HANDBOK FÖR PLANERING AV ÖVNINGS-PROGRAM OCH VERKSAMHET INOM DIGI-TAL SÄKERHET

Väestörekisterikeskus

Innehållsförteckning

1 Verksamhetens utgångspunkter och bakgrund

1.1 Inledning

Denna handbok är avsedd som stöd för den strategiska planeringen av övningsverksamheten för direktörer och experter som ansvarar för beredskapen i nätverk, riskhanteringen och övningsverksamheten i organisationer. Dessutom informerar handboken den högsta ledningen om varför det är nödvändigt att planera övningsverksamheten på lång sikt för att trygga den kontinuerliga verksamheten och höja beredskapsnivån inom organisationen. I handboken tillhandahålls också en grund för förhands- och årsplaneringen av olika övningar.

Övning är ett effektivt sätt att testa organisationens verksamhet och identifiera utvecklingsobjekt. Övning bidrar till att rikta verksamhetsmöjligheterna till aspekter som är väsentliga med tanke på verksamheten. Den här handboken, övningsmodellen och -planen för att utveckla och ordna olika övningar kring digital säkerhet har producerats som en del av Befolkningsregistercentralens utvecklingsprogram för digital säkerhet inom den offentliga förvaltningen (JUDO).

Övningsprogrammet och -verksamheten är viktiga delar i organisationens långsiktiga beredskap för eventuella kriser och störningssituationer. Man försöker vanligen förbereda sig för olika störningssituationer genom planer som görs upp på förhand. I planerna beaktas sådana hot och risker som kan ge upphov till en störningssituation. Dessutom tar man i planerna ställning till hur den personal som behövs ska utbildas, hur man ska planera organisationens ledningsmodeller och alternativa handlingssätt som lämpar sig för störningssituationer samt fastställs tillfälliga lokaler och andra utrymmen som behövs i en störningssituation. I planerna beaktas vanligtvis den tid som behövs för återhämtning och beskrivs de verksamhetssätt med vilka man bäst eller så snabbt som möjligt når en tillräcklig servicenivå. Det krävs övning för att testa en sådan här plan och konstatera att den fungerar.

Övningarna utgår från hot- och riskanalyser. Grundligt utarbetade analyser gör det lättare att skapa sig en bild av de situationer som övningsverksamheten bör inriktas på. Det är nyttigt att fokusera övningarna på hot som har en omfattande inverkan.

För en nätverksbaserad verksamhetsmiljö krävs att hela leverans- eller servicekedjan ses över eftersom uttrycket ”Ingen kedja är starkare än sin svagaste länk” stämmer bra även vad gäller övningsverksamhet. Såväl enskilda offentliga organisationers som privata företags verksamhet kan med tanke på samhället ha en avgörande betydelse då en störningssituation rättas till.

Det krävs betydande ekonomiska resurser för att upprätthålla verksamheten särskilt i allvarliga störningssituationer eller undantagsförhållanden. Även om undantagsförhållanden kan betraktas som mycket osannolika är det ändå bra att förbereda sig för sådana med planer som testas genom övning.

Utöver att läsa denna handbok är det bra att även ta del av den anvisning för cyberövningar som Transport- och kommunikationsverket (Traficom) publicerat. I den beskrivs mer detaljerat hur en övning ordnas, och den fungerar bättre som handbok för den som leder övningen eller ansvarar för genomförandet.

1.2 Använda handboken

Centrala termer som används i den här handboken är övningsprogram, övningsverksamhet och övning i en digital säkerhetsmiljö.

Med övningsprogram avses systematisk kartläggning och samling av övningar. I övningsprogrammet beaktas behoven av att delta med tanke på utvecklandet av organisationens egna funktioner. I vissa fall kan övningsprogrammet utarbetas av en utomstående organisation, till exempel Säkerhetskommittén (VALHA), Försörjningsberedskapscentralen (TIETO) eller ENISA (Cyber Europa).

I övningsprogrammet antecknas vanligen också innehållet i övningsverksamheten, det vill säga en beskrivning av typerna av övningar och målsättningen med dem. Övningsverksamheten inbegriper alla aspekter som behövs för att ordna organisationens övningar. Ansvaren för övningsverksamheten kan till exempel anförtros en person i ledningsgruppen som en del av ansvaren för beredskap och säkerhet, men ofta är det beredskapschefen eller en motsvarande expert som får ansvaret för att utarbeta och upprätthålla övningsprogrammet.

En övning är en enskild händelse, och de som deltar agerar enligt ett program som har planerats och förberetts på förhand. Man samlar in respons om övningen. Responsen analyseras för att ta fram en lista över utvecklingsåtgärder, bland vilka man väljer de viktigaste för genomförande. Övningsprogrammet och -verksamheten beskrivs närmare senare i denna handbok.

1.3 Läsarens stig

Den här handboken omfattar tre steg som inviger läsaren i den strategiska planeringen av ett övningsprogram. Dessa steg omfattar strategiska riktlinjer för övningsprogrammet, element i den strategiska planeringen samt operativ årsplanering.

Organisationens insikter om den egna mognadsnivån (med andra ord om vilken nivå av övningsverksamhet organisationen klarar av) har en direkt inverkan på den strategiska planeringen av övningsprogrammet och samtidigt även på organisationens förmåga att öva.

Handboken innehåller såväl bakgrundsinformation för planeringen och budgeteringen som planeringsunderlag och minneslistor för de personer som ansvarar för övningsprogrammet, övningsplanen och övningen.

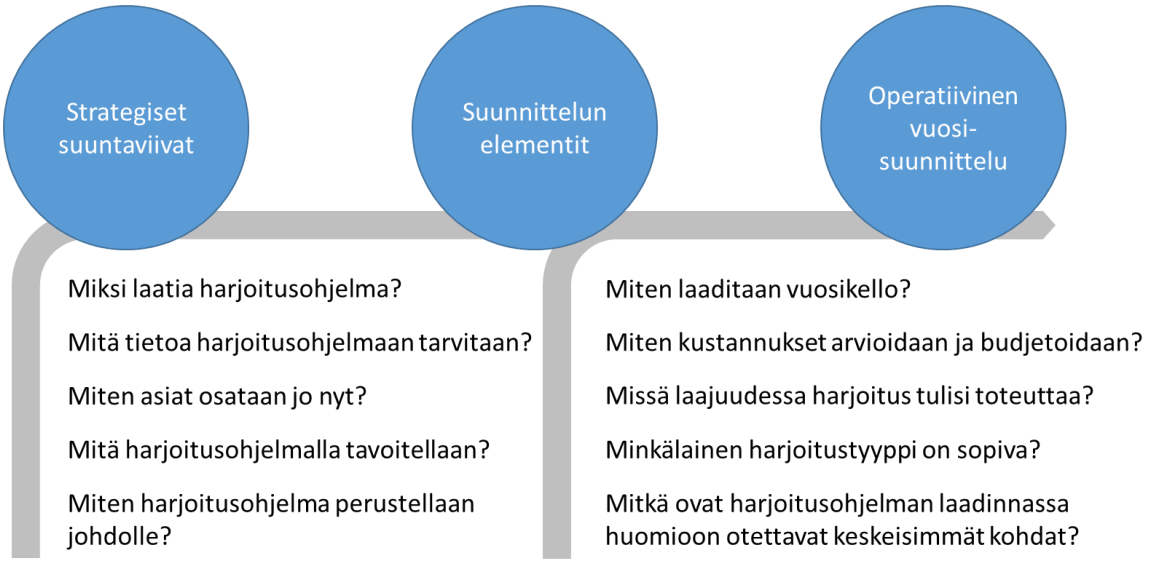

Bild 1: Läsaren stig – de tre helheterna i handboken

2 Strategiska riktlinjer för övningsprogrammet

2.1 Koppla övningsprogrammet till organisationens mål

En av de viktigaste aspekterna i organisationsledning är att tydligt fastställa mål. I en verksamhetsmiljö som förändras snabbt kan målen och de arbetssätt som överenskommits för att nå dessa enkelt glömmas bort, om de inte lyfts fram tillräckligt. Om målen är tydliga och de anställda vet hur målen kan nås, kan olika personer göra val som stödjer målen i sin dagliga verksamhet.

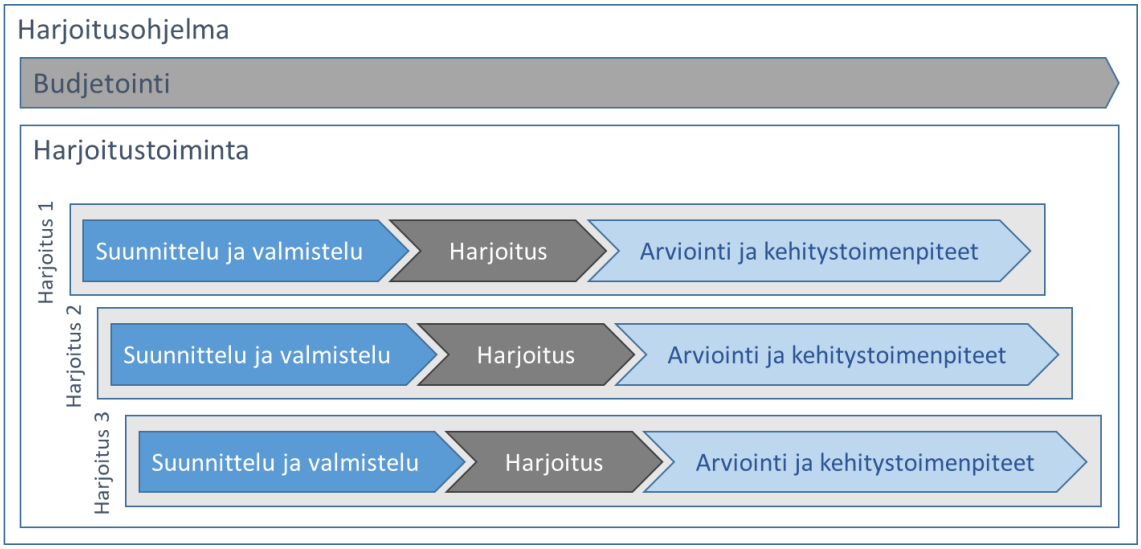

Bild 2: Övningsprogrammets olika delar

Med hjälp av ett övningsprogram kan organisationens mål regelbundet repeteras och de arbetssätt som kopplas till dem lyftas fram. Därför är det synnerligen viktigt att övningsprogrammet alltid kopplas till organisationens operativa mål. Den strategiska planeringen av övningsprogrammet utgår från följande:

1 Planeringen av övningsprogrammet ska utgå från organisationens syfte och från hur övningsverksamheten hjälper och stödjer samarbetet mellan individer och grupper.
2 Organisationens verksamhetsidé (mission), vision och värderingar – verksamhetsprinciper som arbetsgemenskapen har ansett vara bra och viktiga – ska synas i planeringen av övningsprogrammet.
3 Den långsiktiga planen för övningsprogrammet ska svara mot de framtida utmaningar som organisationen identifierat och den verksamhetsplan eller strategi som utarbetats utifrån dessa. Genom att planera övningsprogrammet på lång sikt strävar man efter att rikta resurserna rätt, bekämpa hot som identifierats och utnyttja de erfarenheter övningarna gett då man utvecklar kontinuitetsstyrningen, riskhanteringen och säkerhetsledningen samt eventuellt ser över strategin.

Med hjälp av övningsprogrammet bygger organisationen upp sin egen reaktionsberedskap inför störningssituationer. Övningar som följer övningsprogrammet hjälper organisationen att snabbbare återgå till normalläget före krisen efter en eventuell störningssituation. I samband med planeringen och genomförandet av de övningar som hör till övningsprogrammet kan man göra nya,

viktiga observationer som bör utnyttjas för att förebygga och förutspå eventuella störningssituationer.

2.2 Basinformation som behövs för planeringen av övningsprogrammet

Övningsprogrammet utgår från det behov av övning som organisationen identifierat. En lång period utan störningar kan försämra organisationens förmåga att reagera på störningssituationer. Vissa organisationer kan ha en lagstadgad skyldighet att upprätthålla beredskapen, men mängden övningar och övningarnas karaktär har vanligen inte fastställts så noga. Övningarna spelar emellertid ofta en viktig roll för hur organisationen hanterar störningssituationer och återhämtar sig från dem. Till exempel en brandkår kan öva särskilt aktivt då läget varit lugnare en längre tid. Då en eldsvåda uppstår är varje minut viktig.

Basinformation som behövs vid strategisk planering av ett övningsprogram för digital säkerhet är:

A. en risk- och effektivitetsanalys av vilken framgår händelser som hotar organisationens verksamhet och effekterna av dem

B. en beskrivning av organisationens kritiska funktioner av vilken framgår den inbördes växelverkan mellan processer och aktörer

C. en beskrivning av yrkesgrupper, roller och uppgifter som behövs i organisationens verksamhet eller produktionen av tjänster. Information om antalet anställda per enhet underlättar planeringen ytterligare.

D. en lista över organisationens verksamhetsställen

E. en lista över dokument som organisationen använder (planer, anvisningar osv. med anknytning till ämnet)

F. en beskrivning av de verksamhetssätt, processer och verktyg som tillämpas i beredskapen och kontinuitetsstyrningen

G. en beskrivning av hur övningsverksamheten ser ut för närvarande

H. organisationens arkivbildnings- eller informationsstyrningsplan utifrån vilken man kan fastställa behovet av att skydda dokumentationen av övningsprogrammet och -verksamheten (offentlig, sekretessbelagd, säkerhetsklass I–IV).

Den basinformation som vanligtvis behövs beskrivs i organisationens dokumentation kring riskhantering och beredskap, som omfattar bland annat riskhanterings-, beredskaps-, kontinuitets- och kriskommunikationsplaner. Den person som ansvarar för övningsverksamheten ska känna till planerna väl för att kunna samla informationen. Framskaffandet av basinformation underlättas också av internationella standarder såsom SFS-EN ISO 22301.

2.2.1 Avtal

Då man planerar övningsprogrammet och -verksamheten stöter man ofta på situationer där det behövs hjälp av en viss tjänsteproducent för att en övning som organisationen har nytta av ska kunna genomföras. Om det i övningen saknas en leverantör av en servicehelhet som kan agera

på det sätt störningssituationen kräver för att rätta till problemet, kommer det att saknas en viktig del av övningen. Exempel på sådana situationer är utkontrakterade tjänster för underhåll av informationssystem eller certifikattjänster.

Om tjänsterna helt eller delvis skaffas av en tjänsteproducent ska man komma överens om beredskapen i avtalen. Vanligtvis ingår det dock inget krav på att delta i övningsverksamhet i avtalen. För att få med övningsverksamheten i avtalet krävs det i praktiken att kraven detaljerat och entydigt antecknas i avtalet redan i upphandlingsskedet. Det kan till exempel krävas att leverantören deltar i övningar som en del av den normala avtalsbaserade serviceverksamheten. I avtalen strävar man efter att övningsverksamheten ska ses som en del av det ömsesidiga utvecklingsarbetet och inte endast betraktas som en källa till extra kostnader.

Kraven som berör övningsprogrammet och -verksamheten utvidgas att omfatta även avtal som påverkar kontinuiteten vad gäller kritiska funktioner inom organisationen. Sådana är till exempel avtal om utkontrakterade tjänster, köpta tjänster eller materialanskaffningar, till exempel hyresavtal för fastigheter. Övningsverksamheten ska beaktas även vid gemensamma upphandlingar.

Vid långsiktig planering är det skäl att beakta hur de avtal som ingåtts med leverantörer påverkar tidspannet för planeringen och kostnaderna. Om man måste ingå ett separat avtal med en leverantör om deltagande i en övning ska resurser reserveras i god tid så att man kan säkerställa att leverantörens experter kan delta. Avtal där övningar redan ingår i servicen kopplas till organisationens övningsprogram.

Den avtalsbaserade beredskapen är en etablerad del av kontinuitetsstyrningen. Det har utarbetats handböcker och anvisningar för avtalsbaserad beredskap. Handböckerna och anvisningarna finns fritt tillgängliga för organisationerna. Exempel hittas i bilaga A.

2.2.2 Norm- och standardgrund

Beredskapen och kontinuiteten kring digital säkerhet tryggas genom författningar som gäller elektronisk kommunikation, dataskydd och försörjningsberedskap. Sådana författningar är bland annat beredskapslagen, räddningslagen, dataskyddslagen, lagen om tryggande av försörjningsberedskapen och informationssamhällsbalken.

De principbeslut och strategier som statsrådet publicerat skapar å sin sida en grund för övningsprogram och -verksamhet. Exempel på sådana är målen för försörjningsberedskapen, den allmänna säkerhetsstrategin och den nationella cybersäkerhetsstrategin.

Inom statsförvaltningen innehåller publikationer av Juhta och VAHTI gott om rekommendationer för utveckling av den digitala säkerheten. Organisationer kan också ha egna anvisningar för digital säkerhet

Tryggandet av livsviktiga funktioner i samhället är ett livsvillkor för den nationella välfärden. Därför har det utarbetats lagar, förordningar, principbeslut, strategier, anvisningar och standarder som gäller beredskap och tryggande av kontinuiteten. De skapar en grund för övningsprogram och övningsverksamhet, men i vissa fall ålägger de också organisationer att upprätta sådana. Detta presenteras närmare i bilaga B.

2.3 Bedömning av nuläget för övningsprogram och -verksamhet

Allmänt taget kan man konstatera att åtgärderna för kontinuitetsstyrning varierar stort inom den offentliga sektorn. Enligt en utredning som Statens revisionsverk gjorde 2018 (Statens revisionsverks revisionsberättelse 20/2018) hade ämbetsverken i mycket varierande grad utarbetat planeringshandlingar för riskhantering och tryggande av kontinuiteten. Hälften av ämbetsverken hade både en riskhanterings- och en kontinuitetsplan eller åtminstone en av dessa medan en tredjedel av ämbetsverken inte hade någon plan alls. Planerna var dock oftast inte uppdaterade eller testade, och man hade sällan övat åtgärderna i dem.

I sin utredning konstaterar Statens revisionsverk dessutom att det inte har gjorts någon planering på förhand, att ledningsansvaret inte har fördelats och att ingen centraliserad anvisning har upprättats med tanke på störningssituationer. En betydande eller allvarlig störning i en tjänst eller verksamhet som sker i normala förhållanden kan emellertid leda till att verksamheten avbryts eller att servicenivån försämras avsevärt. I värsta fall kan verksamheten helt och hållet avbrytas och då går det inte att nå det strategiska mål som är viktigt för verksamheten. En störning leder alltid till skador eller kostnader och kan medföra betydande kostnader även för andra parter.

Om utgångspunkterna beaktas har övningsverksamheten mycket att ge med tanke på uppnåendet av målen för hela organisationens riskhantering och strategi. Övningsverksamheten kan inte nonchaleras utan den strategiska planering som förknippas med den måste tas på allvar. Riskhanteringen och kontinuitetsstyrningen och övningsverksamheten i anslutning till dessa måste göras till en del av organisationens dagliga ledning och verksamhet.

Bedömningen av nuläget är en av utgångspunkterna i utvecklandet av övningsverksamheten. Det finns fritt tillgängliga verktyg för organisationer för att bedöma nuläget. I bilaga C presenteras en modell.

2.4 Beskrivning av målen för övningsverksamheten

Genom övningsverksamhet strävar man efter att upprätthålla och utveckla organisationens beredskapsnivå och resiliens. Alla personer inom organisationen som arbetar med att säkerställa kontinuiteten, leda hanteringen av störningssituationer och återställa situationerna ska känna till de handlingsplaner som gjorts upp och sin egen roll för att rätta till störningssituationerna.

Krisberedskapen eller en lyckad övningsverksamhet kan betraktas som en uppfattning av och reklam för hur skicklig organisationen är och hur snabbt den kan reagera på förändringar i verksamhetsmiljön eller på plötsliga, överraskande och allvarliga störningssituationer.

Genom övningsverksamheten identifieras missförhållanden och brister i organisationens handlingsanvisningar samt kontinuitets- och återhämtningsplaner.

De personer som ansvarar för verksamhetens kontinuitet och beredskap får ofta frågan om varför man måste öva och vad man vill uppnå med beredskapen och övningarna. Det lönar sig att sammankoppla svaret på frågan med organisationens mål och vision. Ett bra svar innehåller följande element:

1. Uppfylla organisationens syfte och mål

- I svaret lyfts fram oron över hur organisationen har sett till att de egna uppgifterna genomförs och målen uppnås. Genom övningsverksamheten vill man försäkra att organisationen kan sköta de egna uppgifterna och nå sina mål även vid olika störningssituationer i verksamhetsmiljön.

- Övningsverksamheten ger möjlighet att systematiskt testa och utveckla kontinuitetsstyrningen och hanteringen av störningssituationer samt utveckla samarbetet mellan olika nyckelpersoner och team. Det ger inte ett lika bra resultat att enbart ta hand om störningssituationer i det verkliga livet. Utbildningar, besök, bedömningar eller auditeringar ger inte lika bra möjligheter till utveckling och lärdomar som övningar och deltagande i verkliga situationer.

2. Identifiera och beskriva konsekvenserna av risker som riktas mot organisationens verksamhet

   - Genom konkreta övningar kan man lyfta fram de helheter med anknytning till identifierade risker som man inte har beaktat eller kunna förutspå i riskanalyser. Som ett exempel kan nämnas att personalen under en störningssituation som berör arbetsutrymmena börjar utföra distansarbete, vilket i sin tur kan leda till att organisationens datakommunikationsnät överbelastas.

   - Det går vanligtvis att fastställa ett pris för risknivån och de realiserade riskerna. Genom satsningen på övningsverksamheten kan man minska sannolikheten för att riskerna realiseras och därmed även minska de ekonomiska förluster som skulle uppstå om riskerna realiserades.

3. Beskriva syftet och målen med övningsverksamheten genom scenarier

   - Ett välmotiverat skäl till övning väcker intresse, stannar i folks minne och lyfts fram i olika diskussioner. Exempelvis aktuella händelser kan utnyttjas som eventuella övningsscenarier eftersom de hjälper åhörarna att koppla ihop målen för övningsverksamheten med dagliga händelser.

   - Ett välbeskrivet scenario och ett mål som kopplats till detta skapar en naturlig diskussion om hur störningssituationer kan påverka organisationens dagliga verksamhet.

4. Använda ett enkelt och enhetligt språk

   - Varje person som deltar i övningar och även andra anställda inom organisationen bör få en förklaring på hur målet med övningen ansluter till deras eget arbete. Detta kräver att man anpassar budskapet till olika åhörare. Ledningen får koncis information medan man för till exempel tekniska experter detaljerat beskriver målen med övningarna.

5. Testa befintliga verktyg

   - De verktyg som används vid övningarna är desamma som används vid verkliga störningssituationer. Under övningarna säkerställs att de verktyg som valts är lämpliga och fungerande.

Genom övningsverksamheten utvecklas organisationens förmåga att fungera i förhållanden som avviker från de normala. Dessutom kan den påverka hur snabbt organisationen kan återhämta

sig från en störningssituation och hur eventuella konsekvenser, till exempel ekonomiska förluster, kan begränsas.

Den centrala uppgiften för ägaren eller den som genomför eller ansvarar för övningsverksamheten är att se till att övningsverksamheten systematiskt utvecklas och sträva efter att processerna, handlingsmodellerna och verktygen i den hela tiden utvecklas. På detta sätt blir verksamheten effektivare. Det är bra att hålla det enkelt och att utnyttja befintliga processer för beredskap och kontinuitetsstyrning.

3 Element i den strategiska planeringen av övningsverksamheten

3.1 Fastställa objekt för övningsverksamheten

3.1.1 Riskidentifiering och lista över kritiska funktioner

Organisationens kontinuitetsplanering ska grunda sig på en riskanalys där det bedöms hur sannolikt det är att händelserna inträffar och effekterna av dem i sådana fall. Risker som hotar organisationens verksamhet anknyter ofta till följande helheter:

1. Informationssystemen eller någon avgörande teknik är inte tillgängliga
    - Datareserver, informationssystem, anordningar, verktyg eller dataförbindelser är inte tillgängliga eller fungerar inte utan avbrott på grund av en omfattande störning. Detta kan bero på till exempel problem i elförsörjningen, skador i anordningarna, störningar i datakommunikationen eller problem i en tredje parts verksamhet.
2. Personalens arbete hindras
    - Ett betydande antal personresurser inom organisationen, en enhet eller funktion är otillgängliga. Detta kan bero på exempelvis en strejk eller storolycka.
3. Störningar som en tjänsteleverantör eller intressentgrupp råkat ut för stoppar tillgången till en viktig tjänst eller funktion
    - På grund av avbrott i en tredje parts (till exempel en viktig tjänsteleverantör, motpart, intressentgrupp, klienter eller liknande) verksamhet är en viss tjänst otillgänglig eller så produceras inte den nödvändiga informationen eller tjänsten. Exempel på detta är bland annat allvarliga störningar i ett finansierings- och betalningssystem, störningar i tillgången till finansiering av den offentliga ekonomin, störningar i kraftförsörjningen eller allvarliga störningar i samhällstekniken.
4. Lokaler är inte tillgängliga
    - Tillträdet till verksamhetsutrymmen som är viktiga för verksamheten stoppas eller en lokal som är avgörande för verksamheten är inte tillgänglig på grund av antingen externa eller interna faktorer. Orsaker till detta kan vara till exempel en eldsvåda, störning i leveransen av fjärrvärme eller liknande. Genom övningar kan man utreda vilka investeringar som krävs för att upprätthålla tillfälliga lokaler.

I den långsiktiga planeringen av övningsverksamheten bör man i synnerhet fästa uppmärksamhet vid att övningarna omfattar alla enheter i organisationen (inklusive stödfunktioner) som har en viktig roll i att sköta kärnfunktionerna. Likaså bör man ge akt på att nyckelpersoner för kontinuitetsstyrningen och hanteringen av störningssituationer samt deras ersättare (minst två ersät-

tare) och/eller alla olika skift och deras team regelbundet får övning i dessa uppgifter. I en enskild övning ligger fokus på att hantera en enskild störningssituation (till exempel en omfattande, långvarig datateknisk störning, brist på personalresurser eller eldsvåda), men den långsiktiga strategiska planen för övningsverksamheten ska omfatta alla betydande risker som hotar verksamheten i hela organisationen.

På webben finns fritt tillgängliga verktyg för riskanalys för organisationer (vissa verktyg är endast på finska): Riskhanteringsanvisning (på finska), Finansministeriets publikationer 22/2017; http://urn.fi/URN:ISBN:978-952-251-862-0 (Riskienhallintatyökalu - Excel - perusversio, Riskienhallintatyökalu - Excel - laajempi versio, Ohje riskienhallintatyökaluun) samt Försörjningsberedskapsscenarier 2030: https://cdn.huoltovarmuuskeskus.fi/app/uploads/2018/06/28140030/FBC-SCENARIER-2030.pdf

3.1.2 Kritiska funktioner

Det främsta objektet för övningsverksamheten är organisationens kritiska funktioner, det vill säga de processer, tjänster, ledningsmodeller och den infrastruktur utan vilka organisationen inte kan utföra sina uppgifter.

Då man väljer objekt kan man utnyttja en konsekvensanalys av organisationens funktioner. I konsekvensanalysen försöker man kartlägga de funktionella effekterna om olika risker realiseras. Då man identifierat verksamhetsmiljön, de objekt som ska skyddas samt kärnprocesserna och -funktionerna i anslutning till dem kan de klassificeras i kategorier enligt hur kritiska de är utifrån den information som samlats in. Utifrån kategorierna kan man välja objekt vars beredskap behöver utvecklas och därmed objekt för övningsverksamheten. I bilaga A finns en länk till ett verktyg för prioritering av funktioner.

3.1.3 Personalgrupper

Syftet med övningsverksamheten är att utbilda grupper, ledare, koordinatorer och andra nödvändiga personer med anknytning till beredskapen så att de är medvetna om sina roller i en störningssituation och sina uppgifter då störningssituationen ska rättas till. Övningsverksamheten riktas vanligtvis till följande grupper:

Personalgrupp	Roll i övningen
Direktörer	Tar ansvaret för ledningen under en störningssituation och för att återställa verksamheten till normalläge
Koordinatorer	Fungerar som stöd för ledningen och sörjer för koordineringen av de uppgifter som situationen kräver samt för uppföljningen av verksamheten och övervakningen
Kommunikationsexperter	Ansvarar för den informering till interna och externa intressentgrupper som situationen kräver
Experter på riskhantering och säkerhet	Sörjer för att sammanställa en lägesbild samt för att analysera och förutspå eventuella konsekvenser

Organisationens anställda, verksamhetsexperter	Försnabbar genom sin verksamhet återställandet till normalläge, ansvarar till exempel för att planera och genomföra korrigerande åtgärder
Externa intressentgrupper	Påverkar genom sin verksamhet organisationens återställningstid; externa aktörer bör tas med i planeringen och genomförandet av övningsverksamheten

Tabell 1: Personalgrupper som deltar i övningsverksamheten

3.2 Typer av övningar och val av dessa

3.2.1 Typer av övningar

Det finns olika typer av övningar att tillgå i övningsverksamheten. Organisationerna kan sammanställa en helhet som är lämplig med tanke på dess verksamhet och mognadsnivå.

Bild 3: Exempel på dimensionen för ett övningsprogram och övningsverksamheten

Övningsverksamheten består av olika övningar som alla har ett eget syfte och mål. Utan övning kan organisationen inte agera effektivt i en omfattande störningssituation. Cybersäkerhetscentralens handbok hjälper den som ordnar övningen att välja vilka typer av övningar som ska ingå i övningsprogrammet. Verksamheten kan utvecklas genom både lätta övningar och simulerade spelsituationer. De olika typerna av övningar kan indelas i exempelvis följande kategorier:

A. Skrivbordsövning

— I en skrivbordsövning bedöms organisationens funktionsförmåga i ett visst scenario. Deltagarna samlas för att diskutera vilka åtgärder som krävs i övningsscenariot.

— De personer som deltar i övningen har i uppgift att fundera på vilka åtgärder som krävs för att återhämta sig från störningssituationen. I diskussionen utnyttjas kontinuitets-, återhämtnings- eller beredskapsplaner samt andra etablerade verksamhetssätt inom organisationen.

— Då verksamheten under övningen jämförs med befintliga planer och metoder kan man identifiera utvecklingsobjekt och fastställa en tidtabell för utvecklandet och prioritetsordningen.

B. Pre mortem-övning

— I en pre-mortem-övning bedömer man vilken risk eller händelsekedja som kan leda till att en sådan situation som beskrivs i scenariot uppstår. Med andra ord beskriver deltagaren vilka faktorer som orsakar störningssituationen. Övningen genomförs typiskt i form av en elektronisk enkät som man fyller i på distans. Övningen är enkel och snabb att genomföra.

— Vanligtvis används pre mortem-övningar för att planera framtida övningar och bedöma beredskapsplaner.

C. Operativ övning

— I en operativ övning simuleras en riktig kris och man övar handlingsförloppet i sina verkliga roller och med verktyg som organisationen använder dagligen.

— För en operativ övning utarbetas ett scenario där en på förhand vald process eller funktion inom organisationen har råkat ut för en olycka eller störning.

— Till skillnad från en skrivbordsövning genomförs en operativ övning i den egna arbetsmiljön så att deltagarna använder befintliga verktyg och handlingssätt utan att ha fått anvisningar på förhand.

D. Teknisk övning

— I en teknisk övning simuleras fel- och störningssituationer för att till exempel testa reaktionsförmågan.

— En teknisk övning har en lång planeringscykel och kräver omfattande förberedelser.

E. Stora gemensamma övningar

— Övningar som baserar sig på ett simulerat scenario. Dessa övningar kräver en lång planeringsprocess och en grupp som sörjer för att genomföra övningarna.

— Gemensamma övningar genomförs decentraliserat i riktiga verksamhetsmiljöer. För övningen utarbetas ett verklighetstroget scenario utifrån en riskanalys och en eventuell pre mortem-övning.

— De personer som behövs för att leda situationen i scenariot och återhämta sig från störningssituationen deltar i övningen. Detta är vanligtvis organisationens ledning, experter, yrkesutbildade personer inom kommunikation, den operativa personalen och valda samarbetsaktörer.

3.2.2 Val av övningar

Den strategiska planeringen av övningsverksamheten inbegriper en periodindelning av organisationens olika enheters och teams deltagande i övningarna. Utifrån organisationens riskanalys,

nuvarande kunskapsnivå och tillgängliga resurser väljs en lämplig övningshelhet. Tidtabellen för denna fastställs till en tidsperiod under vilken det är realistiskt att genomföra helheten.

De olika typerna av övningar stödjer utvecklandet av olika slags kunskaper. Traditionellt används tekniska övningar för att stöda experternas och det tekniska underhållets kunskaper, medan det för ledningen ordnas övningar i ledarskap och affärsverksamhet. En samarbetsövning som berör alla utvecklar hela personalens och intressentgruppernas kunskaper.

Ledarskapsövningar testar ledningsprocessen, så målgruppen och målen ska fastställas enligt behoven hos de aktörer som ansvarar för ledningen eller utvecklar ledningen. Övningsstrukturen VALHA på statsförvaltningsnivå är ett exempel på en ledarskapsövning.

I en övning i affärsverksamhet ligger fokus på att upprätthålla verksamheten. Eftersom mycket få organisationer inom statsförvaltningen har ett sådant produktionsansvar som fabriker har, kan leverantörer som är viktiga för staten genomföra övningar i affärsverksamhet. Det att företagens verksamhet fungerar utan störningar tryggar i regel kontinuiteten, så en välskött affärsverksamhet kan anses producera produkter som är livsviktiga för medborgarna i alla förhållanden.

Flera aktörer deltar ofta i en samarbetsövning. Det kan vara fråga om verksamhet mellan olika parter i ett verksamhetsnätverk, till exempel en övningsgrupp bestående av aktörer som ansvarar för reglering, övervakning, produktion, tjänster och råvaror. Till exempel för att trygga kontinuiteten i en störningssituation är det viktigt att identifiera samarbetsaktörerna, deras utmaningar och behov.

Tekniska övningar har vanligen mycket detaljerade handlingsmodeller. I övningarna söker teknikexperter med djup kompetens utmaningar och löser dessa, till exempel på kodnivå. Cyberövningskonceptet (KYHA) som ordnas för myndigheter är ett exempel på en teknisk övning.

Ett beslut om övningsätt och -typ bör fattas i början av planeringsprocessen. Vilka mål man har med övningen är centralt då man väljer övningssätt. Valet av övningssätt påverkas i hög grad av vilka resurser som finns tillgängliga vad gäller såväl planering som deltagare.

	IT systemstörning	Leverantörs-problem	Personalen förhindrad	Brist på tillgängliga lokaler
Kritisk funktion 1	Kritisk övning	Kritisk övning	Viktig övning	Inget behov av övning
Kritisk funktion 2	Viktig övning	Inget behov av övning	Viktig övning	Kritisk övning

Tabell 2: Hur kritiska funktioner och risker påverkar planeringen av övningarna

Det är bra att alltid väga målen med övningen och övningssättet tillsammans. Till exempel har en övning som inbegriper verksamheten på fältet vanligtvis helt andra mål än en så kallad skrivbordsövning. Då man väljer övningstyp och -helhet utgår man från de kritiska funktionerna och de enheter inom organisationen som kopplas till dessa.

3.3 Tidtabell och resursfördelning för övningar

Organisationer som har planerat övningsverksamheten på lång sikt har märkt att övningar bör ordnas regelbundet för att de strategiska målen ska kunna nås. I praktiken innebär detta en långsiktig plan för övningsverksamheten i vilken övningar som ingår i övningsprogrammet under de kommande åren beaktas. Samtidigt tar organisationen i beaktande vilken övningsrytm som passar den egna verksamheten och det är enklare att engagera personalen i övningsverksamheten. Med en långsiktig plan skapas en övergripande bild och övningarna blir kontinuerliga.

Tidtabellen för övningsverksamheten påverkas av såväl organisationens egna strategiska planer som övningar som andra ordnar. Antalet övningar ersätter inte nödvändigtvis kvaliteten, så det kan vara ändamålsenligt att först utreda eventuella internationella och nationella storövningar. Det kan vara kostnadseffektivt för organisationer på samma nivå och av samma typ att ordna gemensamma övningar.

Det lönar sig att placera och resursfördela organisationens egna interna övningar utanför andra övningar.

Den person som ansvarar för övningsverksamheten har i praktiken två alternativ för att genomföra övningarna: 1) övningen produceras på egen hand eller 2) en extern tjänst anlitas för att ordna övningsverksamheten. I verkligheten sammanslås i den strategiska planeringen av övningsverksamheten två modeller så att övningarna ska vara så effektiva och högklassiga som möjligt, nämligen den övningsverksamhet som planerats av de ansvarspersoner organisationen utsett och enskilda övningar som genomförs med hjälp av externa resurser.

3.3.1 Producera övningar på egen hand

Sättet på vilket de olika typerna av övningar genomförs avviker från varandra i synnerhet vad gäller resursbehov för planering och genomförande. Pre mortem- och skrivbordsövningar som klassificerats som enkla övningstyper kan genomföras med ganska små insatser.

En orsak till att det är bäst att producera övningar själv är det behov av sakkunskap som planeringen kräver. Organisationen är själv bäst på att beskriva scenarier och fundera på eventuella övningsstrukturer samt på vad som eftersträvas med övningsverksamheten.

Det kan hända att den egna personalen engagerar sig mer och är öppnare för en övning som genomförs i den egna miljön och med bekanta personer. Övningslokalerna, som kan vara till exempel tillfälliga lokaler för avvikande förhållanden, kan planeras så att de enkelt kan användas på nytt vid nästa övning. Då höjs utnyttjandegraden för de tillfälliga lokalerna avsevärt och de har testats för eventuella krissituationer.

3.3.2 Köpa övningar som en tjänst

Gemensamma övningar som berör flera organisationer ordnas bäst genom samarbete mellan aktörerna eftersom man då kan utnyttja eventuella färdiga övningsmiljöer utan att störa den egna produktionen. I en extern teknisk miljö kan det vara möjligt att öva sådana saker som inte ens kan genomföras i produktionsmiljön. Anlitandet av utomstående personer ger möjlighet att utkontraktera rutinerna, och den som ansvarar för övningarna kan fokusera på att styra projektet.

Med tanke på de totala kostnaderna är det vanligtvis förmånligare att skaffa en tjänst som underleverans än att producera den själv. Övningsverksamheten hör inte nödvändigtvis till organisationens kärnverksamhet och det lönar sig inte att skaffa stora eller bestående personalresurser för övningarna. Dessutom kan den egna personalen koncentrera sig på den normala kärnverksamheten i stället för att förbereda och ordna övningar.

Ett underleverantörsarrangemang kan också hämta med sig nya tankar kring scenarier, övningsmodeller och effektivitet eftersom underleverantören ofta har stor erfarenhet av att ordna övningar. En underleverantör kan också anlitas i situationer där man vill komma igång med övningsverksamheten.

Ett ramavtal med underleverantörren kan göra det lättare att uppskatta budgeten och gör det i synnerhet lättare att flexibelt skaffa små övningar. Det lönar sig dock att starta processen i god tid, senast året före övningen.

4 Element i årsplaneringen av övningsverksamheten

Den person som ansvarar för övningsverksamheten gör upp en långsiktig plan samt en verksamhetsplan för året (en så kallad årsklocka), som ger organisationen en bild av hur övningsverksamheten stödjer uppnåendet av de årliga målen.

Enbart planering räcker dock inte för att övningsverksamheten ska ge någon nytta. Årsplanen ska också genomföras på ett högklassigt sätt, och detta kräver tillräckliga resurser. Dessutom ska verksamheten bedömas och utvecklas utifrån bedömningarna. I långsiktiga planer ska de utvecklingsförslag som gjorts utifrån bedömningarna tas i beaktande.

För övningsverksamheten utarbetas ofta en verksamhetsplan som binds till årets kalender och som godkänns av organisationens ledning. I planen syns övningar, tidtabellen för och deltagare i dem samt mål, behov och organiseringsansvar. Dessutom kopplas verksamhetsplanen till en budget där kostnader för övningsverksamheten och den finansiering som behövs beskrivs.

Utöver årsplaneringen kan långsiktig planering påverka genomförandet av omfattande övningar eftersom det kan ta upp till flera år att planera dem. För att genomföra stora samarbetsövningar krävs till exempel långa förberedelser och beslut som styr finansieringen under kommande redovisningsperioder.

Man bör vara beredd på att det kan ske förändringar i verksamhetsplanerna. Man bör i planen förbereda sig för förändrade situationer och förhållanden genom att se till att verksamhetsplanen är flexibel och säkerställa en fungerande process för att hantera förändringarna.

4.1 Årsklocka för övningsverksamheten

Den person som ansvarar för övningsverksamheten utarbetar en årsplan och genomför den inom ramen för den budget som överenskommits. Övningar som organisationens ledning har godkänt på förslag av den person som ansvarar för övningsverksamheten ordnas enligt årsklockan. Dessutom väljer organisationens ledning utifrån risk- och effektivitetsanalyser vilka enheter, tjänster och processer som ska delta i övningarna. Årsklockan och de övningar som ingår i den planeras så att en enhet inte behöver delta i alla övningar.

Uppgift

Januari	*Säkerställande av resurser för vårens övningar*
	— se över övningsplanen för året — se till att övningsbudgeten har bekräftats — informera och engagera deltagarna
	Komplettering av verksamhetsplanen
	— utred utbudet av externa övningar för det pågående året och möjligheten att delta i och anmäla sig till dem i efterhand — ordna en verkstad för att planera årsklockan där också den mer långsiktiga övningsplanen beaktas
Februari	*Detaljerad planering av övningarna*
	— gör upp detaljerade planer för enkla övningar tillsammans med leverantören (i detta exempel två övningar) — genomförs i mars och maj
	Utbildning av personal
	utbilda personalen i övningsverksamheten
Mars	*Fastställande av övningar för följande år och preliminär reservering av resurser*
	— utred utbudet av övningar för kommande år — fastställ kommande övningstyper, antal deltagare, behov gällande arrangemang, kostnader
	Övningsarrangemang
	— Genomför en enkel övning (skrivbords- eller pre mortem-övning) enligt planen
April	*Budgetering*
	— förbered budgeten
Maj	*Övningsarrangemang*
	— kartlägg de viktigaste sakerna och områdena som bör utvecklas – ordna en enkät — delta i debriefing efter övningarna — Genomför en enkel övning (skrivbords- eller pre mortem-övning) enligt planen — kom överens om debriefing med leverantören
Juni	*Precisering av följande års verksamhetsplan utifrån respons på de övningar som genomförts*
	— uppdatera/utarbeta en årsklocka för övningsverksamheten och en mer långsiktig övningsplan — utarbeta utvecklingsförslag med tanke på framtida planering — presentera planeringsläget för ledningen och engagera ledningen i övningsplanen
Augusti	*Reservering av följande års totalbudget*
	— inför övningsplanen i organisationens verksamhetsplan och budgetram
	Sändning av anbudsförfrågningar för övningsverksamheten
	— skicka anbudsförfrågningar till leverantörer / förhandla/begär ett anbud — skaffa en arrangör av följande års övningar

September	*Utbildning av personalen i kontinuitetsstyrning*
	— engagera följande års övningsarrangörer i övningsplanen
Oktober	*Omfattande övning (operativ övning eller samarbetsövning)*
	— delta i samarbetsövningen
November	Resultatförhandlingar
	— ta med övningsverksamheten i resultatförhandlingarna — ta med övningsverksamheten i utvecklingssamtal — uppmuntra deltagarna att göra detsamma — se till att övningsverksamheten och budgeten för denna finns med i organisationens planer
	Val av leverantörer
	— informera leverantörerna om vem som valts
December	*Specificering av verksamhetsplanen för följande års höst utifrån respons*
	— inför en sammanfattning av övningsverksamheten som inbegriper alla övningar under året i organisationens årsrapport — inför övningsverksamheten i planen för kompetensutveckling tillsammans med HR

Tabell 3: Årsklocka för övningsverksamheten

4.2 Budgetering

Övningsbudgeten bör beaktas som en del av organisationens årsbudget och långsiktiga planering. Det lönar sig att inkludera övningarna i budgetplaneringen senast under den budgetperiod som föregår övningen så att en kort beskrivning av övningarna med tidpunkter, antal personer och kostnadsuppskattningar finns med i organisationens verksamhetsplan och resultatförhandlingar. Traditionellt är målet i organisationens årsklocka att följande års övningar ska fås med i planerna i augusti. I fråga om vissa större övningar kan man vara tvungen att reservera ekonomiska resurser redan flera år före övningen för att täcka planerings- och förberedelsekostnaderna.

Då kostnaderna ska uppskattas kan man utnyttja erfarenheter från en övning som en annan organisation ordnat. Man kan också basera uppskattningen till exempel på erfarenheter från tidigare övningar. Det måste finnas utrymme för flexibilitet i budgeten eftersom det är svårt att identifiera alla kostnader på förhand. Syftet med den här anvisningen är att ge riktgivande ramar för att uppskatta kostnaderna. En noggrannare uppskattning kan göras bland annat med hjälp av tabellen i bilaga D.

4.3 Personresurser

Personalen som övar är den viktigaste delen av övningsverksamheten. För att övningen ska lyckas krävs att de som övar har tid att sätta in sig i övningsscenariot och koncentrera sig på verksamheten under övningen samt ge respons.

Det finns två aspekter som bör tas i beaktande då personalresurser reserveras: 1) resurser som behövs före övningen och 2) resurser som behövs under övningen. Dessa två aspekter avviker

från varandra och förutsätter olika typer av kunskaper. Personalresurser för planering och genomförande av övningen bör reserveras i samband med att budgeten fastställs.

I bilaga E finns en tabell där det har sammanställts vilka resurser och genomsnittliga personalbehov som vanligtvis behövs vid en övning. I fråga om personalstyrkan är det skäl att beakta huruvida det är fråga om en egen övning eller en övning som ordnas av någon annan. Om organisationen till exempel ansvarar för att genomföra en samarbetsövning ska man beakta att utomstående ska bjudas in att delta i förberedelserna och genomförandet. Undersökningar har visat att en grupp är effektivast om den har högst sju medlemmar.

5 Kompetensutveckling och resultat av övningarna

5.1 Kompetensutveckling

Det lönar sig att sammankoppla övningsverksamheten med utvecklandet av personalens kompetens. Med tanke på uppföljningen av övningarna kan man införa ett system i vilket deltagarnas prestationer antecknas. Utifrån prestationerna (till exempel ett tillräckligt antal prestationer eller deltagande i vissa fastställda övningar) kan ett intyg, certifikat eller en annan sporrande belöning ges. Dessutom kan prestationerna antecknas i personens CV.

Övningsverksamheten knyts till säkerställandet av verksamhetens kontinuitet, planeringen av beredskapen och den utbildnings- och övningsplan som denna omfattar. En långsiktigare plan för övningsverksamheten kan byggas upp till exempel så att man i början genom olika typer av separata övningar övar enskilda kompetensområden och delmål för kompetensen. Övningscykeln kan kulminera i en lång övning där olika övningsformer och målgrupper involveras. Det är inte alltid möjligt att bygga upp och genomföra ett övningsprogram utan luckor där man systematiskt går från enklare till svårare övningar. Detta beror på att organisationer, deras mål och nyckelpersoner kan bytas ut med kort förvarning.

Beredskapscheferna eller motsvarande personer ansvarar för kompetensutvecklingen och utbildningen i anslutning till genomförandet av kontinuitetsplanen samt för planeringen av och målen för dessa. Utbildningen ska vara kontinuerlig och ges enligt de behov som olika grupper och roller har. Utbildningarna inbegrips i årsklockan för kontinuitetsstyrning som en del av den övriga normala verksamheten. Årsklockan för kontinuitetsstyrning upprätthålls av till exempel säkerhets- eller beredskapschefen.

Dessutom är det bra att fundera på hur förhandsuppgifter kan tas i beaktande och hur de ges till dem som deltar i en övning. Finns det förhandsuppgifter? Hur noga ska man berätta om övningen, dess tema och innehåll före övningen? Lärdomarna kan vara större om man har hållit ett prov på förhand och deltagarna kan fokusera på att lära sig de saker man borde kunna.

En förutsättning för övningar i kontinuitetsstyrning är att organisationens personal har fått utbildning i att agera i störningssituationer. Varje enhet ansvarar för att upprätthålla den egna personalens kunskaper om kontinuitetsstyrning. Enheterna ansvarar för ändringar i kontinuitetsplanerna och för att förankra dessa bland de aktörer som identifierats i kontinuitetsplanerna.

De resurser (inklusive stödfunktioner) som behövs för att hantera störningssituationen deltar i övningen. Övningarna genomförs så att de medför så få olägenheter som möjligt för den egentliga verksamheten. Ansvaret för att genomföra en övning fastställs enligt typen av övning i testnings- och övningsplanen.

Efter övningen får deltagarna respons. Resultaten av övningen registreras och kontinuitetsplanerna kompletteras utifrån de observationer som gjorts. Ansvaret för att registrera utvecklingsåtgärder och koordinera kompletterandet av kontinuitetsplanerna ligger hos de personer som ansvarar för att genomföra övningen.

5.2 Bedömning av övningsverksamheten

Övningsprogrammet och -verksamheten måste bedömas för att kunna utvecklas. Utifrån resultaten av bedömningen kan man specificera bland annat den kompetensutveckling som övningsprogrammet omfattar, övningarnas karaktär, antalet övningar och hur ofta de genomförs. Det lönar sig att i kompetensutvecklingen fästa uppmärksamhet vid progressiviteten på lång sikt; till exempel ska kravnivån ökas vid följande övningar i och med att deltagarna utvecklas. Övningarnas karaktär och omfattning, antalet övningar och hur ofta de upprepas påverkar vilka resurser som behövs. Om respons samlas in planmässigt kan man skaffa hållbara grunder för utvecklingen.

Bedömningen av övningarna ska grunda sig på de mål som fastställts för övningarna. Därför bör man satsa på utformningen av målen då övningen planeras. Vid stora övningar är det skäl att utse en bedömningsgrupp samtidigt som man fattar beslut om grunderna för styrningen och genomförandet av övningen. Det är bra om bedömningsgruppen i god tid fördjupar sig i sin uppgift och gör upp bedömningskriterier för att mäta målen. För små övningar utses en bedömningsansvarig. Utöver målen bedöms även övningsarrangemangen.

Bedömningsgruppen eller den bedömningsansvarige bör ha erfarenhet av att bedöma övningar. Bedömningsarbetet inleds med att göra upp en bedömningsplan. Den egentliga bedömningen görs under övningen och en rapport ges så snart som möjligt efter övningen. Det är lättare att rapportera om resultaten utgående från en omsorgsfullt utarbetad bedömningsplan och en genomförd bedömning.

Uppföljningen och bedömningen av en övning bör fokusera på exempelvis följande frågor:

- Uppfyllde övningen målen?
- Testades de saker man önskade?
- Gick övningen enligt planerna?
- Hur agerade medlemmarna i gruppen för hantering av störningar?
- Observerades det några på förhand okända risker i övningen?

Respons på övningen bör samlas in av deltagarna. Man kan ordna ett responstillfälle genast efter övningen, då deltagarna ännu har övningen i färskt minne. Information om övningsarrangemangen och de saker som övades kan samlas in med en elektronisk blankett eller pappersblankett. Vid behov kan svaren också ges anonymt. Man bör dock beakta sekretesskrav som berör ärendet som behandlas då respons samlas in. Elektroniska metoder uppfyller inte nödvändigtvis alla säkerhetskrav för det ämne som övas. I bilaga A finns en länk till en artikel om bedömning av övningar.

5.3 Utveckling av övningsverksamheten utifrån bedömningen

Resultaten av övningen kräver ofta fortsatta åtgärder, som är viktiga att rapportera till ledningen och deltagarna. Samtidigt bör man berätta hur de tas i beaktande i övningsverksam-

heten. Övningen har lyckats om resultaten bekräftar den befintliga praxisen eller pekar ut utvecklingsbehov. Ofta ligger tyngdpunkten i resultaten dock på utvecklandet av verksamheten. Resultaten av övningar visar att de mest traditionella förändringstrycken berör uppdateringen av handlingsanvisningar och -modeller samt verktyg för att leda störningssituationer. Resultaten kan också ge grunder för att ordna en ny övning samt ett tema för övningen. Dessutom ger resultaten förslag på hur övningarna och övningsverksamheten samt de verktyg som används i övningsverksamheten kan utvecklas.

För att resultaten ska finnas tillgängliga bör man bestämma hur och var de förvaras. De som deltagit i övningen eller utvecklar verksamheten kan behöva ta del av dem i efterhand, så man bör bestämma vem som får utnyttja resultaten och hur detta görs.

Hanteringen av resultaten av bedömningen är en del av helhetsplanen för övningsverksamheten. Resultaten av bedömningen av övningsverksamheten bör styra organisationens utveckling. Bedömningen kan visa att fördjupning på egen hand eller den utbildning som getts inte är tillräcklig utan att organisationen behöver omfattande övning för att verksamheten ska utvecklas.

6 Begrepp och definitioner

Begrepp	Definition
Budget	Organisationens uppskattning av inkomster och utgifter inom statsförvaltningen.
Digital säkerhet	En holonym (överordnat begrepp) som omfattar till exempel följande delområden: riskhantering, informationssäkerhet, cybersäkerhet, verksamhetens kontinuitet (beredskaps-, och kontinuitetsplanering) och dataskydd.
ENISA	EU:s byrå för nät- och informationssäkerhet
Övningsprogram	En plan på strategisk nivå som organisationen gjort upp. I planen behandlas bland annat behovet av övningar och mål för övningarna, övningsverksamhetens koppling till utvecklandet av personalens kompetens och planeringen av verksamheten samt reserveringen av resurser, i synnerhet budgetering. I övningsprogrammet samlas de övningar som ska planeras och genomföras under året. Dessutom är det skäl att utarbeta ett program på strategisk nivå som sträcker sig minst fyra år framåt. Det är vanligtvis beredskapschefen eller en expert inom området som ansvarar för övningsprogrammet.
Övningsverksamhet	En händelse i kompetensutvecklingen eller en konsekvent serie av sådana. Övningsverksamheten genomförs då man förbereder sig för att agera vid på förhand fastställda hot. Det kan vara ovanligt att hoten realiseras, men övningar är nödvändiga att genomföra. Övningsverksamheten kan vara lagstadgad.

Övningsscenario	Helhet av händelser i övningen och bakgrundsbeskrivningar som beskriver innehållet i en övning. Enbart ”scenario” används också. Scenariot skapar grunden för händelser och meddelanden i samband med övningen.
Typ av övning	Spelsätt och -typ som valts för övningen. Till exempel skrivbordsövning, operativ övning eller teknisk övning.
Övningsmiljö	Den tekniska och operativa miljön. Övningsmiljön omfattar vanligtvis de informationssystem och de lokaler där övningsrelaterade ärenden behandlas.
JUDO	Utvecklingsprogrammet för den digitala säkerheten inom den offentliga förvaltningen
Efteranalys	Görs efter övningen. Sammanställning av lärdomar från övningen och granskning där man behandlar lärdomarna från övningen och bestämmer vilka aspekter som behöver utvecklas.
Cyberövning	Säkerhetsövning där fokus ligger på störningar i informationssystemen eller informationssäkerheten och de omfattande effekter dessa får för organisationen.
Responstillfälle	Hot wash-up: Responstillfälle som ordnas omedelbart efter övningen.
Pre-mortem	Pre mortem-övning, en övning där man utgår från följderna och söker eventuella grundorsaker till dem.
Simulering	En beskrivning av fiktiva övningshändelser i en övning.
Observatör	En deltagare i en övning som har i uppgift att observera övningen och anteckna sina observationer.
Teknisk övning	En övning som kräver fördjupad teknisk sakkunskap. I en digital miljö innebär detta till exempel att man söker sårbara element och skadliga program i övningsmiljön.
VALHA	Beredskapsövning inom statsförvaltningen.

A Anvisningar, handböcker och nyttiga länkar (vissa endast på finska)

Prioritering av funktioner

Verktyg för prioritering av funktioner som är fritt tillgängligt för organisationer: Palveluiden kriittisyysluokittelutyökalu;

https://vm.fi/documents/10623/6745219/Palveluiden_kriittisyysluokittelut y%C3%B6kalu_1602018.xlsx/ebe27c1d-17e1-4017-b001-b5566db03d48

Avtalsbaserad beredskap, anvisning för aktörer inom social- och hälsovården

http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161630/STM_15_2019_Avtalsbaserad%20beredskap.pdf?sequence=1&isAllowed=y

Försörjningsberedskapscentralens Sopiva-klausuler (på finska)

Försörjningsberedskapscentralen har utarbetat exempel på klausuler för att trygga kontinuiteten i avtal. I avtal ska satser som hänvisar till övningsverksamheten särskilt tas i beaktande i de mer utförligare specifikationerna.

https://www.huoltovarmuuskeskus.fi/sopiva/

Hansel-avtal

Det är bra om organisationen tar del av befintliga Hansel-avtal med tanke på tjänster som anknyter till övningsverksamheten.

Bedömning av en övning

https://www.msb.se/siteassets/dokument/publikationer/english-publications/evaluation-of-exercises.pdf

Ordnande av övningsverksamhet

Kyberturvallisuuskeskuksen käsikirja harjoituksen järjestäjälle

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

B Lagar, anvisningar och standarder som berör utarbetandet av ett övningsprogram

Utöver de lagar som berör beredskap har man inom statsförvaltningen godkänt strategier som behandlar ämnet. Säkerhetsstrategin för samhället som godkänts som statsrådets principbeslut siktar på att trygga livsviktiga funktioner inom olika delområden.

Tryggandet av livsviktiga funktioner i samhället grundar sig i huvudsak på arrangemang i normala förhållanden. I beredskapslagen (1552/2011) finns bestämmelser om agerande under undantagsförhållanden. Enligt 12 § omfattas bland annat statliga myndigheter av skyldigheten att vidta förberedelser, det vill säga är skyldiga att planera sin verksamhet även under undantagsförhållanden.

I lagen om tryggande av försörjningsberedskapen (1390/1992) och statsrådets beslut

om målen med försörjningsberedskapen (1048/2018) finns bestämmelser om tryggandet av ekonomiska funktioner och därtill hörande tekniska system som är nödvändiga för befolkningens utkomst, landets näringsliv och landets försvar. Dessutom spelar statsrådets principbeslut om utvecklandet av informationssäkerheten (2009), om en säkerhetsstrategi för samhället (YTS2017), om en strategi för bekämpning av terrorism (2014) samt Finlands cybersäkerhetsstrategi en viktig roll i styrningen av beredskapen och utformningen av krav.

Bestämmelser om myndighetens skyldigheter att skydda informationssäkerheten, myndigheternas servicenät och kommunikationssystem samt om beredskap i undantagsförhållanden finns bland annat i lagen om offentlighet i myndigheternas verksamhet (621/1999) och förordningen om informationssäkerheten inom statsförvaltningen (681/2010) som utfärdats med stöd av denna, dataskyddslagen (1050/2018), förordningen om behandling av personuppgifter i EU (dataskyddsförordningen, EU-förordning 2016/679, tillämpas 25.5.2018), informationssamhällsbalken (917/2014), lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013) och lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015). Även räddningslagen (379/2011) kräver beredskap.

Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen VAHTI har utfärdat en anvisning om hantering av kontinuiteten i verksamheten (VAHTI 2/2016, på finska) och en anvisning om kraven på ICT-beredskap (VAHTI 2/2012, på finska). I anvisningarna finns en noggrannare bedömning av skyldigheter i gällande lagstiftning vad gäller kontinuitetsstyrning.

I utarbetandet av organisationens övningsprogram och -verksamhet ska bland annat följande beaktas:

1. Lagar och förordningar:

- Reglementet för statsrådet 1522/1995 (34 §, 35 §, 37 §)
- Bestämmelserna om grundläggande fri- och rättigheter i Finlands grundlag 731/1999 (1 §, 22 §, 23 §, 84 §)
- Beredskapslagen 1552/2011
- Lagen om tryggande av försörjningsberedskapen 18.12.1992/1390 (2 §, 6 §, 8 §)
- Statsrådets beslut om målen med försörjningsberedskapen 1048/2018
- Räddningslagen 379/2011 (2 §, 28 §, 48 §, 64 §, 70 §, 77 §, 84 §, 90 §, 92 §, 105 §)

- Lagen om statsbudgeten 423/1988 och lagen om ändring av lagen om statsbudgeten 1053/2016
- Förordningen om statsbudgeten 1243/1992 och förordningen om ändring av denna 263/2000
- Dataskyddslagen 1050/2018 (1 §, 2 §, 4 §, 29 §, 35 §, 36 §)
- Lagen om tjänster inom elektronisk kommunikation 917/2014 (243 §, kap. 35, 298 §, 301 §, 304 §, 320 §)
- Lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster 1226/2013 (15 §) och ändring av denna 923/2019
- Lagen om offentlighet i myndigheternas verksamhet 621/1999 samt ändring av denna 907/2019
- Statsrådets förordning om informationssäkerheten inom statsförvaltningen 681/2011
- Förordningen om offentlighet och god informationshantering i myndigheternas verksamhet 1030/1999
- Förordningen om behandling av personuppgifter i EU 679/2016 (Avsnitt I)
- Arkivlagen (831/1994)
- Lagen om informationshantering RP 284/2018; godkänd i riksdagen 18.3.2019; träder i kraft 1.1.2020 (mål)
- Lagen om verksamheten i den offentliga förvaltningens säkerhetsnät 10/2015 (1 §, 2 §, 5 §, 7 §, 9 §, 11 §, 12 §, 13 §, 14 §, 15 §)
- Lagen om identitetskort 663/2016
- Lagen om integritetsskydd i arbetslivet 759/2004
- Lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster 661/2009
- Lagen om förbud mot vissa avkodningssystem 1117/2001 (även i strafflagen 38 kap. 8 b §)
- Lagen om ändring av strafflagen (368/2015) (orsakande av fara för informationsbehandling [34 kap. 9 a §], kränkning av kommunikationshemlighet [38 kap. 3 §], dataintrång [38 kap. 8 §, 8 a §, 8 b §], dataskyddsbrott (38 kap. 9 §, 9 a §)
- Lagen om elektronisk kommunikation i myndigheternas verksamhet 13/2003 samt ändringen av denna 908/2019
- Lagen om stark autentisering och betrodda elektroniska tjänster 617/2009
- Statstjänstemannalagen 750/1994

2. Strategier och principbeslut:

- Säkerhetsstrategin för samhället
- Den nationella cybersäkerhetsstrategin
- Den nationella strategin för bekämpning av terrorism
- Målen för försörjningsberedskapen
- Utveckling av statens informationssäkerhet
- Försörjningsberedskapscentralens scenarier för 2030
- Den nationella riskbedömningen

3. Standarder

- SFS-EN ISO 22301 Yhteiskunnan turvallisuus. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset (svensk standard SS-EN ISO 22301:2014 Samhällssäkerhet - Ledningssystem för kontinuitet - Krav)

- SFS-EN ISO/IEC 27001:2017 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset (SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav)
- SFS-EN ISO/IEC 27002:2017 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet (SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder) ISO 90001
- SFS-EN ISO 14001 Ympäristöjärjestelmät. Vaatimukset ja niiden soveltamisohjeita (SS-EN ISO 14001 Miljöledningssystem - Krav och vägledning)
- SFS-ISO 45001:2018 Työterveys- ja työturvallisuusjärjestelmät. Vaatimukset ja niiden soveltamisohjeita (SS-ISO 45001:2018 Ledningssystem för arbetsmiljö - Krav och vägledning) SFS-EN ISO 50001:2018 Energianhallintajärjestelmät. Vaatimukset ja soveltamisohjeita (SS-EN ISO 50001:2018 Energiledningssystem - Krav med vägledning för användning)

4. Anvisningar (på finska)

- VAHTI 2/2016 om hantering av kontinuiteten i verksamheten
- Traficom: Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle (Anvisning för cyberövningar. Handbok för den som ordnar en övning)

C Blankett för bedömning av nuläget

Krav	Genomförs	Under arbete	Genomförs inte	Kritiskhet
Ansvar för att utveckla beredskapskunskaperna har fördelats (lednings- och expertnivå)				
Organisationen ordnar själv övningar varje år				
Organisationen deltar i andras övningar varje år				
Organisationen har ett övningsprogram eller en motsvarande plan				
Organisationen har en kontinuitetsplan				
Organisationen har en beredskapsplan				
Organisationen har en kriskommunikationsplan				

D Kostnadsfaktorer att beakta i planeringen av en övning

Som bilaga en tabell med ett färdigt detaljerat beräkningsunderlag för kostnadsposter

	Planering	Genomförande	Omfattning	Lokaler	Anordningar, licenser
Fråga för att kartlägga kostnaderna	Ordnar organisationen övningen själv eller köps den som en tjänst? Behövs det utomstående hjälp med planeringen?	Deltar organisationen i en övning som någon annan ordnar eller i en internationell övning?	Hur många personer deltar i övningen? Hur många enheter deltar? Hur omfattande är det scenario som används i övningen? Hur många övningsdagar behövs det?	Vilka utrymmen krävs för att ordna övningen? Ordnas övningen i egna utrymmen? Behövs det andra utrymmen för att planera och genomföra övningen?	Behövs det utöver de anordningar som används under normala förhållanden även andra anordningar eller tillämpningar? Kräver den typ av övning och det scenario som valts tekniska underlag?
Typiska kostnader för övningen	Om organisationen ordnar övningen själv utgörs kostnaderna av den arbetstid som används, i synnerhet för planering och beredning av de meddelanden som används under övningen. Kostnader för en övning som ordnas i form av en köpt tjänst är i regel den arbetstid konsulten använder för att planera och förbereda övningen. Visualisering och skapande av innehåll till meddelanden i anslutning till scenariot och övningen kan ge upphov till betydande tilläggskostnader: t.ex. videoproduktioner, animerande produktioner osv.	Kostnaderna består av eventuella deltagaravgifter, den arbetstid som går åt till övningen och resekostnader. Eventuella kostnader för översättning av innehållet i övningen.	Kostnaderna består av den arbetstid som går åt till att planera och förbereda övningen och arbetstiden för det egentliga deltagandet i övningen. Dessutom uppstår kostnader för de verktyg som använts, till exempel licenser för simulator eller kommunikationsunderlag.	Kostnaderna utgörs av hyror för lokaler eller landområden. I övningen kan till exempel behövas särskilda lokaler för planering och ett spelrum där meddelandena koordineras. Dessutom kan det behövas tillfälliga lokaler, presslokaler eller andra motsvarande lokaler. Måltidsservering. Kontorstillbehör. Kostnader för datakommunikation.	Kostnaderna består av licensavgifter och hyror av anordningar. Underlag som används i övningar är till exempel en spelsimulator eller ett underlag för kriskommunikation. Vid fältövningar materielkostnader.

E Tabell för bedömning av personalresurser för övningsverksamheten

Resurs	Beskrivning	Scenario	Skrivbord	Operativ	Samarbets-	Obs!
Före övningen (planering)						
Lednings-/styrgrupp	Ansvarar för övningarnas teman och mål utifrån organisationens vision, mål, strategi och hotbilder	3 pers	3 pers	5 pers	1 pers, om utomstående 4–6 pers, om egna	
Beredskapschef eller motsvarande	Ansvarar för helheten (tidtabell, budgetering, allmän planering)	1 pers	1 pers	1 pers	1 pers	
Kontaktperson (point of contact)	Ansvarar för kommunikationen vid externa övningar	1 pers	1 pers	1 pers	1 pers	Rekommenderas alltid då någon annan ordnar övningen
Planeringsgrupp	Förbereder mål, innehåll, meddelanden och andra spelhändelser kring övningen	2–3 pers	2–3 pers	4–6 pers	0–1 pers, om utomstående, 4–6 pers, om egna	
Sekreterare	Koordinerar de praktiska arrangemangen (måltider, bokning av lokaler, reservation i kalendern o.dyl.). Dokumenterar övningen medan den pågår	1 pers vid sidan om det egna arbetet	1 pers	1 pers	0–1 pers, om utomstående 1 pers, om egen	
Under övningen (genomförande)						
Övningens ledningsgrupp	Beslutar om spelets gång och händelser. Stöder vid behov facilitatorn. Vid stora övningar är det bra om ledningsgruppen utöver en ledare för övningen även består av bl.a. en facilitator, informatör, chef för spelgruppen, IC-chef från stödgruppen och en säkerhetschef. Vid samarbetsövningar även representanter för de mest centrala deltagarorganisationerna	1 pers	2 pers	4–6 pers	0–1 pers, om utomstående 1 pers, om egen	Vid externa övningar enligt behov
Facilitator/ koordinator	Styr övningens gång (beredskapschefen eller motsvarande fungerar inte som koordinator för övningen)	1 pers	1 pers	1 pers	0–1 pers, om utomstående 1 pers, om egen	Kan vara till exempel PoC, vid externa övningar
Bedömningsgrupp	Observerar övningen och antecknar sina iakttagelser (ska utses genast då målen står klara)	2–3 pers	3–6 pers	4–6 pers	0–1 pers, om utomstående 4–6 pers, om egna	Vid externa vanligtvis endast på inbjudan
Stödgrupp	Genomför stödet under övningen (mat, tekniskt stöd, säkerhet o.dyl.)	1–2 pers	2–6 pers	4–6 pers	0–1 pers, om utomstående 4–6 pers, om egna	Vid externa vanligtvis endast på inbjudan.
Spelgrupp	Sköter meddelanden och andra spelhändelser beroende på scenariot och övningsmodellen	1 pers	4–6 pers	4–6 pers	0–1 pers, om utomstående x pers, om egna	Vid externa vanligtvis endast på inbjudan
Övningsgrupp	Deltar i övningen och agerar enligt meddelandena	ca 4–10 pers	x pers, t.ex. hela organisationen	x pers, t.ex. hela organisationen	1–x pers, om utomstående x pers, om egna	De största samarbetsövningarna kan ha hundratals deltagare

Kommunikation	Gör upp de meddelanden som behövs i övningssituationen och ansvarar för kommunikationen	1 pers vid sidan om det egna arbetet	1 pers	1 pers	1 pers, om egen	Vid externa övningar vanligen på någon annans ansvar