MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Strategisk riskhantering av digital säkerhet inom den offentliga förvaltningen

Allmän riskö̈versikt, hösten 2022

23.1.2023

Tel. **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi/sv**

DTYT / Reivo Juho (MDB) 23.1.2023

Innehållsförteckning

DTYT / Reivo Juho (MDB) 23.1.2023

1 JHDTSRH – Föregripande riskövеrsikt, hösten 2022

Strategisk riskhantering av digital säkerhet inom den offentliga förvaltningen (JHDTSRH) granskar både riskerna och därmed även riskhanteringens tillstånd. Granskningen grundar sig på en modell som beskrivits för detta ändamål och som specificerar processerna för olika aktörer och granskningsnivåer. Med hjälp av modellen strävar man efter en riskhantering som utvecklas och högklassig producerad information när verksamhetens maturitetsnivå inom olika delområden utvecklas. En central dataprodukt som produceras är en förutseende uppfattning av riskerna och riskhanteringen inom den digitala säkerheten på strategisk nivå som omfattar den offentliga förvaltningen. Det här dokumentet är ett utdrag ur det. En mer omfattande version kan laddas ner för de organisationer som deltar i enkäten på plattformen Digital säkerhets riskhanteringsuppgifter.

Rapporten innehåller säkerhetsmateriel som ska behandlas med vederbörlig omsorg med beaktande av lagen om offentlighet i myndigheternas verksamhet (621/1999) och lagen om informationshantering inom den offentliga förvaltningen (906/2019). En eventuell noggrannare klassificering anges på pärmbladet.

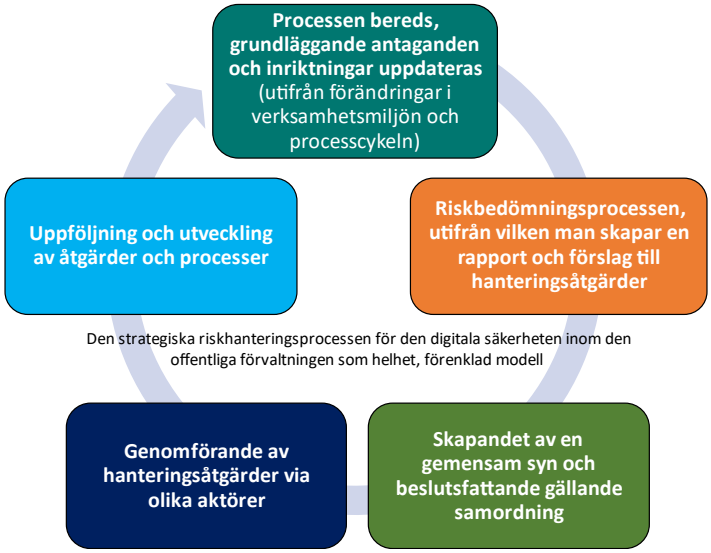
Myndigheten för digitalisering och befolkningsdatas grupp för digital säkerhet producerar vid behov granskningar och jämförelseuppgifter om läget för den digitala säkerheten som helhet och för olika delområden, inkl. riskhantering: digiturva@dvv.fi

1.1 Riskhantering av digital säkerhet inom den offentliga förvaltningen

Organisationerna genomför riskhantering utifrån sina egna utgångspunkter och fokuserar på den egna verksamheten, så som är standardenligt inom riskhanteringen. De behöriga myndigheterna ansvarar särskilt för vissa åtgärder som kan anses ha samband med riskprocessen. Riskhanteringen ska återspegla hur organisationen (eller något annat objekt eller en helhet som granskas) fungerar och ser på sig själv samt sitt förhållande 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.

Riskhanteringsmodellen är särskilt avsedd att göra det möjligt att identifiera tväradministrativa och omfattande delade risker (i denna kontext) inom den offentliga förvaltningen som grundar sig på en decentraliserad struktur. Dessutom vill man bedöma och styra dem till behandling samt effektivisera hanteringsåtgärderna för det gemensamma bästa. I den strategiska riskbilden identifieras från flera nationella och internationella informationskällor sådana risker som om de förverkligas i stor utsträckning skulle orsaka allvarliga olägenheter för såväl staten som andra aktörer inom den offentliga förvaltningen. Risker som samtidigt ändå som kontext placerar sig under den nationella riskbedömningen och granskar frågor som påverkar den digitala säkerheten i större utsträckning.

Strategisk riskhantering av digital säkerhet inom den offentliga förvaltningen (JHDTSRH-modellen) består av en omfattande och systematisk process som kan upprepas och utvecklas samt uppgifter i anslutning till den. Den ser lite annorlunda ut för olika organisationer, beroende på deras delaktighet i åtgärder utanför den egna riskhanteringen, såsom att utveckla hanteringsåtgärderna. För de flesta samlar processen in information för den egna riskhanteringsprocessen. Inom den offentliga förvaltningen är det viktigt att man i processen har lyft fram beslutsfattandet som ett krav på god förvaltningssed, varvid det kunskapsbaserade och riskbaserade beslutsfattandet synliggörs.



Figur 1: Förenklad presentation av riskhanteringsprocessen som den offentliga förvaltningen genomför.

Det kommer att ta flera år att öka verksamhetens maturitet enligt riskhanteringsmodellen till en önskvärd nivå inom alla delområden, bl.a. på grund av insamlingen av trenddata, eller med andra ord, utvecklingsdata. De observationer och urval som nu presenteras i rapporten stöds också av expertutlåtanden samt extern rapportering för att stärka innehållets kvalitet. Rapporteringens innehåll, valda källor och layout kommer att utvecklas vidare i fortsättningen.

Avsikten är att granskningen i JHDTSRH-modellen ska riktas till en tidsperiod på cirka 2–5 år för att den offentliga förvaltningen ska kunna bereda och producera de hanteringsåtgärder som behövs som en del av de normala processerna. I den enkät som använts i denna rapport har man ombetts göra bedömningar för en tidsperiod på cirka 1–3 år, då de nuvarande situationerna eventuellt redan har förändrats och följande förändringar eventuellt är på kommande.

1.2 Använda enkäter

Enkäten om risksyn i tjänsten som samlar in information om riskhantering inom digital säkerhet ingår i hanteringen av strategiska risker i den digitala säkerheten inom den offentliga förvaltningen. Enkäten har pilottestats under tidigare år och därför finns det partiell jämförelseinformation om den. Nu består granskningen av 40 enkäter med riskpåståenden som gjorts för sakkunniga i organisationer inom den offentliga förvaltningen.

Svaren samlades in mellan maj och november, eftersom man utanför den egentliga svarstiden (21.9–11.10.2022) kunde inkludera svar från de testorganisationer som svarat på förhand samt respondenter som enligt separat överenskommelse svarat senare. Tiotals respondenter började svara genom att skapa åtminstone en användarprofil i tjänsten för riskhanteringsuppgifter för digital säkerhet, men sparade slutligen inte sina svar.

Inbjudan till enkäten om risksyn skickades till 540 organisationer inom den offentliga förvaltningen. Enkäten besvarades av 97 organisationer, varav svaren av 96 organisationer användes i statistiken (N=96). I statistiken används filtrering av avvikande

svar (formeln Tukey's fences) för att förhindra att små jämförelsegruppers resultat snedvrids. För hela enkäten, där man för riskbedömning inom den offentliga förvaltningen använde skalan (1–4), koncentrerades resultaten i regel – som väntat – kring värdet 2. Antalet svar visar dock på skillnader både inom enskilda riskpåståenden och inom de klassificeringsmodeller som används. Av respondenterna var 46 st., cirka 48 %, kommuner och städer och representerade cirka 15 % av kommunfältet (309 st. 2022).

Information som kompletterar riskinformationen om riskhanteringens tillstånd är en enkät för organisationer om den digitala säkerhetens helhetsbild. Den genomfördes under perioden 21.6.-24.8.2022. Inbjudan till enkäten skickades till 612 organisationer inom den offentliga förvaltningen. 116 organisationer deltog som respondenter (N) i denna enkät. I enkäten granskades genomförandet av åtgärder inom olika delområden av digital säkerhet på bred front. Av respondenterna var 57 st., cirka 49%, kommuner och städer och representerade cirka 18% av hela kommunfältet (309 st. 2022).

1.3 Sammanfattning av de centrala punkterna i risksynen

Rapporten utgår från två enkäter som har besvarats av cirka hundra organisationer inom den offentliga förvaltningen. Organisationerna har ombetts granska riskerna (40 st.) 1–3 år framåt i tiden. Enkäterna har upprepats i början av hösten 2021 och 2022. Resultaten kan anses vara riktgivande och **rapporteringen kommer att vidareutvecklas**.

Som helhet **anses sannolikheten för risker inte ha ökat märkbart** mellan granskningstidpunkterna. Detsamma gäller angrepp på myndigheternas infrastruktur och tjänster för digital säkerhet, som betraktas som de största riskerna. Detta anses återspegla förtroendet för den nationella kompetensen och beredskapen.

Av riskernas influensområden **anses de ekonomiska effekterna i allmänhet öka**. De ekonomiska effekterna framhävs i synnerhet i anslutning till riskerna för återhämtning från störningar, även om sannolikheten för dem är relativt måttlig. Oron för att återhämtningen misslyckas, både vad gäller utrustning och informationskapital, gäller kostnaderna för både förhandsberedskap och eftervård. I synnerhet **kostnaderna för eftervården av en attack kan förväntas öka** eftersom man i största delen av dessa har observerat en strävan att skada säkerhetskopiorna, varvid återställningen av systemen inte lyckas som planerat.

Den mest sannolika risken anses vara kvaliteten på bestämmelser, föreskrifter och anvisningar, samt att de är splittrade. Detta kan skapa svagheter och indirekt skapa eller förvärra sårbarheter. Åtgärder vidtas redan för att förtydliga hanteringen av helhetsbilden och styrningen, men man måste satsa på hanteringen av denna information även i organisationerna, eftersom de borde känna till de bestämmelser och den styrning som påverkar deras eget agerande för att gestalta helhetsbilden av ansvaren.

Riskhanteringen inom den digitala säkerheten är fortfarande svag inom den offentliga förvaltningen jämfört med dess övriga delområden. Situationen har förbättrats något, men endast cirka en fjärdedel av organisationerna gör det regelbundet och heltäckande, nästan en femtedel inte alls. Endast en tredjedel av objekten som ska skyddas och endast cirka hälften av de kritiska objekten har identifierats. Största delen berättar dock att de utvecklar sin riskhantering systematiskt och de flesta kommunicerar om riskerna med den digitala säkerheten till hela sin organisation.

DTYT / Reivo Juho (MDB)

23.1.2023

2 Allmänna synpunkter på riskutvecklingen

För hela enkätens del är medelvärdena för sannolikheten för och effekterna av alla olika risker inte en särskilt bra indikator på risknivån i sig, men ändringen i den kan anses återspegla den allmänna situationen. Ändringarna bör endast betraktas som riktgivande på grund av det ändrade sättet att genomföra enkäten och dess ändrade innehåll.

Medelvärdet för sannolikheten var 1,94, vilket var något högre än tidigare (2021: 1,88), vilket kan anses ingå i granskningens inexakthet. Betydelsen av denna obefintliga förändring framhävs när den jämförs med medelvärde för effekterna, 2,10, som dock steg med över en tiondel (2021: 1,98). I förhållande kan man se att betydelsen av effekterna öka mer.

2.1 Skillnaden mellan de olika respondenttyperna har framhävts

I grupperingen enligt olika organisationstyper kan man se olika utvecklingsriktningar. Kommunernas och social- och hälsovårdsaktörernas risker anses öka, eventuellt delvis på grund av de förändringar som välfärdsområdena medför. Men i enkäten framhävdes detta dock inte i sig som en uttrycklig risk. Poänggenomsnittet som SOTE-aktörerna fick i enkäten om helhetsbilden av den digitala säkerheten var klart bättre än i kommungruppen, vilket skiljer dessa två åt. Statsförvaltningens poängsättning i helhetsbilden av den digitala säkerheten var ännu bättre, vilket verkar återspeglas mer naturligt i risksynen.

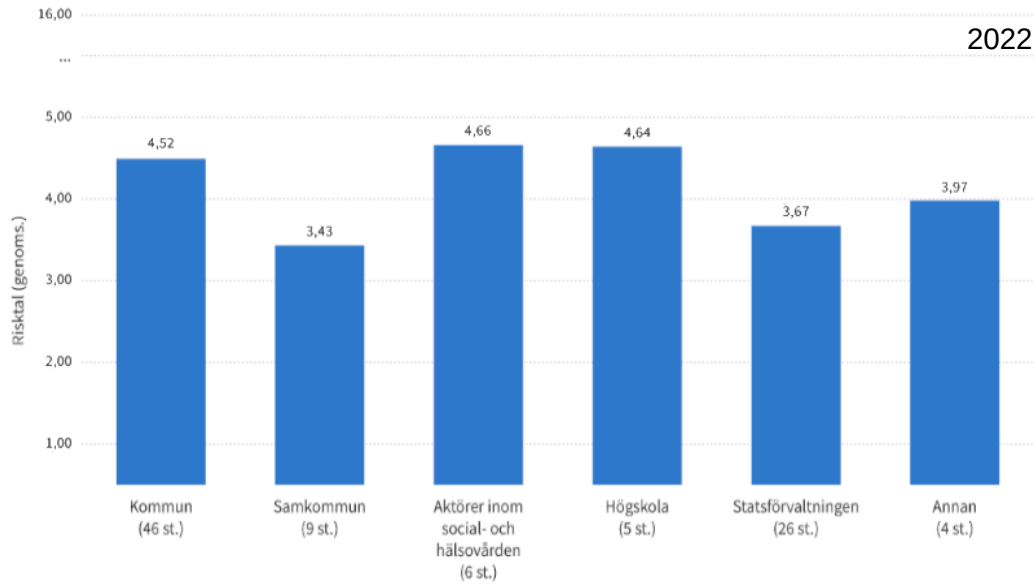
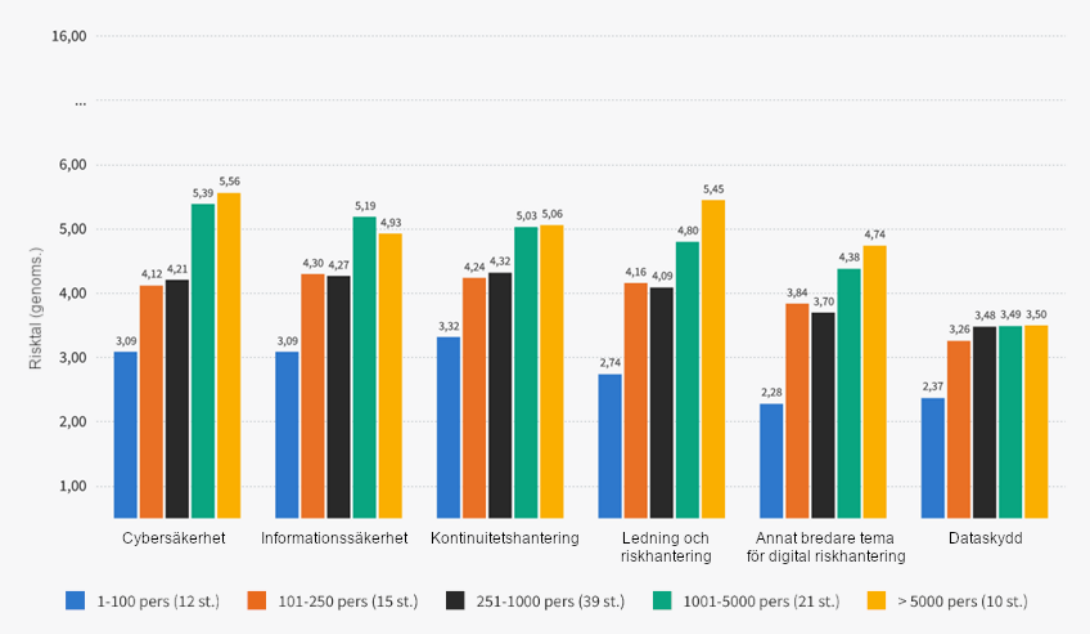


Bild 2b: Medelvärden för risktalen för 2022 enligt organisationstyp.

På basis av risktalen kan man se tydliga skillnader mellan respondenterna i olika storleksklasser. De små och medelstora respondenternas syn på riskerna var klart lägre än de stora (1001–5000 personer) och mycket stora (5000 personer) organisationernas. Här kan man mellan tidpunkterna för enkäterna se en ökning i den ovan beskrivna differentieringen. Storleken på de stora aktörernas risker kan som fenomen vara förknippat med en betydande ökning av komplexiteten i hanteringen av hot, frågor som ska skyddas och skyddsarrangemang.



Figur 3: Medelvärden för risktalen för de olika delområdena inom digital säkerhet enligt de svarande organisationernas storlek.

2.2 Den digitala säkerhetens ekonomiska riskeffekter anses öka

Riskernas effekter granskades genom att den delades in i tre delar: effekter för ekonomin, effekter för anseendet samt effekter för produktionen av tjänster [dvs. funktionsförmågan]. Av dessa är en betydande förändring att de ekonomiska effekterna accentueras jämfört med året innan, 1,76 (2021) steg till 1,88 (2022). I fråga om anseendet var förändringen endast något mindre, 2,10 steg till 2,18. Förändringen i fråga om produktionen av tjänster var minimal, 2,17 steg till 2,19.

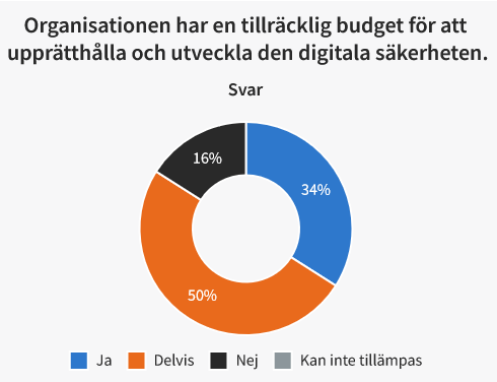
Eftersom man i granskningen av enkäten riktade blicken framåt, 1–3 år framåt, måste man dra slutsatsen att den digitala säkerhetens samband med ekonomin för organisationerna inom den offentliga förvaltningen kommer att få större betydelse i framtiden. Detta återspeglar utsikterna för det allmänna ekonomiska läget och den ökade förståelsen för de ökade ekonomiska kostnaderna om de digitala riskerna realiseras. Sannolikhetsnivån för risker förblir dock i genomsnitt på en ganska stabil nivå. Detta kan ses som förtroende för det finländska samhällets kompetens, beredskap och förmåga att möta utmaningar inom digital säkerhet, och uppfattningen har inte förändrats nämnvärt i och med de snabba förändringarna i hotbilderna inom säkerhetsmiljön. Det bör dock noteras att detta inte indikerar eventuella förändringar i enskilda risker eller riskområden som varierar.

Enligt de allmänna ekonomiska prognoserna[1] kommer kostnaderna att öka på olika sätt[2] och enligt indikatorerna kommer detta att pågå i två eller tre år. Överföringen av en risk som stöder sig på försäkringar, till exempel stora skador eller avbrott i verksamheten, kan stöta på problem, eftersom det på grund av marknaden inte kommer att finnas tillgång till kapital för återförsäkring som motsvarande de tidigare beloppen.

[1] https://vm.fi/sv/ekonomiska-prognoser
[2] https://www.enisa.europa.eu/news/cybersecurity-investments-in-the-eu-is-the-money-enough-to-meet-the-new-cybersecurity-standards

Detta kan både öka försäkringskostnaderna, eller till och med göra stora försäkringar omöjliga. För att minska den skärpta finansieringsrisken kan det uppstå krav i anslutning till digitala risker, att hanteringsåtgärderna och kontrollerna i anslutning till dem har skötts på behörigt sätt och att detta kan påvisas till exempel genom standardenlighet. Försäkringarna har liten betydelse inom den offentliga förvaltningen, men de kan också framkomma indirekt i anslutning till den digitala säkerheten, till exempel via serviceproducenter. Detta kan orsaka extra påfrestning, men i ett bredare perspektiv kan tilläggskraven också betraktas som en positiv bieffekt i utvecklingen av den digitala säkerheten.

I enkäten om helhetsbilden av den digitala säkerheten kan man se tecken på brister i den ekonomiska resursfördelningen inom den offentliga förvaltningen för närvarande. Hälften av respondenterna ansåg att budgeteringen till vissa delar var bristfällig och mer än var tionde ansåg att budgeteringen var klart otillräcklig. Detta är oroväckande eftersom de förberedande åtgärderna i det långa loppet är mer ekonomiska och även förebygger andra effekter. Naturligtvis handlar det också om prioriteringar inom digital säkerhet, digital verksamhet men också inom organisationers totala budgetar. Mellan dessa borde man göra tillräckliga inbördes jämförelser som en del av riskhanteringen, så att inriktningen är motiverad och den digitala säkerheten prioriteras tillräckligt. Även olika sätt att effektivisera resursanvändningen, till exempel genom gemensam användning eller upphandling, bör övervägas.



Figur 6: Situationen för den digitala säkerheten inom den offentliga förvaltningen i fråga om budgetering.

2.3 Delområdesspecifika synpunkter

Vid analysen av svaren i granskningen användes olika klassificeringar inom vilka svaren fungerar som indikatorer för olika rubriker. Rubriker som står i proportion till varandra hjälper till att ensamt och separat identifiera mer omfattande strategiska teman till vilka man eventuellt borde rikta särskild uppmärksamhet. Detta är betydelsefullt, eftersom hanteringsåtgärderna sällan är helt symmetriska i förhållande till de upplevda hoten och omfattande åtgärder kan riktas effektivare mot utmaningar som riktar sig till samma område. För att genomföra de praktiska hanteringsåtgärderna kan dessa synpunkter på strategisk nivå exempelvis ändras till delområden i ISO27001- eller NISC CSF-modellerna.

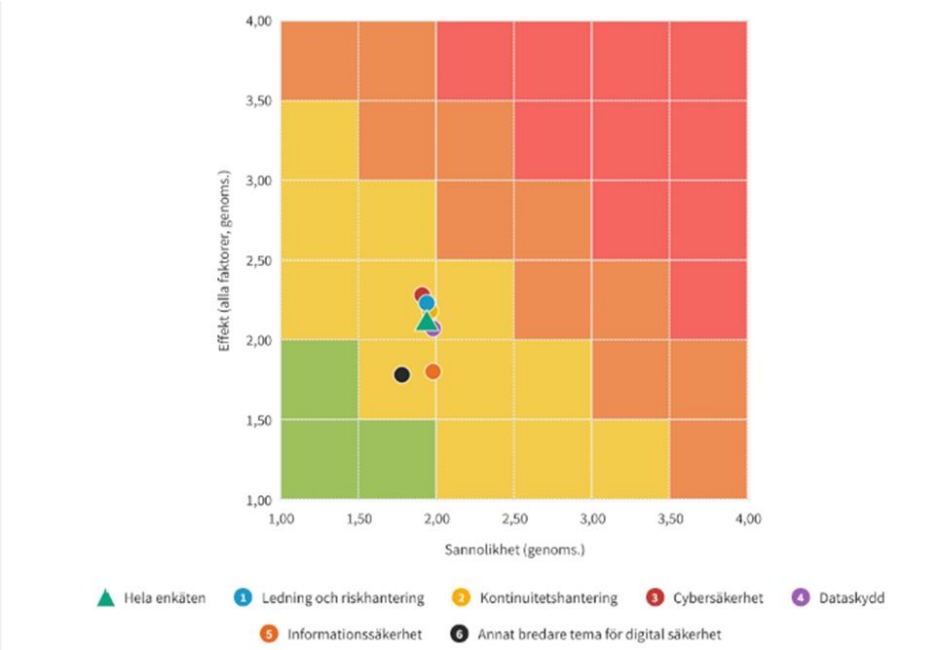
Klassificeringar, och de rubriker som användes för att gruppera dem var:

- Organisation for Economic Co-operation and Development, dvs. OECD (*Nationell och internationell säkerhet, Lagövervakning, Ekonomisk och samhällelig välfärd*)
- World Economic Forum eller WEF (*Skadlig teknisk utveckling, Allvarlig störning i den digitala infrastrukturen, Försummelse av den digitala säkerheten, Koncentration av digitala resurser, Misslyckad styrning av den digitala säkerheten, Ojämlikhet i den digitala verksamhetsmiljön*)

- Modell för hantering av digital säkerhet (*Ledning och riskhantering, Kontinuitetshantering, Cybersäkerhet, Dataskydd, Informationssäkerhet, Annat bredare tema för digital säkerhet*)

När man granskar trender och förändringar jämfört med föregående år i varje klassificering och även beaktar effekternas olika delområden kan man observera några enskilda avvikelser. Av betydelse för dessa förändringar är de rubrikområden i klassificeringarna som skiljer sig från varandra och som beter sig olika. Vid tolkningen av dem ska man dock beakta att enkäterna för 2021 och 2022 inte var helt identiska och att nya riskteman lades till klasserna.

När man granskar klassificeringen av delområdena inom digital säkerhet är det anmärkningsvärt att riskerna som tangerar dataskyddet anses vara betydligt mindre tillsammans med bredare ämnen inom digital säkerhet. Vid en närmare granskning av dessa två punkter kan man se att de indikatorer som används i dem beskriver flera sekundära hot, vars effekter inte är direkta, vilket kan påverka uppfattningarna om dem. I många andra risker kan man också identifiera att följderna, om de realiseras, ofta skulle leda till att dataskyddet äventyras. Å andra sidan, som ett noggrant reglerat delområde, innebär iakttagandet av dataskyddskraven att riskerna är under kontroll, varvid de inte heller anses utvecklas negativt. Detta stöds av organisationers svar som kartlade den digitala säkerhetens tillstånd, där delområdet dataskydd fick de högsta genomsnittspoängen.



Figur 7: Riskernas placering grupperade enligt den digitala säkerhetens klasser.