Revisionsverkets ställningstaganden

Riskhantering inom statsförvaltningen och verksamhetens kontinuitet

Statens revisionsverk utvärderade de statliga ämbetsverkens, inrättningarnas och ministeriernas beredskap för att trygga verksamheten vid störningar under normala förhållanden.

Syftet med risk- och kontinuitetshanteringen är att säkerställa att organisationens kärnverksamhet kan pågå utan avbrott under normala förhållanden, vid störningar under normala förhållanden och under undantagsförhållanden. Enligt beredskapslagen (1552/2011) leds och övervakas förberedelserna under undantagsförhållanden av statsrådet samt av varje ministerium inom sitt ansvarsområde. Statsrådets kansli ansvarar bland annat för att sammanställa en gemensam lägesbild för statsrådet och samordna den övergripande hanteringen av störningar.

För störningar som inträffar under normala förhållanden finns däremot varken på förhand bestämd ansvarsfördelning eller centraliserad styrning och ledning. Ändå kan betydande eller allvarliga störningar i en tjänst eller verksamhet under normala förhållanden leda till att verksamheten avbryts eller förhindras eller att ett strategiskt viktigt syfte inte kan uppfyllas. Störningen kan dessutom orsaka stora skador eller kostnader för andra samt leda till betydande kostnader för hela statsförvaltningen.

Fortsatt verksamhet under undantagsförhållanden bygger delvis på att organisationen har infört system och rutiner som säkerställer att dess verksamhet kan pågå utan avbrott under normala förhållanden och vid störningar under normala förhållanden. Gränsen mellan normala förhållanden och undantagsförhållanden är inte alltid helt tydlig. I fråga om bland annat leveranssäkerheten inom elförsörjningen är skillnaden mellan undantagsförhållanden och normala förhållanden ofta hårfin: produktions- och nätverkskapaciteten och tillgången på el överlag ska räcka till både under normala förhållanden och under kriser som förorsakar undantagsförhållanden.

En långvarig störning under normala förhållanden kan eskalera så att situationen börjar likna undantagsförhållanden och då aktualiseras bland annat frågan om försörjningsberedskap.

I revisionen utreddes också organiseringen av centraliserade funktioner, horisontala projekt och komplexa funktionskedjor inom statsförvaltningen. Därtill utreddes om risk- och kontinuitetshanteringen inom statsförvaltningen ger en tillräckligt gedigen bild som underlag för beslut av statsrådet.

Avsikten var att bekräfta att de statliga myndigheterna har säkerställt sin funktionssäkerhet och serviceförmåga. Utvecklingsbehoven och utvecklingsmöjligheterna i fråga om statens risk- och kontinuitetshantering kartlades också. Resultaten av revisionen kan användas för utveckling av risk- och kontinuitetshanteringen inom statsförvaltningen.

Revisionen riktades inte på försörjningsberedskapen, som inte omfattar störningar under normala förhållanden, utan undantagsförhållanden. Cybersäkerhet och vissa aspekter av säkerställande av oavbruten tillgång till e-tjänster lämnades också utanför revisionen. Dessa teman behandlas i effektivitetsrevisionsberättelserna 15/2017 och 16/2017 om styrning av funktionssäkerheten i e-tjänster respektive organisering av cyberskyddet.

I föreliggande rapport används för enkelhets skull beteckningen *ämbetsverk* om alla statliga enheter, det vill säga ministerierna, ämbetsverken och inrättningarna. Dessutom används beteckningen *ministerium* då det handlar uttryckligen om ministerierna.

Ämbetsverken ska lägga upp planer för att trygga kontinuiteten

När man ser på de statliga ämbetsverkens kontinuitetsplaner som helhet så håller de inte måttet.

Ämbetsverken befann sig på väldigt olika nivå i fråga om riskhantering- och kontinuitetsplanerna. Hälften av ämbetsverken hade både en riskhanteringsplan och en kontinuitetsplan eller åtminstone endera, medan en tredjedel av ämbetsverken saknade bådadera. Dessutom fanns det betydande brister i många av planerna. Ofta hade ämbetsverken varken uppdaterat eller testat planerna eller övat att handla enligt dem.

En del ämbetsverk hade redan börjat upprätta och utveckla planer. Under revisionen började dessutom flera ämbetsverk att se över och utveckla sina risk- och kontinuitetshanteringsprocesser. Genom resultatstyrningen kan ministerierna också uppmärksamma de underställda ämbetsverken på risk- och kontinuitetshanteringen. Risk- och kontinuitetshanteringen måste integreras i ämbetsverkens dagliga ledning och verksamhet.

Risk- och kontinuitetshantering i ämbetsverken räcker inte alltid till – oavsett hur bra den är

Ett enskilt ämbetsverks begränsade urval av åtgärder och en snäv lägesbild med fokus på det enskilda ämbetsverket räcker inte till för att svara på de allt mer komplexa riskerna i den föränderliga omvärlden. Statsförvaltningens verksamhetssätt i dag kräver ofta mer heltäckande risk- och kontinuitetshantering jämfört med tidigare. Ämbetsverk har ersatt egna funktioner för kontinuitetskritiska tjänster med köptjänster från en riksomfattande leverantör, och bland annat IKT, ekonomiförvaltning och lokaltjänster sköts centraliserat. Dessutom hänför sig problemen inom risk- och kontinuitetshanteringen allt oftare till långa funktions- och interaktionskedjor, hela förvaltningsområdet eller förvaltningsövergripande frågor. Många av riskerna är sådana att ett enskilt ämbetsverk inte kan hantera dem allena eller på ett ekonomiskt ändamålsenligt sätt.

Finanscontrollerfunktionens nya rekommendation[1] (2017) om en modell för riskhanteringspolitik har gett positiva effekter, visserligen endast på ämbetsverksnivå för vilken rekommendationen är avsedd.

Ämbetsverken måste hantera allt mer komplexa och omfattande helheter – trots att tvingande lagstiftning saknas

De enskilda ämbetsverkens ansvarar i hög grad för statsförvaltningens risk- och kontinuitetshantering trots att både samhällets och statsförvaltningens funktionssätt och problem har blivit allt mer komplexa och omfattande.

Det saknas en statsövergripande risk- och kontinuitetshantering, och statsförvaltningen utgör inte heller en sådan helhet för vilken det under normala förhållanden skapas en heltäckande lägesbild av riskexponeringen och riskhanteringen. Den systematiska kontinuitetshanteringen omfattar oftast enskilda datasystem, processer eller ämbetsverk.

Samma risker påverkar ofta flera olika myndigheter oavsett förvaltningsområde, och förvaltningsövergripande risker drabbar flera förvaltningsområden. Det behövs både förvaltningsspecifika och förvaltningsövergripande lösningar för att hantera dem. Statsförvalt-

ningen har inga etablerade enhetliga och systematiska metoder för hanteringen av sådan omfattande riskexponering. Det ämbetsverksspecifika perspektivet bör utvidgas till risk- och kontinuitetshantering på förvaltningsområdets eller statsrådets nivå, trots att inte bestämmelser tvingar till det.

Teknologiberoende, centralisering av statsförvaltningens interna tjänster och verksamhetsmodeller i nätverk förutsätter att kontinuitetsriskerna granskas och hanteras med en ämbetsverks- och förvaltningsområdesövergripande syn.

Revisionsverket rekommenderar att

1. alla de ämbetsverk, inrättningar och ministerier som ännu inte har utarbetat en riskhanteringspolitik enligt finanskontrollerfunktionens rekommendationer av 2017 omgående ska upprätta ifrågavarande dokument enligt modellen eller med motsvarande innehåll.
2. ministeriernas ledning inom ramen för ledningssystemet ska se till att säkerställa att ämbetsverkets verksamhet kan pågå utan avbrott och att ämbetsverken vid risk- och kontinuitetshanteringen tillämpar Vahti-anvisningarna *Toiminnan jatkuvuuden hallinta* (2016) och *Ohje riskienhallintaan* (2017) eller motsvarande rekommendationer och normer. Genom att frågor som anknyter till risk- och kontinuitetshantering utgör ett element för ledningen är det viktigt att de integreras i resultatstyrningen och överförs till konkreta mål och skyldigheter i resultat- och ledningsavtalen.
3. det under ledning av statsrådets finanscontrollerfunktion inleds en utredning av behovet av att utvidga risk- och kontinuitetshanteringen till förvaltningsområdes- eller statsrådsnivån. Vidare bör det utredas vilka metoder för insyn och styrning som är ändamålsenliga samt ansvaret för risk- och kontinuitetshanteringen bör fördelas. Finansministeriet och statsrådets kansli bör medverka i utredningen, liksom också de övriga ministeriernas ledning då deras deltagande är relevant.
4. Finansministeriet genom sin styrning ser till att kontinuiteten av de centraliserade tjänster som levereras av Statens center för informations- och kommunikationsteknik samt säkerställandet av kontinuiteten kan verkställas på ett sätt som är ändamålsenligt för både kunden och Statens center för informations- och kommunikationsteknik.

[1] Modell för riskhanteringspolitik: Dokumentmodell för beredning av ämbetsverkets riskhanteringspolitik, inkl. bilagor, 2017.