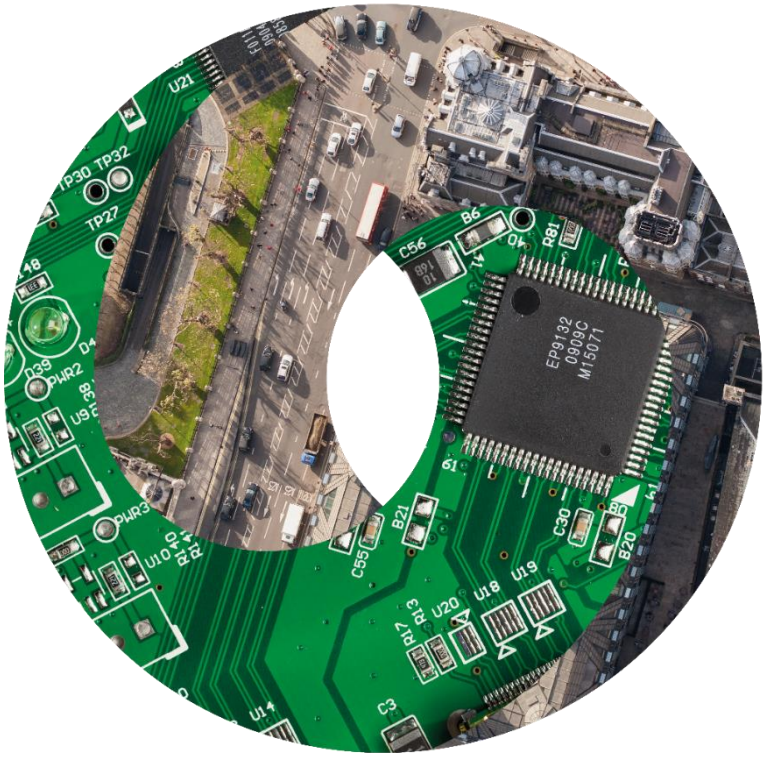
Deloitte.



Krisberedskap och krishantering vid IT-relaterade störningar

Vetlanda kommun

Oktober 2024

Innehåll

Sammanfattning

Deloitte AB har av de förtroendevalda revisorerna i Vetlanda kommun fått uppdraget att genomföra en granskning avseende krisberedskap och krishantering vid IT-relaterade störningar.

Revisionsfråga

Säkerställer Vetlanda kommun i tillräcklig utsträckning kontinuitet i verksamheten vid bortfall av IT-system och data genom sin krisberedskap och krishantering?

Svar på revisionsfråga

Vår sammanfattande revisionella bedömning är att Vetlanda kommun **till stor del** säkerställer kontinuitet i verksamheten vid bortfall av IT-system och data genom sin krisberedskap och krishantering.

Vetlanda kommun har implementerat flera viktiga åtgärder för kontinuitet vid IT-bortfall, inklusive identifiering av kritiska funktioner och kontinuitetsplaner. Vissa kännbara brister kvarstår, men de bedöms vara hanterbara och möjliga att åtgärda inom rimlig tid för att ytterligare stärka beredskapen.

Iakttagelser och slutsatser

- Kommunen har identifierat och prioriterat de mest kritiska funktionerna och IT-systemen, men ytterligare dokumentation behövs för att säkerställa konsekventa och hållbara prioriteringar över tid. Det finns även möjlighet att förbättra konsekvensen i prioriteringen mellan förvaltningarna.
- Det finns en stor variation mellan förvaltningarna i hur deras kärnverksamheter upprätthålls vid IT-relaterade störningar. Exempelvis arbetar vissa förvaltningar med regelbundna tester av manuella rutiner och har välutvecklade backupsystem, medan andra enbart har basala manuella processer utan dokumenterad redundans. Vissa förvaltningar arbetar aktivt med redundans och backupsystem tillsammans med manuella processer för att säkra sina mest kritiska funktioner, medan andra förvaltningar endast har möjlighet att arbeta med manuella processer.
- Alla förvaltningar har inte tydligt identifierat sitt eget ansvar för att säkerställa kontinuitet vid bortfall av IT-system och funktioner, vilket skapar inkonsekvenser i beredskapen.
- De kontinuitetsplaner och det arbete som skett för att säkra kontinuitet i övriga verksamheter är upprättade av förvaltningarna själva, utifrån de ansvarsområden som beskrivs i "Informationssäkerhetspolicy för Vetlanda kommun".
- Åtgärder för att säkerställa kontinuitet vid IT-bortfall varierar kraftigt mellan förvaltningarna. Tekniska kontoret har backuplösningar genom externa leverantörer, medan vård- och omsorgsförvaltningen samt socialförvaltningen huvudsakligen förlitar sig på manuella processer.
- Vissa förvaltningar behöver ytterligare åtgärder för att säkerställa redundans i sina IT-system.
- Tekniska förvaltningen upplever inte ett lika stort beroende av IT-system och funktioner som övriga förvaltningar, trots att IT-stöd är centralt för deras verksamhet. Det är viktigt att öka medvetenheten kring beroendet av IT-stöd för att säkerställa kontinuitet på ett enhetligt sätt mellan olika verksamheter.
- Krisberedskapsplanen behöver uppdateras i enlighet med gällande krav, såsom nationella riktlinjer för krisberedskap och IT-säkerhet. Det finns förbättringspotential i att inkludera en aktuell hotbildsanalys och genomföra regelbundna tester och övningar som speglar nuvarande risker och behov. Flera förvaltningar har ännu inte genomfört tillräckliga tester av sin IT-relaterade

krisberedskap, och tidigare genomförda övningar behöver utvärderas mer strukturerat.

- Det saknas en tydlig plan för hur ofta och på vilket sätt krisberedskapsplanen ska uppdateras och testas.
- En större IT-relaterad övning har genomförts med kommunen, Höglandsförbundet och länsstyrelsen, men det finns förbättringspotential i hur övningen utvärderades och hur resultatet användes för att förbättra beredskapen i förvaltningarna.
- Förvaltningarnas förmåga att upprätthålla verksamheten utan IT-system varierar och är starkt beroende av tillgången till väldokumenterade manuella processer. En del förvaltningar bedömer att de kan upprätthålla verksamheten i upp till 1–4 veckor, men utan enhetliga och testade rutiner är denna förmåga osäker.
- Det saknas en övergripande riskbedömning på kommunnivå och kommunövergripande dokument över hotbilden mot kommunens IT-system. Detta är viktigt för att samordna potentiella hot och säkerställa en gemensam strategi för riskhantering. Nuvarande riskbedömningar fokuserar främst på konsekvenshantering snarare än förebyggande åtgärder.
- Hanteringen av vissa risker, såsom cyberattacker och elavbrott, varierar mellan förvaltningarna. Förvaltningar som saknar adekvata åtgärder kan behöva stärka sin beredskap för att bättre hantera dessa typer av störningar.
- Flera styrdokument från olika avsändare (Höglandsförbundet, Höglandets IT och Vetlanda kommun) överlappar och skapar oklarheter kring ansvar och åtgärder, vilket kan leda till ineffektivitet i krishanteringen.
- Vissa förvaltningar är i hög grad beroende av externa leverantörer för att säkerställa kontinuitet, och kommunen är dessutom till fullo beroende av Höglandets IT för att både etablera och upprätthålla sina IT-relaterade system och funktioner. Detta beroende innebär en sårbarhet som behöver hanteras bättre genom dokumenterade planer och överenskommelser med leverantörerna.

Rekommendationer

Rekommendationer till kommunstyrelsen:

Kommunstyrelsen rekommenderas att:

- Säkerställa att alla styrdokument är uppdaterade och tydligt samordnade för IT-beredskapen.
- Genomföra en kommunövergripande riskbedömning för att identifiera hur nämnderna ska upprätthålla kontinuiteten vid IT-avbrott.

Rekommendationer till samtliga nämnder (inklusive ks som nämnd)

Nämnderna rekommenderas att:

- Tillse att förvaltningen och verksamheterna har tydliga och uppdaterade kontinuitetsplaner vid IT-bortfall som regelbundet testas.
- Säkerställ att kontinuitetsplaner och krisberedskap regelbundet övas och testas.

Specifika rekommendationer till enskilda nämnder

- *Vård- och omsorgsnämnden rekommenderas att* säkerställ att kontinuitetsplanerna för kritiska tjänster som trygghetslarm och äldreomsorg är uppdaterade och tydligt testade för att hantera IT-bortfall.
- *Tekniska nämnden rekommenderas att* utveckla och implementera en dokumenterad kontinuitetsplan för verksamheter med IT-beroende, trots att beroendet inte alltid upplevs som kritiskt.

Jönköping den 2024-10-22

DELOITTE AB
Revsul Dedic
Certifierad kommunal revisor

1. Inledning

Bakgrund

I en alltmer digitaliserad värld är kommuner i hög grad beroende av fungerande IT-system och tillgång till data för att bedriva sin verksamhet och leverera viktiga tjänster till medborgarna. Samtidigt ökar riskerna för IT-relaterade störningar, såsom cyberattacker, strömavbrott och hårdvarufel, vilket kan få allvarliga konsekvenser för kommunens förmåga att fungera.

Vetlanda kommun är inget undantag från denna verklighet. Med en stor del av verksamheten styrd och understödd av IT-system är kommunen sårbar för störningar som kan påverka allt från socialtjänst och skola till räddningstjänst och teknisk förvaltning.

Mot bakgrund av detta har revisorerna i Vetlanda kommun initierat en granskning av kommunens krisberedskap och krishantering för IT-relaterade störningar. Syftet med granskningen är att utvärdera kommunens förmåga att upprätthålla kontinuitet i verksamheten och leverera viktiga tjänster till medborgarna även vid bortfall av IT-system och data.

Syfte och avgränsning

Granskningens syfte är att säkerställa att Vetlanda kommun i tillräcklig utsträckning har säkerställt kontinuitet i verksamheten vid bortfall av IT-system och data genom sin krisberedskap och krishantering. Granskningen fokuserar på att bedöma hur nämnderna kan upprätthålla kontinuiteten vid IT-avbrott, snarare än att förebygga själva avbrottet.

Granskningen har begränsats till att inte omfatta: Detaljerade tekniska analyser av IT-system, granskning av enskilda incidenter, fysiska säkerhetsåtgärder för IT-utrustning och lokaler, bedömning av enskilda medarbetares kompetens, granskning av externa IT-leverantörer eller utveckling av detaljerade framtidsscenarier.

Revisionsfråga

Säkerställer Vetlanda kommun i tillräcklig utsträckning kontinuitet i verksamheten vid bortfall av IT-system och data genom sin krisberedskap och krishantering?

Underliggande frågeställningar

- Har kommunen identifierat och prioriterat de mest kritiska funktionerna och IT-systemen som är nödvändiga för att upprätthålla grundläggande tjänster och verksamhet vid IT-störningar?
- Har kommunen genomfört en riskbedömning för att identifiera och utvärdera de mest sannolika hoten mot IT-systemen (till exempel, cyberattacker, strömavbrott, hårdvarufel) och deras potentiella konsekvenser?
- Har kommunen vidtagit åtgärder för att minska/ reducera sårbarheten för IT-relaterade störningar, såsom backupsystem, redundans, brandväggar?
- Har kommunen etablerat alternativa arbetssätt, procedurer och manuella processer för att säkerställa kontinuitet i verksamheten vid bortfall av IT-system?
- Har kommunen en kommunikationsplan för att informera medborgare, personal och andra intressenter vid IT-relaterade störningar?
- Har kommunen regelbundet testat och uppdaterat sin krisberedskapsplan för att säkerställa att den är aktuell och effektiv?

Metod och granskningsinriktning

Granskningen har genomförts genom dokumentstudier och intervjuer med följande befattningshavare:

- Kommundirektör.
- Kommunstyrelsens ordförande.
- Enhetschef, Höglandets IT.
- Förvaltningschef, vård- och omsorgsförvaltningen.
- Förvaltningschef, barn- och utbildningsförvaltningen.
- Förvaltningschef, tekniska kontoret.
- Fastighetschef, tekniska kontoret.
- Förvaltningschef, socialförvaltningen.

Granskningen har delats in i följande faser:

- Planering av intervjuer.
- Samla fakta/underlag genom intervjuer och dokumentgranskning.
- Genomgång, sammanställning och analys av insamlat material. Vid behov komplettering med mer material.
- Framtagning av viktiga iakttagelser och rekommendationer samt svar på revisionsfråga.
- Rapportskrivning inkl. sakavstämning.
- Presentation av granskning till revisorer.
- Godkänd rapport skickas till berörda nämnder & revisorer.

Revisionskriterier

Kommunallagen, Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH)

Av lagen framgår att kommuner inom sitt geografiska område i fråga om extraordinära händelser i fredstid ska verka för att informationen till allmänheten under sådana förhållanden samordnas.

Förordning (2006:942) om krisberedskap och höjd beredskap

Av förordningen framgår att varje myndighet ansvarar för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Därvid ska behovet av att säkra ledningssystem särskilt beaktas. Förordning (2008:1003). Vidare ska myndigheten beakta behovet av säkerhet och kompabilitet i de tekniska system som är nödvändiga för att myndigheterna ska kunna utföra sitt arbete, samt beakta behovet av deltagande i det samhällsgemensamma radiokommunikationssystemet Rakel. Slutligen ska varje myndighet ansvara för att personalen vid myndigheten får den utbildning och övning som behövs för att den skall kunna lösa sina uppgifter i samband med krissituationer. En planlagd övningsverksamhet ska genomföras, och MSB ska informeras för att övningsverksamheten ska kunna samordnas med den övningsverksamhet som MSB planerar.

Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter (2015:5) om kommuners risk- och sårbarhetsanalyser

Föreskriften definierar kritiska beroenden som sådant som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Sådana beroenden karaktäriseras av att ett bortfall eller en störning i levererade verksamheter relativt omgående leder till sådana funktionsnedsättningar som kan få till följd att en kris inträffar.

Samhällsviktig verksamhet – en verksamhet som uppfyller minst ett av följande villkor:

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Sårbarhet – de egenskaper eller förhållanden som gör samhället, ett system eller egendom mottagligt för skadliga effekter av en händelse. I föreskriften listas ett antal indikatorer för bedömning av kommunens generella krisberedskap, där IT och

informationsverksamhet lyfts som en del av kommunens verksamhet som bör involveras i arbetet med risk- och sårbarhetsanalyser.

I samma lista över indikatorer har såväl kommunikation som informationssäkerhet varsitt delkapitel, där informationskanaler, alternativa lösningar kopplat till it-, tele- och radiosystem och information till allmänheten lyfts som indikatorer inom kommunikation. Inom informationssäkerhet lyfts kommunens rutiner för att identifiera och hantera kritiska beroenden av system och tjänster för informationshantering som är av central betydelse för kommunens verksamhet.

Därtill lyfts kommunens kravställande på informationssäkerhet vid upphandling av informationshantering av extern aktör. Inom samverkan lyfts också rutin för samordning av information till allmänheten vid en extraordinär händelse som en indikator.

Kvalitetssäkring

Kvalitetssäkring har skett genom Deloittes interna kvalitetssäkringssystem. Rapporten har även kvalitetssäkrats av de intervjuade personerna.

2. Granskningsresultat

Utifrån genomförda intervjuer och granskat material har en övergripande beskrivning av Vetlanda kommuns IT-relaterade krisberedskap och krishantering gjorts nedan. De iakttagelser som framkommit till följd av intervjuer och dokumentstudier redogörs under den rubrik som ansetts mest lämplig.

2.1 Har kommunen identifierat och prioriterat de mest kritiska funktionerna och IT-systemen som är nödvändiga för att upprätthålla grundläggande tjänster och verksamhet vid IT-störningar?

Av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter (2015:5) om kommuners risk- och sårbarhetsanalyser definieras kritiska beroenden som sådant som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Mer ingående går att läsa om MSB:s rekommendationer i revisionskriterierna i inledningen av rapporten.

Av det höglandsgemensamma krisberedskapsdokumentet går att utläsa att prioriterade risker har identifierats utifrån vilka risker som orsakar flest skador på personer, flest dödsfall eller störst kostnader för samhället vid inträffande. Av de risker som efter risk- och sårbarhetsanalysen har identifierats som högprioriterade är inga relaterade till IT, digitalisering eller cyber. I samma krisberedskapsdokument nämns dock bortfall av elförsörjning som något som har identifierats som en övergripande sårbarhet inom Höglandsförbundet. Vidare nämns att arbetet med kommunernas krisberedskap inom mandatperioden (2020–2023) fokuserades på kontinuitetshantering för kommunens samhällsviktiga verksamheter, däribland elförsörjning.

Av den Höglandsgemensamma IT-policyn framgår att förbundet har som mål att säkerställa robust och säker drift, vilket innebär hög tillgänglighet till kommunikationsnät och digitala resurser. Vidare framgår att det är särskilt viktigt att förhindra att störningar orsakar allvarliga konsekvenser för kommunen eller dess invånare. IT-säkerhetsarbetet verkar för att säkerställa skyddet. Åtgärder för att uppnå

målen väljs i förhållande till kostnader, säkerhetsnivåer, risker, konsekvenser vid störningar och deras inverkan på den dagliga verksamheten.

Av Vetlanda kommuns ”Plan för hantering av allvarliga och extraordinära händelser” framgår svikt i informations- och kommunikationssystem som ett exempel på händelser som är eller kan utvecklas till extraordinär.

Av kommunens informationssäkerhetspolicy framgår att en god informationssäkerhet själv främjar verksamhetens funktionalitet. Verksamheterna ansvarar själva för sin informationssäkerhet då de har bäst kunskap om hur känslig och kritisk deras information är, och därmed kunskap om informationens skyddsvärde.

Av intervju med kommundirektör framgår att det inom krisledningsstaben har genomförts ett arbete för att identifiera de IT-system och funktioner som är mest kritiska. Enligt det arbetet är det vård- och omsorgsförvaltningens trygghetslarm och medicinlistor som anses mest kritiska.

Av intervjuerna framgår att även respektive förvaltning har identifierat sina mest kritiska funktioner, och att de åtgärderna som vidtas direkt vid inträffad händelse är prioriterade till de funktionerna. Däremot framgår att åtgärderna inte nödvändigtvis är dokumenterade, som i tekniska kontorets fall. Detta är enligt kommunstyrelsens ordförande något som inom närtid kommer att dokumenteras för att säkerställa att alla har tillgång till det vid inträffad händelse.

Av de intervjuade fyra förvaltningarna framgår att respektive förvaltning identifierat vilka funktioner och IT-system som är mest kritiska för att upprätthålla den dagliga verksamheten. Däremot varierar det upplevda beroendet av IT-relaterade tjänster mellan förvaltningarna, samt vikten av att systemen fungerar.

Störst vikt lägger vård- och omsorg vid att funktioner och IT-system fungerar, vars verksamhetssystem och trygghetslarm säkerställer kommuninvånares hälsa. Prioriteringen av att funktionerna ska fungera sker främst genom manuella processer.

Även socialförvaltningen lägger stor vikt vid att systemen behöver fungera för att kunna leverera en rättssäker och kvalitativ verksamhet, men att telefonkontakt till mottagningsenheten är det viktigaste tekniska hjälpmedlet. Prioriteringen av att funktionerna ska fungera sker främst genom manuella processer, samt genom att vid inträffad händelse lyfta ut framför allt mottagningsenheten till en av kommunens etablerade trygghetspunkter.

Barn- och utbildningsförvaltningen upplever inte att deras verksamhetssystem är kritiska för liv och hälsa, men arbetar aktivt med kontinuitetsplan och förbättringsarbeten på området. Prioriteringen av att funktionerna ska fungera sker i nuläget främst genom manuella processer, men ett arbete för att säkerställa att systemen fungerar även vid IT-störning har initierats.

Tekniska kontoret identifierar inbrotts-, brand- och kyl- och fryslarm som de mest kritiska systemen inom förvaltningen, men att beroendet av IT inte är kritiskt. Larmfunktionerna larmar genom internetuppkoppling till SOS, men de är också uppbyggda med redundans, så att de vid bortfall av internet larmar genom GSM (Global System for Mobile Communications). Prioritering av att funktionerna ska fungera sker främst genom backup och redundans från tredjehandsleverantör, tillsammans med möjlighet för manuella processer.

Av intervju framgår vidare att det från politikernas håll inte finns något system eller någon funktion som måste fungera för att upprätthålla grundläggande verksamhet, utöver mailfunktionen. I stället riktas fokus mot de IT-system och funktioner inom framför allt vård- och omsorgsförvaltningen, där invånarnas liv och hälsa står på spel. Vidare framgår av intervju ett hundraprocentigt beroende av Höglandets IT i allt som är IT-relaterat inom kommunen – från internetuppkoppling till brandväggar.

Administrations- och lönesystem nämns i flera intervjuer som viktigt, men mindre viktiga i förhållande till förvaltningarnas centrala verksamhetssystem. Åtminstone barn- och utbildningsförvaltningen nämner sig kunna hantera lönesystemets funktioner manuellt.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen genom förvaltningarna och krisledningsstab har identifierat och prioriterat de mest kritiska funktionerna och IT-systemen som är nödvändiga för att upprätthålla grundläggande tjänster och verksamheter vid IT-störningar. Däremot är åtgärderna för att säkra funktionerna och IT-systemen inte nödvändigtvis dokumenterade.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:
Såväl de fyra intervjuade förvaltningarna som kommundirektör och kommunstyrelsens ordförande har en tydlig bild över vilka system och funktioner som är mest kritiska inom kommunens organisation och inom vardera förvaltningen. Identifieringen av de kritiska systemen på kommunövergripande nivå har skett inom krisledningsstaben, och på förvaltningsnivå av respektive förvaltning. Det finns inte en plan för hur de kritiska systemen eller funktionerna i sig ska upprätthållas vid IT-störningar, men planer för hur verksamheten ändå kan bedrivas genom manuella processer under en begränsad tid finns dokumenterat för alla intervjuade förvaltningar förutom tekniska kontoret.

Det nämns under intervjuer ett hundraprocentigt beroende av Höglandets IT i alla IT-relaterade frågor inom kommunen, både för att etablera funktioner och system, men även för att upprätthålla de vid inträffade störningar.

2.2 Har kommunen genomfört en riskbedömning för att identifiera och utvärdera de mest sannolika hoten mot IT-systemen (till exempel cyberattacker, strömavbrott, hårdvarufel) och deras potentiella konsekvenser?

Av både det Höglandsgemensamma krisberedskapsdokumentet och den Höglandsgemensamma IT-säkerhetspolicyn framgår att risk- och sårbarhetsanalyser regelbundet ska genomföras. Av krisberedskapsdokumentet framgår att risk- och sårbarhetsanalysen kontinuerligt uppdateras under hela mandatperioden och att den för mandatperioden 2020–2023 fokuserade på bland annat elförsörjning.

Av policyn framgår att avbrott i tillgången till information kan vara kritiskt och att felaktig information kan ge allvarliga konsekvenser. Vidare framgår av policyn att viktiga förmågor i arbetet med informationssäkerhet är att kunna identifiera hot, sårbarheter och risker rörande kommunens informationstillgångar. Därtill är en viktig förmåga att kunna utforma- och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå. Som nämnts under tidigare delfråga är kontinuitetsplanering medlet för informationssäkerhetsarbetet inom kommunen, med målet att upprätthålla kritiska verksamheter på fastställd nivå. Detta ska övas regelbundet genom olika simulerade informationssäkerhetsincidenter. Enligt den höglandsgemensamma IT-säkerhetspolicyn inriktas IT-säkerhetsarbetet på hot och skydd förenade med användningen av digital teknik.

Som nämnts under tidigare underliggande frågeställning framgår också av policyn att verksamheterna har ansvar för sin informationssäkerhet, och bäst kunskap om hur känslig den är. Kommunen arbetar med verksamhetsdriven informationssäkerhet, vilket innebär att verksamheterna, utifrån informationens skyddsvärde, ställer krav på de aktörer som hanterar informationen. Skyddet av information ska vara anpassat till informationens skyddsvärde, risk och lagkrav. Information ska klassas, som anger olika nivåer av skyddskrav, baserat på interna och externa krav på informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Av informationssäkerhetspolicyn framgår att arbetet med informationssäkerhet ska utgå från kontinuitetsplanering och ha beredskap för avbrott och störningar, där de kritiska verksamheterna ska kunna upprätthållas på fastställd nivå.

Av intervju framgår att ett av de större identifierade hoten övergripande för kommunen är att spamfilter för mejl skulle sluta fungera, då uppemot 10 000-tals mail dagligen blockeras av kommunens spamfilter. Om illvilliga mail tar sig genom kommunens filter blir kommunen beroende av att den tjänsteperson eller politiker som mottager mailet har tagit lärdom av de utbildningar som givits på området, vilket introducerar den mänskliga faktorn till riskbilden.

Vidare framgår av intervju att riskbedömningar av sannolika hot mot IT har genomförts på förvaltningsnivå, men att det inte finns något sammanställt kommunövergripande dokument över hotbilden, och heller inget styrdokument kopplat till det. Av intervjuer framgår att ingen övergripande riskbedömning av de risker kommunen utsätts för har genomförts.

Vård- och omsorgsförvaltningen lyfter att det finns förbättringspotential att från förvaltningsledning inkludera medarbetare i de riskbedömningar som sker på förvaltningsnivå. Riskbedömningarna från förvaltningarna handlar till största del om sannolikheten för IT-störningar, samt vilka system som kan tänkas att påverkas. Riskbedömningarna har mynnat ut i de kontinuitetsplaneringar de flesta av förvaltningarna upprättat och handlar alltså inte i första hand om vilka risker förvaltningarna ställs inför och vilka konsekvenser en inträffad händelse kan medföra.

Av intervju med Höglandets IT framgår att kommunerna själva behöver initiera en riskbedömning, som i sig kan leda till att åtgärder vidtas inom IT. Om det sker någon förändring relaterad till IT genomför Höglandets IT riskbedömningar relaterat till förändringen, för att exempelvis råda bot på sårbarheter i en ny plattform eller nytt system. De fyra intervjuade förvaltningarna menar att de inte är mer utsatta för IT-relaterade eller generella hot i större utsträckning än andra, motsvarande förvaltningar i andra kommuner. Däremot nämns tidigare förekomster av hackerattacker samt internationell hotbild mot specifika förvaltningar, som mycket väl kan leda till IT-relaterade attacker.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen genom förvaltningarna till viss del har genomfört riskbedömningar för att identifiera och utvärdera de mest sannolika hoten mot IT-system och deras potentiella konsekvenser.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:
Av intervjuer framgår tydligt att de riskbedömningar som har genomförts har skett på förvaltningsnivå och inte övergripande för kommunen. Inga övergripande dokument över hotbilden mot kommunen har tagits fram, och heller inga styrdokument på området. Riskbedömningarna som genomförts på förvaltningsnivå handlar mest om vilka system som påverkas vid konstaterad händelse och vilka konsekvenser det medför, snarare än att handla om vilka risker förvaltningarna potentiellt utsätts för.

2.3 Har kommunen vidtagit åtgärder för att minska/ reducera sårbarheten för IT-relaterade störningar, såsom backupsystem, redundans, brandväggar?

Av den Höglandsgemensamma grundläggande riktlinjen för informationssäkerhet framgår att ett systematiskt och riskbaserat informationssäkerhetsarbete är viktigt och minskar konsekvenserna av incidenter. Ett fungerande informationssäkerhetsarbete syftar till att förebygga och hantera allvarliga störningar och kriser.

Vidare framgår av den Höglandsgemensamma IT-policyn att förbundet har som mål att säkerställa en robust och säker drift, vilket innebär en hög tillgänglighet till kommunikationsnät och digitala resurser så att de kan nyttjas till dess avsedda funktion. IT-säkerhetsarbetet ska verka för att säkerställa skyddet mot bland annat intrång och otillåten användning, och åtgärderna för att uppnå målen väljs i förhållande till kostnader, säkerhetsnivåer, risker, konsekvenser och inverkan på den dagliga verksamheten.

Av intervjuer med förvaltningarna framgår generellt en hög nivå av back up-system och redundans. Tekniska kontoret har redundans för de olika typerna av larm som finns i kommunens lokaler, samt back-up genom externa system för den data som hanteras i de byggprojekt förvaltningen är delaktig i. Därtill uppges att förvaltningen vid intrång i kommunens system ändå kan komma åt mycket av det förvaltningen är beroende av genom egna telefoner och datorer.

Det framgår av intervjuer att barn- och utbildningsförvaltningen har god back up för förvaltningens mest kritiska system såsom elevregister, personalscheman och lönehantering, och att betyg och elevdata kan återställas efter IT-avbrott. Backupsystem är integrerade i det ordinarie verksamhetssystemet.

Av intervjuer framgår det att vård- och omsorgsförvaltningen inte arbetar utbrett med back up-system och redundans av kritiska system, utan att de i stället säkerställer verksamhetens kontinuitet genom bland annat manuella processer.

Socialförvaltningen arbetar likt vård- och omsorgsförvaltningen inte heller utbrett med backup-system eller redundans av kritiska system, utan säkerställer kontinuitet främst genom en övergång till manuella processer vid händelse av IT-relaterade störningar.

Av intervju med Höglandets IT framgår att verksamheterna i många fall inte själva vet hur långa backups de har i sina system. Höglandets IT arbetar utefter en generell back up-längd som appliceras i de fall en verksamhet inte uttryckligen begärt förlängd back up, vilket Höglandets IT i de fallen säkerställer. Gällande redundans av system är det främst redundans av inloggningsmöjligheter som nämns, då systemen i sig i många fall driftas av tredjepartsleverantörer, där vård- och omsorgsförvaltningens och socialförvaltningens verksamhetssystem nämns som exempel. Om Vetlanda kommun skulle träffas av IT-störningar kan Höglandets IT säkerställa åtgång till det tredjepartslevererade systemen genom redundans av de inloggningsmöjligheter Höglandets IT tillhandahåller. Höglandets IT arbetar därtill med flera av tredjepartsleverantörerna för att säkerställa kontinuitet och redundans av deras leverans till verksamheterna. Redundanta brandväggar, routrar och uppkopplingar är något som Höglandets IT säkerställt sedan länge.

Av kommunstyrelsens ordförande och kommundirektör framgår att redundans och kontinuitet av verksamheterna är något som förvaltningen själva arbetar fram tillsammans med Höglandets IT. På en kommunövergripande nivå finns en kriswebb på andra servrar än kommunens egna, som fungerar om kommunens övriga webbsidor ligger nere till följd av intrång. Från politikernas håll framgår det inte finnas något reellt behov av ytterligare backup och redundans utöver det som finns inbyggt i Outlook och Microsofts system.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen genom förvaltningarna till viss del har vidtagit åtgärder för att minska/reducera sårbarheten för IT-relaterade störningar, såsom backupsystem, redundans och brandväggar.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:

Förvaltningarna har en varierande nivå av backupsystem och redundans av kritiska IT-system. Tekniska kontoret uppges ha såväl redundans som backupsystem säkrade, främst genom externa leverantörer och vid behov möjligheten att använda privata enheter för åtkomst av system.

Barn- och utbildningsförvaltningen arbetar främst med backupsystem integrerat i existerande system. Vård- och omsorgsförvaltningen samt socialförvaltningen arbetar inte utbrett med backupsystem och redundans av system, utan säkerställer kontinuitet genom manuella processer.

Höglandets IT kan hjälpa förvaltningarna med den backuplängd, de backupsystem och den redundansen av system förvaltningen behöver, men det behöver ske på initiativ av förvaltningen själv. Redundanta brandväggar finns för alla kommunens förvaltningar.

2.4 Har kommunen etablerat alternativa arbetssätt, procedurer och manuella processer för att säkerställa kontinuitet i verksamheten vid bortfall av IT-system?

Av den Höglandsgemensamma IT-säkerhetspolicyn framgår att arbetet med IT-säkerhet bland annat innebär att samtliga system inom Höglandsförbundet och dess medlemskommuner är identifierade och förtecknade och att systemägare och systemansvarig är utsedda. Vidare framgår av policyn, som avhandlats under tidigare delfråga, att målsättningen med IT-säkerhetsarbetet inom förbundet är att säkerställa en robust och säker drift, vilket uppnås genom hög tillgänglighet till kommunikationsnät och digitala resurser.

Av Vetlanda kommuns informationssäkerhetspolicy framgår att arbetet med informationssäkerhet bland annat ska ha beredskap för avbrott och störningar, och att kommunens kritiska verksamheter ska kunna upprätthållas på fastställd nivå vid olika typer av incidenter.

Av de fyra intervjuade förvaltningarna framgår att samtliga har alternativa manuella processer som kan vidtas i händelse av bortfall av IT-tjänster. Barn- och utbildningsförvaltningen uppger ha personalscheman och skolans planering för hela terminen utskriven på papper. Även lönesystemet kan hanteras manuellt, och elevdata hanteras i nuläget uteslutande manuellt i fysiska mappar. Barn- och utbildningsförvaltningen beräknar kunna bedriva sin verksamhet utan IT-stöd i upp till fyra veckor.

Vård- och omsorgsförvaltningen skriver ut bland annat journaler, medicinering, personalplanering och besöksrutiner. Varje funktion inom förvaltningen har en egen beredskapsplan som passar deras dagliga verksamhet och behov. Det lyfts att verksamhetssystemet är svårt att klara sig utan även om utskrivna papperskopior finns. Vård- och omsorgsförvaltningen uppskattar att man klarar sig mindre än en vecka utan tillgång till sina system innan patientsäkerheten äventyras.

Tekniska kontoret har inga dokumenterade kontinuitetsplaner att arbeta efter vid inträffade händelser, men har efterfrågat vilka scenarier de ska planera för. Tekniska kontoret har ej övervägt att ha utskrivna backups, och upplever inte att de har något system som måste fungera utan fördröjning. Det uppges att den information som riskeras att försvinna vid bortfall av IT-system är all information tekniska kontoret hanterar, inklusive vissa avtal som endast finns lagrade digitalt.

Gällande kontinuitet i verksamhetens dagliga arbete framgår att förvaltningen har möjlighet att styra och sköta sina arbetsområden manuellt, och att goda möjligheter för manuella processer finns då större delen av förvaltningen består av personal som är ute på plats och arbetar, utan vidare beroende av IT. Arbetssättet gäller för samtliga av tekniska kontorets funktioner – alla arbetsområden kan säkerställa kontinuitet genom manuellt, praktiskt arbete, vilket förvaltningen ser som en styrka i sig. Tekniska kontoret uppskattar att man vid kortare bortfall av IT-systemen klarar sig i alla avseenden, men att det vid längre avbrott börjar uppstå problem.

Socialförvaltningen har en dokumenterad och utskriven kontinuitetsplan för alla de system förvaltningen använder. Varje enhet inom förvaltningen har en egen, anpassad kontinuitetsplan, som ska träda i kraft fyra timmar efter inträffad händelse. Enheterna har möjlighet att gå över till manuella processer och på så sätt hålla verksamheten fungerande, om än med längre väntetider och sämre kvalitet. Socialförvaltningen har svårt att uppskatta hur länge de klarar sig utan IT-system, men att det blir svårare att upprätthålla verksamheten ju längre avbrottet är.

Av intervjuer med förvaltningarna framgår att de inte fått hjälp av kommunledningsförvaltningen med att upprätta sina eventuella kontinuitetsplaner. Kontinuitetsplanerna har i huvudsak upprättats av förvaltningarna själva, och i vissa fall med hjälp från Höglandets IT.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen genom förvaltningarna till stor del har etablerat alternativa arbetssätt, procedurer och manuella processer för att säkerställa kontinuiteten i verksamheten vid bortfall av IT-system.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:
Samtliga av de fyra förvaltningar som intervjuats inom ramen för denna granskning uppger sig ha alternativa manuella processer som kan säkra verksamhetens kontinuitet i händelse av bortfall av IT-system. Kontinuitetsplaneringen ser olika ut för olika förvaltningar, där tekniska kontoret ej arbetar med utskrivna backups eller dokumenterade kontinuitetsplaner, men ändå skattar sig själva förberedda inför eventuella IT-relaterade störningar.

Frågor uppstår kring kontinuitetsarbetet främst hos tekniska kontoret. Majoriteten av beredskapen är inte dokumenterad, förvaltningen förlitar sig i stället mycket på den egna personalens initiativförmåga, muntliga överenskommelser, Höglandets IT, tredjepartsleverantörer och antaganden kring bästa förfarande. Stort förtroende till personalen är i sig inte negativt, men vår bedömning är att förvaltningen i stort underskattar sitt beroende av IT-system och funktioner, och att eventuella bortfall inte ges den vikt det borde. Det finns en risk att förvaltningen inte ser ansvaret för att själva säkerställa att verksamheten kan bedrivas kontinuerligt vid bortfall av IT.

Av de förvaltningar som intervjuats framgår en uppskattad beredskap utan IT-system på mellan 1–4 veckor, vilket kan komma att både förkortas och förlängas beroende på vilka IT-system som träffas. Den förvaltning som uppskattar kortast kontinuitet vid bortfall av IT-system är vård- och omsorgsförvaltningen, beroende på verksamhetens känsliga natur.

Slutligen bedömer vi att kommunledningsförvaltningen bör involveras mer i etableringen av de alternativa arbetssätten, kontinuitetsplanerna eller manuella processerna som finns i de flesta verksamheterna. Detta för att säkerställa likvärdig kontinuitet genom hela kommunorganisationen Arbetet med att säkra kontinuitet i verksamheterna har utförts av förvaltningarna själva, med viss hjälp av Höglandets IT.

2.5 Har kommunen en kommunikationsplan för att informera medborgare, personal och andra intressenter vid IT-relaterade störningar?

I det Höglandsgemensamma dokumentet Handlingsprogram skydd och säkerhet 2020–2023 framgår att Nässjö och Vetlanda kommuner arbetar för att åtgärder som vidtas av olika aktörer inom kommens geografiska område samordnas. Kommunen ska också arbeta för att information till allmänheten från berörda organisationer samordnas. Kommunens invånare hänvisas i dokumentet i händelse av kris till kommunens informationskanaler för löpande information. Vidare framgår av dokumentet att kriser hanteras enligt rutin för kriskommunikation. Kommunen har därutöver en kriswebb på externa servrar som invånarna kan vända sig till vid händelse av intrång på kommunens servrar, som nämnts under tidigare delfråga.

Av Vetlanda kommuns Plan för hantering av allvarliga och extraordinära händelser framgår riktlinjer för kriskommunikation. Kommunikationsfunktionen, som leds av kommunikationschefen eller dennes ersättare, ingår i staben som vid extraordinär händelse fungerar som stöd till händelsegruppen. Stabens uppdrag är bland annat att initiera och samordna intern och extern kriskommunikation. Arbetet genomförs enligt särskild fastställd kommunikationsplan.

Vetlanda kommun har en speciellt antagen rutin för kommunikation vid allvarliga och extraordinära händelser. Av den framgår tydligt under vilka omständigheter rutinen ska användas, hur kommunens krisorganisation ser ut och vem som är informationsavsändare. Vid en extraordinär händelse är krisledningsnämnden ytterst ansvarig för kommunens information, medan det för en allvarlig händelse är kommunchefen som är ytterst ansvarig. Informationsavsändare är kommunikationsenheten i krisledningsnämndens namn, och informationen ska

samordnas mellan kommun och samverkande myndigheter så långt det är möjligt. Av rutinen framgår hur såväl intern- som extern kommunikation ska ske. Av rutinen framgår inte särskilt hur kommunen ska kommunicera i händelse av IT-relaterade störningar eller kriser.

Även Höglandsförbundet har en kriskommunikationsplan, där IT-relaterade händelser tydligare avhandlas. Av kriskommunikationsplanen framgår att omfattande IT-avbrott klassas som extraordinär händelse, och att kommunikationsbehovet då kan styras utifrån förbundets krisledningsstab. Vid en extraordinär händelse framgår av kriskommunikationsplanen att krisledningsstabens kommunikationsfunktion ska vara den enda informationsavsändaren, och informationen ska sändas i krisledningsstabens namn. Av krisinformationsplanen framgår också hur krisinformation går till vid stora IT-störningar. För stora IT-störningar framgår hur kommunerna larmas, hur kommunikation från Höglandsförbundet når kommunerna, och hur ansvarsfördelningen mellan förbund och kommun ser ut. Av kriskommunikationsplanen framgår även hur kommunikationen administreras internt inom förbundet och kommunerna, och externt till bland annat allmänheten och media. Av rutinen framgår det tydligt vilka ansvarsområden och vilka målgrupper som ska kontaktas genom vilka kommunikationsmedel.

Av de fyra förvaltningar som intervjuats har alla förutom tekniska kontoret en dokumenterad kommunikationsplan för inträffade händelser. Planerna som finns täcker i första hand intern kommunikation inom förvaltningarna, och säkerställer att i första hand chefer nås av information för vidarekommunikation internt.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen har en kommunikationsplan för att informera medborgare, personal och andra intressenter vid IT-relaterade störningar.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:
Kommunens kommunikation vid extraordinära händelser avhandlas på ett eller annat sätt i minst fyra olika styrdokument: Handlingsprogram skydd och säkerhet 2020–2023, Plan för hantering av allvarliga och extraordinära händelser, Rutiner för kommunikation vid allvarliga och extraordinära händelser, samt i Höglandsförbundets Kriskommunikationsplan.

IT-relaterade störningar berörs endast konkret i Höglandsförbundets Kriskommunikationsplan. Däremot framgår av planen att omfattande IT-avbrott räknas som extraordinär händelse, vilket gör att kommunens egna kommunikationsplaner för extraordinära händelser omfattar IT-relaterade störningar, även då de inte uttryckligen nämns. Av planerna framgår tydligt hur medborgare, personal och andra intressenter ska informeras vid inträffade händelser, även då inte alla planerna uttryckligen nämner IT-relaterade störningar. Viss förvirring uppstår till följd av den mängd styrdokument som på ett eller annat sätt rör kommunikation.

2.6 Har kommunen regelbundet testat och uppdaterat sin krisberedskapsplan för att säkerställa att den är aktuell och effektiv?

Vetlanda kommuns krisberedskapsplan samordnas tillsammans med Höglandsförbundets Räddningstjänstförbund och Nässjö kommun i Handlingsprogram skydd och säkerhet 2020–2023. Vetlanda kommun har utöver det höglandsgemensamma Handlingsprogram skydd och säkerhet 2020–2023 en egen Plan för hantering av allvarliga och extraordinära händelser i Vetlanda kommun. Dokumentet ska revideras minst en gång per mandatperiod, vilket inte skett sedan 2016.

Av det höglandsgemensamma handlingsprogrammet för skydd och säkerhet framgår att förbundet har som mål att kommunerna ska arbeta för en bättre krisorganisation genom att öva enskilda krisfunktioner samt samöva hela krisorganisationen. Enligt programmet ska såväl övningarna inom enskilda krisfunktioner som de övergripande samövningarna utvärderas. Vidare framgår av handlingsprogrammet att risk- och sårbarhetsanalysen är en kontinuerlig process som ständigt uppdateras under hela mandatperioden, men inte att krisberedskapsplanen i sig uppdateras.

Som nämnts under tidigare delfråga framgår av Vetlanda kommuns informationssäkerhetspolicy att arbetet med informationssäkerhet utgår från återkommande risk- och sårbarhetsanalyser som kontinuerligt uppdateras. De kritiska

verksamheternas upprätthållande på fastställd nivå övas på regelbundet genom simulerade informationssäkerhetsincidenter.

I det höglandsgemensamma krisberedskapsdokumentet nämns att risk- och sårbarhetsanalysen kontinuerligt uppdateras under hela mandatperioden, men inte att krisberedskapsplanen uppdateras.

Av intervjuer framgår att det genomfördes en större IT-relaterad övning nyligen, där kommunen bland annat stresstestades genom simulerat bortfall av internet. Därtill har alla politiker och tjänstemän genomgått en utbildning för att få kunskap om hur vardera personen kan motverka intrång i datanätet. Vidare framgår att ytterligare en större övning i Höglandsförbundets regi planeras på IT-området.

Ingen av de intervjuade förvaltningarna upplever att några övningar genomförts där förvaltningens IT-relaterade krisberedskap har testats. Däremot framgår av flertalet intervjuer att det har genomförts en övergripande scenarioövning för kommunen inriktad mot cybersäkerhet tillsammans med Höglandsförbundet och länsstyrelsen. Det råder tvivel kring i vilken utsträckning resultatet av övningen utvärderades och användes för att stärka förvaltningarnas beredskap. Feedbacken som delades efter övningen var i stället övergripande för hela samlingen.

Därtill framgår av Höglandets IT att övningar har genomförts inom förbundets olika nätverk, där varje medlemskommun har representanter från exempelvis vård- och omsorg i ett nätverk, och representanter från medlemmarnas tekniska förvaltning i ett annat. Det råder delade meningar bland förvaltningarna om just de har varit delaktiga i några övningar kopplat till IT-säkerhet i Höglandsförbundets olika nätverk.

Vård- och omsorgsförvaltningen uppger att de bett beredskapssamordnare att ordna en övning för att träna på och testa de dokumenterade rutinerna förvaltningen har. Övningen räknar man med kommer hållas under hösten. Ytterligare en övning planeras av Höglandets IT, där det planeras att i skarpt läge bryta något av IT-systemen. Av kommundirektör framgår att det finns målsättningar för hur ofta och i vilken omfattning övningar ska genomföras, men att de målen har varit svåra att nå av bemanningsskäl.

Utbildningsinsatser på IT- och cybersäkerhetsområdet uppges av samtliga intervjuer ha genomförts tidigare under året av alla medarbetare i kommunen. Av Höglandets IT framgår vidare att förbundet nyligen lanserat en utbildningsplattform för att kunna erbjuda alla medlemskommuner relevanta och likvärdiga utbildningsmöjligheter.

Av intervju med Höglandets IT framgår att krisberedskapsplanen är inaktuell och att en översyn av krisberedskapsplanen planeras. Anledningen till att en ny, uppdaterad och aktuell krisberedskapsplan ännu inte antagits uppges vara till följd av att Höglandsförbundet växt så pass mycket sedan den senaste utfärdade planen, samt till följd av ett identifierat behov av att inkludera cybersäkerhet i en mycket högre utsträckning än tidigare.

Gemensamt för flera av de förvaltningarna som intervjuats är en efterfrågan om fler övningar vad gäller kontinuitetsplanering generellt, men även IT-specifikt. Ingen av de intervjuade förvaltningarna har övat på sin krisberedskapsplan eller kontinuitetsplan.

Bedömning och kommentarer

Vår samlade revisionella bedömning är att kommunen till viss del har testat sin krisberedskapsplan, men inte att krisberedskapsplanen uppdaterats för att säkerställa att den är aktuell och effektiv.

Vår bedömning baseras på nedanstående iakttagelser, kommentarer och slutsatser:
Det höglandsgemensamma dokumentet Handlingsprogram skydd och säkerhet 2020–2023, som fungerar som kommunens styrdokument i krisberedskap, är som framgår av handlingsprogrammets titel utdaterat.

Det pågår ett arbete för att ta fram ett nytt höglandsgemensamt krisberedskapsdokument, som är försenat bland annat till följd av att IT- och cybersäkerhet ska inkluderas i en högre utsträckning än tidigare.

Det framgår av intervjuer att det har genomförts minst en scenarioövning inriktat mot cybersäkerhet under mandatperioden, men att utvärdering och utveckling av respektive förvaltnings krisberedskap efter övningen hade kunnat förbättras.

Ingen av de intervjuade förvaltningarna upplever att övning genomförts där förvaltningens IT-relaterade krisberedskap och kontinuitet har testats, vilket av flera förvaltningar efterfrågas.

Det finns två olika dokument som kan antas fungera som krisberedskapsdokument för kommunen – ett på kommunnivå och ett på höglandsgemensam nivå. Att det finns två kan leda till förvirring, inte minst då båda är utdaterade. Inget av krisberedskapsdokumenten har under perioden uppdaterats.

Deloitte.