MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Strategisk riskhantering för den digitala säkerheten inom den offentliga förvaltningen

Riskhanteringsmodellens struktur

15.12.2022

Reivo Juho (MDB)

15.12.2022

Innehållsförteckning

1 Inledning ... 3
1.1 Modellens utvecklingsväg ... 4
1.2 Observationer och ändringar efter kommentarer ... 5
2 Strategisk riskhanteringsmodell ... 7
2.1 Beskrivning av nuläget ... 7
2.2 Årsplanering av riskhanteringen ... 8
2.3 Beskrivning av riskhanteringsprocessen på strategisk nivå ... 10
2.3.1 Processens aktörer och roller ... 10
2.3.2 Processens delar och faser ... 13
3 Bakgrundsantaganden för riskhanteringsmodellen ... 18
3.1 Användningsändamål och aktörer ... 18
3.2 Grundläggande antaganden och avgränsningar ... 19
3.2.1 Interna utsikter och ett för granskningen betydelsefullt perspektiv ... 20
3.2.2 Verksamhetsmiljöer inom vilka granskningen görs ... 21
3.2.3 Strategisk definition i denna modell ... 21
3.2.4 Tidsfönster ... 23
3.2.5 Informationens kvalitet och effekterna av det praktiska genomförandet ... 24
3.2.6 Informationssäkerhet ... 25
3.2.7 Förhållandet till organisationernas egen riskhantering ... 26
3.2.8 Förhållande till andra risk- och säkerhetsbedömningar ... 27
3.2.9 Förhållande till standarder ... 28
3.3 Om kostnader och effektivitet ... 28
3.4 Utveckling av riskhanteringsmodellen ... 30
3.4.1 Första utvecklingsfasen ... 32
3.4.2 Skiss över den andra utvecklingsfasen ... 32
3.4.3 Eventuella skeden i den fortsatta utvecklingen ... 33

Reivo Juho (MDB)

15.12.2022

Strategisk riskhantering av digital säkerhet inom den offentliga förvaltningen - Riskhanteringsmodellens struktur

I detta dokument beskrivs verksamhetsmodellen för hantering av strategiska risker inom digital säkerhet och hur modellen utvecklas i den utsträckning som den enligt planerna ska genomföras inom den offentliga förvaltningen. Utvecklingen av modellen inleddes 2020 och den har kommenterats offentligt våren 2022 och på basis av dem har kompletteringar gjorts. Detta dokument är en bakgrundsöversikt för experter på digital säkerhet och riskhantering. För det praktiska genomförandet kommer ett mer riktat stödmaterial att skapas.

Den föreslagna verksamhetsmodellen och de tillhörande uppgifterna utgör den offentliga förvaltningens strategiska riskhanteringsmodell för digital säkerhet. Modellens uppgift är att göra det möjligt att identifiera, bedöma och styra hanteringen av tvärad-ministrativa och allmänt fördelade risker inom den offentliga förvaltningen. Den presenterade helheten är en beskrivning av verksamhetsmodellen och de processer som ingår i den. Den är av permanent karaktär, eftersom den digitala säkerheten behöver utvecklas långsiktigt. Till helheten hör dock också delar som behöver utvecklas och som beaktar den kontinuerliga förändringen i verksamhetsmiljöerna och som styrs av kommande mål och behov som klarnar vid sidan av riskhanteringsarbetet. Det praktiska genomförandet har presenterats i huvudsak för att förstå processen och dess utveckling, bland annat i fråga om säkerhetsaspekter.

Den riskhanteringsprocess som en enskild organisation eftersträvar beskrivs i standarden ISO31000. Jämfört med det finns det centrala skillnader i denna riskhanteringsmodell som omfattar hela den offentliga förvaltningen. Skillnaderna beror på att det finns instanser med vissa befogenheter medan andra är decentraliserade i förvaltningen och den digitala verksamhetsmiljön.

- Utifrån riskhanteringsprocessen kan en noggrannare utveckling av de förvaltningsåtgärder som vidtas för det gemensamma bästa ske separat av behöriga myndigheter, vilket kan innebära en eller flera aktörer. Ändå ansvarar organisationen för att genomföra dessa åtgärder i sin egen verksamhet. Tvärad-ministrativ verksamhet är en utmaning som löses genom samarbete som bygger på god förvaltningssed i stället för en stelare författningsbaserad struktur.
- I den föreslagna riskhanteringsprocessen har man beaktat den offentliga förvaltningens naturliga behov av en struktur för tydligt beslutsfattande, som beroende på kontexten kan omfatta en eller flera aktörer. Att beskriva den skapar skenbart en avvikelse från standarden. Beaktandet av god förvaltningssed bryter dock inte mot standarden utan stöder informationsledning och riskbaserat beslutsfattande.
- Även om riskhanteringsprocessen beskrivs i sin helhet betonas behandlingen av den information som skapas i början av modellen. De praktiska åtgärder som vidtas – såsom insamling och analys av information – fokuserar på att stödja detta, så att riskhanteringsåtgärderna under den senare hälften av processen kan stödas och styras effektivt.

Dokumentet har efter inledningsdelen delats in i två delar. Först presenteras modellen med hjälp av processen och dess delar. I den senare delen granskas bakgrundsantaganden och begränsningar i anslutning till modellen samt ett utkast till utveckling av modellen under de kommande åren. På lång sikt kunde en riskhanteringschef för digital säkerhet som eventuellt placeras vid Myndigheten för digitalisering och befolkningsdata ansvara för planeringen och främjandet av de centrala delarna av modellen inom den offentliga förvaltningen.

Reivo Juho (MDB)

15.12.2022

1 Inledning

Organisationerna genomför riskhantering utifrån sina egna utgångspunkter och fokuserar på sin egen verksamhet, så som de ska. De behöriga myndigheterna svarar separat för vissa åtgärder i anslutning till riskprocessen. Riskhanteringen ska återspegla hur organisationen (eller något annat objekt eller en helhet som granskas) fungerar och ser på sig själv samt förhållandet till den omgivande verksamhetsmiljön. Modern riskhantering och gestaltning av moderna, i synnerhet digitala, risker kräver en mer omfattande granskning även över de egna gränserna, till exempel risker som uppstår för kunder och intressentgrupper. Såväl tätt kopplade kedjor som lösare ekosystem kan påverka organisationens förmåga att agera. På motsvarande sätt bör även organisationer inom den offentliga förvaltningen identifiera hur deras åtgärder påverkar utvecklingen av den digitala säkerheten hos andra, inklusive individer.

Riskhanteringen på statsrådsnivå är under beredning[1]. På statsrådsnivå har det inte funnits någon skyldighet att regelbundet samla in riskinformation som omfattar förvaltningsområdena och som identifierar fenomen och mer omfattande risker eller jämför utsikterna med dem. Detta gäller både alla risker som helhet och separata ämnesområden, såsom digital säkerhet. Det finns ingen aktuell och heltäckande lägesbild av de allt mer komplicerade eller gränsöverskridande riskerna i den föränderliga verksamhetsmiljön. I brist på helhetsbild har man endast kunnat rikta bristfällig styrning och resurser till stöd för riskhanteringsåtgärder inom den offentliga förvaltningen. Eftersom definitionen och uppföljningen av förvaltningsåtgärderna inte har gjorts organisationsspecifikt har man inte heller kunnat bedöma effekterna av de utvecklingsåtgärder som vidtagits inom den offentliga förvaltningen på ett heltäckande sätt[2].

I den strategiska riskbilden identifieras sådana risker från flera nationella och internationella informationskällor som om de förverkligas skulle orsaka allvarliga olägenheter för såväl staten som andra aktörer inom den offentliga förvaltningen. Den allmänna styrningen av den offentliga förvaltningens informationshantering, förberedelser inom tjänster och tjänsteproduktionen, beredskap och säkerhet hör till finansministeriets (FM) uppgifter. Den ska kunna bedöma kostnaderna för säkerheten för den allmänna styrningen av den digitala säkerheten samt rikta resurserna så effektivt som möjligt. Nyttan av de planerade riskhanteringsåtgärderna (åtgärdernas effekt) ska kunna följas upp och stå i ett godtagbart förhållande till kostnaderna för genomförandet.

[1] Rapport av arbetsgruppen som berett ärendet (referat på svenska): https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163184/VM_2021_28.pdf I förhållande till målen i utvecklingsförslaget (rapport s. 11) skulle den information som produceras med hjälp av denna modell vara tillgänglig även i den processen då den i praktiken kan ta emot den. Före det och därutöver är informationen tillgänglig i de normala tjänstekanalerna via behöriga myndigheter. Det bör dock observeras att riskkontextens nivå och perspektiv förändras, varvid informationen bedöms utifrån olika utgångspunkter och olika behov (rapport s. 27).

[2] Effektivitetsrevisionsberättelse av Statens revisionsverk 20/2018 (på finska)

1.1 Modellens utvecklingsväg

För riskhanteringen inom den offentliga förvaltningen har man utarbetat ganska omfattande anvisningar både för att stöda organiseringen av riskhanteringen och för att förenhetliga de centrala delarna av processen. Anvisningarna gäller såväl jämförbarhet, revisionernas effektivitet som god praxis. Finansministeriets controllerfunktion är en central handledare i riskhanteringen inom den offentliga förvaltningen. Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen, dvs. VAHTI (ursprungligen ledningsgruppen för informationssäkerhet inom statsförvaltningen) och en underordnad arbetsgrupp för utveckling av riskhanteringen, har gett anvisningar för den digitala säkerheten som helhet. Effekten av VAHTI-anvisningarna framgår av att man fortfarande (delvis felaktigt) hänvisar till dem även om de inte är förpliktande. Det senaste VAHTI-stödmaterialet om riskhantering öppnade upp begreppen och kommunikationen[3] kring riskhantering i den digitala verksamhetsmiljön, vilket även detta dokument följer. De givna instruktionerna, handledningen i anslutning till dem eller andra tillgängliga informationskällor har dock inte gett någon tydlig bild av tillämpningen av dem eller de risker som framkommer – i synnerhet inte när informationsbehovet utvecklas under årtiondenas lopp.

Utgångspunkten för riskhanteringsmodellen är statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen 8.4.2020 (FM 2020: 23)[4]. I beslutet listas sex principer för utveckling, av vilka riskhanteringsmodellen utgår från principen: "Vi leder det digitala samhällets säkerhet tillsammans utifrån lägesinformation och riskbedömning".

I enlighet med genomförandeplanen för digital säkerhet 2020–2023 (Haukka)[5] har en tväradministrativ strategisk ledningsgrupp för digital säkerhet (DTS-JORY) tillsatts. Den ska bland annat utvärdera den strategiska situationen för den digitala säkerheten inom den offentliga förvaltningen, skapa och samordna en samarbetsmodell samt utvärdera, styra, koordinera och övervaka centrala tjänster för digital säkerhet som ska utvecklas[6]. Bearbetningen och pilottestningen av modellen inleddes tillsammans med den tillsatta ledningsgruppen. Gruppens betydelse framhävs under den senare hälften av riskhanteringsprocessen som ett centralt samarbetsforum med hjälp av vilket de behöriga myndigheterna kan koordinera hanteringsåtgärderna och samordningen av dem. På längre sikt kan de administrativa strukturerna förändras, vilket betyder att koordineringen av de gemensamma riskhanteringsåtgärderna också kan genomföras på något annat sätt som utnyttjar en ändamålsenlig samarbetsstruktur och att modellen är således inte bunden till den här gruppens tidsbundenhet.

Den uppgiftshelhet om riskhantering som ingår i Haukka-projektet inleddes 2020 och har styrts av styrgruppen för projektet för utveckling av den digitala säkerheten inom den offentliga förvaltningen (JUDO). Utvecklingen av den ursprungliga processmodellen, pilotförsöket och dess utvidgade fortsättning styrdes av informationsförvalt-

[3] https://dvv.fi/documents/16079645/110675816/VAHTI-ordlista+om+riskhantering+i+digital+verksamhetsmilj%C3%B6.pdf/aec58883-3c7c-430d-8d3c-658b98bed212/VAHTI-ordlista+om+riskhantering+i+digital+verksamhetsmilj%C3%B6.pdf?t=1674484460823

[4] Digital säkerhet inom den offentliga förvaltningen

[5] Genomförandeplan för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka) FM 33/2020

[6] Tillsättandet av den strategiska ledningsgruppen för digital säkerhet, 19.12.2019 (VN/13510/2019) Beskrivningarna i detta dokument om ledningsgruppens roll och hur riskhanteringen ska genomföras motsvarar och tolkar dessa uppgifter i den mån de ingår i ledningsgruppens arbete. Utanför dessa ansvarar varje behörig myndighet för riskhanteringen och uppgifter i anslutning till den. Läs mer här 2.3.1

ningsrådet Tuija Kuusisto. Utvecklingen av projektuppgiften överfördes 2021 till Myndigheten för digitalisering och befolkningsdata (MDB), specialsakkunnig Juho Reivo har verkat som projektchef.

Man har ansett att det finns ett långvarigt behov av att granska risker och riskhantering och därför borde den föreslagna modellen med de tillhörande uppgifterna göras till permanenta delar av ledningen av den digitala säkerheten.

1.2 Observationer och ändringar efter kommentarer

Detta dokument kunde kommenteras offentligt i april 2022, då 34 olika aktörer inom den offentliga förvaltningen gav respons och kommentarer.[7] På ett allmänt plan fanns det mycket variation bland kommentarerna, men helt klart ansåg största delen att det var önskvärt att utveckla riskhanteringen och modellen för digital säkerhet både med tanke på organisationerna och det allmänna bästa. Även om modellen inte direkt erbjuder lösningar på några enskilda hot eller risker möjliggör informationen och de dataprodukter som förädlats från informationen en självstyrning av organisationernas egna förvaltningsåtgärder. Dessutom kan de utnyttjas som en del av styrningsåtgärderna och de behöriga myndigheternas åtgärder kan utvecklas effektivare för gemensamt bruk. I dokumentet skapades också preciseringsbehov av de administrativa ändringar i anslutning till styrningen av den digitala verksamhetsmiljön och den digitala säkerheten som är under utveckling samtidigt.

I kommentarerna framkom inga behov av att ändra strukturen i den modell som uppfattas som en slag styrande ramverk. På basis av dem lyfter man dock fram delar av den process som ingår i modellen på ett bättre sätt, med betoning på dess början. Den tydligast synliga delen är riskbedömningsprocessen (insamling av information i anslutning till identifiering samt analys och utvärdering av denna), och utifrån det praktiska genomförandet förstår man också modellen bättre. Modellen förutsätter inga tillfälliga arbetsgrupper trots att de kan användas och tar inte ställning till med vilka strukturer förvaltningsåtgärder genomförs inom den offentliga förvaltningen. Information – insamling, behandling och delning av information – får lite mer uppmärksamhet än en modell för beslutsfattande vid riskhantering där man litar på befintliga strukturer och verksamhetssätt. På så sätt förblir strukturen standardiserad och det är lättare att uppfatta olika gränssnitt i organisationernas egen riskhantering.

I flera kommentarer fäste man uppmärksamheten på frågor som var aktuella eller skulle utvecklas på praktisk genomförandenivå. Dessa har i mån av möjlighet beskrivits i större utsträckning. Det var uppenbart att många som kommenterade inte på ett heltäckande sätt kände till den mer omfattande digitala säkerheten, riskhanteringsprocessen eller att de inte hade bekantat sig med pilotprojekten. I fortsättningen strävar man efter att producera mer utbildnings- och stödmaterial för att stödja detta. En del ansåg att den föreslagna modellen var mycket tydlig, medan andra ville ha tydligare material med betoning på kommunikationsaspekter och användning. För dessa strävar man efter att producera mer förenklat material av typen "bruksanvisning", till skillnad från denna rapport som öppnar projektet och modellen djupare.

På en mer allmän nivå är modellens betydelse att den beskriver verksamhet som man redan delvis strävar efter att utföra, men utan tydlig form. Den helhet som ska

[7] Begäran om utlåtande På tjänsten Lausuntopalvelu.fi 7.–29.4.2022, efter vilket ännu två utlåtande inkommit (på finska)

utvecklas är planerad att genomföras genom att utvidga de befintliga riskhanteringsprocesserna i organisationerna och den anses inte skapa en ny process som är fristående från den övriga verksamheten. Genom att beskriva modellen kan den utvecklas systematiskt och heltäckande, vilket i sin tur gör det möjligt att stödja den digitala säkerheten inom den offentliga förvaltningen på ett bättre sätt. Syftet med den offentliga förvaltningens gemensamma riskhantering är att kunna identifiera och tillsammans möta större utmaningar som berör de flesta, men som kan vara omöjliga att hantera av en enskild organisation.

2 Strategisk riskhanteringsmodell

Riskhanteringsmodellen består av en omfattande, systematisk, upprepbar och utvecklande process samt tillhörande uppgifter. Genomförandet av den planerade modellen – tillsammans med andra åtgärder i anslutning till riskhanteringen – utgör ett riskhanteringssystem, dvs. ett systematiskt sätt att hantera risker. Modellens riktning och gränser utgör en strategisk riskhanteringsmodell för digital säkerhet. Dessa specifikationer beskrivs närmare under 3.2 i detta dokument.

Riskhanteringsmodellen är särskilt avsedd att göra det möjligt att identifiera tväradministrativa och omfattande delade risker inom den offentliga förvaltningen som grundar sig på en decentraliserad struktur samt att bedöma och styra dem till behandling samt att effektivisera hanteringsåtgärderna. För att genuint nyttiga åtgärder ska vara möjliga måste flera detaljer som påverkar genomförandet beaktas. I modellen betonas sammanställningen och bedömningen av riskerna med den digitala säkerheten samt utarbetandet av riskanalyser på strategisk nivå i den form som behövs, inom ramen för maturiteten i genomförandet. Med hjälp av dem produceras flöde och alternativ för att skapa, fatta beslut om och genomföra olika förvaltningsåtgärder. På så sätt möjliggörs ett mer högklassigt riskmedvetet och kunskapsbaserat beslutsfattande.

2.1 Beskrivning av nuläget

Innan utvecklingen av den strategiska riskhanteringsmodellen för digital säkerhet inleddes hade riskerna inte bedömts tväradministrativt på ett kontinuerligt, heltäckande och omfattande sätt. Riskerna med digital säkerhet har bedömts på olika håll som en engångsföreteelse gällande syftet och som mest omfattande inom ett avgränsat förvaltningsområde. Ämnet har tidigare i första hand behandlats med tanke på informations- och cybersäkerheten eller till exempel endast gällande den brottslighet som hänför sig till dem.

Hösten 2020 genomförde finansministeriet ett första pilotförsök för kommunerna för att samla in information om riskerna som grund för utvecklingsarbetet av den modell som presenteras här. Bakom den låg en global granskning av World Economic Forum (WEF)[8], som har tillämpats i datainsamlingen. Enkäten om synen på risker utvecklades och upprepades hösten 2021 inom hela den offentliga förvaltningen[9].

Enkäten bidrar till att genomföra riskbedömningsprocessen, som är en del av riskhanteringsprocessen. Bedömningsprocessen består av identifiering av risker, dess bedömning och analys. Vid sidan av analysen ingår också ett preliminärt utkast till riskhanteringsmetoder. Enkäterna är ett effektivt sätt att sammanställa en bred expertuppfattning om de valda frågorna. Även om de erhållna resultaten redan kan utnyttjas, kunde man utifrån de genomförda pilotprojekten identifiera flera utvecklingsobjekt med vilka processen och dess kvalitet kan utvecklas. Exempel på utvecklingsobjekt:

- En begränsad expertgrupp har identifierat riskerna, vilket inte garanterar täckningen. Detta bidrar å andra sidan till att rikta och begränsa enkätens omfattning.
- För att styra riskbildningen hade bland annat verksamhetsmiljön och kriterierna inte definierats på ett heltäckande sätt.

[8] Pilotprojektet föregicks av WEF:s raport: https://www.weforum.org/reports/the-global-risks-report-2019, samt följande 2020, 2021

[9] https://dvv.fi/documents/16079645/110675816/Digitala_s%C3%A4kerheten_risksenk%C3%A4t_resultaten_%E2%80%93_h%C3%B6sten_2021.pdf/e3fb5f75-a1ef-4271-9ffe-e4324093a43d/Digitala_s%C3%A4kerheten_risksenk%C3%A4t_resultaten_%E2%80%93_h%C3%B6sten_2021.pdf?t=1645524081024

- I svaren till enkäten baserade sig bedömningarna på expertutlåtanden från tjänstemän i olika organisationer. För att kunna göra noggrannare bedömningar och garantera statistisk betydelse bör antalet svar vara större.
- Analysen söker ännu sin form eftersom den grundar sig på ett begränsat antal källor och inte innehåller t.ex. förändringstrender som grundar sig på historiska uppgifter.
- Den producerade informationen grundar sig på en begränsad analysmetodologi, som visserligen är beroende av mängden och kvaliteten på den information som samlas in.

När riskhanteringsmodellen ännu var på utvecklingsstadiet kunde man inte heller erbjuda en exakt eller heltäckande syn på risker som var bundna till de strategiska målen, även om man kunde fästa uppmärksamhet vid kända delområden som var utmanande. Eftersom det inte är praktiskt att hantera en omfattande mängd data som uppdateras kontinuerligt som en traditionell enkät, genomförs enkäterna om riskhantering i fortsättningen som en elektronisk tjänst. De viktigaste långsiktiga utvecklingsobjekten är att bygga upp en bredare process och utveckla stödsystemen i anslutning till den. Utvecklingsåtgärderna beskrivs närmare i senare delar av detta dokument.

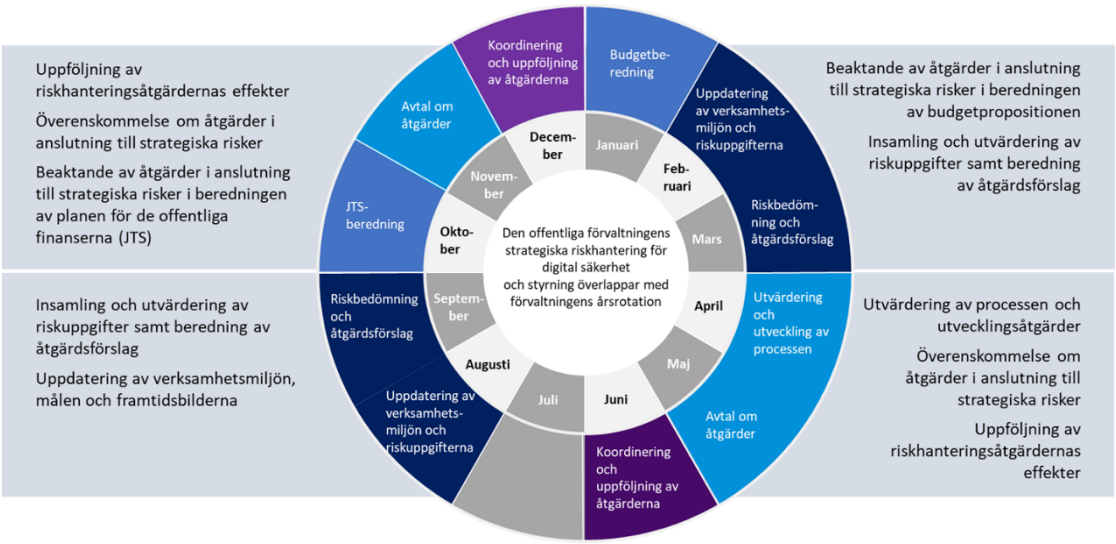
2.2 Årsplanering av riskhanteringen

I 69 § i förordningen om statsbudgeten (11.12.1992/1243) fastställs att ”*ämbetsverkens och inrättningarnas ledning skall se till att vid ämbetsverket eller inrättningen vidtas sådana med tanke på omfattningen av dess ekonomi och verksamhet och innehållet i dessa samt därtill anslutna risker ändamålsenliga förfaranden*”, på vilka kravet på riskhantering grundar sig. Detta omfattar också ”*sådana funktioner och uppgifter som ankommer på ämbetsverket eller inrättningen men som har givits i uppdrag åt något annat ämbetsverk eller någon annan inrättning, en sammanslutning eller enskilda eller som ämbetsverket eller inrättningen annars svarar för*". Dessutom fastställer 13 § i lagen om informationshantering inom den offentliga förvaltningen (9.8.2019/906) att *"en informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel*”. ”*Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen*”. Dessa bestämmelser styr genomförandet av riskhanteringen på bred front, vilket också omfattar medvetenheten om effekterna och förändringarna inom det omgivande verksamhetsfältet samt vid behov den mer omfattande globala situationen.

Riskhantering är en process vars faser upprepas cykliskt både för att upptäcka förändringar och för att utveckla processen. Riskhanteringscykler, och i vissa fall enskilda faser, kan genomföras på basis av jämn rytm eller behov (s.k. dynamiskt). Om riskhanteringen upprepas regelbundet är den ofta bunden till strukturer som styr verksamheten, såsom planerings- och rapporteringsprocesser, kan ett dynamiskt behov av riskhantering till exempel vara ett hot eller en överskridning av uppföljningsgränsvärdet. Allmänt taget måste man i riskhanteringen kunna både och, men det beror på organisationens verksamhetssätt i vilket förhållande dessa två används och vilkendera som bäst stöder verksamhetens behov i vilken situation.

I den strategiska riskhanteringsmodellen för digital säkerhet har tyngdpunkten på grund av styrningsbehov och granskningsnivå nästan helt och hållet legat på en process som genomförs på en på förhand överenskommen tidtabell. Tidtabellen för den i förhållande till finansministeriets styrprocess (Planen för de offentliga finanserna, planen för de offentliga finanserna) samt organisationernas egna styrprocesser (budgetpropositionen, TAE) presenteras i huvudsak i årsklockan nedan. Den eftersträvade

cykeln i riskbedömningsprocessen skulle genomföras två gånger om året, vilket skulle stöda årsplaneringen och utvecklingsbehoven både i organisationernas egen verksamhet och den offentliga förvaltningens gemensamma behov. När modellen genomförs ska man sträva efter att den genomförs i rätt tid, så att man hinner planera och fatta beslut om åtgärder som har en ekonomisk inverkan på alla nivåer. I övrigt kan hanteringsåtgärderna i omfattande helheter överföras till följande år, vilket man borde sträva efter att minimera. På samma sätt kan man inte förbigå JTS-processen gällande åtgärder som förutser framtiden på strategisk nivå.



Figur 1: Eftersträvad årsklocka för strategisk riskanalys av digital säkerhet. Avsikten är att riskbedömningsprocessen ska genomföras två gånger om året, i början av våren och hösten. Efter bedömningarna kommer rapporteringen och de utvecklingsåtgärder som grundar sig på dem. I slutet av cykeln är avsikten att granska hur åtgärderna framskrider, vilket på grund av de omfattande utvecklingsprojektens längd innehåller uppgifter från flera tidigare cykler. I årsklockan har man i stora drag beaktat förberedelserna inför höstens planering av de offentliga finanserna, förberedelserna av organisationernas budgetförslag i början av året samt sommarens semesterperiod. Det är bra att göra upp en tidtabell för större planerade ändringar i anslutning till utvecklingen av riskhanteringsmodellen som helhet. Ändringarna bör i huvudsak utföras på våren, vilket möjliggör en granskning av de åtgärder som eventuellt påverkar budgeten i god tid inför höstens ekonomiska planering.

Under det första och tredje kvartalet inleds riskanalysprocessen genom att samla in den bakgrundsinformation som behövs som stöd för identifieringen av risker, bland annat om verksamhetsmiljön och den offentliga förvaltningens strategiska mål. Processen fortsätter med insamling av information om risker, riskbedömning och analys. Efter en klassificering och samlad analys av de insamlade riskuppgifterna sammanställs en analysrapport som expertgruppen verifierar och på basen av vilken lämpliga hanteringsåtgärder preciseras.

Efter variationen bedömer olika myndigheter riskerna och åtgärdsförslagen samt samordnar deras inriktning och samarbete, fattar beslut om uppföljning och precisering av riskerna eller rekommendationer om hanteringsåtgärder. Samordningen kan ske i samarbetsgrupper, såsom den strategiska ledningsgruppen för digital säkerhet (DTS-JORY), eller så kan den erbjudas direkt till behöriga myndigheter. Åtgärderna kan genomföras i hela den offentliga förvaltningen eller organisationsspecifikt. För gemensamma åtgärder, såsom projekt, fastställs en ansvarig instans och en styrgrupp för hanteringsåtgärderna enligt allmänt verksamhetssätt. Utifrån riskinformationen produceras också en rapport och man informerar den offentliga förvaltningen om riskerna för att organisationerna ska inleda egna åtgärder. I slutet av det andra och fjärde kvartalet

sammanställs en lägesöversikt där man granskar helhetssituationen och framstegen för de gemensamma förvaltningsåtgärderna som inletts tidigare.

2.3 Beskrivning av riskhanteringsprocessen på strategisk nivå

I den strategiska riskhanteringsmodellen för digital säkerhet inom den offentliga förvaltningen betonas insamlingen av information och skapandet av en lägesbild i riskbedömningsprocessen (risker identifieras, deras betydelse bedöms och vid behov analyseras deras karaktär noggrannare). Processen beskriver överföringen av information och hur ansvaret för genomförandet av de olika delarna fördelas mellan aktörerna. Processen kan kallas decentraliserad eftersom olika aktörer beroende på sin roll endast ser delar av processen. Processdefinitionerna beskrivs närmare i del 3.2.

2.3.1 Processens aktörer och roller

I olika skeden av processen finns annorlunda centrala roller. I en enskild organisation skulle dessa roller ingå tydligt i uppgiftsbeskrivningarna och ansvaret skulle fördelats på linjeorganisationen, sakkunniga inom de funktioner som genomborrar organisationen och ledningens stöd, såsom den interna revisionen. Det är anmärkningsvärt att företrädarna för de organisationer som deltar i processen kan fungera under mycket olika benämningar, men de förväntas föra fram sin organisations helhetssyn i informationsinsamlingen. Det innebär såväl en granskning av olika tjänsters produktion, sakkunskap inom olika områden för genomförande av digital säkerhet, som en uppfattning på ledningsnivå om deras betydelse. Deltagandet i processen kan ske stegvis, varvid den som har den lämpligaste sakkunskapen främjar processen, men för att möjliggöra detta måste överföringen av information och de arrangemang som stöder den säkerställas. Detta bör uppmärksammas, eftersom det till skillnad från en enskild organisation inte finns någon sådan riskhanteringschef inom den offentliga förvaltningen som kan vara med och facilitera alla skeden inom hela den offentliga förvaltningen eller som har så omfattande bestämmanderätt eller budgetering.

Vid genomförandet av processen för riskhanteringsmodellen och i synnerhet i riskbedömningsprocessens olika skeden behövs följande roller:

Roll	Beskrivning
Riskhanteringschefen	En uppgift inom digital säkerhet inom den offentliga förvaltningen som placerats vid Myndigheten för digitalisering och kommunikation (MDB) och vars ansvarsområde omfattar utveckling av ett system enligt riskhanteringsmodellen, upprätthållande av processen, förbättring av kvaliteten samt bildande och rapportering av sammanställande lägesbilder. I detta ingår sammanställning, katalogisering samt underhåll av data och uppföljning av valda risker för den digitala säkerheten. I uppgiften ingår att producera bedömningar och analyser av risker och riskhantering samt annat material som utvecklar riskhanteringen för digital säkerhet inom den offentliga förvaltningen, både självständigt och med hjälp av expertgrupper.
Expertgrupp	Experternas uppgift är att skapa en uppfattning om riskerna och riskhanteringen i form av bedömningar och

	analyser. Experterna används bland annat för att säkerställa att de strategiska riskerna är betydelsefulla och jämförbara samt för att utveckla hanteringsåtgärderna. Syftet med experternas deltagande är inte bara att stöda riskhanteringschefen, utan en granskning ur olika synvinklar är en central faktor som påverkar processens kvalitet. Beroende på det behov som riskhanteringschefen fastställt kan experterna vara från den offentliga förvaltningen eller utanför den.
Produktägare av Tjänsten för helhetsbild	Den som ansvarar för att utveckla, samordna och utnyttja lägesbildsdatasystemet för digital säkerhet, som produceras av Myndigheten för digitalisering och befolkningsdata, och som ansvarar för att utveckla tjänsterna i samråd med riskhanteringschefen.
Organisationer inom den offentliga förvaltningen och deras centrala experter	Experter på riskhantering och/eller digital säkerhet i organisationer producerar, överför och utvärderar (på nytt) information om hot, risker och sin riskhantering för att skapa en helhetsbild, som representerar den överordnade synen på digitala risker inom sin organisation. Samtidigt får de information om den egna organisationens riskbild i förhållande till andra motsvarande aktörer och hela den offentliga förvaltningen. Utifrån dessa kan organisationerna utveckla sin egen riskutsikt och sina riskhanteringsåtgärder och skicka meddelanden till den högre ledningsnivån med syfte att styra verksamheten. Organisationerna kan genom sina experter också delta i de allmänna förvaltningsåtgärder som genomförs och i tillämpningen av dem i den egna organisationen.
Behöriga myndigheter	De behöriga myndigheterna är kunder till den information som produceras. På basis av informationen kan de inom sitt ansvarsområde styra åtgärderna och sin egen verksamhet. I processen fungerar de i enlighet med sitt eget verksamhetsområde som ansvariga aktörer som producerar nödvändiga och ändamålsenliga åtgärder för riskhantering, inklusive delning av hot- och riskuppgifter. I omfattande strategiska risker inom den offentliga förvaltningen kan detta också innebära gemensamma projekt mellan flera parter. Vid fastställandet av behörigheten bör det observeras att man i stället för en snäv definition betonar avtalsenlighet. I lagen definieras behörigheten i huvudsak som uttrycklig och begränsad (regional, graderad eller riktad), men organisationerna har också omfattande möjligheter och skyldigheter att genom avtal påverka riskerna, delta via olika samarbetsorgan och sprida information som utvecklats i den egna verksamheten. Verksamhet som gäller risker och riskhantering kan alltså på många sätt behandlas som gemensamma ärenden utan att ansvaret överförs eller fördunklas.

Experter som genomför hanteringsåtgärder	Via separata utvecklingsprojekt planeras och genomförs riskhanteringsåtgärderna av experter vid behöriga myndigheter samt deras samarbetspartner. Det kan också vara fråga om en helhet som genomförs av flera aktörer. De behöriga organisationerna bör säkerställa att information om de verkställande instansernas resultat även återställs till riskhanteringsprocessen (t.ex. den offentliga förvaltningens nätverk, såsom VAHTI), så att åtgärdernas effektivitet och inriktning inom den offentliga förvaltningen kan utvärderas effektivt.

Tabell 1a: Centrala aktörsroller i riskhanteringsprocessen för digital säkerhet

Dessutom finns det aktörer som kan ha en betydande roll för att främja och utveckla processen för riskhanteringsmodellen. Detta är inte en uttömmande förteckning och innehåller inte till exempel arbete som främjar säkerheten och samarbetet inom olika områden av genomförande inom den digitala säkerheten (till exempel säkerhetskommitténs roll i främjandet av cybersäkerhet eller dataombudsmannens arbete i anslutning till dataskydd) eller aktörer vars verksamhet som tjänsteleverantör möjliggör ett omfattande inflytande. Förteckningen omfattar inte heller de många myndighetsaktörer med vilka informationsutbyte är möjligt.

Aktör	Beskrivning
Digitaliserings-byrån	Den permanenta samarbetsgruppen inom ansvarsområdet för digitalisering och dataekonomi har som uppgift att stärka samarbete, koordinering och informationsutbyte mellan ministerierna i fråga om digitalisering och dataekonomi. Digitaliseringsbyrån har ingen direkt koppling till riskhanteringsprocessen, men samordningsåtgärderna inom dess uppgiftsområde kan vara en betydande påverkare i hanteringen av olika omfattande strategiska risker och i förädlingen av möjligheterna i anslutning till dem. De strategiska målen som koordineras av Digitaliseringsbyrån ("den digitala kompassen") har en betydande inverkan även på identifieringen och bedömningen av riskerna med digital säkerhet.
Strategiska ledningsgruppen för digital säkerhet	De behöriga myndigheterna representeras av den strategiska ledningsgruppen för digital säkerhet (DTS-JORY)[10], som har till uppgift att behandla risklägesbilden och de åtgärdsförslag som eventuellt ingår i den för att genomföra den tvärgående samordningen inom den offentliga förvaltningen. Den stöder inrättandet av nödvändiga utvecklingsprojekt för digital säkerhet av behöriga myndigheter. Här jämställs DTS-JORY med behöriga myndigheter, eftersom de bildar ledningsgruppen. Ledningsgruppen deltar också i utvecklingen av riskhanteringsmodellen i form av respons och expertis. Ur riskhanteringsmodellens synvinkel är DTS-JORY:s roll att effektivisera riskhanteringen, särskilt i fråga om genomförandet av hanteringsåtgärderna.

[10] https://vm.fi/sv/projekt?tunnus=VM025:00/2020 (på finska)

VAHTI-ledningsgruppen (ledningsgruppen för digital säkerhet inom den offentliga förvaltningen) samt VAHTI-arbetsgrupperna	Funktionen som överfördes till Myndigheten för digitalisering och befolkningsdata i början av 2020 och som fungerar som samarbets-, berednings- och samordningsorgan för centrala operativa organisationer inom den offentliga förvaltningen. VAHTI-ledningsgruppen behandlar bland annat den riskrapportering som producerats för gruppen och situationen för den digitala säkerheten samt de åtgärder som eventuellt utvecklas utifrån dessa, inklusive deltagande i styrningen av utvecklingen av verksamhetsmodeller och system som stöder dessa med sin respons. Ledningsgruppen sammanträder fem gånger om året. För närvarande har fem VAHTI-arbetsgrupper tillsatts under VAHTI-ledningsgruppen. En av arbetsgrupperna har till uppgift att utveckla riskhanteringen inom digital säkerhet.

Tabell 1 b: Aktörer som stöder riskhanteringsprocessen för digital säkerhet

2.3.2 Processens delar och faser

Tre centrala utsikter har utarbetats för riskhanteringsprocessen, eftersom man i helhetsprocessen producerar svar på tre behov.

1. Den första utsikten gäller organisationer inom den offentliga förvaltningen som via riskhanteringsdelen i Tjänsten för helhetsbild kan jämföra sin egen risk- och riskhanteringssituation med jämförelseorganisationerna samt få information om sin egen riskhantering via den samlade risklägesbilden för den offentliga förvaltningen.
2. Den andra utsikten innehåller information som bildas för att stödja verksamheten styrning och ger de behöriga myndigheternas och förvaltningsområdenas ledning en utsikt över riskhanteringsprocessen som en helhet som omfattar hela den offentliga förvaltningen.
3. Den tredje utsikten betjänar den strategiska informationshanteringsprocessen[11], dvs. erbjuder i huvudsak riskchefen en bild över helheten (även om det inte är möjligt att få en fullständig bild av hur processens slutdel genomförs i praktiken i den decentraliserade strukturen). Dess permanenta uppgift är att svara på en "begäran om information" om riskfaktorer som påverkar den digitala säkerheten, vilket riskchefen genomför. Inom ramen för detta kan inriktningen göras enligt tyngdpunkterna och målen för styrningen av den offentliga förvaltningen, men också med beaktande av utvecklingen i verksamhetsmiljön och dess fenomen. Slutresultatet är att producera information för olika dataprodukter, anpassade till olika användningsändamål och olika synvinklar.

Beslutsfattande enligt god förvaltningssed förutsätter att det lyfts fram i den klassiska fyrdelade kontinuerliga utvecklingsprocessen[12]. Detta ändrar inte egentligen proces-

[11] Processen för strategisk informationshantering, den så kallade underrättelsecirkeln (informationen "utvecklas" och preciseras i processen, dvs. grunden för den nya eller uppdaterade rapporteringen är tidigare), består av olika faser och i allmänhet beskrivs bland annat begäran om information, en noggrannare definition av den, insamling av information, behandling av information, analys av information, utformning av rapportering samt kommunikation om rapporten. Förenklat fungerar den som referensram för de mer omfattande utredningsuppgifter som ledningen ger experterna. Detta har också tillämpats på den föreslagna strukturen för produktion av information i den strategiska riskhanteringsmodellen. Till skillnad från annan forskning är produkten till sin natur "bästa tillgängliga information" som kan sammanställas inom utsatt tid och inom andra begränsningar.

[12] PDCA (plan, do, check, adjust / act) och dess variationer, dvs. ”planera, gör, kontrollera, korrigera / gör permanent”. Märkbart är den upprepbara processen som stöder utvecklingen och riskhanteringsprocessen ISO31000 innehåller detta.

sen, utan understryker att man övergår från planering till genomförande på ett godtagbart sätt med iakttagande av överenskomna beslutsprocesser. I detta skede sker ett riskmedvetet beslutsfattande där man till exempel beaktar förhållandet till andra mål samt dokumenterar och godkänner kvarstående risker.

Det är skäl att märka att alla delar av processen innehåller flera åtgärder och delprocesser. Den allmänna strukturen förblir oförändrad även om innehållet i delarna kompletteras i framtiden. Processens delar kan också i praktiken genomföras överlappande, i synnerhet när omfattande förvaltningsåtgärder utvecklas, eftersom det kan ta flera processcykler att slutföra dem.

Den övergripande riskhanteringsprocessen inom den offentliga förvaltningen kan anses vara decentraliserad, eftersom den genomförs av olika aktörer i olika skeden i stället för av en enda organisation. Riskerna inom den offentliga förvaltningen är ofta gemensamma hot som riktas mot de flesta aktörerna och vars betydelse delas mellan dem. Att betrakta dem som "virtuella helheter" kan erbjuda analogi för gestaltningen. Även denna typ av struktur producerar riskhantering genom att tillämpa en standardiserad struktur för processen. Till decentraliseringens fördelar kan räknas att den är omfattande (kompetens, resurser) och tålig mot störningar, men på motsvarande sätt är den mindre effektiv än en enskild aktörs process.

Av de bifogade strukturbilderna som visar processen är sammanhållningen mellan olika aktörer identifierbar.

Bild 2: Generell bild av huvudfaserna i riskhanteringsmodellens helhetsprocess Det femte skedet, som har lagts till den traditionella fyrdelade utvecklingsprocessen, är det beslutsfattande som betonas inom den offentliga förvaltningen. Den ingår också i den allmänna (grovt förenklade) processen med fyra faser, men den måste betonas eftersom den utgör en viktig referenspunkt i förvaltningsprocesserna. Den delar processens två delar och en av de viktiga funktionerna i processen är att producera information för beslutsfattande där riskuppgifter kombineras med annan information och andra synpunkter. I beslutsfattandet ingår också dokumentering av ansvar, inklusive godkännande av kvarstående risker på en tillräckligt hög beslutsnivå. Den generella bilden preciseras och utvidgas till tre något avvikande utsikter av processerna som är kopplade till varandra. Riskhanteringen omfattar dessutom stödfunktioner, såsom kommunikation, som på olika sätt anknyter till varje fas i processen.

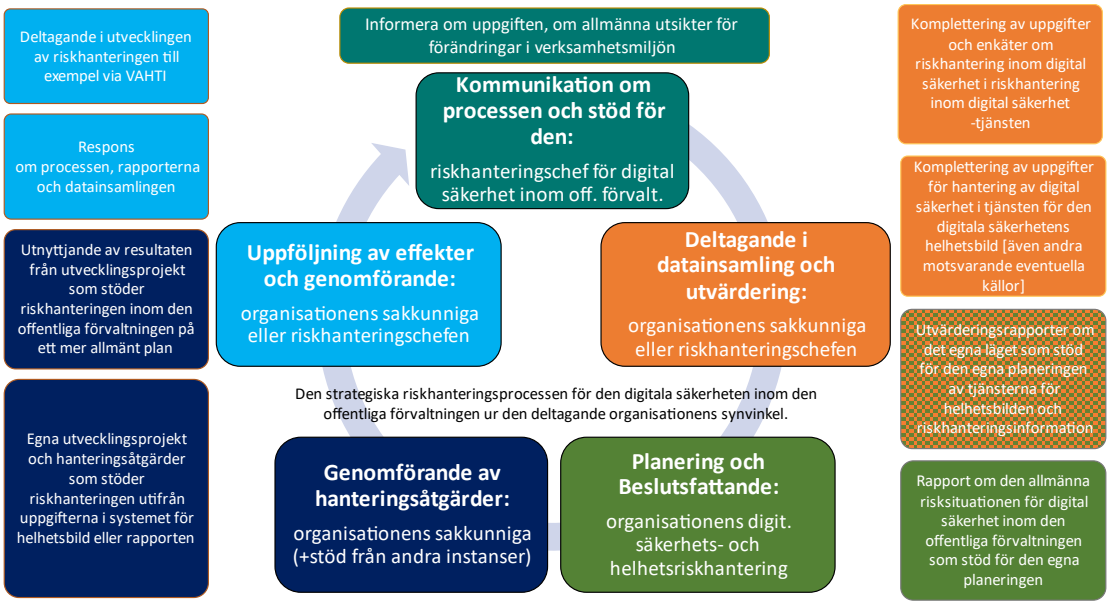


Bild 3: Den strategiska riskhanteringsprocessen för den digitala säkerheten inom den offentliga förvaltningen ur den deltagande organisationens synvinkel. Betoningen ligger på den offentliga förvaltningens strategiska riskhantering för att stödja organisationens egen riskhantering. I det praktiska genomförandet är jämförelseinformationen i synnerhet i det första skedet riktgivande och anonymiserad, baserat på olika grupperingar (till exempel enligt organisationens storlek och verksamhetsområde). Organisationerna kan tillämpa processen som stöd för planering, genomförande och uppföljning av det egna beslutsfattandet.

Bild 4: Den strategiska riskhanteringsprocessen för den digitala säkerheten inom den offentliga förvaltningen ur styrningens synvinkel. Tyngdpunkten ligger på produktion av information för riskhanteringsåtgärder och annat beslutsfattande på högre nivå. Behoven för styrning kopplar också direkt eller indirekt processen till mer omfattande handledningsstrukturer, varvid den fungerar som ett flöde även till ett bredare beslutsfattande utanför riskhanteringen för digital säkerhet. Man bör komma ihåg att många risker som identifieras med tanke på säkerheten kan påverka den övriga verksamheten, till exempel genom att redan i planeringsskedet förebygga uppkomsten och utvecklingen av risker.

Bild 5: Den strategiska riskhanteringsprocessen för den digitala säkerheten inom den offentliga förvaltningen ur informationshanteringens synvinkel. Betoningen ligger i början av processen, i processen för informationsproduktion, där man kan utbyta information med andra aktörer och informationskällor. I processen för informationsproduktion framställs prognostiseringsinformation samt alternativ och förslag till flöden i beslutsfattandet. Hur dessa utnyttjas beror på frågor gällande beslutsfattandet som står utanför riskhanteringsprocessen (övriga strategiska mål, resurser osv.).

I processens första skede sammanställs utgångsuppgifterna för riskbedömningsprocessen på strategisk nivå för digital säkerhet. I den fastställs både den digitala säkerheten och mer omfattande strategiska mål som påverkar den offentliga förvaltningen och ordnandet av dess digitala säkerhet. Genom dessa identifieras och bedöms olika risker. Utöver de interna riktlinjerna samlas information in om den externa verksamhetsmiljön och i vilka riktningar den förändras. Dessa synpunkter förmedlas i behövlig utsträckning till dem som deltar i utvärderingsprocessen för att stödja en enhetlig utvärderingsuppfattning.

De deltagande organisationernas datainsamling (bakgrundsinformation om organisationen, basuppgifter om den digitala säkerheten och riskhanteringen) sker i tjänsten för helhetsbild om digital säkerhet som upprätthålls av Myndigheten för digitalisering och befolkningsdata (MDB) och som innehåller delar för organisationens administrativa digitala säkerhet samt delar för information om risker med digital säkerhet. Tjänsten för riskhantering inom digital säkerhet fungerar som ett verktyg för riskhantering och säkerställer att den insamlade informationen är säker, enhetlig och används på lång sikt. Tjänsten är en del av det praktiska genomförandet av processen och används för att producera jämförelseinformation till deltagande organisationer om risker och riskhantering inom den offentliga förvaltningen för att utveckla verksamheten självständigt.

Andra nationella och internationella informationskällor (rapporter, undersökningar, databaser, dataprodukter etc.) kan användas som komplement till tjänsten för riskinformation om digital säkerhet. Tjänsten som sammanställer en helhetsbild av den digitala säkerheten är den viktigaste tjänsten som fungerar på samma plattform. Tjänsten har även egen del som granskar riskhanteringsarrangemangen. Genom att göra

det möjligt att utnyttja de insamlade uppgifterna i kors i den mån det behövs, besparar man användarna besvär i båda enkäterna och ger vid granskningen av uppgifterna en bättre kontext för bedömningen.

I riskbedömningsprocessen ingår också att utarbeta en rapport om de centrala riskerna med den digitala säkerheten inom den offentliga förvaltningen, där den erhållna informationen bearbetas i en för målpubliken relevant form. Den innehåller preliminära skisser gällande hanteringsåtgärderna, främst utifrån en uppfattning om riskerna och bilden av riskhanteringen. Av kvalitetsstyrningsskäl ska rapporteringen och de riskbedömningar som gjorts styras till expertbedömning. I den beaktas både interna och externa mål, förändringsfaktorer, begräsningar och möjligheter. Därefter utarbetar experterna skisser för hanteringsmetoderna som beslutsförslag för den fortsatta behandlingen.

I skedet för beslutsfattande och koordinering går de behöriga myndigheterna igenom de rapporterade uppgifterna. Dessutom utvärderar de uppgifterna i förhållande till mer omfattande administrativa behov samt besluter om fortsatt behandling. De fortsatta åtgärderna kan gälla bland annat uppföljning av risker, behov av tilläggsutredningar eller metoder och åtgärder gällande hanteringen. I beslutsfattandet beaktas utöver risk- och riskhanteringsuppgifter även uppgifter och bedömningar om den digitala säkerheten. Även andra uppgifter som används beaktas, såsom funktionella och ekonomiska faktorer, som kan styra alternativen. Organisationer inom den offentliga förvaltningen ska beakta mer omfattande riskutsikter som en del av den övergripande riskhanteringen i organisationen.

I genomförandet av riskhanteringsåtgärderna ingår att de behöriga myndigheterna till behövliga delar preciserar olika åtgärder. Dessa kan vara införande av projekt, arbetsfördelning som avtalas med eventuella samarbetspartner, förtydligande av målen och tidtabellen för finansieringen, verksamhetsramen eller projekten. Dessutom kommer man överens om uppföljningen av hur åtgärderna framskrider och om konsekvensbedömningen samt säkerställer uppföljningen. Information om hur genomförandet av hanteringsåtgärderna framskrider ska ges i ändamålsenlig omfattning och på ett ändamålsenligt sätt till föremålen för åtgärderna samt till de aktörer som deltar i koordineringen, inklusive chefen för riskhanteringen för digital säkerhet inom den offentliga förvaltningen, som upprätthåller riskutsikterna.

Den information som organisationerna producerar för sina egna riskbedömningsprocesser fungerar som basinformation för den strategiska riskanalysen. Distributionen av dem producerar jämförelseinformation om situationen för risk- och riskhanteringen inom den offentliga förvaltningen. Med hjälp av informationen man kan utveckla en gemensam utsikt om den digitala säkerheten för organisationerna. Organisationerna drar nytta av mer omfattande riskhanteringsåtgärder inom den offentliga förvaltningen som vidtas för att hantera tväradministrativt betydande, omfattande eller delade risker.

Man samlar in observationer och respons om hanteringsåtgärderna, deras effekter, riskhanteringsprocessen samt den information som producerats och de verktyg som använts för den, så att helheten kan vidareutvecklas kvalitativt och motsvara behoven. Respons behövs av varje aktör som deltar i helheten. Utifrån responsen och utvecklingsplanen utvecklas processen mot en nivå där kvaliteten, tillförlitligheten, täckningen och aktualiteten hos den riskhanteringsinformation som den producerar ger ett betydande mervärde för den förebyggande styrningen av den digitala säkerheten.

3 Bakgrundsantaganden för riskhanteringsmodellen

Bakgrundsantagandena och förståelsen för dem är väsentliga för att man ska förstå den information som produceras och kunna ställa dess betydelse i rätt proportion. All information har begränsningar och är kontextbunden. Med tanke på utvecklingen av helheten är dessa egenskaper dessutom sådana som kan användas för att göra strategiska ändringar och inriktningar i processen. Dessa bakgrundsantaganden, eller de preciseringsmöjligheter som bygger på dem, ger aktörer på strategisk nivå möjligheter att på ett förståeligt och definierat sätt inrikta riskhanteringen enligt behoven.

3.1 Användningsändamål och aktörer

Detta dokument har utarbetats för att beskriva den struktur och de processer som används i riskhanteringsmodellen på ett allmänt plan. Endast delar av helheten kan beredas på en gång, eftersom helheten nödvändigtvis ska vara anpassbar till krav som förändras och utvecklas. Skisser har nu gjorts av utvecklingsskedena inom modellens delar. Dessa kan ändras i takt med att behoven, teknologin och verksamhetsmiljön utvecklas.

Riskhanteringsmodellens uppgift är att fungera som stöd när man förutser kommande utmaningar inom digital säkerhet, bland annat genom att producera gemensam information. Syftet med processerna är att säkerställa en strävan efter tillförlitlig kvalitet och kontinuitet. Syftet är att skapa en lägesbild av riskerna och riskhanteringen på strategisk nivå för digital säkerhet. Med hjälp av lägesbilden kan man påverka bland annat utvecklingsverksamheten och budgeteringen.

Myndigheten för digitalisering och befolkningsdata (MDB) ansvarar för detta dokument och riskhanteringsmodellen för digital säkerhet med stöd av lagen om Myndigheten för digitalisering och befolkningsdata (304/2019 3 §). Målen i riskhanteringsmodellen är bundna till de centrala delområdena inom genomförandet av den digitala säkerheten (ledning och riskhantering, cybersäkerhet, informationssäkerhet, dataskydd och kontinuitetshantering). Varje organisation genomför självständig dessa och eventuella andra särskilda delområden inom genomförandet av den digitala säkerheten i organisationen. Det finns dock även utsedda ansvariga myndigheter. Riskhanteringsmodellens särskilda syfte är att tillgodose dessa myndigheters behov av beslutsfattande och verksamhet genom att producera gemensam information för att utveckla delområdena inom digital säkerhet.

Riskhanteringsmodellen och den information som den producerar kan behandlas och utvärderas på ett samlat sätt i myndigheternas samarbetsorgan. Den av finansministeriet tillsatta strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (DTS-JORY)[13], vars första mandatperiod är 1.1.2020–31.12.2024, har som uppgift att bedöma och koordinera åtgärder gällande strategiska risker för digital säkerhet inom den offentliga förvaltningen. Den består av centrala behöriga myndigheter för digital säkerhet. DTS-JORY:s uppgift är att granska bilden av risksituationen för hantering av den digitala säkerheten, informationssäkerhet, dataskydd, cybersäkerhet samt kontinuitet och beredskap, utifrån vilka man kan komma överens om fortsatta åtgärder. Det är viktigt att ledningsgruppen så långt som möjligt följer upp hur

[13] https://vm.fi/sv/projekt?tunnus=VM025:00/2020 (på finska)

de fortsatta åtgärderna genomförs samt ger respons på information som stöder beslutsfattandet för att förbättra processens kvalitetsledning.

Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen, VAHTI (ursprungligen "ledningsgruppen för informationssäkerheten inom statsförvaltningen"), vars nuvarande mandatperiod är 1.3.2020–31.12.2024, är ett samarbets-, beredningsoch samordningsorgan för utvecklingen av den digitala säkerheten inom den offentliga förvaltningen. Dess verksamhet utvecklar riskhanteringen för den digitala säkerheten och den kan kommentera strukturerna och genomförandet av riskhanteringsmodellen som en del av det stöd för utvecklingen av den digitala säkerheten inom den offentliga förvaltningen som antecknats som verksamhetens mål. Till VAHTI-ledningsgruppens uppgifter hör också att koordinera och främja samarbetet mellan de organisationer som ansvarar för den offentliga förvaltningens serviceproduktion och säkerhet inom den digitala säkerhetens olika delområden samt att främja och delta i verkställandet av finansministeriets principbeslut, utvecklingsprogram och projekt som gäller den digitala säkerheten inom den offentliga förvaltningen. Via VAHTI-ledningsgruppen och arbetsgruppen för utveckling av riskhanteringen kan de organisationer som deltar i den strategiska riskhanteringshelheten påverka dess utveckling.

Avsikten är att den offentliga förvaltningens organisationer ska få stöd för sitt eget riskhanteringsarbete genom den lägesbildsinformation om risker, riskhantering och riskhanteringssystem som produceras under processens gång samt genom mer omfattande hanteringsåtgärder. Jämförelseinformationen ska också möjliggöra självutvärdering och självstyrning i ordnandet av digital säkerhet. Mer allmänt genomförs riskhanteringsprocessen för en större helhet inom den offentliga förvaltningen virtuellt och logiskt när olika aktörer genomför olika delar av den, när organisationerna genomför sin egen interna riskhantering eller deltar i produktionen av gemensamma riskuppgifter. I praktiken kan man dock anta att det stöd som produceras i den här presenterade riskhanteringsmodellen i huvudsak kräver tillämpning (individualitet i organisationerna) eller är indirekt (bl.a. förvaltningsstrukturer och asymmetri i förhållande till riskerna). Detta förväntas leda till att de positiva konsekvenserna överförs till kundernas och intressegruppernas nivå och upplevelse av digitala säkerhet i organisationerna.

3.2 Grundläggande antaganden och avgränsningar

Vid planeringen och genomförandet av riskhanteringsmodellen har internationella riskhanteringsstandarder[14] tillämpats. För att förstå betydelsen av de risker som den process som beskrivs i modellen medför har man strävat efter att identifiera de centrala kontexterna, avgränsningarna och valen i strukturen. Man försöker lyfta fram dessa. Utöver dessa måste man när processen upprepas granska vilka antaganden och definitioner som görs i anslutning till verksamhetsmiljön och förändringarna i den. Förutom att verksamhetsmiljöns betydelse ska beaktas med tanke på riskerna ska man vid behov också bedöma om riskhanteringsmodellens grundläggande antaganden och avgränsningar måste uppdateras och modellen ändras så att den motsvarar verkligheten och de behov som ställs på den.

I begreppen strävar man efter att följa den helhet av ordlistor (2022)[15] som utvecklats för riskhantering av digital säkerhet och som kompletterar ordlistorna ISO31000 och

[14] ISO 31000:2018 (Riskhantering. Anvisningar), IEC 31010:2019 (Riskhantering. Riskbedömningsmetoder), ISO/TR 31004 (Riskhantering. Instruktioner för tillämpning av ISO 31000)

[15] En djupgående genomgång av riskhanteringsprocessen och kommunikation med termer inom detta område publiceras i VAHTI God Praxis stödmaterialet https://dvv.fi/sv/publikationer-om-digital-sakerhet och en ordlista publiceras i Interoperabilitetsplattformens ordlisteverktyg https://sanastot.suomi.fi/ även på svenska och engelska.

ISO73[16] samt i tillämpliga delar ordlistorna för övergripande säkerhet[17] och cybersäkerhet[18]. En mer omfattande presentation av hanteringen av den digitala säkerheten som helhet finns i bilaga 1 till riskhanteringsordlistan. Definitionerna och exemplen i detta dokument är tillämpningar av gemensamt överenskomna definitioner i riskhanteringsordlistan.

3.2.1 Interna utsikter och ett för granskningen betydelsefullt perspektiv

Granskningen är i huvudsak begränsad till organisationer inom den offentliga förvaltningen i Finland. Detta anses i stor utsträckning omfatta statliga ämbetsverk, affärsverk, ministerier och andra aktörer samt kommuner och olika samkommuner. I detta sammanhang förstås den offentliga förvaltningen i samma omfattning som informationshanteringsenheterna definierats i informationshanteringslagen.

Gränsdragningen till offentlig förvaltning innebär att medborgare och företag inte omfattas. Valet beror på finansministeriets styrning som riktar in perspektivet i förhållande till den övriga förvaltningen. Granskningen återspeglar dock medborgarnas behov via servicestrukturer och företagens roll i produktionen av olika tjänster. Den riskhanteringsinformation som produceras kan också tillämpas utanför den offentliga förvaltningen och ge medborgarna en bild av den offentliga förvaltningens förmåga att sörja för den digitala säkerheten, vilket kan vara av betydelse för demokratin och förtroendet. I de riskhanteringsåtgärder som utvecklas ska man sträva efter att beakta den offentliga förvaltningens underleverantörskedjor och aktörer som verkar utanför dem.

Digital säkerhet har valts som ett särskilt ämne för granskning som används för en tvärsektion av områden inom den offentliga förvaltningen. Det måste tas som en intern definition, även om själva termen är heltäckande. Detta beror på definitioner och val som görs i genomförandet av den digitala säkerheten, dvs. på de metoder och infallsvinklar som man har kommit överens om att använda inom den offentliga förvaltningen. En del av definitionerna görs till exempel i lagstiftningen, men de centrala delområdena av genomförandet är ledning och riskhantering, cybersäkerhet, informationssäkerhet, dataskydd och kontinuitetshantering. Historiskt sett har det övergripande begreppet i digitaliseringens historia förändrats till såväl termer som innehåll, och denna förändring förväntas inte upphöra. I frågor som räknas till digital säkerhet kan man ta snävare eller mer omfattande perspektiv, vilket återspeglas i risker som anses vara betydande och som inkluderas i granskningen och uppföljningen.

Uppfattningen om den digitala säkerhetens tillstånd och mål inom den offentliga förvaltningen grundar sig både på information som producerats under processens gång och på dokument som producerats av andra källor. Centrala dokument är digitaliseringsplanerna, utvecklandet av den offentliga förvaltningen, säkerhets-, digitaliserings- och cybersäkerhetsplanerna, rapporterna och redogörelserna. Dessa bildar strategiska fixpunkter genom vilka bedömningen och analysen i riskhanteringsmodellen för digital säkerhet sker.

16 ISO 31000:2018 (Riskhantering. Riktlinjer), SFS Guide 73 (Riskhantering. Ordlista; ISO GUIDE 73:2009)
17 https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto (på finska)
18 https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto (på finska)

3.2.2 Verksamhetsmiljöer inom vilka granskningen görs

I denna modell för riskhantering består den fastställda verksamhetsmiljön av flera områden som korsar varandra. Den mest centrala av dem är den digitala verksamhetsmiljön. I enlighet med definitionen av digital säkerhet kan man som en del av verksamhetsmiljön granska faktorer som påverkar den digitala verksamhetsmiljön eller verksamheten i den samt frågor som den digitala verksamhetsmiljön och verksamheten där påverkar. Dessa digitala gränsöverskridande konsekvenser kan vara negativa (till exempel avbrott i kablar, brist på kunniga personer, attacker) eller sådant som skulle vara negativt om det utsattes för hinder (till exempel energi, komponenter, tjänster). Det bör också observeras att den digitala verksamhetsmiljön ständigt utvecklas och omdefinieras, eftersom den interagerar med många andra verksamhetsområden. Detta formar och skapar nya hot och möjligheter som kan utgöra risker.

I granskningen av den fysiska miljön är vi bundna till finska statens territorium. Även om den digitala verksamhetsmiljön är global, definieras den regionala verksamhetsmiljön av flera system, använda språk, kunder, tjänster, experternas placering, datanät samt andra funktioner och anslutningspunkter med den verkliga världen. Den offentliga förvaltningens verksamhetsmiljö består av dessa. Parallellt med detta finns en politisk verksamhetsmiljö för den offentliga förvaltningen och staten, till vilken bland annat grannstater och internationella aktörer, såsom EU, är förbunden med.

I en mer abstrakt granskning beskrivs utvecklingsförloppet i den omfattande sociotekniska verkligheten med begreppet VUCA (volatility, uncertainty, complexity, ambiguity)[19]. Med dessa beskrivs hur saker och ting förändras kontinuerligt, framtiden är osäker, betydelserna och kontakterna är komplexa och mångfacetterade. Permanenta, tydliga, avgränsade och entydiga utsikter är således inte sannolika på strategisk nivå.

Utvecklingen i anslutning till den digitala verksamhetsmiljön kan följas upp i medierna, rapporterna och utredningarna, men det är också skäl att bedöma förändringarna i granskningar under längre tidsperioder. VUCA-prognoser och prognostiseringsarbete som produceras av olika organisationer kan ge en bild av hur framtidsfenomenen utvecklas. Ovan nämnda innehåller bland annat utsikter med anknytning till den fysiska och politiska miljön.

3.2.3 Strategisk definition i denna modell

Det finns ingen enskild tydlig definition av strategin och denna modell definierar inte den absoluta och bestående "strategiska" betydelsen, vilket skulle vara problematiskt i en föränderlig verksamhetsmiljö och om den föråldras snabbt skulle uppföljningen av riskerna vara betydelselös. Riskhanteringen är alltid kontextbunden och därför är det inte heller meningsfullt att försöka definiera en enda betydelse. Syftet med modellen är att identifiera de mest centrala riskerna som påverkar samhället. På så sätt

[19] Efter VUCA har man också diskuterat akronymen BANI (Brittle, Anxious, Non-linear, Incomprehensible) och huvudsakligen i USA RUST (Rapid, Unpredictable, Paradoxical, Tangled). Dessa är tankeverktyg för att uppfatta större verksamhetsmiljöer. BANI kan anses vara en fortsättning eller komplettering av VUCA-tänkandet, varvid människans kontext beaktas mer. Digital säkerhet är ett perspektiv genom vilket man kan sträva efter att hantera och minimera dessa aspekter genom att skapa förtroende för systemens, myndigheternas och hela samhällets förmåga att hantera dessa utmaningar.

produceras alternativ för beslutsfattande och inriktning av förvaltningsåtgärder inom digital säkerhet. En mer omfattande och för förvaltningsområden specifik strategisk riskhantering genomförs för närvarande som en del av arrangemangen kring verksamhetens styrning. I framtiden kommer riskhanteringen på statsrådsnivå[20] att granska dessa i större omfattning än den offentliga förvaltningen och ur statsledningens egen kontext.

Granskningen av strategiska risker, även om den uppfattas som omfattande på högre nivå, kan inte antas vara komplett heltäckande på grund av begränsade resurser och kapacitet, utan granskningen måste vara inriktad med vissa begränsningar. Granskaren har alltid sin egen kontext utifrån vilken granskningen görs. Med tanke på den deltagande organisationen bör man särskilt beakta att dess egen kontext alltid innehåller olika risker som är typiska för den och som varken kan eller behöver inkluderas som sådana i den allmänna genomgående granskningen av den offentliga förvaltningen. På övergripande nivå inom den offentliga förvaltningen är det ännu svårare att definiera den strategiska kontexten, eftersom den borde representera en gemensam diskurs för flera aktörer. Andras behov kan vara mycket konkreta, men samtidigt förknippas de ofta med mycket abstrakta strävanden, såsom att förbättra förtroendet, känslan av trygghet eller resiliens. Inriktningen begränsar inte heller de saker som ska granskas endast till frågor som betraktas som kritiska eller centrala eller kriser, utan utvidgar uttryckligen granskningen till mer vardagliga aspekter som också är förknippade med digital säkerhet. Därför måste den strategiska behandlingen vara heltäckande även inom de olika avgränsningarna.

Strategiskt är också ett proportionellt begrepp i verksamheten och det måste jämföras med målen. Även detta måste dock förstås tillräckligt omfattande, eftersom den direkta kopplingen till digitala risker inte alltid är en tydlig koppling till organisationens centrala funktioner och tjänster eller strävanden i anslutning till dem. Beroende på organisationens storlek och förvaltningsstrukturer kan dess strategiska mål enbart ingå i den registrerade helhetsstrategin, eller så kan de härledas från andra strategiska planer, såsom eventuella säkerhetsstrategier eller till och med delstrategier (som inte förutsätts). Nivån på och noggrannheten i dokumentationen av strategiska riktlinjer och mål varierar av många orsaker och all strategisk information är inte offentlig.

I anslutning till det praktiska genomförandet av modellen är den strategiska risken inte tydligt definierbar och en noggrant avgränsad definition stöder inte den riskhantering som genomförs i modellen. Definitionen är mer funktionell och dynamisk, så att den lämpar sig väl för mångsidiga fenomen och aktörer. Med strategisk avses den relativa strukturen, där den ligger på en högre nivå när det i mitten finns interna åtgärder inom organisationen och i andra ändan mer funktionella ärenden. En strategisk aktör tar alltså i sig inte ställning till värdet, storleken eller vikten, även om dessa definitioner ofta följer med när man granskar konsekvenserna för större helheter än en organisation, såsom konsekvenserna för den offentliga förvaltningens funktionsförmåga, aktörernas system, kundkretsen eller samhällsresurserna i vidare bemärkelse. I en sådan granskning kan ett funktionellt problem för en enskild organisation identifieras som strategiskt inom den offentliga förvaltningen, om det upprepas på flera ställen. Å andra sidan kan en strategisk risk i en organisation vara unik, men om den förverkligas kan den påverka många andra via nätverken. Därför måste definitionen

[20] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163184/VM_2021_28.pdf (presentationsblad på svenska)

vara öppen för att betydelsefulla fenomen ska kunna identifieras. När man uppfattar den strategiska risken på praktisk nivå måste man i sista hand lita på de experter som deltar i processen och sträva efter att bygga upp processen så att förståelsen och kvaliteten på informationen utvecklas så att den stöder den prognostisering av strategiska risker som behövs vid respektive tidpunkt.

3.2.4 Tidsfönster

I den strategiska granskningen av riskhanteringen ska man definiera det tidsfönster inom vilket granskningen görs. Enligt traditionellt tänkesätt är den strategiska utsikten cirka 2–5 år framåt, men denna tid bestäms enligt flera faktorer. Även snabba beslut kan ha långtgående konsekvenser och att särskilja dem från andra händelser kan uppta hela tidsfönstret eller mer. Det kan ta tid för saker att utvecklas till betydande, men under den digitala eran kan de skalas överraskande snabbt. Tidsfönstret placeras, beroende på definitionen, på det så kallade medellånga siktet.

Tidsfönstrets maximigräns bestäms av den gräns som man inte med den säkerhet som behövs för att kunna styra verksamheten kan skapa en bild om man ser över den med de metoder som används i riskhanteringen. Särskilt långtgående bedömningar kan stöda bedömningen av alternativen samt det allmänna framtidsrelaterade prognostiseringsarbetet, men det är inte nödvändigtvis motiverat att använda dem för konkreta mål. Liksom riskhanteringen är prognostiseringsarbetet systematiskt, strukturerat, inkluderande och utvecklande, men fokuserar på en längre tid, på att gestalta eventuella framtidsscenarier och kan anses stödja inriktningen av strategierna mer än att säkerställa att de genomförs. Definitionen av maximalt tidsfönster kan vara förknippad med situationsspecifik prövning och i vissa situationer kan det finnas betydande osäkerhetsfaktorer även om man ser över ett mycket kort tidsperspektiv.

Tidsfönstrets minimigräns bestäms av hur aktuell och rättidig vyn är. Målet med produktionen av information om riskhantering är att producera en tillräcklig förhandsvarning för att kunna vidta nödvändiga åtgärder för att förebygga eller ändra utvecklingen. Förhandsvarningen ska ges i så god tid att de nödvändiga åtgärderna hinner vidtas. I annat fall måste den rådande situationen hanteras med den befintliga förmågan och kapaciteten – eventuellt genom avvikande, brådskande och ofullständiga (men nödvändiga) åtgärder. Man kan argumentera för att även en liten varning är nödvändig, men det är eftersträvansvärt att i riskhanteringen producera prognostiseringsinformation som kan behandlas via normala förvaltningsstrukturer som en del av den normala ledningen och arbetet.

Tidsfönstret är alltså inte exakt avgränsat i någondera riktningen, men styr till att fokusera på en viss tidsperiod. Fördröjningen av genomloppstiden för processens alla delar definierar den kortaste möjliga tiden då modellen kan ge stöd för riskhanteringen. Den är beroende av olika bakgrundssystem, men också av omfattningen och djupet av den utvärdering och analys som behövs. Processen är dessutom bunden till en administrativ årsklocka som synkroniserar dess verksamhet med andra processer och strävar efter att producera information i rätt tid.

3.2.5 Informationens kvalitet och effekterna av det praktiska genomförandet

Informationens kvalitet varierar beroende på organisationers kompetens och engagemang, men detta förväntas bli bättre med tiden. Redan på basis av pilotprojekten har man identifierat tecken på att riskhanteringen också är förknippad med behov av kompetensutveckling, varav en del är förståelse som ackumuleras genom erfarenhet. Om datainsamlingen inom liknande enheter årligen i huvudsak förblir jämförbara, bör jämförbarheten av uppföljningen av förändringarna förbli god. Detta stöder uppföljningen av betydelsen av förändringar i verksamhetsmiljön som formats av olika händelser, vilket delvis är riskhantering.

Antalet respondenter förbättrar den statistiska kvaliteten och därför är deltagarnas aktivitet viktig. Man strävar efter att anpassa svarsinsamlingen till de årliga JTS- och TAE-cyklerna[21], varvid den producerade informationen stöder verksamhetsplaneringen i organisationerna. På den praktiska systemnivån kan man göra det möjligt att samla in och uppdatera information och granska sina egna jämförelseuppgifter året runt. Aktiviteten och möjligheten att delta behöver alltså inte vara bundna till en viss tidpunkt, men stora avvikelser i den kan försämra uppgifternas jämförbarhet.

Respondenterna kan till stöd för de deltagande organisationerna lägga till egna anteckningar som endast syns för organisationens egna användare i det nuvarande tekniska genomförandet. Detta och möjligheten att granska tidigare enkäter bör underlätta utvecklingen av en kvalitativt sett mer jämn syn. Andra åtgärder för kvalitetssäkring av övriga delar i processen är bland annat användning av flera riskinformationskällor (tillräcklig omfattning av materialet), användning av andra experter i olika skeden (analysens och bedömningarnas omfattning) samt insamling av användarrespons i olika former (utvärdering av processen samt produkter och utvecklingsbehov). Även i dessa fall utvecklas det exakta genomförandet, som är i balans med effektiviteten och resurserna, tillsammans med det praktiska genomförandet.

Med hjälp av respondenternas bakgrundsuppgifter kan man i jämförelserna beakta till exempel olika stora aktörers prioriteringar. Detta gör det möjligt att bättre identifiera de grupper som olika typer av aktörer bildar och de risker som de utsätts för. Till exempel i rapporteringen av pilotprojektet 2021 granskades kommunrespondenter av olika storlek och skillnaderna mellan dessa när de möter samma risker.

Man bör sträva efter att bedöma digitala risker för verksamheten och genomförandet av kärnfunktionerna. Där bör man i mån av möjlighet beakta riskerna för kunder, underleverantörer och andra intressentgrupper, om riskerna kan stråla över till dessa via nätverk. Utmaningen är att identifiera de digitala funktionernas roll i alla skeden eller faktorer som påverkar genomförandet av den digitala säkerheten. Att skapa en gemensam syn är en identifierad utmaning och den kommer att utvecklas under de kommande åren. Det är fråga om att ständigt utveckla en delad förståelse (diskurs), som särskilt påverkas av de ledande instansernas synpunkter och kommunikation. Redan deltagande i riskhanteringen kan antas utveckla sakkunskapen, vilket förbättrar kvaliteten under årens gång.

[21] Riskhanteringens årsplanering och årsklocka, del 2.2 i detta dokument

3.2.6 Informationssäkerhet

I behandlingen av säkerhetsfrågor är informationssäkerheten av största vikt. Även här ska riskhantering tillämpas och därför måste man förklara karaktären hos den information som behandlas med modellen i förhållande till kraven. I synnerhet när det gäller information som delas ut ska man beakta den kontext som används, dvs. digital säkerhet på strategisk nivå inom den offentliga förvaltningen. Även om det här också kan inkludera mer omfattande och sensitiva säkerhetsutsikter kommer skillnaden mellan dem i det praktiska genomförandet och de informationsbehov som eftersträvas för processen. Olika aspekter av digital säkerhet överlappar naturligtvis varandra, eftersom det inte heller i den digitala säkerheten finns en enda helhet av säkerhet eller säkerhetsinformation - till exempel informationssäkerhet och dataskydd, där samma sak kan granskas utifrån olika utgångspunkter. En omfattande granskning av den digitala säkerheten kan leda till både mer begränsade granskningar av säkerheten i den digitala verksamhetsmiljön och mer omfattande helheter.

Processmodellen tar inte i sig ställning till hur djupt vissa säkerhetsområden granskas, utan förutom behoven styrs detta av lagen och praxis. De informationsbehov som styr den praktiska datainsamlingen är annorlunda än hur de uppfattas till exempel i kontexterna "nationell säkerhet" eller "cybersäkerhet", vilket för sin del förändrar informationens innehåll. Den information som samlas in ska i vilket fall som helst bedömas och kunna skyddas på det sätt som krävs (i synnerhet 18 § 1 mom. i informationshanteringslagen och 3 § i Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen)[22]. Ur riskhanteringssynvinkel ska man dessutom beakta skapandet av en så oskälig risk genom att samla in onödigt sensitiv och detaljerad information med tanke på behovet, liksom även kostnaderna för de åtgärder som behövs för hanteringen av den risk som uppstår och hur krävande hanteringen är. Man måste också komma ihåg att insamlingen av information kan omfatta flera sätt och system, inklusive informationsutbyte mellan myndigheter på olika nivåer samt öppna källor.

Mot dessa gränser kan man bedöma att den sammanställda informationen på sin höjd blir "konfidentiell" på längre sikt, utan att det stör syftet med processen. I enlighet med de system och arrangemang som för närvarande stöder processmodellen får informationen vara på högst begränsad nivå (säkerhetsklass 4, TL IV)[23], vilket är lämpligt med beaktande av informationsutbytet mellan myndigheterna. I praktiken är klassificeringen av den information som samlas in dock "sekretessbelagd" och grundar sig bland annat på erfarenheter från pilotförsöken. Det bör särskilt påpekas att en enskild uppgift kan ha klassificerats som offentlig av den deltagande organisationen, men att sammanställda rapporter och andra dataprodukter kan klassificeras på ett högre eller lägre sätt, varvid lämpliga krav ska tillämpas på den vidarebehandlade informationen.

Säkerhets- och förtroendefrågor i anslutning till lagring av riskuppgifter blir tydligare för användarna i och med det praktiska genomförandet, vilket är en egen helhet. FM och Myndigheten för digitalisering och befolkningsdata har redan 2020 och 2021 samlat in information som stöder processen. Lärdomarna från detta har införlivats i den nya helheten. Eftersom den enkät som används som stomme har en strategisk

[22] Mer information: Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet

[23] Mer information: Rekommendation om behandling av säkerhetsklassificerade handlingar

inriktning och i den efterfrågas bedömningar av den relativa betydelsen, samlas endast statistiskt användbar information i systemet. I frågorna efterfrågas till exempel inte uppgifter om detaljer i datasystemen. Detta är inte heller ändamålsenligt med tanke på den eftersträvade betydelsen, eftersom genomförandet av delområdena i olika organisationer varierar mycket. I insamlingen av information har man alltså beaktat lågriskhet i planeringen (security by design -tänkandet) samt strävat efter balans i form av den information som behövs och för att minimera mängden i förhållande till användningsbehoven. Generaliserat kan man konstatera att förutom eventuella angripare ska även den offentliga förvaltningen kunna samla in tillräcklig information om sin egen situation för att rikta in åtgärderna för digital säkerhet.

Kraven på och genomförandet av de system som används för insamling och hantering av separat praktisk information från processmodellen har utvecklats under pilotskedena. I Suomi.fi-mobilapplikationens serviceadministration används bland annat stark autentisering och organisationerna har via sin egen huvudanvändare kontroll över vem som har befogenheter att hantera uppgifterna. Dessutom finns det möjlighet att fastställa klassificeringsnivån för informationen i enkäterna. Uppgifterna har sparats i MDB:s skyddade miljö. Tjänsten uppfyller dessutom kraven på tvåspråkighet och tillgänglighet.

3.2.7 Förhållandet till organisationernas egen riskhantering

Eftersom den strategiska utsikten över riskerna är kontextbunden är det bra att påminna om att varje organisations egna risker för den digitala säkerheten ska inkluderas i organisationens övergripande riskhantering. Enligt modellen med tre försvarslinjer ingår granskningen av riskerna för digital säkerhet i granskningen av riskerna i linjeorganisationerna, en del av experttjänsterna som genomsyrar organisationen (såsom informationsförvaltning eller säkerhetstjänster) samt ett eventuellt objekt för intern granskning.

I den övergripande riskhanteringen, liksom i digitala risker, kan man göra olika klassificeringar enligt risktyper och egenskaper, och dessa hjälper till att uppfatta vad granskningsområdet består av. Betoningarna inom digital säkerhet, både i fråga om centrala genomförandeområden och andra aspekter, ska grunda sig på organisationens egen verksamhet och behov. De risker för centrala uppgifter och mål som är förknippade med den digitala dimensionen som granskas i den övergripande riskhanteringen bör kunna härledas till riskerna med den digitala säkerheten. Sambandet är inte nödvändigtvis direkt utan ett indirekt påverkansförhållande eller en koppling. De digitala riskerna är alltså inte separata utan en del av riskhanteringen som helhet.

Med tanke på den övergripande riskhanteringen – man gör det i en organisations kontext eller inom olika samhällsdelar eller statsförvaltningens delområden – kan olika splittrade konstruktioner i och med ämnesbaserade riskgranskningar (såsom digital säkerhet, men även till exempel logistik, kommunikation e.d.), lyfta fram frågor som kräver närmare granskning ur nya perspektiv. Detta ingår i god förvaltning och gagnar i och med samarbetet flera aktörer – även utanför de deltagande organisationerna. På grund av standardstrukturen och frivilligt deltagande samt styrningen av användningen av statliga medel, stöder den modell som presenteras i detta dokument den riskhantering som styrs av finansministeriets controllerfunktion.

3.2.8 Förhållande till andra risk- och säkerhetsbedömningar

Den strategiska riskbedömningen av den digitala säkerheten är en tväradministrativ granskning av situationen för olika fenomen som är bunden till den digitala verksamhetsmiljöns kontext[24]. För att möjliggöra granskningen av detta avgränsade specialområde är den insamlade informationen tillgänglig som en källa med vissa förbehåll även i andra granskningar i anslutning till ämnet eller som en delanalys i mer omfattande granskningar. Den information som producerats redan i pilotskedet har använts inom statsförvaltningen som en del av bedömningarna av säkerheten och digitaliseringen[25]. Den ligger således till exempel under den nationella riskbedömningen, men kan i större utsträckning granska fenomen som tangerar säkerheten inom sitt område.

Det bör dock observeras att kontexterna och granskningsnivåerna för olika bedömningar kan variera[26], varvid informationen vid behov ska analyseras och bedömas på nytt med tillräcklig noggrannhet för det nya användningsändamålet. Detta är en del av alla uppgifter med anknytning till dataprodukter.[27] När information förs in i en organisations egen riskbedömningsprocess rekommenderas också annan rapportering och andra informationskällor för de delområden inom digital säkerhet som upplevs som viktiga. När man skapar en bredare bild kan man som tilläggsinformation använda till exempel Cybersäkerhetscentrets mer tekniska bedömningar och meddelanden, eftersom det är bra att veta vilka praktiska fenomen större ämnesområden innehåller.

För att definiera kontexten för identifiering av risker, det vill säga sammanställa interna behov, mål och strategier samt identifiera den externa verksamhetsmiljön och de förändringsfaktorer som finns i den, måste ett omfattande bakgrundsmaterial sammanställas. Dessa bildar en fixpunkt (eller punkter) genom vilken man identifierar vilka hot som är centrala risker som man måste fästa uppmärksamhet vid. Delvis samma material och andra källor erbjuder också tankar om nya hot och deras strukturer, men också om hur riskerna utvecklas. Dessa ska utnyttjas som material som stöder identifieringen av risker, för att man ska kunna säkerställa att granskningen är heltäckande, men att också olika synvinklar på ämnen och fenomen beaktas.[28]

---

[24] Enligt definitionen anknyter den digitala tryggheten till saker som sker i den digitala verksamhetsmiljön, men också till frågor som står utanför verksamhetsmiljön, men som påverkar den samt konsekvenser som riktas utanför den. I vissa fall behandlas ärenden som kan räknas som digitala risker dock inte ur detta perspektiv, utan en annan definition kan vara mer signifikant eller av särskilda skäl vald. Till exempel behandlas vissa hot som kan räknas till cybersäkerheten i den (utrikes)politiska kontexten.

[25] Lägesbildshelheten för digitaliseringen modellerades på ett nytt sätt genom ett systemiskt tillvägagångssätt. Material: Https://vm.fi/digitalisaation-mittarit-ja-tilannekuva (på finska)

[26] Till exempel riktas regionala eller nationella riskbedömningar på lite olika sätt och är inriktade på något olika behov, men behandlar också delvis samma ämnen.

[27] Exempel på riskuppgifter som behandlas i denna modell kan ses i den öppna rapporteringen om pilotprojektet 2021.

[28] Exempel på bakgrundsmaterial: Digihumaus-rapporten (MBD), Threat Landscape (Enisa), Försörjningssäkerhetens scenarier 2030 (HVK), Threat Horizon 2022 (Information Security Forum), Kansallinen riskiarvio (på finska) (SM), Global Risk Report (WEF), Den digitala kompassen (Digitaliseringsbyrån), Digitaliseringens lägesbild (FM), Säkerhetsstrategi för samhället (Säkerhetskommittén), Cybersäkerhetsstrategi (Säkerhetskommittén)

3.2.9 Förhållande till standarder

Det är utmanande att skapa riskhanteringssystem som följer standarden inom den offentliga förvaltningen och i stora komplicerade organisationer. Detta gäller särskilt vid arrangemang som förenar mer omfattande förvaltnings- och näringsgrenar (till exempel kring ämnesområdet, såsom digital säkerhet eller någon näringsgren), som skapas för att stöda olika riskhanteringshelheter. I den modellstruktur som beskrivs i ISO31000 ingår inte de funktioner som behövs för en omfattande organisation eller en större helhet, med vilka en utbredd organisationsstruktur eller omfattande datamängd kan behandlas effektivt i olika faser. De mekanismer som behövs för att dela upp behandlingen i kategorier eller sammanställa den i kategorier och statistik skall därför införas i de olika faserna.

Det är viktigt att beakta att varje organisation eller en del av den genomför riskhanteringen samt identifierar och bedömer riskerna i första hand ur sitt eget perspektiv, även om de strävar efter att beakta andra. Perspektiven kan sällan överföras som sådana från en organisationskontext till en annan. Vid överföring av riskuppgifter mellan organisationer både i sidled och mellan hierarkiska nivåer ska informationen alltid omvärderas i förhållande till det nya perspektivet och den nya organisationen. Detta kan göras i avsändande och mottagande ändar, men bedömningen grundar sig på tolkning. När man sammanställer en vision på strategisk nivå för en bredare granskning måste man som standard acceptera att den grundar sig på indikerande information och signaler som kan tolkas inexakt, även om de bakomliggande uppgifterna är av hög kvalitet.

För de organisationer eller organisationssystem vars hantering stöds av en verksamhet som planerats i enlighet med ISO27000-serien, förutsätter riskhanteringen att standarden följs. Eftersom den riskhanteringsprocess som används i ISO27000-serien grundar sig på ISO31000, finns det vid behov ett gränssnitt och en möjlighet att koppla samman den med en mer omfattande riskhantering. Motsvarigheter kan också finnas i andra processmodeller. Organisationens egen övergripande riskhantering är primär i förhållande till enskilda delområden eller denna riskhanteringsmodell som omfattar hela den offentliga förvaltningen.

Finanscontrollerfunktionen har utarbetat anvisningar för riskhantering[29] samt en modell för riskhanteringspolitik. Modellen innehåller de rekommenderade minimikraven för politiken samt vissa andra styrande egenskaper.[30] Rekommendationerna grundar sig på riskhanteringsstandarden ISO 31000.

3.3 Om kostnader och effektivitet

Effekterna och verkan av den strategiska riskhanteringen inom den offentliga förvaltningen är omfattande helheter. Mätningen av dem försvåras av det decentraliserade genomförandet, definitionen av inriktningen och kontexten i stället för till enskilda organisationer även till kunder och andra intressegrupper samt utmaningen att mäta värdet av den ogenomförda effekten, dvs. det omvända värdet av effekten av den risk som undviks med hanteringsåtgärder. Till de delar som effekterna av genomförandet av denna riskhanteringsmodell granskas, vilket kan bedömas enklare, kan man anse

[29] https://vm.fi/riskienhallinnan-ohjeita

[30] https://vm.fi/riskienhallinta/riskienhallintapolitiikka

att viktiga satsningar är små i förhållande till de potentiella olägenheter och förluster, som de omfattande riskerna kan medföra om de realiseras.

Riskhanteringschefen som upprätthåller och utvecklar helhetsprocessen och svarar för dataprodukterna ska fungera som ledande expert (eller ansvarig, beroende på uppgiftshelheten) vid Myndigheten för digitalisering och befolkningsdata och ha dessa uppgifter som huvuduppgift. Lönebikostnaderna för detta årsverke samt den preliminära budget som behövs för utveckling och kommunikation uppgår till sammanlagt cirka 170 000 euro per år, men siffran kan förväntas öka i och med utvecklingsåtgärderna. Som kostnader för MDB ska man också beakta utnyttjandet av experter på digital säkerhet och konsulter. Vid bedömningen av särskilda risker och planeringen av åtgärder för att hantera dem, ska som sakkunniga även anlitas sakkunskap från andra aktörer inom den offentliga förvaltningen, vilket inte räknas med här. Utöver detta kommer underhållskostnaderna för systemen, som är kopplade till MDB:s övriga kostnader, inklusive till exempel tjänsten för helhetsbilden av den digitala säkerheten, vars uppgifter även utnyttjas i riskhanteringen enligt denna modell.

De organisationer som deltar i produktionen av risk- och riskhanteringsuppgifter uppskattas använda cirka 1-3 dagsverken per år för detta. Flera sakkunniga kan delta i produktionen och satsningen är beroende av hur organisationerna ordnar riskhanteringen i övrigt. Den tid som används för inmatning av uppgifter kan antas sjunka tydligt efter de första processcyklerna, eftersom tröskeln för ibruktagande i början kan vara högre. Användningen av de erhållna rapporterna i den egna riskhanteringen tar, beroende på hur de behandlas, lika lång tid, och utöver detta kommer naturligtvis separat indirekta konsekvenser för eventuella hanteringsåtgärder. Via tjänsten för helhetsbild skulle organisationer som inte deltar i informationsfördelningen inom riskhanteringen dra nytta av den allmänna rapporteringen om riskhantering inom digital säkerhet samt eventuella allmänna riskhanteringsåtgärder inom digital säkerhet. Inriktningen av åtgärderna kan dock lida av brist på täckning om antalet deltagare är litet.

Den information som produceras i riskhanteringsprocessen orsakar uppgifter för de behöriga myndigheter till vilka riskhanteringsåtgärderna styrs. För samordningsåtgärderna finns det en strategisk ledningsgrupp för digital säkerhet bestående av centrala myndigheter. Tidsanvändningen i anslutning till ledningsgruppens verksamhet ingår i de planerade mötena. I fråga om de verkställande myndigheterna är konsekvenserna specifika från fall till fall och en del av åtgärderna vidtas inom ramen för normala processer, men i större projekt måste man göra en separat resursfördelning. VAHTI-ledningsgruppen och arbetsgruppen för utveckling av riskhanteringen VAHTI, inom vilka man frivilligt kan delta i uppgifter i anslutning till utvecklingen av processen, anses inte ha någon betydande direkt belastning.

Genom strategisk riskhantering är det möjligt att påverka omfattande helheter vars konsekvenser direkt eller indirekt återspeglas hos flera aktörer. Även om säkerhetens säkerställande betonas inom ämnesområdet, strävar man genom riskhanteringen framför allt efter att möjliggöra strategiska funktioner och stödja uppnåendet av de strategiska målen samt göra det möjligt för organisationen att fungera i vardagen. Utöver att riskernas effekter kan minskas och neutraliseras bör man i den strategiska riskhanteringen också sträva efter att beakta möjligheterna, dvs. att omvandla nackdelar till ett positivt slutresultat.

Att få en lyckad förvarning om riskhanteringen innebär i allmänhet en betydande kostnadsbesparing jämfört med att risken omvandlas till en oförberedd akut situation. Dessutom kan förvaltningsåtgärderna omfatta till exempel förnyelse av säkerhetsrelaterade eller andra funktioner som effektiviserar och berikar tjänsterna eller möjliggör idrifttagning av nya teknologier eller verksamhetssätt och effektiviserar utnyttjandet av information. Det kan vara omöjligt att mäta hur dessa fördelar uppnås, i synnerhet i euro, men att fastställa värdet på de uppgifter inom digital säkerhet som ska stöda dem som mätare av effektiviteten är en del av de behov av styrning och utveckling som ingår i modellen.

3.4 Utveckling av riskhanteringsmodellen

Att bygga upp en heltäckande riskhanteringsmodell till ett fungerande system som motsvarar de behov som uppstår är en lång process. Modellens utveckling inleddes med en enkät som genomfördes 2020 och som har utvecklats och upprepats. Enkäten och de synpunkter på riskerna som samlas in med den är dock bara en del och ett perspektiv. Riskhanteringshelheten omfattar flera delområden som bör utvecklas. Enligt CMMI-modellens[31] femstegsindikator kan den nuvarande situationen bedömas uppfylla högst nivå två.

Den presenterade helheten är en beskrivning av verksamhetsmodellen och de processer som ingår i den. Modellen är av permanent karaktär, eftersom den digitala säkerheten behöver utvecklas långsiktigt. Till den hör dock också delar särskilt på en praktisk nivå som behöver utvecklas och som beaktar den kontinuerliga förändringen i verksamhetsmiljöerna och som styrs av kommande mål och behov som klarnar vid sidan av riskhanteringsarbetet. I den föreslagna modellen har man strävat efter att beakta bägge utmaningar.

Utvecklingsobjekt som observerats i samband med pilotförsöken och granskningen av nuläget samt testningen av användningen kunde vara:

- En systembaserad informationsbehandling och interoperabilitet med olika definitioner kan effektivisera riskhanteringen, eftersom vissa delar av den kan automatiseras och de data och den information som produceras åtminstone till vissa delar är mer jämförbara och strukturerade. Man skulle till exempel kunna utveckla tillämpningen av de skalor som används för bedömning och klassificering. Organisationerna skulle snabbare kunna jämföra riskuppgifterna och utnyttja dem i verksamhetsstyrningen. Vissa organisationer har redan kommit längre, men vissa fungerar fortfarande nästan manuellt. En nivåförbättring vore önskvärd med tanke på kvaliteten på riskhanteringen inom den offentliga förvaltningen som helhet.
- Det är viktigt att öka antalet deltagare och svar för att förbättra noggrannheten i det data som fås från enkäterna och för att säkerställa kvaliteten. Tillräckliga data ger förutom tillförlitlighet även tillräcklig information om i synnerhet mindre jämförelsegrupper. Detta är viktigt för att åtgärderna ska riktas rätt.
- Nyttan av deltagarnas data och deltagande i processen kan ökas med tiden när data ackumuleras. Då kan man producera mer och mer kreativa informationsprodukter och kombinera dem med andra källor. En längre historia jämnar också slutligen ut eventuella snedvridningar mellan olika tidpunkter. Värdet som ackumuleringen av data ger ökar också snabbare än bara i formen av linjär tillväxt mot slutet av årtiondet.

[31] Capability Maturity Model Integration

- För att säkerställa innehållet i den insamlade informationen och insamlingens omfattning ska man sträva efter att använda flera källor samt utomstående utvärderingar för att komplettera informationen och analysen.
- För att säkerställa kvaliteten bör man i analysmetoden sträva efter mångsidighet inom ramen för genomförbarheten. Å andra sidan bör man i presentationen av information i dataprodukter sträva efter effektivitet och tydlighet som betjänar läsaren på rätt sätt. Även om de är separata punkter i processen, har de en indirekt koppling till varandra. Det är viktigt att lägga fram rätt betydelse på rätt sätt för att man ska kunna ta till sig frågan och undvika informationsflödet.
- Allteftersom de vanligaste dataprodukterna utvecklas och informationsbehoven klarnar torde det uppstå ett behov av att utveckla noggrannare och mer specialiserade granskningar. Även om avsikten är att processens struktur ska vara bestående, förutsätter dess nytta en kontinuerlig utveckling för att nya risker och utvecklingsbehov ska kunna beaktas.
- I det inledande skedet har man inte inkluderat någon särskild mekanism för att dela och producera hotuppgifter för de deltagande organisationerna. Antagandet är att organisationers normala verksamhet för digital säkerhet omfattar observation och uppföljning av situationen i anslutning till den egna verksamheten och verksamhetsmiljön. För en bättre uppfattning av helheten kunde man sträva efter att producera sammanställda utsikter över hoten som organisationerna sedan kunde använda för att bedöma sina egna risker, som en del av sin riskbedömningsprocess.
- Även om hot kan identifieras utifrån en allmän uppfattning eller en expertuppfattning, bör riskerna bedömas i förhållande till de uppställda målen. Den digitala säkerheten ska stödja de mål som ställts upp i olika strategier, beslut och planer. Målen kan vara mer allmänna eller riktas mot den digitala verksamhetsmiljön. Ett mer systematiskt genomförande av utvärderingen i praktiken, eventuellt även delvis i fråga om motstridiga mål, bör bearbetas både i processen och i mån av möjlighet även utanför den i den strategiska måluppställningen.
- I riskhanteringen bör man granska utnyttjandet av de utsikter och förändringsvägar som produceras i prognostiseringsarbetet för att stöda de önskade utvecklingstrenderna på lång sikt.

Utvecklingsobjekt i processen för strategisk informationshantering kunde vara:

- Utveckling av uppgiften att styra och stöda riskhanteringen ("begäran om information"), det vill säga hur man utformar rätt frågor för att kunna producera de svar som behövs.
- Utvidga och fördjupa datainsamlingen, säkerställa täckningen i olika faser, utveckla och berika jämförelsedata samt externa informationskällor.
- Utveckling av informationsbehandlingen; effektivisering, utveckling av enhetliga behandlingssätt, klassificering samt utnyttjande av lärande system till exempel vid identifiering och prognostiseringen av förändringar.
- Faktorer i anslutning till utvecklingen av analysen och rapporteringen om metoder och verktyg, visualisering av information samt en bredare lägesbild och förståelse av den.

Både i observationer som gjorts genom testning och genom att analysera strukturen ser man flera liknande utvecklingsområden. Många av dessa är redan ensamma små projekt och innehåller många förändringar på praktisk nivå, men alla av dem skulle

inte vara synliga utåt. På grund av antalet alternativ måste genomförandet av dessa prioriteras.

3.4.1 Första utvecklingsfasen

Uppgifterna i den första utvecklingsfasen fokuserade på insamling av information, även om man redan i det andra pilotförsöket 2021 utvecklade preciseringar i anslutning till begäran om information för en riktning av enkäten. För att effektivisera, trygga och förenhetliga insamlingen av information har man tagit i bruk ett datasystem där man producerar dataprodukter med anknytning till helhetsbilden av den digitala säkerheten genom att utnyttja samma bakgrundsinformation om organisationerna. Övergången till att använda systemet innebär att det med tanke på dataproduktens innehåll är möjligt att utnyttja bakgrundsinformation om digital säkerhet. Med hjälp av den skapas en bild av en situation i riskhanteringen som kan ställas i relation till riskerna, men också ställas i relation till olika aktörer och skapade pararellgrupper. Dessutom kan aktuell och uppdaterad information tillhandahållas genom automatisk rapportering. Till en början kommer rapporteringen att vara i grundform, men när mängden data samlas in kan den utvecklas. Repeterbarheten och möjligheten att jämföra insamlad data som tidsserier gör det möjligt att genomföra olika enkäter. De ger information om förändringar under årens lopp, vilket möjliggör utsikter gällande indikativa framtidstrender.

Med dessa åtgärder kan man skapa en grund för den informationsinsamling om riskbedömningsprocessen som organisationerna gör. I och med detta skapas processens centrala resultat för de deltagande organisationerna, dvs. en jämförande rapport om riskens lägesbild samt en lägesbild av riskhanteringen i förhållande till andra aktörer inom den offentliga förvaltningen. För styrningen bildas en datakälla som utvecklas och vars värde ökar med tiden. Till en början måste man visserligen finslipa processens funktion genom pilotförsök och i den ingår en ändring som användarna upplever när de övergår till att använda en ny typ av tjänst, vilket torde generera arbete. Risken är att antalet användare i början blir litet, vilket fördröjer mängden data som samlas i systemet och stör tillgången till heltäckande utsikter.

3.4.2 Skiss över den andra utvecklingsfasen

I den andra fasen bör man koncentrera sig på att förbättra tidigare förmågor så att nyttan av dem kan "öka räntan" i ett tidigt skede. För en meningsfull och trovärdig uppföljning av förändringarna behövs upprepningar under cirka 3–5 års tid. Denna beräkning kan dock inledas först när en tillräcklig grupp deltagare har anslutit sig till processen.

Den befintliga enkäten om riskutsikter bör kompletteras och man bör lägga till enkäter som använder andra metoder och perspektiv och som kan svara på andra slags risker och behov i anslutning till riskhanteringen. Dessa metoder kunde vara skisser med anknytning till förändringsfaktorer i framtidens digitala säkerhet (utvecklingsförlopp som är mer omfattande än hot och risker), en upprepad utredning som skapar utrymme för och interoperabilitet hos de verktyg som används i riskhanteringen, informationsinsamling i anslutning till observation och hantering av risker på olika nivåer och så vidare. Vissa av exemplen stöder i högre grad de deltagande organisationernas egen riskhantering och andra en mer omfattande utveckling och styrning av riskhanteringen inom den offentliga förvaltningen.

Dessutom bör man granska och till exempel genom pilotprojekt testa att utvidga datainsamlingen till andra källor (externa beställda bedömningar), göra analysmetoderna mångsidigare (systemisk lägesbild, nätverksanalys) samt definiera valideringen (process, kvalitetskriterier). Dessutom bör utvecklingen av producerade dataprodukter, såsom rapporter, fortsätta. Man bör säkerställa att den övergripande processen fungerar och göra den permanent, vilket i praktiken är en förutsättning för den ovan nämnda kvalitetsutvecklingen.

3.4.3 Eventuella skeden i den fortsatta utvecklingen

I den tredje utvecklingsfasen bör riskhanteringen för den digitala säkerheten inom den offentliga förvaltningen i tillräcklig utsträckning samordnas med prognostiserings- och framtidsarbetet. Då skulle den strategiska utsikten för den digitala säkerheten vara mer överensstämmande med utvecklingsutsikterna för den övriga allmänna digitaliseringen. Till samordningen hör också en utveckling av riskhanteringen på statsrådsnivå, som samlar information om de vertikala silobaserade förvaltningsområdenas riskhantering. Den process som beskrivs här är naturligtvis ett tväradministrativt urval av ett visst ämnesområde.

När datamängden ackumuleras och blir mångsidigare bör behandlingen och analysen av informationen automatiseras för att effektivisera och precisera den. Detta kan innebära att man utvecklar gränssnitt mellan kompatibla system, men också att man utnyttjar system som lär sig att identifiera olika företeelser och klassificeringsgrupper, varvid man kan vidta riktade riskhanteringsåtgärder. Detta kan också fungera som ett meddelande till riskhanteringen på operativ nivå i organisationernas egen riskhanteringskontext.

När framtida förändringar skapar nya risker, men också när man formar verksamhetsmiljön och tekniken, är det ytterst viktigt att identifiera nya källor till riskerna och kanaler för påverkan. Om dessa inte kan identifieras kan de inte heller beaktas i riskhanteringen. Den modell och process för riskhantering som presenteras här ska utvärderas kontinuerligt och regelbundet och man ska bedöma om den motsvarar sitt syfte och effektivt producerar den information som behövs. Utöver de inkrementella granskningarna bör man regelbundet hålla särskilda evenemang som granskar utvecklingen av den strategiska riskhanteringen, kvaliteten och framtida förändringar.