totalförsvaret också komma att omfattas av en straffrättslig skyldighet att stanna kvar i sin anställning och fortsätta utföra sina arbetsuppgifter för att stödja totalförsvaret.[14] För företag som bedriver verksamhet som är av särskild betydelse för genomförandet av betalningar är det Riksbanken som kan fatta beslut om vilka arbets- och uppdragstagare som omfattas av allmän tjänsteplikt.[15] Skyldigheten för enskilda att stanna kvar i sin anställning gäller dock endast under den tid som anställnings- eller uppdragsavtalet gäller och i den omfattning som är avtalad.[16]

Arbetsgivare som i sin beredskapsplanering har identifierat arbetstagare som ska tjänstgöra i dess krigsorganisation kan välja att krigsplacera dessa med stöd av anställningsavtalet. En sådan krigsplacering innebär i sig inga skyldigheter eller rättsliga konsekvenser för den anställde.[17] Först om den anställde omfattas av ett beslut om allmän tjänsteplikt blir personen straffrättsligt skyldig att fortsätta arbeta i sin tjänst. Om anställningen upphör, upphör också krigsplaceringen. Krigsplacering är i dessa fall ett sätt att verifiera att identifierade nyckelpersoner är tillgängliga för verksamheten vid höjd beredskap och inte tas i anspråk för andra uppgifter inom totalförsvaret.

I föreslagna ändringar i riksbankslagen och lagen om totalförsvarsplikt, som avses att träda i kraft den 1 januari 2027, anges att företag av särskild betydelse för genomförandet av betalningar ska registrera de totalförsvarspliktiga som till följd av anställningsavtal eller uppdragsavtal är placerade i företagens krigsorganisation.[18]

[14] 6 kap. 1 § och 2 § 2 lagen (1994:1809) om totalförsvarsplikt.

[15] 5 kap. 7 § riksbankslagen.

[16] Det innebär att arbetstagare med en tidsbegränsad anställning inte behöver kvarstå i anställning eller utföra ytterligare uppdrag efter att anställningsavtalet har löpt ut.

[17] Det finns därmed en skillnad mot när begreppet används för värnpliktiga och civilpliktiga, där krigsplaceringen medför skyldigheter för den enskilde i fredstid och vid höjd beredskap.

[18] Prop. 2025/26:302 s. 31 och 54.

Planeringsdialoger om personalförsörjning

Planeringsdialoger om personalförsörjning sker bilateralt mellan företag av särskild betydelse för genomförandet av betalningar och Riksbanken.

Frågor kan ställas till CBB@riksbank.se. Tänk på att information om krigsorganisationen och dess bemanning vid höjd beredskap kan omfattas av säkerhetsskydd och därför måste hanteras enligt särskilda regler.

Stödfrågor – personal och bemanning

- Vilka befattningar krävs för att lösa uppgifter i krig?
- Vilka bland befintlig personal ska bemanna befattningarna i krigsorganisationen?
- Är någon del av betalningsverksamheten särskilt sårbar för personalbortfall?
- Behöver personal finnas fysiskt på arbetsplatsen eller möjliggör arbetsuppgifterna att personal kan arbeta hemifrån?
- Kan vissa arbetsuppgifter genomföras av färre personer än vanligt?
- Är det möjligt att tillfälligt omplacera personal till de mest prioriterade uppgifterna? Har personal som kan komma att omplaceras rätt kompetens för uppgiften?
- Finns det några uppgifter som kräver specialistkompetens?
- Hur ska särskild nyckel- och specialistkompetens överföras till andra i organisationen?
- Finns det möjlighet till skiftgång eller uthållig bemanning över tid?
- Finns särskilda behov bland personalen som kan påverka tillgänglighet, uthållighet eller möjlighet att tjänstgöra under höjd beredskap?
- Finns tillgång till nödvändiga stödfunktioner för personalen?



Läs mer i Myndigheten för civilt försvars **Vägledning Krigsbemanningsplan** och **Planeringsstöd för bortfall av personal, varor och tjänster**

5.4 Lokaler och anläggningar

Företagens planering av lokaler och anläggningar bör utgå från analysen av vilka uppgifter som ingår i betalningsverksamheten under höjd beredskap, hur den ska organiseras och ledas samt vilken personal som behövs för detta. I planeringen bör även företagen analysera behovet av alternativa och skyddade verksamhets- och ledningsplatser.

Vilka behov som företagens lokaler och anläggningar behöver tillgodose påverkas av hur verksamheten är organiserad. Verksamhet som bedrivs från geografiskt spridda platser kan ha en inbyggd redundans, medan verksamhet som är koncentrerad till en enda plats normalt kräver större behov av skyddsåtgärder och alternativa lösningar.

Företagen kan behöva förbereda arbetsplatser och lokaler som kan användas om ordinarie lokaler och anläggningar inte är tillgängliga, exempelvis genom att teckna avtal om tillgång till tillfälliga lokaler. Dessa bör regelbundet kontrolleras och övas så att de snabbt kan tas i bruk vid behov.

Vid planeringen av lokaler bör företagen särskilt beakta behov av robusthet, säkerhet och uthållighet.

Robusthet: Planeringen bör omfatta åtgärder som bidrar till att lokaler och dess tekniska system kan motstå och hantera förväntade störningar. Det kan exempelvis handla om bortfall av elförsörjning eller datakommunikation, avbrott i externa försörjningssystem eller störningar i kritisk infrastruktur. Exempel på åtgärder kan vara reservkraft med tillräcklig drivmedelsförsörjning, alternativa kommunikationslösningar samt redundanta anslutningar till kritiska tjänster.

Säkerhet: Planeringen bör omfatta åtgärder för att skydda personal, information, utrustning och lokaler mot obehörig åtkomst, skada eller påverkan. Det kan exempelvis handla om skydd mot inbrott, sabotage, dataintrång eller annan antagonistisk verksamhet. Företagen bör beakta att betalningsverksamhet kan utgöra ett samhällsviktigt mål och anpassa säkerhetsnivån därefter. Säkerhetsåtgärder kan bland annat bestå av förstärkning av fysiskt skydd, tillträdesskydd, övervakning, informationssäkerhetsåtgärder och andra skyddsåtgärder anpassade efter verksamhetens skyddsvärden.

Uthållighet: Planeringen bör omfatta åtgärder som bidrar till att lokaler och dess tekniska system kan användas under den tid verksamheten ska upprätthållas vid höjd beredskap. Det kan exempelvis omfatta tillgång till reservdelar, kritisk utrustning och försörjningsresurser. Åtgärderna kan vara lagerhållning av kritiska resurser, planering för återanskaffning samt lösningar för långvarig drift under störda förhållanden.

Stödfrågor – lokaler och anläggningar

- Vilka funktioner kräver fysiska lokaler och vilka kan bedrivas på distans?
- Är ordinarie lokaler dimensionerade för att möta verksamhetens behov vid höjd beredskap?
- Hur länge kan lokalerna fungera vid strömavbrott?
- Hur påverkas verksamheten vid bortfall av internet, telefoni eller andra kommunikationstjänster?
- Finns alternativa kommunikationsvägar?
- Är vattenförsörjning, värme, ventilation och sanitära funktioner tillräckligt robusta vid exempelvis skiftgång?
- Har lokalerna geografisk spridning eller är verksamheten koncentrerad till ett specifikt geografiskt område?
- Hur ser tillgång till alternativa lokaler ut för prioriterad verksamhet vid höjd beredskap?
- Behöver teknik och utrustning flyttas med till alternativa verksamhetsplatser?
- Finns andra beroenden till leverantörer, fastighetsägare eller tekniska tjänster för att kunna bedriva verksamheten i lokalerna?

Se även avsnitten **Informationsteknik**, **Kritiska beroenden** och **Skydd och bevakning**.

Läs mer i Myndigheten för civilt försvars **Vägledning Ledningsplatser – Med planering av lokaler, skydd och bevakning** samt Säkerhetspolisens **vägledningar vad gäller säkerhetskänslig verksamhet**.

5.5 Informationsförsörjning

Att planera för att kunna tillgodose betalningsverksamhetens behov av information innebär bland annat att identifiera vilken information som är kritisk, var den finns och hur den ska hanteras. Det är också viktigt att tydliggöra vilka delar av den egna verksamheten som behöver informationen.

I planeringen bör företaget kartlägga vilka aktörer som förfogar över den information som krävs för verksamheten. Information kan finnas internt, hos leverantörer, kunder, branschorganisationer och offentliga aktörer, men också hos internationella företag och organisationer eller utländska samarbetsparter. Eftersom informationsbehov ofta är ömsesidiga är det även viktigt att föra dialog med dessa aktörer för att identifiera beroenden i informationsförsörjningen.

Planeringen kan även beskriva hur information ska inhämtas och eventuellt delas. Det omfattar vilken information som efterfrågas, i vilket format den ska lämnas och vilka kanaler som ska användas. Arbetssätten bör kunna anpassas när förutsättningarna förändras.

Stödfrågor – informationsförsörjning

- Vilken information är kritisk för att upprätthålla betalningsverksamheten?
- Vilka delar av verksamheten behöver ta del av informationen?
- Skiljer sig informationsbehovet mellan vardag, kris och höjd beredskap?
- Vilka interna funktioner och externa aktörer har den kritiska informationen?
- Finns beroenden i informationskedjan som företaget har ansvar för?
- När och på vilket sätt ska informationen samlas in och delas?



Läs mer i Myndigheten för civilt försvars **Nationella plan för informationsförsörjning**.

5.6 Informationsteknik

För en fungerande informationsförsörjning behövs informationsteknik som säkerställer att informationen är tillgänglig, korrekt och användbar även vid störningar. Att planera för att kunna tillgodose företagets behov av informationsteknik under höjd beredskap omfattar såväl skydd av information som av system, nätverk, resurser och tjänster.

En viktig utgångspunkt i arbetet är att informationssystem, elektronisk kommunikation, elförsörjning och annan kritisk infrastruktur kan drabbas av långvariga och omfattande störningar. Särskilt viktigt är därför planering av redundans för kritiska system, återställningsförmåga samt kontinuitet för verksamhetskritiska tjänster.

Planeringen bör omfatta organisatoriska, administrativa, fysiska och tekniska säkerhetsåtgärder. Organisatoriska och administrativa säkerhetsåtgärder kan exempelvis innebära säkerhetsstyrning, behörighetsstyrning och kontinuitets- och incidenthanteringsrutiner. Fysiska säkerhetsåtgärder kan utgöras av tillträdesskydd och bevakning. Tekniska säkerhetsåtgärder kan exempelvis bestå av reservkraft, säkerhetskopiering, alternativa nätverksförbindelser, nätverkssegmentering, kryptering, skydd mot skadlig kod samt lösningar för att upptäcka, hantera och återställa efter cyberangrepp. Utgångspunkten bör vara att de tekniska säkerhetsåtgärderna ständigt anpassas utifrån aktuell hotbild, teknikens utveckling samt förändringar i omvärlden.

Motsvarande säkerhetsåtgärder bör även beaktas vid anskaffning, utveckling och förvaltning av verksamhetskritiska system. Motståndskraften kan exempelvis stärkas genom geografiskt separerade datahallar, alternativa leverantörer, möjlighet att flytta kritiska tjänster till alternativa driftsmiljöer samt robusta och beprövade backuplösningar anpassade för att motstå kvalificerade hotaktörer. Företaget kan behöva säkerställa tillgång till lokal reservkraft där det är nödvändigt samt regelbundet testa återläsning av data och återställning av system, förslagsvis genom tester som omfattar flera verksamhetskritiska system samtidigt.

Stödfrågor – informationsteknik

- Vilka system, nätverk och digitala tjänster är kritiska för att upprätthålla betalningsverksamheten?
- I vilken mån är verksamhetskritiska system och informationsmängder skyddade mot allvarliga driftstörningar, kvalificerade cyberangrepp och antagonistiska handlingar?
- Vilka säkerhetsåtgärder finns för att förebygga, upptäcka och hantera ett kvalificerat cyberangrepp?
- Vilka reserv- och återställningslösningar finns för verksamhetskritiska funktioner?
- Vilka beroenden finns till externa leverantörer, molntjänster och kommunikationslösningar?
- Vilken redundans finns i it-infrastrukturen så att verksamheten kan upprätthållas vid bortfall av en driftmiljö eller annan kritisk infrastrukturkomponent?
- Har driftmiljöernas geografiska placering planerats med hänsyn till geografiska beroenden och koncentrationsrisker?
- Finns möjlighet att flytta verksamhetskritiska tjänster till alternativa it-miljöer eller leverantörer vid långvariga störningar?
- Hur lång tid tar det att återställa verksamhetskritiska system och data efter ett avbrott, och vilka konsekvenser uppstår om återställningen fördröjs?
- Hur ofta testas återläsning av data och återställning av system?
- Finns behov av reservkraft eller andra åtgärder för att säkerställa driften av de verksamhetskritiska systemen vid långvariga störningar i elförsörjningen?
- Vilka behov finns för att trygga bränsleförsörjningen till reservkraft?

5.7 Skydd och bevakning

Att planera för att kunna tillgodose företagets behov av skydd och bevakning under höjd beredskap omfattar skydd av personal, lokaler, anläggningar, utrustning, information och andra tillgångar så att verksamheten kan upprätthållas även vid allvarliga störningar och exempelvis antagonistiska hot. Planeringen bör utgå från verksamhetens skyddsvärden och beakta risker för bland annat sabotage, intrång, spionerі, otillbörlig påverkan, stridshandlingar och händelser som involverar farliga ämnen, CBRNE[19]. I denna planering bör företagen även utgå från att hotbilden kan förändras och att tillgången till samhälleliga resurser kan vara begränsad. Företaget kan därför utgå från att i större utsträckning behöva förlita sig på egna skydds- och bevakningsåtgärder utöver de skyddsåtgärder och resurser som samhället tillhandahåller.

Företaget bör planera för organisatoriska, fysiska och tekniska skyddsåtgärder för att förebygga, upptäcka och hantera störningar och angrepp under höjd beredskap. Sådana åtgärder kan exempelvis omfatta säkerhetsrutiner, incidenthantering, utbildning och övning, tillträdesskydd, bevakning, larm, passerkontroll och förstärkt informationssäkerhet. Planeringen bör särskilt beakta behovet av åtgärder för att skydda personalen, såsom möjligheter till utrymning, alternativa arbetsplatser, distansarbete, tillgång till skyddsutrustning samt utbildning i relevanta säkerhets- och beredskapsfrågor.

Valet av skydds- och bevakningsåtgärder bör anpassas efter verksamhetens förutsättningar och behov av kontinuitet. Ett konkret exempel är planering för alternativa verksamhetsplatser. Om verksamheten snabbt kan flyttas till en annan plats eller bedrivas genom distansarbete kan behovet av omfattande fysiska skydds- och bevakningsåtgärder på den ordinarie platsen minska. Om verksamheten däremot är beroende av att bedrivas från en specifik plats under längre tid ökar kraven på fysiskt skydd och uthållighet. Det kan exempelvis innebära behov av förstärkt bevakning, reservkraft, skydd för kritisk utrustning, etablerad samverkan med räddningstjänst och andra aktörer, tillgång till skyddsutrustning samt mer omfattande utbildning och övning av personalen, inklusive hantering av CBRNE-relaterade händelser.

[19] Kemiska, biologiska, radiologiska, nukleära och explosiva ämnen.

Stödfrågor – skydd och bevakning

- Vilka lokaler, anläggningar, informationstillgångar, funktioner och resurser är mest kritiska för att upprätthålla verksamheten under höjd beredskap? Vilka av dessa tillgångar bör prioriteras för skydd om resurserna är begränsade?
- Vilka risker har identifierats utifrån rådande hotbild?
- Finns det geografiska faktorer som gör verksamheten särskilt sårbar? Kan risker från närliggande verksamheter eller infrastruktur påverka verksamheten, exempelvis CBRNE-risker?
- Vilken skyddsnivå krävs för olika lokaler, anläggningar och andra skyddsvärda tillgångar?
- Vilken förmåga har verksamhetens skalskydd, passerkontroll, inbrottsskydd, larm och övervakning att förebygga, upptäcka och fördröja intrång eller sabotage?
- Hur länge kan skydds- och bevakningsåtgärder upprätthållas vid bortfall av externa tjänster, leverantörer eller samhällsstöd exempelvis vid avbrott i elförsörjning eller elektroniska kommunikationer?
- Vilka beroenden finns till externa bevakningsföretag eller andra säkerhetsleverantörer?
- Vilka skydds- och bevakningsåtgärder behöver förstärkas under höjd beredskap?
- Finns alternativa lösningar för att upprätthålla skydd och bevakning vid personalbrist eller leveransstörningar?
- Vilka myndigheter, leverantörer och andra aktörer behöver företaget samverka med för att stärka skyddet och bevakningen under höjd beredskap?



Läs mer i Myndigheten för civil **försvars Vägledning Ledningsplatser – Med planering av lokaler, skydd och bevakning**.

5.8 Kritiska beroenden

Betalningsverksamhet är ofta beroende av externa och internationella aktörer för exempelvis betalningsinfrastruktur, it-drift och elförsörjning. Inför höjd beredskap behöver planeringen därför utgå från att kritiska tjänster kan bli otillgängliga, kraftigt fördröjda eller fungera endast i begränsad omfattning. En viktig del i analysarbetet är att identifiera externa beroenden för att synliggöra vilka varor och tjänster som verksamheten är beroende av samt hur verksamheten kan upprätthållas med egna eller alternativa resurser. Detta för att kunna upprätthålla den mest kritiska verksamheten, åtminstone på en reducerad nivå, så långt det går.

Planeringen och förberedelsen kan innefatta att analysera om verksamhetskritiska processer kan upprätthållas genom interna lösningar, system eller manuella rutiner om externa tjänster inte är tillgängliga. Det omfattande och ökande beroendet av it-tjänster och datalagring utomlands behöver beaktas i planeringen. Företagen bör överväga hur kritiska funktioner kan upprätthållas även vid begränsad tillgång till sådana tjänster, exempelvis genom lokala eller nationella alternativ. Motsvarande överväganden kan behövas för att säkerställa tillgång till kritiska data. Andra åtgärder för att stärka verksamheten kan vara att införskaffa reservkraft, lagerhålla kritiska komponenter, överföra nyckelkompetens, ta fram reservrutiner eller hitta alternativa sätt att hantera kritisk utrustning.

Ett viktigt förhållningssätt som bör genomsyra planeringsarbetet är att motsvarande krav som ställs mot den egna verksamheten, även kan behöva regleras gentemot leverantörer av externa tjänster. Det kan exempelvis handla om att ställa krav på leverantörer avseende samverkan och informationsutbyte, incidentrapportering, drift och underhåll, it-säkerhet, redundans, reservrutiner och kontinuitetshantering.

Även beroendet av internationellt stöd och specialistkompetens kan behöva hanteras genom att säkerställa att den egna personalen har tillräcklig kompetens för att kunna driva och underhålla verksamheten mer självständigt. Det kan också handla om att säkerställa att informationsdelning kan upprätthållas vid begränsad eller utebliven uppkoppling, exempelvis genom alternativa kommunikationsvägar.

Stödfrågor – kritiska beroenden

- Vilka externa aktörer är kritiska för betalningsverksamheten?
- Finns det beroenden som är särskilt sårbara i ett förändrat säkerhetsläge?
- Finns det koncentration till enstaka leverantörer eller geografiska områden?
- Vilka krav finns idag på leverantörer avseende kontinuitet och tillgänglighet?
- Vilka förutsättningar eller överenskommelser finns med leverantörer för att säkerställa fortsatt funktion, till exempel genom force majeure-klausuler för höjd beredskap?
- Finns det alternativa leverantörer eller lösningar för kritiska beroenden?
- På vilket sätt kan störningar som ändå riskerar att uppstå hanteras?
- Finns det kvarstående risker som ska accepteras efter att företaget vidtagit åtgärder för att minska påverkan av ett bortfall? Hur dokumenteras dessa och följs upp?

Relationen till Dora-förordningen

Vissa företag omfattas av EU-förordningen för digital operativ motståndskraft (Dora-förordningen). Förordningen ställer bland annat krav på hur företagen ska hantera risker kring informations- och kommunikationsteknologi (IKT).

Regleringen som rör företagens planering inför fredstida kriser och höjd beredskap har ett annat syfte än Dora-förordningens. De riskanalyser som företagen har genomfört enligt Dora-förordningen kan dock, i relevanta delar, användas i planeringen, förutsatt att de kompletteras med de bedömningar som krävs inför fredstida kriser och höjd beredskap.

5.9 Omlokalisering

Behovet av planering för omlokalisering kan variera för företagen beroende på hur geografiskt spridd betalningsverksamheten är. Företagen behöver se över vilka beroenden de har till olika geografiska områden och vilka åtgärder de ska vidta för att upprätthålla sin betalningsverksamhet om något av dessa måste utrymmas.

Med utgångpunkt i övriga planer för krigsorganisationen bör planeringen för omlokalisering inledningsvis kartlägga var kritiska funktioner, system och personal finns. Planeringen kan också omfatta under vilka omständigheter verksamhet bör flyttas och hur ett sådant beslut bör omsättas i praktiken, exempelvis genom att säkerställa att personalen vet hur de ska agera vid ett beslut om omlokalisering. Planeringen bör även omfatta hur organisationens behov av fysiskt skydd och säkerhet ska upprätthållas på en acceptabel nivå, samt hur skydd av information ska säkerställas under omlokaliseringen. Syftet med planeringen är att skapa förutsättningar för att snabbt kunna anpassa verksamheten till förändrade geografiska förutsättningar och därmed upprätthålla kritiska funktioner även om delar av verksamheten tvingas flytta eller tillfälligt upphöra.

Stödfrågor – omlokalisering

- Vilka funktioner är mest kritiska att upprätthålla vid en omlokalisering?
- Finns verksamhetsplatser där ett omlokaliseringsbeslut skulle få särskilt stora konsekvenser?
- Har företaget definierat vilka omständigheter som kan utlösa ett beslut om omlokalisering? Finns det kriterier för när verksamhet ska flyttas respektive tillfälligt upphöra? Hur prioriteras vad som ska flyttas respektive lämnas?
- Finns tydliga beslutsvägar och mandat för att fatta beslut om omlokalisering?
- Är roller och ansvar för omlokalisering dokumenterade och kommunicerade?
- Hur snabbt kan verksamheten flyttas till alternativa lokaler? Har företaget identifierat accepterade avbrottstider för kritiska funktioner vid omlokalisering?
- Vilka åtgärder krävs för att kritiska betaltjänster kan upprätthållas under och efter en omlokalisering?
- Finns rutiner för att kommunicera beslut om omlokalisering till personalen?
- Vilka stödfunktioner har personal som omlokaliseras behov av?
- Vilka behov finns av att samverka med myndigheter och andra aktörer inför eller vid en omlokalisering?



Läs mer i Myndigheten för civilt försvars **Vägledning Omflyttningsplan**.

6 Övning och utbildning

Genom att arbeta systematiskt med övning och utbildning skapas förutsättningar för att betalningsverksamheten ska kunna upprätthållas även under störda förhållanden. En flerårig utbildnings- och övningsplan möjliggör att brister identifieras och åtgärdas över tid samt bidrar till en långsiktig förmågeutveckling.

I den gemensamma övningsinriktningen för totalförsvaret, som Försvarsmakten och Myndigheten för civilt försvar har tagit fram, framgår övergripande prioriteringar för övningsverksamheten under de kommande åren. Inriktningen är att typsituationerna bör användas som ett konkret stöd för att öva identifierade förmågor. Särskild vikt ska läggas vid övningar som stärker aktörernas förmåga att prioritera, förebygga och hantera effekterna av allvarlig påverkan samt förmågan att snabbt återställa verksamhet och samhällsfunktioner efter en störning. Att öva samverkan och samarbete mellan totalförsvarets aktörer är också centralt. Förmågan att ta fram lägesbilder för inriktning och samordning samt förmågan till övergången av fredstida organisation till krigsorganisation är andra viktiga delar att öva.[20] Befintliga beredskapsplaner kan ligga till grund för planering och genomförande av övningar för att pröva och verifiera genomförbarheten av planerna.



Läs mer i Försvarsmaktens och Myndigheten för civilt försvars **Gemensam övningsinriktning för totalförsvaret** och i Myndigheten för civilt försvars **Metodstöd för fleråriga utbildnings- och övningsplaner**.

[20] Gemensam övningsinriktning för totalförsvaret (FM2026-7982:1 och MCF 2026-02489-1).

7 Planeringsstege

Planeringsstegen kan användas som stöd för företagens arbete med att utveckla sin beredskap och krigsorganisation, med ambitionen att successivt nå en så hög nivå som möjligt.

Tabell 1. Planeringsstege

1	Företaget har påbörjat beredskapsarbetet för upprätthållandet av betalningsverksamheten.
2	Företaget har analyserat vilka delar av sin verksamhet som ingår i betalningsverksamheten och vilka uppgifter som är prioriterade under höjd beredskap.
3	Företaget har utifrån sin analys fastställt hur betalningsverksamheten ska organiseras och ledas vid höjd beredskap. Företaget har även planerat och dokumenterat övergången till krigsorganisationen. Företaget har även analyserat och fastställt krigsorganisationens behov av personal och hur dessa behov ska tillgodoses. Företaget har en bemannad krigsorganisation.
4	Företaget har utifrån krigsorganisationens uppgifter, verksamhet och behov fastställt hur behov av lokaler samt information och informationsteknik ska tillgodoses vid höjd beredskap. Företaget har även identifierat kritiska externa beroenden och analyserat hur betalningsverksamheten påverkas vid bortfall av dessa. Vidare har företaget fastställt hur behov av skydd och bevakning ska tillgodoses samt planerat för utrymning av områden där företaget har betalningsverksamhet.
5	Företaget har en utbildad och övad krigsorganisation. Företaget har planerat åtgärder för att minska påverkan vid bortfall av kritiska externa beroenden. Företaget har fastställt hur behov av skydd och bevakning ska tillgodoses samt planerat för utrymning. Företaget har övat hur övergången och krigsorganisationen ska fungera. Planeringen ses över minst årligen.
6	Företaget har vidtagit åtgärder för att minska påverkan vid bortfall av kritiska beroenden. Utöver ovan har företaget analyserat och fastställt eventuella övriga behov för att kunna upprätthålla betalningsverksamheten vid höjd beredskap. Företaget övar regelbundet övergången till krigsorganisation samt hur krigsorganisationen ska fungera. Planeringen ses över och uppdateras vid behov. Erfarenheter och åtgärdsbehov från övningar omhändertas och implementeras i planeringen vid behov.



SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se