



MYNDIGHETEN FÖR
DIGITALISERING OCH
BEFOLKNINGSDATA

VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation

VAHTI God Praxis stödmaterial

15.11.2022

15.11.2022

VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation

Detta dokument är en presentation av VAHTI-ordlistan om riskhantering och relaterade ämnen som stöder riskhanteringen, särskilt med hänsyn till riskkommunikation. Ordlistan och det material som beskriver ämnet har producerats inom ramen för projektet JUDO vid Myndigheten för digitalisering och befolkningsdata som en del av stödmaterialiet VAHTI God Praxis¹. De egentliga termerna som läggs fram i detta dokument publiceras elektroniskt i Interoperabilitetsplattformens² termbank på adressen <https://sanastot.suomi.fi/> (FI, SV, EN). Ordlistan är öppen för alla. Den kan tillämpas i alla aspekter av säkerheten i den digitala verksamhetsmiljön samt för de flesta andra användnings-ändamål som tangerar riskhantering.

Ordlistan förenar flera olika aktörer och verksamhetsområden på ett gemensamt språk. För att stödja detta är detta presentationsdokument avsett att öppna fler begrepp, mer tillhörande funktioner och processer än vanligt. Målet med dokumentet är att göra det lättare att tillägna sig, gå igenom och uppfatta ordlistan som en starkt sammanlänkad helhet i stället för enskilda uttryck. Den utgör en del av en systematisk struktur. Presentationen riktar sig särskilt till sakkunniga, men också för dem som bekantar sig med ämnet och som arbetar till exempel med digital säkerhet, cybersäkerhet, informationssäkerhet, dataskydd, kontinuitetshantering, riskhantering, övergripande säkerhet, försörjningsberedskap, verksamhetsstyrning, ledning, utveckling av förvaltningen, kommunikation, intern revision, informationsförvaltning, projektverksamhet, datasystemutveckling eller annat motsvarande inom företag, samfund eller den offentliga förvaltningen.

Användarna av ordlistan rekommenderas i sina egna dokument i första hand hänvisa till VAHTI-riskhanteringsordlistan samt länka till tjänsten sanastot.suomi.fi för att en aktuell och heltäckande terminologi ska finnas till förfogande. Hänvisningar till detta dokument och dess innehåll rekommenderas när dokumentet används för utbildningsändamål eller som bakgrundsmaterial. Första version publicerades 9.6.2022. Fixad version 15.11.2022 på finska (<https://dvv.fi/digiturvajulkaisut>) och på svenska (<https://dvv.fi/sv/publikationer-om-digital-sakerhet>).

¹ <https://dvv.fi/sv/vahti-natverket>

² <https://dvv.fi/sv/interoperabilitetsplattformen>

15.11.2022

Innehållsförteckning

1	Inledning	4
2	Hur ordlistan togs fram och hur den kommer att utvecklas	6
2.1	Projektet	6
2.2	Förord från terminologen	8
2.3	Om utvecklingen av begreppen kring säkerheten i den digitala verksamhetsmiljön	9
3	Utnyttjande av kommunikation och språk i olika delar av riskhanteringen	11
4	Ämnesområde: Begrepp på överordnad nivå	13
4.1	Digital verksamhetsmiljö	16
4.2	Risk för den digitala verksamheten	16
4.3	Digital säkerhet	16
4.4	Cybersäkerhet	17
4.5	Informationssäkerhet	17
5	Ämnesområde: När något händer	18
5.1	Incidens	18
5.2	Avvikelse	19
5.3	Störning	19
5.4	Attack	19
5.5	Attackens avsedda mål	19
5.6	Kontinuitetshantering	20
6	Ämnesområde: Uppkomst av och förståelse för risker	21
6.1	Osäkerhet	23
6.2	Hot	23
6.3	Sårbarhet	24
6.4	Svaghet	24
6.5	Möjlighet	24
6.6	Risk	25
6.7	Riskuppfattning	25
6.8	Förvrängning	25
6.9	Riskkriterier	26
6.10	Hot som undviker riskens gränsvärden	26
6.11	Riskens livscykel	26
7	Ämnesområde: Riskbedömning	27
7.1	Preliminär bedömning	30
7.2	Preciserande bedömning	30
7.3	Ny bedömning	30
7.4	Riskbedömningsprocess	30
7.5	Verktyg för riskbedömningsprocessen	31
7.6	Bedömning av risker	31
7.7	Riskbedömning	31
7.8	Analys av risker	32
7.9	Risikanalys	32
7.10	Klassificering av risker	32
8	Ämnesområde: Ansvar i riskhanteringen	34
8.1	Ansvarsfull riskhantering	35
8.2	Deltagande i riskhantering	36
8.3	Transparens inom riskhantering	36
9	Ämnesområde: Informationsdelning och kommunikation	37
9.1	Kommunikation och informationsutbyte om risker	38
9.2	Riskrapportering	38
9.3	Riskuppgifter	38



15.11.2022

9.4	Riskregister	38
9.5	Hotuppgifter	39
9.6	Hotprofil	39
10	Ämnesområde: Riskhanteringsstrukturer	40
10.1	Riskhanteringsens ramar	41
10.2	Riskhanteringssystem	41
10.3	Riskhanteringsprinciper	41
10.4	Riskhanteringspolitik	41
10.5	Riskhanteringsverktyg	42
11	Ämnesområde: Uppföljning och lägesbild	43
11.1	Riskuppföljning	44
11.2	Lägesbild över risker	44
11.3	Uppföljning av riskhanteringen	44
11.4	Lägesbild över riskhanteringen	44
11.5	Uppföljning av riskhanteringssystemet	45
11.6	Lägesbild över riskhanteringssystemet	45
12	Ämnesområde: Riskhanteringskontexter och nivåmodeller	46
12.1	Organisationskontext	49
12.2	Informationshanteringsenhet	49
12.3	Bedömningsnivå	50
12.4	Hanteringsnivå	50
12.5	Strategisk nivå	50
12.6	Koordineringsnivå	50
12.7	Operativ nivå	51
13	Ämnesområde: Betydelser av riskhantering och risker	52
13.1	Framförhållning	54
13.2	Riskmedvetet beslutsfattande	54
13.3	Kvarstående risk	54
13.4	Riskbärkraft	54
13.5	Kritiskhet	55
13.6	Värde för oförverkligad effekt	55
14	Ämnesområde: Egenskaper hos riskens uppbyggnad	56
14.1	Direkt risk	57
14.2	Indirekt risk	57
14.3	Överförd risk	57
14.4	Risk med nätverkslik spridning	57
14.5	Kumulativ risk	57
15	Ämnesområde: Riskpåverkan	58
15.1	Kontroll	59
15.2	Planerad att ha få risker	59
15.3	Operativ användbarhet	60
16	Index	61
16.1	Suomi	61
16.2	Svenska	63
16.3	English	65
Bilaga 1: Allmän definition av helheten för digital säkerhet		68
Bilaga 2: Riskhanteringstermer i EU:s kommande NIS2-direktiv		71

15.11.2022

1 Inledning

Inom ämnet riskhantering har det saknats ett gemensamt språk eller så har det inte använts på ett enhetligt sätt mellan olika organisationer och sakkunniga, vilket har syns både i interna och externa samarbeten. Olika aktörer kan närma sig hot och risker via olika handlingslinjer och -nivåer, men alla dessa aspekter borde kunna sammanföras i den övergripande strukturen för digital säkerhet och i den övergripande riskhanteringen i organisationerna. Ett gemensamt språk är en förutsättning för att kunna fungera tillsammans. Rätt sätt att formulera det som behandlas är nyckeln till ett effektivt utnyttjande av riskhanteringen som stöd för ledningen och styrningen av verksamheten – till och med en garanti för organisationens framgång.

De gemensamma definitionerna har redan under en tid orsakat problem för olika aktörer och att lösa dem har varit en del av bakgrundsarbetet till denna ordlista. Tidigare har det funnits ordlistor för riskhantering via standarder, men i dem är uttrycken på en ganska abstrakt nivå och de begränsas till exempel till vissa delar av processen. Utanför dem finns det dock många uttryck och diskussioner om riskerna och hanteringen av dem till exempel i gränssnitt där standardernas strukturer är kopplade till verksamheten eller andra strukturer som styr den – det vill säga hur vardagliga frågor omvandlas till en del av riskhanteringen.

När man granskat termerna har det också tydligt framgått att vissa uttryck har haft både flera liknande officiella och inofficiella enskilda definitioner och ännu fler diskussioner av engångskaraktär och talspråkliga tillämpningar av dem. Detta beror delvis på att de har vuxit fram under årtiondenas lopp, medan världen och digitaliseringen har utvecklats tekniskt och funktionellt. Dessutom har de flesta termer utanför standarderna aldrig skapats systematiskt och byggts upp i förhållande till varandra som en del av en systematisk helhet. Man måste alltså också uppdatera språket, och på samma sätt borde språkets användare uppdatera sina kunskaper och ordförråd för att inte behöva avvärja moderna hot mot med uppfattningar från tidigare årtionden.

Systematiken och de processer som digitaliseringen bygger på måste återspeglas även i vokabulären. Enhetlighet och logik i användningen bäddar också för en bättre automatisk behandling och en bättre kvalitet. I denna ordlista har man strävat efter att anpassa helheten, men det bör märkas att anpassningen trots allt endast sker i begränsad omfattning, i synnerhet när riskhanteringen och den digitala säkerheten korsar varandra. Termerna i ordlistan är således inget egentligt allmänspråk. Dessutom kan det hända att definitionerna av uttrycken klarnar först när man granskar de kompletterande anmärkningarna, men ändå måste man alltid göra tolkningar av definitionerna utifrån den egna kontexten. Detta är normalt eftersom man inte kan uppnå fullständig precision och det skulle göra det opraktiskt och tungt att använda ordlistan – här har man strävat efter balans.

Denna ordlista borde vara en bra utgångspunkt för förankringen av gemensamma uppfattningar, även om den endast omfattar cirka 70 begrepp. Om man räknar med synonymer och hänvisningar är antalet redan cirka 120. En sådan fast punkt ger också möjlighet att vid behov och på goda grunder avvika från dessa definitioner, vilket är viktigt i takt med att kontexterna och behoven förändras. Den fasta punkten gäller dock fortfarande, eftersom det nu är möjligt att berätta var man avviker från den, hur och varför, varvid sambandet och begripligheten bevaras. På ett allmänt plan ska riskhanteringen beskriva den verklighet där den utförs – att definiera den är

15.11.2022

en av de första åtgärderna i processen. Att påtvinga verkligheten olämpliga uttryck och strukturer kan snedvrída eller till och med förblinda oss från vad som händer omkring oss, så att vi inte märker riskerna förrän det är för sent.

Ordlistan strävar efter att vara neutral bland annat i fråga om perspektiv, teknik, verktyg och användare, eftersom den är avsedd för alla, inte bara för den offentliga förvaltningen. Detta är viktigt eftersom kretsen av aktörer som är kopplade till varandra är mångfacetterad och moderna digitala risker (liksom andra risker) överförs och påverkar via dessa kopplingar. Det har dock tidvis varit svårt att sammanställa ordlistan så att den lämpar sig för alla användare, eftersom man har strävat efter att utöver de olika segmenten av aktörer även beakta verksamheten på olika nivåer (som man strävar efter att öppna med nivåmodellen). Dessutom har det varit en utmaning att riskhantering behövs och krävs på lite olika sätt för olika ändamål, såsom skydd av ärenden och personer, ledningens behov av information och ekonomisk effektivitet. Att maximera och rikta begränsade resurser på bästa möjliga sätt är viktigt för att man ska kunna skapa en digital säkerhet om och om igen.

Smidigt samarbete, den systemiska interoperabiliteten och flexibiliteten i den föränderliga miljön bidrar till framgång när man ställs inför framtida utmaningar. Det kan antas att ett mer systemiskt språk även stöder en ständigt mer systemisk och automatiserad verksamhet, såsom mer avancerade verktyg för digital säkerhet och riskhantering. Enbart överföring av information medför dock ingen förändring, utan parallellt behövs (som en del av en standardiserad process) kommunikation om risker och riskhantering, till vilken ordlistan också hör. Med tanke på såväl den digitala säkerheten som riskhanteringen är det viktigt att kommunicera kring hot, utmaningar och metoder för att hantera dessa på rätt sätt. De uttryck vi väljer säger redan i sig hur vi uppfattar saker, hur de borde uppfattas eller om vi överhuvudtaget uppfattar dem på rätt sätt. Ibland måste man vara mycket noggrann och kunna dra gränsen mellan olika saker. Vad är acceptabelt och vad är det inte? Vad hör till vad? Vår förmåga att vara tydlig och exakt ökar trovärdigheten och förtroendet.

Språket är ett verktyg för ledarskap, men inte endast för chefer. När man kommunicerar (oberoende av riktning) mellan olika hierarkinivåer bör tanken placeras i en ny kontext och omvandlas till verksamhet. Förstår man vardera partens behov vid en förflyttning från en trappa till en annan eller lämnar man tolkningen åt slumpen? Även en bra tanke och viktig säkerhetsinformation kan undermineras av ett dåligt uttryck. Ett gemensamt språk och gemensamma termer bidrar till både säkerheten och känslan av trygghet. Ordlistan som presenteras i detta stödmaterial ger alla tillgång till ett förbättrat verktyg – ett gemensamt språk om riskhantering i vår digitala verksamhetsmiljö.

15.11.2022

2 Hur ordlistan togs fram och hur den kommer att utvecklas

Projektet för att sammanställa en ordlista om riskhantering i digital säkerhet genomfördes inom ramen för projektet JUDO³ vid Myndigheten för digitalisering och befolkningsdata och är en del av utvecklingen av riskhanteringen inom digital säkerhet som ingår i genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)⁴. Innehållet i projektet för att sammanställa en ordlista har tagits upp till behandling i VAHTI, som är ett samarbets-, berednings- och samordningsorgan på bred bas för organisationer som svarar för utvecklingen och styrningen av den digitala säkerheten inom den offentliga förvaltningen. Detta dokument publiceras i enlighet med processen för stödmaterial VAHTI God Praxis. Processen omfattar möjligheten att uppdatera detta dokument och ordlistan efter behov.

Ordlistan publiceras för fritt bruk i Interoperabilitetsplattformens⁵ terminologidatabas på adressen <https://sanastot.suomi.fi/>. Med verktyget Terminologiska ordlistor kompilerar och uppdaterar man gemensamma terminologiska ordlistor och begrepp inom den offentliga förvaltningen.

2.1 Projektet

Projektet för att sammanställa ordlistan genomfördes i juni–december 2021. Det föregicks av ett beredningsskede och vintern 2022 utarbetades presentationsmaterialet och publikationen. Den förvalda ordlistan baserade sig på flera ordlistor inom branschen, på ett tidigare projekt för identifiering av riskhanteringstermer och andra källor. Ur projektets synvinkel utgjordes utgångspunkten av den digitala säkerheten med delområden, kunskapsledning och systematik, riskhantering som process och kommunikation om den, kommunikation om risker och förtydligande av deras verkningssmekanismer, en digital verksamhetsmiljö, upplevda problem med uttryck i fråga om de nuvarande riskerna samt eventuella framtida behov av strategi- och prognostiseringsarbeten. Arbetsgruppen valde ut cirka 200 kandidater i förväg i olika källor och bland cirka 3000 termer i tidigare ordlistor. Av kandidaterna valdes cirka 60 termer som ansågs vara centrala med tanke på ämnesområdet för fortsatt behandling.

Under projektets gång lades termer till och togs bort allteftersom förståelsen för uppkomsten för en systemisk struktur ökade. Ett betydande antal risktyper och beskrivningar av särskilda egenskaper uteslöts, eftersom ett heltäckande resultat inte hade kunnat uppnås inom ramen för detta projekt. I urvalet ville man ur projektets synvinkel också säkerställa att sådana uttryck inkluderas som svarar på behoven att formulera hanteringen av moderna utmaningar i riskhanteringen. Dessutom ingår uttryck som möjliggör gränsdragning mellan termer som lätt förväxlas. I definitionen säkerställdes i synnerhet kompatibiliteten med standarden för riskhanteringsprocessen i ISO 31000-serien, varvid interoperabiliteten förverkligas också till exempel med standarden för hantering av informationssäkerhet i ISO 27000-serien.

I definitionen av termerna deltog förutom projektets arbetsgrupp en stor grupp experter från olika branscher samt vissa specialister inom sitt eget område. Expertgruppen sammanträdde sju gånger för att behandla termerna och dessutom användes

³ <https://dvv.fi/sv/projekten>

⁴ <http://urn.fi/URN:ISBN:978-952-367-284-0>

⁵ <https://dvv.fi/sv/interoperabilitetsplattformen>

15.11.2022

elektroniska formulär för kommentarer mellan mötena. Den första versionen av ordlistan kommenteras separat av hela arbetsgruppen, en utvidgad expertgrupp samt VAHTI-experten. Under den senaste kommentarsomgången lades cirka 20 observationer fram, på basis av vilka kompletteringar gjordes, främst i anmärkningarna. Vidare gjordes bifallande bedömning av helhetens kvalitet och lämplighet att tas i bruk i stor utsträckning inom och utanför den offentliga förvaltningen. Efter vårens offentliga kommentarer lades några förord till, preciserades en definition (möjlighet) och kompletterades enskilda observationer samt gjordes språkvård. Samtidigt blev ordlistans betydelse klarare i de öppna diskussionerna.

Detta presentationsdokument är en del av stödmaterialet VAHTI God Praxis. I dokumentet ges vägledande och kompletterande information om hur ordlistan tillämpas i praktiken, både i processer och inom kommunikation. Syftet med stödmaterialet är att hjälpa till att förstå hur termerna anknyter till varandra och vad de påverkar. Riskhanteringen ska inte vara en separat och skild del av verksamheten, utan snarare en knutpunkt som förenar flera funktioner.

Projektets arbets- och expertgrupp har bestått av:

Juho Reivo, projektchef, Myndigheten för digitalisering och befolkningsdata
Lassi Väisänen, projektsekreterare, GRC Partners
Kimmo Rousku, VAHTI-generalsekreterare, Myndigheten för digitalisering och befolkningsdata
Esko Mustonen, controllerfunktionen, finansministeriet
Antti Nyqvist, Digipooli, Teknologiindustrin r.f.
Markku Rajamäki, Finlands Näringsliv
Ville Knuutila, Folkpensionsanstalten
Jari Ylikoski, Kommunförbundet
Julia Fomin, Cybersäkerhetscentret, Traficom
Pasi Koljonen, Försvarsmakten
Juhani Kuparinen, Dataombudsmannens byrå
Pasi Eronen, Säkerhetskommittén (till 10.8.)
Alexander Zilliacus, Säkerhetskommittén (från 10.8.)
Ville Autero, arbets- och näringsministeriet
Sanna Eronen, terminolog, Lingsoft Oy
Pia Seppänen, serviceansvarig, Lingsoft Oy

Övriga experter som deltagit i olika skeden av bearbetningen:

Irina Kudasheva, terminolog, Lingsoft Oy
Armi Helenius, Myndigheten för digitalisering och befolkningsdata
Joonas Aitonurmi, Myndigheten för digitalisering och befolkningsdata
Kirsi Janhunen, Myndigheten för digitalisering och befolkningsdata
Erja Kinnunen, Myndigheten för digitalisering och befolkningsdata
Hanna Heikkinen, Myndigheten för digitalisering och befolkningsdata
Juha Kirves, Myndigheten för digitalisering och befolkningsdata
Tuomas Pelttari, Myndigheten för digitalisering och befolkningsdata
Laura Penttilä, Myndigheten för digitalisering och befolkningsdata
Heta Aho, Myndigheten för digitalisering och befolkningsdata
Tuula Seppo, Myndigheten för digitalisering och befolkningsdata
Rosa Hyvärinen, Myndigheten för digitalisering och befolkningsdata
Marième Korhonen, kommunikationsministeriet

15.11.2022

Ritva Kiiski, Kotka stad
VAHTI-ledningsgruppen
VAHTI-arbetsgruppen för utveckling av riskhanteringen och smågruppen för riskprocessen (2021)

2.2 Förord från terminologen

I denna ordlista definieras de centrala begreppen kring digital säkerhet och riskhantering. Begreppen har valts omsorgsfullt så att definitionen av dem stöder kommunikation och utbildning som berör hantering av digitala risker. Ämnesområdet är dock omfattande och utanför avgränsningen har man redan identifierat begrepp som är centrala ur olika synvinklar för ett eventuellt fortsatt arbete.

Vid definitionen av begreppen har man följt ett standardiserat arbetssätt för terminologi (arbetssättet beskrivs bl.a. i standarden ISO 704: 2009). Det väsentliga i arbetssättet är ett begreppssystem som fungerar som utgångspunkt: de centrala dragen i de relevanta begreppen och relationerna mellan dem identifieras, och utifrån detta utarbetas sinsemellan fungerande definitioner och man undviker t.ex. korshänvisning.

Som utgångspunkt för terminologin har man i enlighet med interoperabilitetsmetoden använt tidigare ordlistor och eftersträvat förenlighet särskilt med Ordlista om cybersäkerhet (TSK 52, 2018), Ordlista om övergripande säkerhet (TSK 50, 2017) och SFS-publikationer som behandlar ämnet (SFS-OPAS 73: 2011, SFS-ISO 31000: 2018 och SFS-EN ISO/IEC 27000: 2020). Tidigare definitioner av begrepp har citerats i ordlistan som sådana varje gång det varit möjligt med hänsyn till ordlistans begreppssystem, användningsändamål och mål. I ordlistans texter nämns vissa termer som har avgränsats utanför detta arbete och i fråga om dem har man säkerställt att definitioner som publicerats i relevanta källor är förenliga med ordlistan.

Man har strävat efter att definiera nya begrepp på en så allmän nivå som möjligt, så att definitionerna kan användas på nytt i andra sammanhang i enlighet med interoperabilitetsprincipen. Begreppens termer och definitioner har utvärderats i workshoppar tillsammans med en expertgrupp ur olika synvinklar. Dessutom har man från flera håll samlat in skriftlig respons för att ordlistan så väl som möjligt ska motsvara olika intressentgruppers synsätt och behov.

I den terminologiska ordlistan ges vid behov tilläggsinformation om begreppen i form av en anmärkning. Uppgifterna i anmärkningen kan gälla termen, definitionen eller något annat som är väsentligt med tanke på ordlistans användningsändamål. I synnerhet i denna ordlista innehåller anmärkningen oftast information som gör det lättare att tolka definitionen och uppfatta begreppets kontext. Dessutom har anmärkningarna i denna ordlista lyft fram skillnader och likheter jämfört med definitioner i andra källor. I synnerhet branschövergripande begrepp som är abstrakta till sin betydelse är ofta besvärliga för dem som använder ordlistor. Därför har ett syfte med anmärkningarna varit att säkerställa att informationen förmedlas på avsett sätt. En djup förståelse av terminologin kräver dock också kännedom om ämnesområdet eller tilläggsutbildning.

Ordlistan har utarbetats på finska, men bakgrundsinformation har också samlats in från källor på engelska och svenska. För en del av begreppen har

15.11.2022

översättningsmotsvarigheter identifierats redan i takt med att arbetet med ordlistan framskridit, och i den slutliga publikationen finns term motsvarigheter för alla begrepp på svenska och engelska.

2.3 Om utvecklingen av begreppen kring säkerheten i den digitala verksamhetsmiljön

Olika definitioner av delområdena inom digital säkerhet, dvs. diskurser i olika ämnen, fastställs kontinuerligt – i praktiken i varje diskussion. Det finns många definitioner inom varje ämne, de genomgår en ständig förändring, de kan inte klämmas ihop till bara några gemensamma delar, och de överlappar delvis olika ämnen. Olika aktörer försöker också tidvis påverka uppkomsten av definitionerna direkt och indirekt, bland annat genom reglering och standarder – eller kommunikationskampanjer (från marknadsföring till hybridpåverkan). Det är alltså inte likgiltigt vilka betydelser och perspektiv vi inkluderar i vårt tal. De största formgivarna är dock de verksamhetssätt som massan förändrat under tidens gång och vars innehåll slutligen ger taktermerna deras innebörd, även om man försöker styra utvecklingen med taktermerna. Förändringskrafter finns alltså både på hög och låg nivå och diskurser kan identifieras till fullo först i efterhand.

Det är svårt att förutse hur termerna kommer att utvecklas. Till exempel virus definierade informationssäkerhetens innehåll på 1990-talet och cyber populariserades som uttryck i dystopibilderna i sci-fi-litteraturen redan betydligt tidigare. Det faktum att begreppen kring digital säkerhet är internationella präglar också detta. I synnerhet användningen av engelska som allmänspråk hos aktörer i olika länder orsakar huvudbry i överföringen av betydelser. Det som här avses med "cyber" är inte exakt samma sak som "cyber" hos aktörer i totalt andra länder. Som ett nytt begrepp på finska har man på senare tid lyft fram "informationstrygghet" ["informaatioturvallisuus"] (bl.a. nyhetsinnehållens tillförlitlighet). Begreppet har tidigare behandlats under cybersäkerhet, och den direkta översättningen (även eng. information security) förenas mer allmänt med informationssäkerhet.

Utöver dessa används talspråk, där man ännu mer bekymmerslöst inkluderar olika saker i definitionerna. Det finns en risk för att förståeligheten lider, att man trampar i gränslöshetens trask och att olika saker formas till en vag samling som man inte får grepp om. Dessutom kan de som vill ha gemensam betydelse börja skapa nya uttryck sinsemellan, varvid det uppstår ännu fler termer, eftersom de gamla mycket sällan försvinner helt. Att de centrala termerna drabbas av "inflation", fördunkling, utgör en risk för effektiv kommunikation om den digitala säkerheten och dess delområden, och därför bör uppmärksamhet fästas vid precisionen och en logisk användning av uttrycken.

Riskerna och åtgärderna för att hantera dem kommer på motsvarande sätt att förändras i och med förändringarna i den digitala miljön. I framtiden, när den digitala verksamhetsmiljön i allt högre grad börjar vara en del av vår övriga verksamhetsmiljö, borde det inte vara långsökt att tänka sig att synpunkterna i den verkliga världen till exempel om miljövård överförs till ett digitalt område under de kommande decennierna. Dessa är delvis frågor som i stället för kommersiella lagbundenheter skulle kräva en demokratisk diskussion, såsom i vilken mån man kan röra sig med



15.11.2022

"allmansrätten" i öppna data och i vilken mån allt inhägnas bakom murar, vad som bevaras som historiska minnen och vad man vågar bevara eftersom oföränderlighet skulle innebära att även risken kvarstår. Och eftersom det i slutändan är fråga om en av människans byggd miljö måste vi också fundera på hur den kan göras säker, hurdan infrastruktur som ska skyddas i den digitala naturen och vilka naturresurser som kan utnyttjas, i synnerhet om webbens strukturer och förbindelser försvinner alltmer från vårt synfält. Eventuella differentieringar av ekosystemen som sker av politiska och kommersiella skäl (som tidigare kallades "balkanisering" av näten) kan vara en betydande förändringsfaktor även för säkerheten. Eller borde man i stället börja bedöma sådana risker som står utanför digitaliseringen. Språket ska följa med och vi måste uppdatera våra egna kunskaper.

15.11.2022

3 Utnyttjande av kommunikation och språk i olika delar av riskhanteringen

En viktig del av riskhanteringsprocessen är kommunikationen i processens olika skeden. Ur den synvinkeln sker ingen riskhantering om man inte är medveten om den och den information den producerar. Hela processen kan anses vara en högklassig process för riskkommunikation. Med tydlig och rätt formulerad information stöder man kunskapsbaserat beslutsfattande och ger hela organisationen en uppfattning om hur verksamheten ska ske i en tillförlitlig riktning. Kommunikation och språk är således strategiskt viktiga för organisationen.

Säkerhetskultur skapas bland annat genom att man uppmuntrar till att lyfta fram missförhållanden. Denna kollektiva behandling i praktiken av riskidentifiering och svaga signaler får inte släta över detaljer som inte fungerar, såsom öppna datakommunikationsportar eller motsvarande sårbarheter, utan borde uppmuntra och till och med belöna för att missförhållanden lyfts fram. Responsen borde leda till konkreta åtgärder för att det ska anses meningsfullt att ge den. Ofta är det dock viktigast att få veta att responsen har beaktats och att det inte var onödigt att ge den. Att bygga upp riskhanteringssystemet som helhet börjar med små saker av den här typen.

Riskhanteringen, såsom den digitala säkerheten, borde sträcka ut sig överallt, även till vår fritid och vår vardag, också hemma. I kommunikationen om risker bör man fästa uppmärksamhet vid att kommunikationen behandlar sådant som hör till varje människas vardag. Riskhantering innebär alltså att man på morgonen tar med sig ett paraply eller byter vinterdäck i tid, på samma sätt som man stannar upp en stund för att fundera på vad som kan gå snett eller störa det egna arbetet. Men för detta behövs en impuls, en påminnelse, ett incitament, anvisningar, en uppmaning, en varning och andra liknande budskap som stöder riskhanteringen. Ju snabbare och tajtare tidtabellerna är eller ju nyare och mer avvikande verksamheten är, desto högre är den tröskel som ska överskridas och desto mer direkt kommunikation och stöd behövs. Även de organisationer där riskhanteringen är en etablerad del av arbetskulturen behöver påminnelser om att upprätthålla och förbättra kvaliteten, förnya sig och undvika att fastna i vanor.

En utgångspunkt i kommunikationen, såsom i utbildningen, är att gå igenom saker punkt för punkt, ämne för ämne eller term för term. Ibland är dessa startskott som klargör detaljerna och samtidigt ger uppslag till mer omfattande diskussioner. Om man inte helt uppfattar var det förekommer utmaningar kan det vara bra att börja med begrepp som är nära förknippade med ämnet och se vilka saker och problemegenskaper som begränsas inom och utanför dem.

Det handlar inte bara om att genomföra processen, utan också om rätt attityd och att skapa den säkerhetskultur som nämndes tidigare och som till stor del bygger på ledning och kommunikation. Såväl experternas som direktörernas ord och exempel står i centrum. Det bör alltså beaktas att man även i riskhanteringen ska kommunicera både ur ett administrativt perspektiv och ur ett ledarskapsperspektiv. Dessutom måste man kunna rikta innehållet, till exempel via den nivåmodell som presenteras i denna ordlista, till ledningen, sakkunniga inom organisationen samt till den operativa nivån, till var och en av dessa i form av budskap som har betydelse för strategin, koordineringen och den operativa verksamheten. Riskhantering är det forum där (bland annat) säkerheten och den övriga verksamheten borde mötas och diskuteras.

15.11.2022

Med tanke på den processrelaterade kommunikationen om riskhanteringen, såsom lägesöversikterna och påminnelserna – samt själva riskerna och mer allmänt om hoten – borde kommunikationen framstå allt tydligare som en planerad helhet. Genom att använda en årsklocka eller en tabell kan man när som helst planera vad som ska kommuniceras och kontrollera att kommunikationen täcker alla väsentliga detaljer. I planeringen av kommunikationen beaktas också bland annat vem som kommunicerar, hur och i vilka kanaler samt vilken annan kommunikation om digital säkerhet (eller annat) som planeras. Liksom i bra planer överlag har det visserligen riskbaserat lämnats utrymme i kommunikationsplanen med tanke på eventuella avvikelser.

I den strategiska riskhanteringen ingår strategiska mål och risker äventyrar genomförandet av strategierna. Förståelsen för detta bör kommuniceras så att det handlar om att trygga verksamhetens kontinuitet i olika former. När man vill engagera organisationsmedlemmarna i en gemensam kultur som stöder detta är delaktiggörandet det viktiga. Människor vill i allmänhet delta i och utveckla frågor som berör dem själva, såsom familjen, hobbykretsar och arbetsgemenskaper. Riskhanteringen bör inte strikt indelas i olika nivåer (vilket är förknippat med begränsningar och därmed är en annan sak än att rikta den information och de åtgärder som behövs för olika synvinklar), utan den måste göras till en gemensam sak för alla.

Riskstatusen bör åskådliggöras för alla. Det skulle vara bra att diskutera konsekvenserna högt och skapa en helhetsförståelse för de risker som bedömts för hela organisationen. Till exempel i kommuner med flera olika typer av sektorer skulle det vara bra att granska över sektorsgränserna huruvida det till exempel inom undervisningsväsendet finns vissa risker, inom småbarnspedagogiken vissa risker, inom förvaltningen och beslutsfattandet vissa risker och så vidare. Även i mindre organisationer kan man på nära håll hitta både lösningar och gemensamma utmaningar. Det handlar inte bara om ledningens rapportering – alla har sin egen roll i helheten.

I fråga om servicekedjor upphör verksamheten inte med gränssnitt och därför är gemensam riskhantering och planering viktigt. Kunden / användaren / konsumenten / medborgaren vet inte nödvändigtvis inom vems riskhanteringsområde hen befinner sig. Både en individs och en organisations hela kundupplevelse kan falla på dåligt eller bristande samarbete. Saker och ting måste diskuteras högt för att de ska kunna ordnas. I en sådan diskussion kan en part behöva stöd för att uttrycka sig korrekt. Ett problem i kommunikationen om riskerna är att vi visserligen talar om samma ämne, men förbi varandra, ur lite olika utgångspunkter och vinklar, utan att kontrollera exakt vad vi hänvisar till.

Riskhanterings-, säkerhets- och beredskapsplaner som bara sysslar med navelskåderi räcker inte längre. De måste samordnas och det ska ske i samarbete. Eftersom riskerna bedöms ur vars och ens egen kontext, men i sammanlänkade strukturer även påverkar den andras situation, behövs tillräcklig informationsdelning om hoten och ordnandet av riskhanteringen. Det finns risk för att en part inte tar tillräcklig hänsyn till risken eller att en risk uppstår i en "gråzon" mellan aktörernas gränssnitt.

Riskhanteringen beaktas i serviceavtal där man i vissa fall är beredd att betala priset för överföringen av riskerna i syfte att undvika dem, men alltför ofta suddas bilden av riskhanteringen och riskerna för servicekedjan eller helhetsprocessen ut vid utläggning på entreprenad. Även dessa ska man i organisationen identifiera och besluta om nyckelfunktionerna, de stödsystem som stöder dem och om det i ärendet ingår serviceavtal där man bör beakta och skriva in något särskilt. Detta är ett sätt att hantera riskerna i anslutning till avtal och leverantörsrelationer. I dessa skriftliga "samtal" är det ännu viktigare att uttrycka sig rätt och identifiera nyanser.

15.11.2022

4 Ämnesområde: Begrepp på överordnad nivå

Begrepp: digital verksamhetsmiljö, risk för den digitala verksamheten, digital säkerhet, cybersäkerhet, informationssäkerhet

För att kunna följa termernas utveckling och förstå förändringar är det viktigt att känna till bakgrunden till ordlistans utveckling och de val som gjorts i den. Särskilt i denna del av ämnesområdet bör man observera att de centrala begreppen på överordnad nivå är mindre viktiga för den önskade användningen av ordlistan (dvs. i stödet för genomförandet av riskhanteringen) än den övriga ordlistan, som är närmare praxisen och processen. Dessa kontextgivande termer ska dock beaktas i den omfattning de behövs för att definiera avgränsningarna för digital behandling, riskhantering, säkerhet och annan behandling. Utan en precisering enligt tema skulle vi vara tvungna att använda mycket allmängiltiga uttryck.

I denna ordlista definieras eller inramas inte de överordnade kontexttermerna helt och hållet, utan endast i den mån det är nödvändigt för att man ska kunna se sambandet – det vill säga som lådor som är öppna åtminstone åt något håll. Detta ger dessa termer utrymme att fungera och utvecklas. En alltför noggrann avgränsning innebär en risk som är förknippad med en viktig riskhanteringsprincip: man måste beskriva (vid behov via språket) den verklighet där verksamheten försiggår och syftet är inte att tvinga verksamheten eller verksamhetsmiljön att passa in i språkliga halmmodeller och konstruktioner. Fel tolkning av dessa snedvrider bedömningarna av riskerna och i värsta fall är detta något som upprepas i flera skeden av processen.

Till digital säkerhet räknas som centrala insatsområden ledning och riskhantering, kontinuitetshantering (inklusive beredskap och beredskap samt återhämtning), cybersäkerhet, dataskydd och informationssäkerhet.⁶ Dessa och andra delområden där digital säkerhet kan genomföras är delvis ett bevis på hur mångsidigt digitaliseringen har smält in i vår värld och hur världens mångfald i sin tur påverkar den digitala miljön. Av dessa fem tas kontinuitetshanteringen upp i följande avsnitt. Dataskydd har däremot definierats väl redan i den lagstiftning som anknyter till det, vilket gör det till en närmare definierad helhet jämfört med andra och har därför inte tagits in separat i denna ordlista. En noggrann definition kommer till uttryck även i genomförandet av dataskyddet, där en central del grundar sig på riskhantering. Denna riskhantering görs i en särskild organisationskontext (t.ex. informationshanteringsenheten) och för vissa typer av risker, varvid vissa bedömningsverktyg och kriterier tillämpas.

Definitionen av cybersäkerhet kan anses vara den mest utmanande av begreppen för digital säkerhet. Den präglas av många intryck från utlandet, men översättningarna grundar sig på olika uppfattningar som varierar mellan digital säkerhet, cybersäkerhet eller informationssäkerhet – eller är blandningar av dessa. När informationssäkerheten närmar sig saken ur ett systems, en tekniks eller en enskild helhets (IT/ICT) synvinkel behandlas inom cybersäkerheten mer omfattande nätverkande helheter och förbindelser samt deras effekter. Olika aktörer delar ägarskapet i termen och definierar den genom sin egen verksamhet. Prefixet "cyber" används fritt i talspråk och har sin bakgrund i årtionden av populärkultur. Cybersäkerhet är inte heller en neutral term i det hänseendet att infallsvinkeln⁷ härrör från konflikter mellan stater inom

⁶ Bilaga 1 innehåller en mer omfattande definition av den digitala säkerheten utanför riskhanteringen.

⁷ Se bl.a. hur populariteten hos ämnesområdena för sökord på internet har utvecklats under åren 2004–2022, <https://trends.google.com>

15.11.2022

cyberkrigföring, där man ofta tänker att hoten är avsiktliga och riktade, utan att beakta olyckor eller möjligheter.

Dessa är endast några orsaker till att cybersäkerheten har flera överlappande definitioner, diskurser, och varför OECD ansåg det nödvändigt med en bredare term med ett tydligare användningsområde.⁸ I helheten för digital säkerhet är cybersäkerheten dock ett viktigt perspektiv på ämnesområdet, genom vilket man möter vissa typer av utmaningar. I de mångsidiga diskurserna i cybersäkerhet har det tidvis skett en inskränkning i takt med aktuella händelser, men också en utvidgning i riktning mot mer omfattande digital säkerhet, särskilt i talspråket. Detta är delvis bra med tanke på att det ibland görs "säkringar" i säkerhetsdiskussionen, vilket stänger och begränsar behandlingen. Det är problematiskt att sporadiska och inexakta definitioner används parallellt: det tär på cybersäkerhetens betydelse och begriplighet, om till och med ergonomi vid arbetsbordet har inkluderats i termen. "Cyberisering" bör därför undvikas.

Användningen av flera termer med anknytning till säkerhetsaspekter stöder riskhanteringen och uppfattningen av riskerna, även om de har utvecklats utifrån olika utgångspunkter. En liten överlappning ger djup även i ordnandet av säkerheten och dessutom lyfter en mer mångfacetterad granskning fram egenskaper och nya sidor som man ofta måste komma ihåg att beakta inför mer komplexa utmaningar⁹. Identifiering och analys av risker samt planering av riskhanteringen bör göras med flera vinklar och kontexter.

I anslutning till riskerna i den digitala verksamheten borde man fråga sig vad som orsakar särskild risk i den digitala verksamheten? Detta kan granskas med hjälp av de fördelar som det medför, genom att vända upp och ner på dem. Som allmänna egenskaper eller mål för digitaliseringen ses bland annat följande:

Effektivitet

- hastighet (automatisering i del- och helhetsprocesser)
- skalbarhet (ska vara enkelt att sätta i förhållande till kostnaderna eller besväret)
- tillgänglighet (24 h, året runt)

Kvalitet

- enhetlighet (maskinella regler ger partiell jämlighet)
- exakthet (vissa fel kan korrigeras och förhindras samt hanteringen kan innehålla noggrannare uppgifter särskilt i numeriska/maskinläsbara ärenden)
- omfattning (möjlighet att använda mer omfattande data samt "bigdata").

Utveckling

- nya verksamhetssätt (automatiserade funktioner, nya användningssätt)
- ny teknik (nya sätt att använda data och system)
- synergieffekter (sammanställning, samarbete, effektivisering, länkning)

Generaliserbarhet

- anpassbarhet och hanterbarhet (användning och kopiering av strukturella delar)
- systematik och regelmässighet (kan läras och upprepas)
- globalisering (verksamhet i och mellan olika system, nätverksbildning)

⁸ Finansministeriets publikation 28/2016, särskilt s. 8 och 30 (FI): <http://urn.fi/URN:ISBN:978-952-251-790-6>

⁹ Exempel på hur vissa ämnen kan behandlas med hänsyn till risker i den digitala säkerheten, se paneldiskussionen under den digitala säkerhetsveckan [29.10.2021 \(FI\)](#) och [12.10.2022 \(FI\)](#).

15.11.2022

Det som allmänt kan betraktas som tillgängligt med digitala medel kan tas ännu längre och effektiviseras i alltmer utvecklade system och processer, med hjälp av automatisering, algoritmer eller maskininlärning och så vidare. På så sätt kan de ovan beskrivna positiva digitala möjliggörarna och den digitala verksamhetsmiljö som uppstår på detta sätt vändas för att skapa hot på alla nivåer, från individen till samhället. Av dessa element uppkommer ett avancerat och effektivt hanterbart massivt angrepp mot flera system och aktörer, där programmet och attackeraren lär sig något nytt för att fortsätta angreppet eller utveckla nästa. Därför är det anledning att som motvikt utveckla identifieringssätt och kontroller för dessa egenskaper och de risker som härleds ur dem.

Den digitala verksamhetsmiljön, som alla behandlade termer direkt eller indirekt anknyter till, är till sin karaktär en särskild och ständigt föränderlig helhet som grundar sig på de regler som människan skapat¹⁰. Den är till vissa delar lika gränslös som fantasin eller hårddiskens storlek och fungerar (delvis) med ljusets hastighet, men är ändå fast i den verkliga världen, som sätter gränser för den. Händelser i den verkliga världen och fysikaliska fenomen kan också skapa risker som äventyrar delar av den digitala verksamhetsmiljön – direkt eller indirekt. Dessa risker kan granskas antingen som en del av de digitala riskerna eller den övriga riskhanteringen, beroende på via vilken verksamhetsmiljö granskningen är mest meningsfull med tanke på den egna verksamheten och riskhanteringen.

Överlag kan det vara mer meningsfullt att tala om flera verksamhetsmiljöer (inklusive de verksamhetsmiljöer som kan fastställas inom den digitala verksamhetsmiljön) som korsar varandra i komplexa frågor, men samtidigt kan man fastställa att organisationen (eller någon annan kontext som är föremål för granskning) endast har en omgivning vars digitala nivå granskas. Båda betraktelsesätten är möjliga. Det senare blir aktuellt när man gör skillnad mellan internt och externt. Till det förstnämnda fogas bland annat organisationskulturen (och naturligtvis dess undertermer säkerhetskultur och digital kultur), målen och tekniken som används, medan det senare omfattar reglering, politiker, kulturer (lokal och global) och motsvarande. Det är vanligt att använda dessa två i strategiska överväganden. Även inom den digitala säkerheten kan man positionera de egna interna strukturerna och funktionerna på ett visst sätt i förhållande till den externa digitala säkerheten (Hurdan digital säkerhet bygger vi?). På motsvarande sätt kan man i den externa verksamhetsmiljön välja ett visst sätt att närma sig eller ett perspektiv på frågor som man möter där, det vill säga hur de interna strukturerna tillämpas eller borde tillämpas för att lösa dem (Hur borde den digitala säkerheten som vi byggt upp fungera här?). När dessa strategiska perspektiv har klarlagts behövs rätt intern och extern kommunikation för verkställandet av dem.

En effektiv och ändamålsenlig användning av dessa termer innebär att man tar till sig vad som avses med en digital verksamhetsmiljö i all dess omfattning och föränderlighet. Den digitala säkerhetens omfattning lyfter i sin tur fram olika synvinklar med vilka man kan närma sig olika säkerhetsområden på ett mångsidigt sätt. En utmaning är visserligen att termerna eller deras innebörd inte är helt etablerade och att de ofta används fritt, men att förbättra situationen med denna ordlista kan ses som en kommunikations- och utbildningsuppgift inom riskhanteringen i varje organisation.

¹⁰ Akronymen VUCA, som används mer allmänt om den moderna verksamhetsmiljön, beskriver den digitala verksamhetsmiljön väl: en förändringskänslig, osäker framtidsbild, komplexa påverkansförhållanden och tolkningsmöjligheter (Volatility, Uncertainty, Complexity, Ambiguity).

15.11.2022

4.1 Digital verksamhetsmiljö

Synonym: cyberverksamhetsmiljö, digital verksamhetsmiljö, digital miljö

Definition: *verksamhetsmiljö som består av ett eller flera digitala informationssystem*

Anmärkning: Jämfört med andra verksamhetsmiljöer kännetecknas den digitala verksamhetsmiljön av användning av elektronik och elektromagnetiska spektrum för behandling av data och information med hjälp av kommunikationsnät. Det digitala informationssystemet betraktas i det här sammanhanget emellertid som ett sociotekniskt system: den digitala verksamhetsmiljön omfattar även de människor som använder det, deras verksamhetssätt samt fysisk utrustning och strukturer som möjliggör verksamheten. I praktiken består den digitala verksamhetsmiljön av olika system och kopplingar mellan dessa, som utöver de funktioner som styr verksamheten även omfattar kulturell praxis. Till exempel sociala medier erbjuder många olika sätt att använda och påverka. Andra exempel på digitala verksamhetsmiljöer är styrsystem för ett kraftverk eller en fabrik, bank- och betalningssystem, digitala inlärningsmiljöer, informationsinsamlingsnätverk för webbpåverkan, programekosystem samt offentliga elektroniska tjänster med datalager. Med cyberverksamhetsmiljö avses samma sak som med digital verksamhetsmiljö, men termen lämpar sig bäst för kontext som behandlar cybersäkerhet.

4.2 Risk för den digitala verksamheten

Synonym: digital risk

Definition: *risk som påverkar den digitala verksamhetsmiljön, riktas mot den digitala verksamhetsmiljön eller beror på den*

Anmärkning: Risker med digital verksamhet är bland annat risker med anknytning till digital säkerhet och cybersäkerhet, risker med anknytning till digitalisering och digitisering samt risker med anknytning till digital kommunikation. Risken för den digitala verksamheten kan granskas snävt, som en intern fråga i den digitala verksamhetsmiljön eller omfattande, varvid den kopplas utanför sin verksamhetsmiljö och även kan jämföras med icke-digitala risker – till exempel genom att delvis eller helt jämföra digitala genomförandesätt med icke-digitala genomförandesätt, såsom insamling av information på en pappersblankett.

4.3 Digital säkerhet

Synonym: -

Definition: *målbild där man kan lita på den digitala verksamhetsmiljön och där verksamheten är säker och kontrollerad, även vid störningar*

Anmärkning: Enligt OECD:s definition är digital säkerhet en omfattande helhet som i tillämpliga delar omfattar bl.a. riskhantering, kontinuitetshantering, dataskydd, informationssäkerhet och cybersäkerhet, dessa omfattar å andra sidan delområden som inte hör till den digitala säkerheten. Medan cybersäkerheten anknyter till säkerheten på nationell och internationell nivå kan den digitala säkerheten gälla till och med bara en enskild persons mål och handlande. Digital säkerhet innehåller bl.a. tekniska, sociala och ekonomiska frågor på bred front, men alla dessa beaktas inte alltid. Den

15.11.2022

digitala säkerhetsnivå som organisationen eftersträvar beror bland annat på organisationens och säkerhetsnivåns syfte, resurser och de krav som ställs på dem. Den digitala säkerheten liksom cybersäkerheten påverkar också den fysiska världens säkerhet samtidigt som den digitala säkerheten påverkas via den fysiska världen.

(En mer omfattande definition av helheten för digital säkerhet utanför riskhanteringen finns i bilaga 1, s. 68 till detta dokument).

4.4 Cybersäkerhet

Synonym: -

Definition: *målbild där de hot och risker som cyberverksamhetsmiljön medför för samhällets vitala funktioner eller andra funktioner som är beroende av cyberverksamhetsmiljön är under kontroll, även om det uppkommer störningar*

Anmärkning: Digital säkerhet och cybersäkerhet är mycket nära som begrepp, men enligt OECD:s definition är digital säkerhet en större helhet som endast utgör en del av cybersäkerheten, å andra sidan har cybersäkerheten delområden som inte hör till den digitala säkerheten. Medan digital säkerhet kan diskuteras med hänsyn till organisationens eller till och med en enskild persons mål och verksamhet, innehåller cybersäkerheten en betoning på säkerhet på nationell och internationell nivå samt samhälls- eller påverkan. I kontexter om cybersäkerhet används i allmänhet termen cybermiljö för den digitala verksamhetsmiljön. I denna definition har man anpassat definitionen i ordlistan om övergripande säkerhet (TSK 50, 2017), som närmar sig begreppet ur ett perspektiv som lämpar sig för riskhantering. Cybersäkerhet är ett delområde inom den övergripande säkerheten. I ordlistan om cybersäkerhet (TSK 52, 2018) avses med cybersäkerhet på basis av anmärkningarna samma begrepp som i denna ordlista, även om definitionen skiljer sig från den som presenteras här.

4.5 Informationssäkerhet

Synonym: datasäkerhet

Definition: *målbild där tillgången till samt integriteten och konfidentialiteten hos informationen och informationssystemen har säkerställts*

Anmärkning: Den informationssäkerhetsnivå som organisationen eftersträvar beror bland annat på organisationens mål, resurser och de krav som ställs på den, och dessa styr hanteringen av informationssäkerhetsrisker. Informationssäkerheten säkerställs genom åtgärder som kan vara administrativa, tekniska eller av annat slag. Informationssäkerheten omfattar utöver det digitala även andra delområden, till exempel hantering av handlingar i pappersform, som kan läsas enligt behov och beroende på processerna antingen utanför eller under den digitala säkerheten bl.a. i och med utskrift, skanning och överföring av digital information.

15.11.2022

5 Ämnesområde: När något händer

Begrepp: attack, attackens avsedda mål, avvikelse, incidens kontinuitetshantering, störning

Med tanke på riskhanteringen är man redan för sent ute om något tråkigt händer. Det innebär inte nödvändigtvis att man före incidenten inte skulle ha identifierat risken för incidenten och satsat på behandlingen av det som hänt för att följderna ska förbli små. Riskhanteringen har förhoppningsvis också genomförts som en del av kontinuitetshantering, varvid man på förhand har kunnat göra rätt slags förberedelser. Detta underlättar hanteringen av den situation som incidenten orsakar, vilket möjliggör en effektivare och snabbare återhämtning till det normala – eller till något annat eftersträvat tillstånd.

I anmärkningen till begreppet incidens har det framförts att det kan finnas olika typer av incidenser, beroende på vilka egenskaper som granskas. Definitionen styr verksamheten och i synnerhet uppfattningen om vad som hänt kan styra den första reaktionen mycket starkt. Detta kan leda i fel riktning beklagligt länge om man inte tänker på att precisera de första bedömningarna. I efterhand kan det framgå att attackens avsedda mål har varit någon annan, men detta är ofta resultatet av en längre utredning om attackeraren har försökt dölja spåren. Det är inte ovanligt att det bland dem som använder samma system är svårt att identifiera vem eller vilka som har utgjort målet – eller om kunderna endast har varit utomstående offer när målet har varit en tjänsteproducent eller kundens kunder.

Nuförtiden söker man ofta någon som är skyldig till störningarna, men man bör också komma ihåg att naturen – bokstavligen från rymden till jordskorpan – fortfarande kan bereda överraskningar för oss. Å andra sidan är det inte alltid klart hur saker kan inträffa i de komplexa systemens strukturer, eftersom deras funktionella användbarhet inte alltid stöder människans behov. Ibland är det bättre att anta oavsiktlig okunnighet eller mänskligt misstag i stället för ett riktat hot. På det hela taget bör man, med tanke på helheten för digital säkerhet, inte anta att det aldrig kommer att hända något. Ett riskhanteringstänkande som bygger på fullständig förhindrande och förebyggande verksamhet är inte effektivt eller hållbart för den övriga verksamheten.

En effektiv och ändamålsenlig användning av dessa termer innebär att man tar till sig och kan välja det mest beskrivande uttrycket för behandling. Ibland kan det tillfälligt och till en början innebära att beskrivningen är mycket vag och abstrakt beskrivning, men att den preciseras och bilden förbättras under den processmässiga verksamheten. Betydelsen av olika incidenser kan också granskas med hjälp av termer som anknyter till uppkomsten av risker eller egenskaperna hos deras uppbyggnad. Dessa behandlas i senare avsnitt.

5.1 Incidens

Synonym: -

Definition: förekomst eller förändring av vissa omständigheter

Anmärkning: Incidenten kan vara enskild eller bestå av många fall och det kan finnas flera orsaker till det. Om följderna av en incidens eller en kedja av incidenser är negativa kan det vara fråga om en attack, en störning, en exceptionell situation eller

15.11.2022

en olycka. En incidens som inte har några konsekvenser eller vars följder är små i förhållande till potentialen kan kallas en farlig situation eller ett tillbud.

5.2 Avvikelse

Synonym: -

Definition: *skillnaden mellan det undersökta objektet och det önskade eller sedvanliga*

Anmärkning: Identifieringen av avvikelser kan underlättas genom att fastställa gränsvärden för mätare som kan följas med nödvändig noggrannhet och tillbörligt granskningsintervall.

5.3 Störning

Synonym: -

Definition: *oväntad eller oönskad incidens som stör systemets funktion, verksamheten för systemets användare eller verksamheten hos någon som är beroende av dessa*

Anmärkning: Som störningar kallas vanligtvis endast incidenter som i sig eller med rätt motåtgärder orsakar en tillfällig och kortvarig olägenhet. Störningen kan till exempel orsakas av en attack eller en oförutsedd kedja av incidenter och kan ofta hänföras till en svaghet, brist eller ett fel.

5.4 Attack

Synonym: -

Definition: *handling eller verksamhet genom vilken man strävar efter att skada eller obehörigen använda ett objekt eller genom vilken man förhindrar att målet för ett objekt uppnås*

Anmärkning: Föremålet för attacken kan till exempel vara ett datanät, ett datasystem, en enhet, information, en person eller en organisations anseende. En attack är alltid en avsiktlig handling som orsakas av människan, men angriparnas motiv varierar och gärningsmännen kan vara flera i stället för en, från några personer till stora organisationer. Det planerade målet för attacken är inte nödvändigtvis detsamma som det objekt som man identifierar att attacken påverkar, och det kan också finnas flera avsedda mål. Attacken kan förutom den organisation som är föremål för attacken påverka även t.ex. dess klienter eller samarbetspartner, vilket kan vara oavsiktligt eller avsiktligt. Eventuella konsekvenser av attackerna kan utgöra indirekta risker via en kedja eller ett nätverk, och därför ökar riskerna i anslutning till attackerna i och med kontakterna mellan aktörerna. I vissa fall kan det uppstå beroendeförhållanden mellan parterna, där någon parts kritiska funktioner eller system är beroende av en annan parts förmåga att hantera risker i anslutning till attacker.

5.5 Attackens avsedda mål

Synonym: -

15.11.2022

Definition: *det mål som attacken syftar till att påverka*

Anmärkning: Det är viktigt att organisationen i sin riskhantering också förbereder sig på attacker där organisationen inte är det avsedda målet för angreppet, men som vid sidan av eller i stället för det avsedda objektet lider av konsekvenserna av en attack. Det verkliga avsedda målet kan till exempel hemlighållas eller döljas genom att angripa flera objekt. Organisationer och personer som är det avsedda målet för attacken eller annars inom dess influensområde är inte alltid medvetna om attacken eller lider av dess konsekvenser.

5.6 Kontinuitetshantering

Synonym: hantering av verksamhetens kontinuitet

Definition: *en organisationsprocess genom vilken man identifierar de risker som är centrala för verksamheten, bedömer deras konsekvenser för organisationen och dess aktörsnätverk samt skapar ett verksamhetssätt för hanteringen av störningssituationer och verksamhetens kontinuitet under alla förhållanden*

Anmärkning: Kontinuitetshantering är en strategisk och operativ verksamhet som godkänts av organisationens högsta ledning och genom vilken organisationen förebygger störningssituationer och förbereder sig på att reagera på dem så att verksamheten kan fortsätta på en på förhand fastställd godtagbar nivå. Ju mer kritisk verksamheten är, desto viktigare är dess kontinuitetshantering. Vid identifieringen av kritiskhet, sårbarhet osv. som kräver kontinuitetshanteringsåtgärder utnyttjas den information som producerats i riskbedömningsprocesserna, och genom god riskhantering kan man både förebygga problem med verksamhetens kontinuitet och vid behov stödja minimeringen av skadorna och återställandet av verksamheten. Kontinuitetshanteringen är i allmänhet frivillig verksamhet, men inom vissa branscher är organisationerna också skyldiga att säkerställa sin verksamhet under olika förhållanden. I synnerhet i organisationer som är kritiska med hänsyn till försörjningsberedskapen är det väsentligt att trygga försörjningsberedskapen.

15.11.2022

6 Ämnesområde: Uppkomst av och förståelse för risker

Begrepp: förvrängning, hot, hot som undviker riskens gränsvärden, möjlighet, osäkerhet, risk, riskens livscykel, riskkriterier, riskuppfattning, svaghet, sårbarhet

Ibland byggs risker upp av en slump – eller åtminstone verkar det så. Men ju mer systematisk strukturen är, desto tydligare kan man i efterhand identifiera den logiska cykeln i de flesta risker. Under deras livscykel kan man koppla olika uttryck till uppkomsten. Man måste dock vara försiktig med föreställningen om att uppkomsten är en okomplicerad process: grenar av flera olika motiv går samman för att producera den slutliga incidensen och dess konsekvenser. Detta kan förstås så att attackeraren vid en eventuell attack först måste lyckas kombinera åtminstone tillfället, medlen och motivet. Alla dessa påverkas av vårt förebyggande skydd och våra beredskapsåtgärder för att minimera konsekvenserna¹¹.

Möjligheterna med alla kombinationer av olika incidenser gör vår framtid osäker. Vi vet inte vad som händer. Osäkerheten och förmågan att tåla osäkerhet är centrala när man ska förstå riskerna. Men vår förståelse påverkas också av brister i de uppgifter som ligger till grund för våra slutsatser samt av våra tillägnade vanor och andra metoder med vilka vi hanterar ringa och missförstådd information. Här döljer sig kanske en av de viktigaste aspekterna på riskhantering. Ett hot, som kan betraktas som allmänt och vagt, omvandlas till en risk när vi identifierar egenskaper hos hotet som kan bedömas på något sätt och med viss exakthet – när vi identifierar vad hotet innebär – och kan bedöma risken i förhållande till både våra mål, förmågor och motsvarande samt till andra risker. På så sätt kommer hotet att tas upp till behandling, åtminstone i den mån vi tror att vi förstår det. Detta gör det möjligt att agera och reagera i rätt riktning.

Sårbarheten i sig är ingen risk. Den är som ett hål i ett vattentätt skyddshölje om man tappar telefonen i vatten (incidens) och förlorar information (risk). Genom att korrigera sårbarheter kan man förhindra att många hot blir risker. Särskilt genom organisationers administrativa strukturer kan man identifiera relativa svagheter mellan olika delområden, eftersom satsningarna sällan är jämna, för att inte säga tillräckliga på alla håll, när man strävar efter effektivitet. Svaghet gör det ofta möjligt för sårbarheter att uppkomma eller bevaras. Det kan till exempel vara brist på tid och kunskap att granska alla egna systemkoder eller att planer och anvisningar saknas för exceptionella situationer. I organisationerna kan hantering och korrigering av svagheter vara ett mer strategiskt och förutseende sätt att hantera risker. Om man inte lyckas fastställa svaga delområden på annat sätt kan man via hot och risker analysera de grundläggande orsakerna och hitta faktorer som påverkar i bakgrunden.

Det kan vara utmanande att definiera riskerna. Risken måste ställas i proportion till målet och resurserna och därmed finns det i allmänhet ett gränsvärde för vad som kan tolereras och vad som inte kan godkännas. På förhand fastställda kriterier i olika former förebygger definiering och värdering av risker på ett slumpmässigt sätt. En enhetlig bedömning möjliggör en trovärdig jämförelse och förebygger vissa snedvridningar genom att vi utifrån känslor, tumregler eller föråldrad lära kanske viktar en risk åt ett eller annat håll. Förebyggandet av snedvridningar är en del av den kvalitetsstyrningen som riskhanteringen i sig är en del av: en process för att producera tillförlitlig

¹¹ En sådan analys kan göras med en så kallad bowtie-analys.

15.11.2022

information som stöd för beslutsfattandet - och därför är en välfungerande process något som bör eftersträvas.

Gränsvärden är i allmänhet också förknippade med någon åtgärd, direkt eller indirekt. Det visar att man måste reagera, men också på så enkla saker som att kan vi ens upptäcka missförhållanden som inte blir tillräckligt stora? Varselgränsen kan vara bokstavlig (virus), systeminställningar för larm (antalet felaktiga lösenordsförsök) eller administrativ (meddelanden om avvikande verksamhet). Den kan också vara absolut, till exempel i driften av kritiska system, eller relativ, dvs. att något lyfts fram bland alla andra signaler och meddelanden.

Kontroll av data och information på olika sätt är en viktig del av en väl genomförd riskhantering och säkerhet. Man måste se till att rätt personer får rätt impulser som innehåller tillräcklig information om vad som händer nära gränssnittet, men så att man inte drunknar i informationen. Finjusteringar måste också göras kontinuerligt i samband med olika ändringar och sondering av sannolika nya hot, på alla verksamhetsnivåer i organisationen. Om det inte finns rätt information för beslutsfattandet kan det indikera ett utvecklingsområde.

En särskild utmaning består i hot och risker som stannar precis på andra sidan olika gränser som engångsincidenser. Den belastning som de skapar kan dock utgöras av att det uppstår många i sig ofarliga fall eller att någon annan egenskap hos dem är exceptionellt framträdande. Det kan bara vara något mer slitsamt eller till och med kräva resursöverföring (vilket leder till en svaghet på annat håll, såsom flaskhalsar), utan att gränsdragningen för identifiering av stora avvikelser skulle överskridas tydligt. Attackeraren kan också avsiktligt försöka manipulera gränsvärdena eller skapa åtgärder som är kopplade till dem. Osäkerheten kring gränserna och tolkningen av dem är en svaghet, för att inte säga en direkt sårbarhet.

Om man endast ser kris och fred, kan man inte handla inom zonen av mellanmodeller av olika grad som bildas mellan dessa ytterligheter. Denna typ av metodik har utnyttjats i olika avsiktliga kampanjer för hybridpåverkan, där man har stört verksamheten genom en bluff som verkar hotande eller genom en extra belastning på normala processer. Eftersom dessa inte har kunnat särskiljas från liknande normala incidenser och fenomen, kan dessa problem inte heller isoleras eller separeras till en effektiv behandling. Detta kan leda till att man vid kriser och när situationen äntligen överskrider gränserna för uppmärksamhet eller tolerans kan vara tvungen att agera på ett sätt som stör eller skadar parter som inte är delaktiga i ärendet. Det speciella med den här typen av verksamhet är dess syften: syftet är inte nödvändigtvis att realisera själva risken, utan att lyfta fram organisationens svagheter eller manipulerbarhet (ryktesskador) eller att på samma sätt som vid en nätverksbaserad risk orsaka konsekvenser för ovan nämnda aktörer som inte är förknippade med risken och som kan vara attackens avsedda mål. I större incidenser kan dessa utomstående vara medborgare och konsekvenserna är att förtroendet för värderingarna och rättigheterna försvagas, men i mindre incidenser är det mer sannolikt att vi talar om mobbning och trakasserier. Medvetenheten är viktig med tanke på hanteringen av dessa risker och den utgår från fastställda gränsvärden som stöder identifieringen av vad som är normalt och vad som inte är det.

I modern riskhantering ska risker inte längre behandlas enbart som negativa faktorer som i bästa fall kan elimineras eller minimeras så att de blir neutrala. Däremot måste man betrakta dem så att riskerna antingen direkt eller till följd av hanteringen av dem

15.11.2022

ger någon nytta, något positivt gemensamt resultat av en incidens konsekvenser som helhet. Riskerna kan i mindre skala ses som möjligheter som styr oss att åtgärda sårbarheter och stärka svagheter. Detta kan handla om att stärka det gamla, men oftare borde det vara utvecklande av något nytt, nya möjligheter. I ett större perspektiv kan man avse en mer utvecklad digital säkerhet och identifiering av nya möjligheter som organisationen hittat, vilket kan vara ännu mer värdefullt. Om man kan och vill utnyttja alla dessa är förstås en annan fråga. Ofta tar det tid att bearbeta detta, och därför bör man upptäcka hot samt identifiera och analysera riskerna i god tid. I riskhanteringen bör man också sträva efter att svara på frågan om hur man med åtgärden för att hantera ärendet kan stöda (strategiska) mål och uppnå fördelar. Om man endast betonar problemen och kommunicerar negativt kring riskerna skapas på lång sikt en tung atmosfär och en företagskultur som undviker tråkiga riskhanteringsfrågor.

En effektiv och ändamålsenlig användning av dessa termer innebär att man tar till sig både riskutvecklingen som händelsekedja och hur olika skeden kommer till uttryck och skiljer sig från varandra. Man kan ta tag i olika skeden och utmaningarna med dem på olika sätt. Det kan emellertid vara svårt att sätta fingret på olika skeden och fenomen och man måste förstå att olika faktorer formar vårt synsätt. Ibland kan man försöka utnyttja detta avsiktligt, ibland gör förhållandena att det bara inte är möjligt att upptäcka ett hot innan det är för sent att göra något åt det på förhand.

6.1 Osäkerhet

Synonym: -

Definition: *brist på information om en kommande incidens karaktär eller tidpunkt*

Anmärkning: Framtiden är alltid förknippad med osäkerhet, vilket leder till att framtiden inte kan förutses, utan man måste förbereda sig på flera möjliga incidenser och jämföra deras egenskaper och sannolikhet i ljuset av tillgänglig information. Man är inte nödvändigtvis medveten om att det finns faktorer som orsakar osäkerhet. Till exempel bristfällig kännedom om de egna processerna eller informationssäkerhetsnivån kan orsaka osäkerhet. Om en incidens är förknippad med osäkerhet kan den ha en positiv, negativ eller neutral inverkan på organisationen om den förverkligas. Man strävar efter att uttrycka information om osäkerhetens effekter som risker. Riskuppgifterna kan ibland grunda sig på en felaktig riskuppfattning, till och med så att en incidens som betraktas som en risk överhuvudtaget inte är möjlig. Osäkerheten kan vara fullständig eller partiell: osäkerhet vars sannolikhet och konsekvenser har bedömts på ett välgrundat sätt kan utöver risken också klassificeras som känd osäkerhet (known unknown).

6.2 Hot

Synonym: -

Definition: *eventuell skadlig incidens eller utveckling*

Anmärkning: Ett hot kan till sin natur vara allmänt och således riktas till flera olika aktörer som uppfattar hotets betydelse utifrån den egna kontexten. Ett hot skiljer sig från en risk genom att dess betydelse inte har bedömts och proportionerats. När hotet betraktas som en risk ur ett visst perspektiv kan man förutom eventuella olägenheter även identifiera möjligheter. Hotet skiljer sig från risken på så sätt att hotet är ett

15.11.2022

osäkrare utvecklingsförlopp och medan risken är en praktisk fråga som ska hanteras med riskhanteringsåtgärder. Se även risk.

6.3 Sårbarhet

Synonym: -

Definition: *brist, fel eller tillvägagångssätt som ökar risken för hot mot säkerheten*

Anmärkning: Sårbarheter kan förekomma till exempel i datasystem, mjukvara, hårdvara, processer eller människors verksamhet. Sårbarhet kan till exempel vara ett fel i ett program som gör det möjligt att kringgå begränsningar som förhindrar missbruk. Sårbarhet kan också handla om att det i beslutsfattandet inte krävs någon annan godkännare eller granskare än undertecknaren, eller att krypteringen av ett e-postmeddelande inte lyckas, varvid uppgifter måste skickas i ett okrypterat e-postmeddelande. Nolldagssårbarhet är en mjukvarusårbarhet i ett datasystem som utgör en hög informationssäkerhetsrisk men som tillsvidare inte kan åtgärdas eftersom programutvecklarna har upptäckt den så nyligen.

6.4 Svaghet

Synonym: -

Definition: *oönskad eller skadlig egenskap i organisationens verksamhet eller egendom med hänsyn till organisationens mål*

Anmärkning: Svagheter kan vara till exempel flaskhalsar i processer, brister i personalutbildningen eller dålig resursfördelning i vissa funktioner. Eftersom organisationen alltid har begränsade resurser kan vissa svagheter endast lindras eller godkännas som sådana i stället för att elimineras. Svagheter påverkar organisationens riskhanteringsförmåga och kan främja uppkomsten av sårbarheter.

6.5 Möjlighet

Synonym: -

Definition: *incidens eller utvecklingsförlopp som eventuellt orsakas av riskens effekter och som kan utnyttjas för att främja målen*

Anmärkning: I riskhanteringen kan man i vissa fall förutom att förebygga, ändra eller minimera risken även identifiera möjligheterna, dvs. att det är möjligt att på något sätt dra fördel av risken. Man kan försöka påverka möjligheten, men det är inte säkert att man lyckas. Man kan också försöka påverka hurdana incidenser och utvecklingsförlopp som överhuvudtaget kan utnyttjas som möjligheter, bl.a. genom att satsa på förmågor och resurser. En möjlighet kan direkt påverka enskilda mål, förbättra situationen mer allmänt eller till exempel möjliggöra nya mål, verksamhetssätt och resurser. Ordet möjlighet används också i talspråk som motsats till hot samt ibland i texter som behandlar riskhantering allmänspråkligt som motsatsen till omöjlighet, varvid den exakta betydelsen beror på kontexten.

15.11.2022

6.6 Risk

Synonym: -

Definition: *osäkerhetens inverkan på målen*

Anmärkning: Risken uttrycks vanligen som en kombination av riskkällor, eventuella incidenser, följderna av dem och sannolikheten för dem. Effekten är en avvikelse från det förväntade. En möjlighet kan vara positiv, negativ eller både och. De positiva effekterna av en risk kan i vissa fall granskas som möjligheter.

Riskerna och effekterna av riskerna kan gälla till exempel människor, djur, egendom, datasystem, miljön, gemensamma värden eller delade betydelser. Om risken realiserar sig kan det leda till flera olika effekter på olika nivåer och för att hantera dem samt för att relatera de olika riskerna till varandra kan det vara nödvändigt att dela in risken i mindre delar eller samla enskilda företeelser i större helheter, beroende på riskhanteringsbehoven. Risken definieras här på samma sätt som i flera källor, bl.a. i standarden SFS-ISO 31000:2018. I allmänspråket har både det finska ordet "riski" och de svenska och engelska motsvarigheterna en negativ innebörd.

6.7 Riskuppfattning

Synonym: uppfattning av risken

Definition: *människans eller organisationens uppfattning om hurdan en risk är*

Anmärkning: Riskuppfattningen påverkas förutom av den tillgängliga informationen, som i fråga om risker alltid till vissa delar är bristfällig på grund av osäkerheten i anslutning till den, även av snedvridningar i tolkningen av informationen. Därför kan riskuppfattningen i hög grad avvika från riskens verkliga karaktär. Utöver den egna riskuppfattningen och den egna organisationens riskuppfattning kan man också granska intressentgruppernas riskuppfattningar. Det är möjligt att påverka riskuppfattningarna bland annat genom informationsanskaffning, djupare analys av riskerna och kommunikation.

6.8 Förvrängning

Synonym: -

Definition: *en aktörs eller ett systems benägenhet att uppfatta och betona information på ett visst sätt som beror på naturliga snedvridningar i människors tänkande*

Anmärkning: Genom att identifiera och ingripa i förvrängningar förbättras bedömningsobjektivitet. En förvrängning kan vara personlig eller kollektiv och den kan upprepas i systemen. Förvrängningar kan förekomma på olika nivåer av beslutsfattande eller i olika skeden av processer. Det finns många sätt att hantera förvrängningar och sätten kan integreras i processen. En definierad, omfattande och utvecklande riskhanteringsprocess i sig är ett sätt att förebygga vissa typer av förvrängning i den producerade informationen.

15.11.2022

6.9 Riskkriterier

Synonym: -

Definition: *grunder för en enhetlig bedömning av riskernas betydelse*

Anmärkning: Riskkriterierna grundar sig bl.a. på mål, resurser och verksamhetsmiljö, och de kan i tillämpliga delar härledas från standarder, lagar, verksamhetsprinciper och andra krav. Riskkriterierna kan uttryckas på olika sätt, till exempel med hjälp av exakta gränsvärden eller mer allmänna verbala beskrivningar.

6.10 Hot som undviker riskens gränsvärden

Synonym: -

Definition: *en attack eller annat hot som försöker undvika motåtgärder genom att hålla sig under de gränsvärden som använts vid riskbedömningen*

Anmärkning: Ett gränsvärde som används i riskbedömningar kan vara kvantitativt, kvalitativt eller en kombination av dessa. Gränsvärdet kan vara för högt, för lågt eller ignorera samverkan med andra risker, varvid risken inte hanteras på ett ändamålsenligt sätt. Även om det gränsvärde som använts i riskbedömningarna i övrigt skulle motsvara målen, kan ett hot som undviker riskgränsvärdet och som är av betydelselös engångsnatur orsaka betydande olägenhet om det drar ut på tiden eller upprepas. Då är man inte nödvändigtvis medveten om hotet eller kan inte, vill eller förmår inte svara på det med tillräckliga följder. I vissa fall blir de hot som undviker riskgränsvärdet även i sin helhet betydelselösa för organisationen, men orsakar betydande skada på högre nätverks- eller samhällsnivå. Exempel på hot som undviker gränsvärdet för risker är bl.a. maskering av åtgärder i anslutning till dataintrång som ofarliga störningar eller strävan efter att undvika utpressningsprogram som attackerar statliga säkerhetsaktörer och andra som lätt vidtar motåtgärder.

6.11 Riskens livscykel

Synonym: -

Definition: *riskens skeden från uppkomsten av hotet till riskidentifiering och vidare ända tills risken eventuellt upphör*

Anmärkning: Som början på riskens livscykel kan betraktas föregående incidenser som orsakar ett hot som i sin tur kan identifieras som en risk. Det är ofta svårt att fastställa slutet på riskens livscykel, eftersom risken kan förändras avsevärt under sin livscykel och många risker kvarstår som små återstående risker. När en risk förändras kan till exempel riskens effekt, sannolikheten för den eller till och med det objekt som risken påverkar förändras. Riskens livscykel påverkas både av förändringarna i verksamhetsmiljön och av organisationens åtgärder.

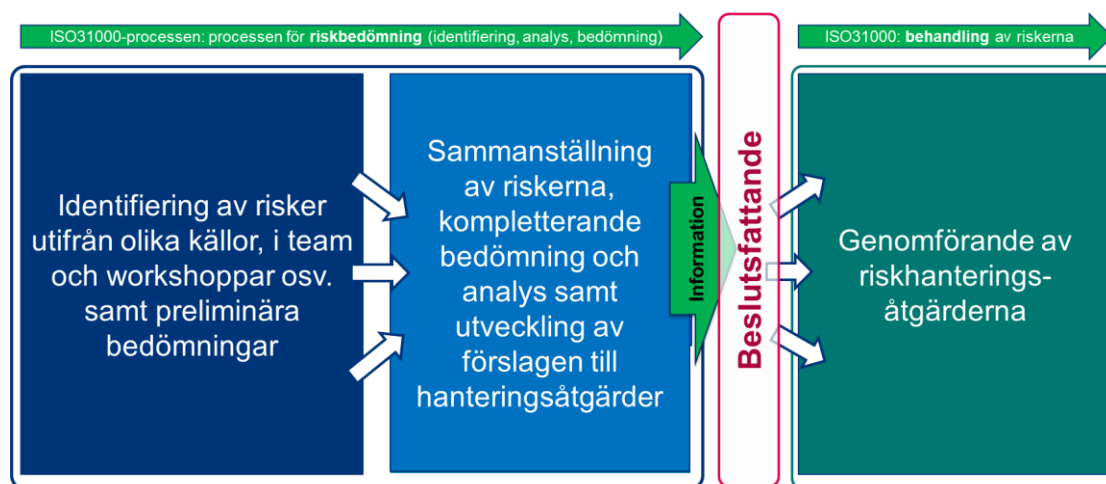
15.11.2022

7 Ämnesområde: Riskbedömning

Begrepp: analys av risker, bedömning av risker, klassificering av risker, ny bedömning, preciserande bedömning, preliminär bedömning, riskanalys, riskbedömning, riskbedömningsprocess, verktyg för riskbedömningsprocessen

Riskbedömning är ett av de begrepp inom riskhantering som bjudit på utmaningar. Begreppet riskbedömning har använts både för att göra en bedömning, för resultaten av den och för att beskriva en processhelhet som omfattar separata delar av identifiering, analys och bedömning (på vilka man kan tillämpa egna metoder). I talspråk förekommer olika användningssätt och det händer att bedömning och analys användas synonymt med varandra.

I denna ordlista beslöt man att separera begreppen i fråga så, att man enligt serien ISO31000 valde det mer exakta alternativet "riskbedömningsprocess" som det uttryck som beskriver en del av processen. Skillnaden mellan bedömning och analys förtydligades, eftersom det handlar om två olika sätt att hantera information om risker, och denna tolkning gör det lättare att vidta rätt åtgärder.



Figur 1: En del av den övergripande riskhanteringsprocessen förenklad, det vill säga bedömningsprocessen och behandlingsskedet samt beslutsfattandet mellan dem, för vilket man producerar information och alternativ. Beslutsfattandet påverkas också av andra faktorer än den information som riskhanteringen producerar. Till bedömningsprocessen räknas identifiering, analys och bedömning av risker enligt standarden. Detta föregås av ett skede utanför figuren där man fastställer granskningens omfattning, de egna målen och verksamhetsmiljöns betydelse samt andra kriterier som påverkar granskningen. Efter behandlingsskedet borde uppföljning och granskning av konsekvenserna ta vid. En mer detaljerad modell finns i avsnittet Riskhanterings kontexter och nivåmodell.

I bedömningen av risker, de ställs i relation till både varandra och målen, verksamhetsmiljön samt resurserna och motsvarande. Detta är ett sätt att hitta de största riskerna, de som verkligen har betydelse – om sådana finns, eftersom vi kanske hade överskattat hoten före den systematiska behandlingen. Samtidigt skapas också en prioritering av i vilken ordning de olika åtgärderna i behandlingen blir effektiva (detta kan visserligen förändras när behandlingsåtgärderna utvecklas) och i vilken utsträckning man bör satsa tid, besvär och andra resurser på varje enskild risk. Bedömningen fokuserar på helheten och tillämpning av kvantitativa värden.

15.11.2022

I analysen av riskerna kan man granska riskgruppens betydelse, men också uppbyggnaden av och egenskaperna hos en enskild risk. Här är det meningen att man ska lära känna risken mer ingående för att få kontroll över dess olika skeden och konsekvenser. Analysen är ofta kvalitativ, men när det gäller stora grupper, nätverk och simuleringar kan man göra en matematisk analys¹². Enbart visualiseringar som görs på olika sätt kan bidra till förståelsen för betydelser och mekanismer, vilket är en del av analysen och kommunikationen om dess resultat i rapporteringen – resultaten måste lyftas fram på rätt sätt.

Bedömningarna preciseras efter hand när kunskapen och förståelsen utvecklas. Därför ska man inte heller i riskhanteringen fastna i en bedömning som gjorts en gång. Detta ska inte förstås till exempel som en upprepning som görs varje år och som har ett eget syfte att hålla informationen relevant. Den bedömningsprocess som ofta genomförs i organisationer inleds med sammanställandet av ett organisationsschema på gräsrotsnivå, varvid de som har att göra med riskerna i praktiken blir tvungna att identifiera och bedöma dem. De har sannolikt den bästa kännedomen om sitt eget arbete och de hot som påverkar substansen i arbetet, men deras bedömning kan snedvridas av att de inte är vana vid arbetssättet i riskhanteringsmodellen, de gränsvärden som beskrivs i den eller av att de har en bristfällig syn på hela verksamhetsfältet. Det kan också vara tungt för dem att genomföra en fullständig analys. För att underlätta detta kan man göra en första bedömning som kompletteras och fördjupas i preciserande bedömningar eller av en expert som fördjupar sig i ärendet. Så här går man redan i viss mån till väga när till exempel uppgifter från riskworkshoppar samlas in och omvärderas som en helhet med hela organisationen som kontext. Syftet med denna upprepning är att förbättra kvaliteten på riskuppgifterna.

Den första punkten i bedömningsprocessen är egentligen inte identifiering av risker. Riskbedömningsprocessen är en del av den övergripande riskhanteringsprocessen, där man först konstaterar och identifierar mål, strategier för att uppnå dessa, verksamhetsmiljön och riktningarna för förändringar i den samt andra antaganden och begränsningar som ska beaktas när riskerna fastställs och vad riskerna bedöms mot. Ofta glöms allt detta bort, vilket leder till att identifieringen eller andra åtgärder utförs utifrån en oenhetlig syn och att man till exempel inte får den nödvändiga täckningen eller inriktningen.

Det finns två grundläggande sätt att identifiera risker som inte definieras separat i denna ordlista. För det första kan risker identifieras genom tidigare incidenser, varvid identifieringen grundar sig på historiska uppgifter om hot, utvecklingsförlopp, orsaker och externa faktorer. Av dessa skapas scenarier för vad som kan hända. Då talar man alltså om hur tidigare hot kan upprepas, eventuellt modifierade i en verksamhetsmiljö som ständigt utvecklas. Ett annat sätt är att granska riskerna med hjälp av objekt som ska skyddas inom den egna strukturen eller med hjälp av sårbarheter och svagheter. Då granskar man vad som finns eller händer i organisationen och skapar scenarier för vad som kan riktas mot det som observerats och vad som kan hända utan dem (delvis eller helt). På så sätt kan angrepps- och försvarsaspekterna placeras i tabellen på rubrikraden och kolumner, varvid man med matrisen kan göra en systematisk genomgång av kombinationen av olika hot för att kunna identifiera de risker som är betydelsefulla för den egna kontexten. Vid denna typ av genomgång vet man hur heltäckande identifieringen är, vilket gör det lättare att förstå betydelsen av (samt bristerna i) riskhanteringen.

¹² En samling olika bedömnings- och analysmetoder samt uppskattningar av deras användbarhet i olika skeden av processen och för olika ändamål ingår bl.a. i ISO31010, men även andra metoder för strukturerad analys kan tillämpas om de producerar den information som behövs eller visualiserar problemet.

15.11.2022

Som man kan slutleda sig till av exemplet med identifiering, börjar det i processen snabbt uppkomma olika slags information och informationsbehandling, vilket ibland gör det tungt att producera riskuppgifterna. Därför är det skäl att slopa de manuella formulären som skapats med hjälp av ett kalkylprogram och ta i bruk ett professionellt digitalt verktyg som stöd för riskhanteringsprocessen. Verktöget kan antingen vara specialiserat på en viss processdel (eller flera, varvid informationen överförs mellan dem till exempel via ett riskregister som skapats i en databas) eller ett system som omfattar en större helhet och som kan vara anslutet till organisationens affärssystem. Det väsentliga är att det är tillräckligt långlivat och flexibelt för att det ska kunna utvecklas eller bearbetas i takt med utvecklingen hos både riskhanteringen och funktionerna i organisationen. Till verktygets viktigaste uppgifter hör att hålla informationsmassorna i rörelse (stöda processen) samt att hålla informationen enhetlig (jämförbar och behandlingsbar), så att användare och sakkunniga kan koncentrera sig på det väsentliga.

Särskild uppmärksamhet bör fästas vid klassificeringen av risker, eftersom dess betydelse ibland glöms bort. Olika typer av klassificering kan göras både i samband med identifiering, bedömning och analys och i samband med utvecklingen av hanteringsmetoderna. Alla dessa har egna betydelser. Vid identifieringen kan klassificeringen vara ett verktyg likt den ovan nämnda matrisen för att säkerställa att alla klasser går igenom eller att risker tas upp till behandling ur alla klasser. Det klassificeringssystem som använts, kategoriseringsstrukturen, kan dels säkerställa inriktningen på önskat sätt, dels begränsa vyn, varvid det är skäl att komma ihåg att tänka även utanför boxen i fråga. I analysen kan klassificeringen av olika risker hjälpa till att identifiera fenomen, kopplingar till riskens verkningsmekanismer eller riskkällor. Då kan vissa typer av risker kanske behandlas som större helheter där endast en viss förutsägbar egenskap förändras. När riskerna bedöms hänför sig klassificeringen i allmänhet till prioritetsgrupper, kritikaliteten eller en motsvarande bedömning som styr verksamheten. Det är viktigt att definiera dem rätt.

Efter detta, när man börjar bearbeta hanteringsmetoderna, delar man med klassificeringen upp riskerna och granskar vilka egenskaper man kan påverka på olika sätt. Olika risker på olika nivåer kan behandlas med en hanteringsåtgärd bara man identifierar en faktor som förenar dem. Detta är det skede där riskhanteringsprocessen visar sin effektivitet. I en ordentlig hanteringsprocess, i synnerhet i en större organisation, bör risker i regel inte behandlas enskilt. Användningen av effektiva klassificeringssätt i processens olika skeden gör det möjligt att hantera även stora mängder riskuppgifter för att de nödvändiga hanteringsåtgärderna ska kunna produceras och rapporteras på ett begripligt sätt.

I detta sammanhang, när man talar om bedömningens omfattning och klassificering, borde uttrycket "på samma nivå och i samma omfattning som den digitala säkerheten" innebära att säkerhetsfrågorna i anslutning till digitaliseringen har beaktats på bred front. Detta innebär att minst alla fem centrala områden av genomförandet går igenom och att övriga områden i anslutning till verksamheten beaktas. Då har denna klassificering använts för att styra granskningen. På så sätt kan riskerna bearbetas delområdesvis, vilket kan underlätta arbetet. Men efter en separat granskning måste riskerna också kombineras för en övergripande granskning och klassificering samt för planeringen av hanteringsåtgärderna. På så sätt kan riskerna i anslutning till samma sak kombineras och kontrolleras effektivt. Sammanställningen kan vara antingen en (mellan-)granskning av helheten för digital säkerhet, vilket stöder åtgärderna inom ämnesområdet, eller direkt en del av sammanställningen av den övergripande riskhanteringen, vilket stöder en mer omfattande samordning och de strategiska målen. Riskerna ska alltså bedömas och behandlas i mindre helheter som behövs för hanteringen, men de ska samlas i organisationen för att man ska kunna se deras

15.11.2022

samordnade effekter för organisationens mål. Uppgifterna om separata riskhanteringsenheter eller riskdelområden kan sammanställas endast om de bygger på enhetliga klassificeringar och gränsvärden.

En effektiv och ändamålsenlig användning av dessa termer innebär att man tar till sig skedena i risbedömningsprocessen och den upprepbarhet, de verktyg och klassificeringar med vilka man kan effektivisera genomförandet av processen. Detta skede betonas ofta, men man måste komma ihåg att detta inte är hela riskhanteringsprocessen. Syftet är att producera information för att styra hanteringsåtgärderna och den övriga verksamheten i organisationen, där man utöver riskerna även beaktar andra faktorer, såsom målen.

7.1 Preliminär bedömning

Synonym: första bedömning, primär bedömning

Definition: *bedömning som görs i början av bedömningsprocessen för att få en grov överblick*

Anmärkning: Exaktheten i den preliminära bedömningen kan variera från enbart identifiering till en analys på någon slags nivå, men vanligtvis innehåller den information på rätt så grov nivå som grundar sig till exempel på klassificering. Den preliminära bedömningen kan vara tillräcklig som sådan, men vid behov kan den förädlas med en preciserande bedömning och vidare med en ny bedömning.

7.2 Preciserande bedömning

Synonym: sekundär bedömning, fortsatt bedömning

Definition: *bedömning som görs efter den preliminära bedömningen för att få en noggrannare bedömning*

Anmärkning: Flera preciserande bedömningar kan göras.

7.3 Ny bedömning

Synonym: -

Definition: *en bedömning eller en serie bedömningar som syftar till att uppdatera eller precisera en tidigare bedömning*

Anmärkning: En ny värdering genomförs i allmänhet som en del av de dynamiska processerna, men bedömningarna kan dessutom omvärderas med jämna mellanrum för att säkerställa att bedömningarna uppdateras så att de motsvarar de förändringar som observerats i verksamhetsmiljön.

7.4 Riskbedömningsprocess

Synonym: -

Definition: *en process som omfattar identifiering av risker, riskanalys och riskbedömning*

15.11.2022

Anmärkning: Riskbedömningsprocessen är en del av riskhanteringsprocessen. I standarden SFS-ISO 31000: 2018 ges rekommendationer för riskhanteringsprocessens olika skeden, inklusive riskbedömningsprocessen (i standarden "riskbedömning").

7.5 Verktyg för riskbedömningsprocessen

Synonym: riskbedömningsverktyg, riskbedömningssystem

Definition: *riskhanteringsverktyg som styr genomförandet av delar av riskbedömningsprocessen på ett konsekvent sätt enligt vissa modeller eller metoder*

Anmärkning: Verktögen för riskbedömningsprocessen stöder effektivt de uppgifter som ingår i processen och upprepningen av dem vid fortlöpande användning mellan flera aktörer. De styr produktionen av sinsemellan jämförbara bedömningar och säkerställer att de saker som man vet är väsentliga bedöms och dokumenteras. Ett enskilt verktyg kan stöda flera delar av riskbedömningsprocessen eller koncentrera sig på ett, till exempel identifiering av risker eller analys av risker.

7.6 Bedömning av risker [aktivitet]

Synonym: bedömning av riskens betydelse, bedömning av riskens effekt

Definition: *utredning av sannolikheten för att riskerna realiserar och deras eventuella inverkan*

Anmärkning: Vid bedömningen av risker utnyttjas ofta på förhand fastställda riskkriterier och dessutom ställs riskerna i relation till varandra. De bedömningar som har gjorts tar till exempel ställning till vilka risker som i första hand ska hanteras eller vilka risker som ska analyseras. Bedömningarna kan vid behov uppdateras genom precisering eller nya bedömningar samt fördjupas genom en mer fritt formulerad riskanalys. Bedömningen av risker är en del av riskbedömningsprocessen, där den föregås av identifiering av risker. Bedömningen av risker kan göras före eller efter analysen av risker och vid behov kan analysen och bedömningen alternera som en iterativ kedja. I standarden SFS-ISO 31000:2018 hänvisar termen bedömning av risker till bedömningsprocessen, medan termen bedömning av riskernas betydelse används för detta begrepp.

7.7 Riskbedömning [resultat]

Synonym: bedömning av riskens betydelse, bedömning av riskens effekt

Definition: *resultatet av bedömningen av risken*

Anmärkning: Utifrån riskbedömningen kan nödvändiga åtgärder planeras. I rapporteringen presenteras en riskbedömning av de viktigaste riskerna, som vid behov kompletteras med en djupare riskanalys (bl.a. egenskaper och påverkningsmetoder samt eventuella hanteringsmetoder). De valda uppgifterna i riskbedömningen kan behöva delas med intressentgrupperna för att hantera riskerna och stödja intressentgruppernas egen riskhantering. Riskbedömningen kan utnyttjas, rapporteras, presenteras

15.11.2022

och sparas på behövt sätt och i önskad omfattning, till exempel genom att föra in de centrala uppgifterna i ett riskregister.

7.8 Analys av risker [aktivitet]

Synonym: riskanalys [aktivitet]

Definition: *utredning av olika riskernas natur som behövs vid bedömning av risker eller riskhantering*

Anmärkning: Riskerna analyseras med olika metoder med en noggrannhet som motsvarar behoven, till exempel riskens uppbyggnad och dess olika egenskaper, förändringar i dessa samt eventuella utvecklingsförlopp. Analysen av risker är i allmänhet mer fritt formulerad än bedömningen av risker, och analysmetoderna kan väljas från fall till fall. Analysen kan vid behov fördjupas och uppdateras som en del av den preciserande bedömningen eller av nya bedömningar. Analysen av risker är en del av riskbedömningsprocessen, där den föregås av identifiering av risker. Analysen av risker kan göras före eller efter bedömningen av risker och vid behov kan analysen och bedömningen alternera som en iterativ kedja. I standarden SFS-ISO 31000:2018 används termen riskanalys för detta begrepp, medan riskanalys i denna ordlista avser resultatet av analysen av risker.

7.9 Riskanalys [resultat]

Synonym: analys av risker [resultat]

Definition: *resultatet av analysen av risker*

Anmärkning: Utifrån riskanalysen kan riskerna bedömas och nödvändiga åtgärder planeras. I rapporteringen kan man med hjälp av en riskanalys förklara bl.a. riskens egenskaper, samband, sätt att påverka samt eventuella hanteringsmetoder, och i samband med analysen inkluderas också en riskbedömning (ofta sannolikhet och effekt eller risktal). De valda uppgifterna i riskanalysen kan behöva delas med intressentgrupperna för att hantera riskerna och stödja intressentgruppernas egen riskhantering. Riskanalysen kan utnyttjas, rapporteras, presenteras och sparas på nödvändigt sätt och i vald omfattning, och delar av dess innehåll kan tas med i uppföljningen som en del av riskregistret och/eller den allmänna uppföljningen av förändringar i verksamhetsmiljön.

7.10 Klassificering av risker

Synonym: -

Definition: *grupperingar för effektiv riskbedömning och riskhantering som gör det möjligt att betrakta likartade eller till samma ansvarsområde hörande risker eller delar av dem som en helhet*

Anmärkning: Klassificeringen av risker kan göras på mycket olika grunder, till exempel enligt ämnesområde och den kompetens som behövs vid behandlingen. Allmänt kända riskklassificeringar är PK-RH (finsk klassificering av risker i små och medelstora företag) som lämpar sig för vissa typer av företag, där riskerna indelas i



15.11.2022

strategiska, operativa, ekonomiska och skaderisker samt CVSS och OWASP som är avsedda för klassificering av hot mot informationssäkerheten. Även indelningen i strategisk nivå, koordineringsnivå och operativ nivå kan användas vid bedömning av ris-
kens inverkan eller inriktningen av olika typer av hanteringsmetoder. Metoderna för hantering av informationssäkerheten och de kontroller som används i dem kan klassificeras bland annat som administrativa och tekniska.

15.11.2022

8 Ämnesområde: Ansvar i riskhanteringen

Begrepp: ansvarsfull riskhantering, deltagande i riskhanteringen, transparens inom riskhantering

Ansvarsfullheten som helhet söker ännu sin form i den digitala verksamhetsmiljön. Ansvarsfullheten förknippas med många saker, men de varierar beroende på vilken kontext frågan diskuteras i. Beaktandet av de traditionella perspektiven på miljö och mänskliga rättigheter är en del av den samhällsgenomträngande utvecklingen, som redan framkommer bland annat i samband med upphandlingar, då man kan presentera villkor för etiska värden till exempel i anslutning till arbetsförhållanden, materialens ursprung, energiförbrukningen i produktionen eller driften, eller egenskaper som bygger på en image. Detta kan delvis också betraktas som en kvalitetsfråga. En tydlig definition behövs inte i sig för att identifiera förekomsten av detta ämnesområde och föra en diskussion via det.

Även i den digitala säkerheten kan man se ansvarsfullheten som en infallsvinkel, som dock skiljer sig från den universella förebilden och innehåller digitala särdrag. Som ovan nämnts kan köp eller försäljning av olika tekniker och säkerhetslösningar innebära frågor om ansvarsfullhet. Till dessa hör mer direkt risker som är förknippade med namn och anseende. Å andra sidan finns det också möjligheter och fördelar med god ansvarsfullhet i och med att så kallade goodwill, god vilja, i en kris kan utgöra en värdefull på förhand förvärvat fördel. Bristen på goodwill kan också visa sig vara en svaghet, till och med en risk.

En särskild ansvarsfråga för den digitala säkerheten är naturligtvis hur de olika delområdena sköts, hur man ger information om dem och hur man tar hand om kunderna, andra intressentgrupper samt helt utomstående aktörer. I synnerhet dataskyddet är förknippat med många känsliga gränssnitt som har privata och offentliga ägare utanför organisationerna. Det räcker inte att sköta informationssäkerheten enligt egna behov, utan man måste beakta andra och även kommunicera tillräckligt för att genom öppenhet kunna bygga upp förtroendet. Bland annat i EU:s NIS2-direktiv har denna aspekt lyfts fram i regleringen (se bilaga 2). Detta har ett direkt samband med hur kunderna använder (eller inte använder) tjänsterna och hurdan offentlig diskussion som förs kring ärendet – nu eller när något händer.

Hanteringen av digitala risker är en del av denna behandling. Inom ramen för en ansvarsfull riskhantering kan man diskutera huruvida riskerna för kunder och intressentgrupper sköts i tillräcklig omfattning, men också på rätt sätt. Kan de hot som riktas mot dem identifieras (och vad är tillräckligt i detta sammanhang) och kan man kommunicera om dessa och om de behövliga hanteringsmetoderna? Är de kriterier som fastställts för riskerna och särskilt för besluten om alternativen förståeliga, tål de dagsljuset och är de motiverade i synnerhet när insatserna är höga och flera syften står i konflikt med varandra inom och utanför organisationen? Överför man risken att axlas av andra, eller satsar man på det gemensamma bästa? Gör man bara det obligatoriska och billigaste, för sent och med tvång i en form, eller skapar man långsiktig verksamhet som utvecklas och där man säkerställer förhållandena, tilldelar tillräckligt med resurser och genuint utövar en ansvarsfull verksamhet? Detta är ansvarsfrågor.

Bland organisationens hanteringsmetoder finns ofta alternativa sätt att agera, i synnerhet i anslutning till mer komplexa risker. En del av metoderna kan vara mer

15.11.2022

önskvärda för andra aktörer och intressentgrupper än andra, och man bör hitta de rätta sätten att fastställa balansen mellan beaktandet av ansvarsfullheten och den extra tid eller kostnad som står till förfogande. I bästa fall medför ett alternativt tillvägagångssätt inte ens extra kostnader, utan det är fråga om en ändring av verksamhets-sättet.

Transparens inom riskhanteringen visar helt enkelt att man i tillräcklig utsträckning kan förstå orsakerna till verksamheten. Ofta söker man efter grunder för att fatta beslut som kan vara bra, men utan transparens kan grunderna inte bedömas. Transparens i sig innebär inte att man avslöjar allt, utan att man tillhandahåller tillräcklig information för att kunna identifiera en ändamålsenlig verksamhet. Det finns ingen bestämd form eller omfattning för detta. För organisationerna är det viktigt med riskhanteringen att avtalsparterna känner till och förstår deras riskhantering, risker och hot som via kedjor eller nätverkseffekter kan överföras från en organisation till en annan. Ett helt ekosystem av aktörer kan utsättas för hot. Ett bra samarbete bygger på öppen kommunikation, en bra dialog mellan parterna och ett tydligt definierat avtal. Detta möjliggör en rätt proportionerad riskhantering för organisationen och dess kunder i förhållande till den tjänst som samarbetspartnern tillhandahåller.

Att kommunicera om hot och risker ligger mycket nära detta. Det ingår i den digitala säkerhetskulturen att med organisationernas egna nätverk och också i vidare omfattning med samhället dela sådan information som kan skydda var och en. Exempel är notifikationer om observerade sårbarheter eller försök till nätfiske som sprids i andra aktörers namn. Det finns särskilda fall där lagen förpliktar till notifikationer.

Det är bra att ha fungerande kanaler även i andra riktningen, från utomstående till sakkunniga i organisationerna, eftersom de även i framtiden kommer att behöva en kanal där det är enkelt att dela med sig av observationer. Detta är en del av transparensen, även om den också kan missbrukas. Perspektivet i anslutning till detta är dock att man genom fungerande dialog kan få information av många slag som påverkar säkerheten, eventuellt från ett nätverk av observatörer som aktiveras och samarbetar. Det kan vara fråga om både intern inriktning inom organisationen och extern inriktning. Detta är en del av delaktiggörandet i riskhanteringen, det vill säga människors vilja och behov av att få påverka frågor som berör dem själva. Även i riskhanteringen borde man kunna visa (åtminstone med god kommunikation) att dessa orosmoment har beaktats tillräckligt på något sätt.

En effektiv och ändamålsenlig användning av dessa termer innebär att man även i riskhanteringen inom digital säkerhet kan tillämpa principerna för gott samarbete för att bygga upp förtroende och främja det allmänna bästa. Detta kan ses som en del av riskhanteringsmålen, eftersom en välmående och trygg verksamhetsmiljö både i och utanför digitaliseringen stöder en enskild organisations välbefinnande och trygghet. Det förbättrar i sin tur allas resiliens mot framtida komplexa hot.

8.1 Ansvarsfull riskhantering

Synonym: -

Definition: *beaktande av andra aktörers intressen eller det allmänna intresset i riskhanteringen*

15.11.2022

Anmärkning: I riskansvarig verksamhet ser man i tillräcklig utsträckning till att även risker som uppstår utanför den egna kontexten identifieras och kommuniceras om. Riskerna överförs inte heller till exempel så att konsekvenserna riktas orimligt mot en intressentgrupp utan dess samtycke och kompensering av konsekvenserna. Ansvarsfull riskhantering är också att hålla andra aktörer medvetna om nya hot som har observerats. Behandlingsåtgärderna kan dessutom väljas så att de medför gemensam nytta eller minimerar gemensam olägenhet i stället för att endast beakta eget intresse.

8.2 Deltagande i riskhantering

Synonym: -

Definition: *göra det möjligt för intressentgrupper att delta i organisationens riskhantering och uppmuntra till detta*

Anmärkning: Att involvera intressentgrupperna på ett lämpligt sätt och i rätt tid i riskhanteringen gör det möjligt att beakta intressentgruppernas kunskaper, synpunkter och observationer. På så sätt ökar man medvetenheten om riskhanteringen och säkerställer en riskhantering som grundar sig på den bästa tillgängliga informationen. Sätten och nivån på delaktiggörandet beror på ömsesidiga behov i fråga om kommunikation, hotuppgifter, riskuppgifter och lägesbilder. Delaktiggörandet kan i sig höra till riskhanteringsmetoderna eller så kan man med hjälp av den anpassa hanteringsmetoderna för att beakta delade behov.

8.3 Transparens inom riskhantering

Synonym: -

Definition: *att göra riskhanteringsbedömning möjlig för intressentgrupper och interna aktörer så att information om riskhanteringen förmedlas till de delar som förmedlingen av informationen i sig inte medför betydande risker*

Anmärkning: Transparens är en del av verksamhetens ansvarsfullhet och främjar dessutom utnyttjandet av information på ett självstyrande sätt i olika delar av ekosystemet bl.a. för att förutse störningar, vilket i sin tur minskar de överförda riskerna och riskerna med nätverkslik spridning. Transparens i riskhanteringen kan beroende på samarbetets karaktär genomföras som regelbunden rapportering för olika aktörer eller om situationen så kräver. Riskhanteringsprinciper, omfattning, beslutsprocess och påverkningsmöjligheter kan ofta öppnas på en allmän nivå även offentligt. Det kan finnas stora skillnader i transparensen i organisationen mellan olika aktörer: För vissa intressentgrupper räcker det med allmänna publikationer, medan man vid kommunikationen mellan två parter på djupet öppnar upp för andra risker och riskhanteringsåtgärder som är relevanta för samarbetet. Varje intressentgrupp har sina egna riskuppfattningar, utifrån vilka de behöver olika slags information för att säkerställa att de risker som påverkar dem behandlas på ett godtagbart sätt. Genom att svara på intressentgruppernas informationsbehov undviker man överlappande riskhanteringsåtgärder, brist på förtroende och negativa följder för anseendet.

15.11.2022

9 Ämnesområde: Informationsdelning och kommunikation

Begrepp: hotprofil, hotuppgifter, kommunikation och informationsutbyte om risker, riskrapportering, riskregister, riskuppgifter

Information om risker används för många ändamål och man kommunicerar om dem på många sätt. Anmärkningar om dessa har gjorts på flera ställen i detta presentationsdokument. En del av detta utgör av en mer formell informationsöverföring och bearbetning där man måste skilja mellan hot och risk.

Vikten av samarbete framhävs i moderna verksamhetsmiljöer där det är svårt att på egen hand få ett grepp om hela fältet. Till och med aktörer i konkurrenssituationen bör hitta en kanal för informationsutbyte inom sina verksamhetsområden, eftersom hoten kan äventyra verksamhetsbetingelserna och snabbt sprida sig – inte bara inom det egna influensområdet utan till kunderna och produktionskedjorna. Mekanismer av detta slag stöder den stabilitet som behövs, vilket i sin tur indirekt gagnar den egna riskhanteringen och målen när uppmärksamheten och resurserna kan riktas till något mer konstruktivt. Nätverkande gör det också möjligt att ta emot information.

I fråga om externa aktörer ska man alltid definiera vad som bör delas, vad som kan delas och hur för att det inte ska uppkomma onödiga tilläggsrisker för den egna verksamheten. I denna granskning är det skäl att skilja på åtminstone hotuppgifter och riskuppgifter. I fråga om hotuppgifter behandlas egenskaperna hos det observerade hotet separat från någon uttrycklig aktör, dess sårbarheter eller andra uppgifter. I fråga om riskuppgifter granskas samma sak med beaktande av aktörens svagheter och andra påverkande särdrag till behövliga delar. Hotuppgifter borde alltså i huvudsak vara information vars utlämnande inte ska störa den egna verksamheten. När det gäller riskuppgifter kan det vara nödvändigt att definiera vad som ska granskas, hur och med vem informationen ska delas, eftersom man i långt framskriden informationsdelning kan avslöja sådant som försämrar säkerheten eller verksamhetsbetingelserna (såsom affärshemligheter). Informationsdelning eller selektiv informationsdelning är i sig inte något nytt, utan syftet med detta är att betona att det är möjligt och kan göras kontrollerat även i riskhanteringskontexter.

För interna aktörer är det viktigt att sprida information om hot och riktade risker på ett mer allmänt plan, så att var och en kan beakta dessa i sitt arbete och sina förfarings-sätt. Dessutom ska man i tillräcklig utsträckning informera om riskhanteringen och det övergripande läget angående riskhanteringen, så att det inte uppstår felaktiga antaganden om organisationens situation via enskilda ärenden som ständigt är på tapeten. Ständiga allmänna varningar och rapporter om attacker runt om i världen kan leda till tvivel om de egna systemens tillförlitlighet, vilket påverkar en korrekt användning av dem, men å andra sidan kan man, i synnerhet om inga risker realiseras, invägga sig i en känsla av trygghet eller underskatta varningarnas betydelse. Även i den digitala säkerheten kan det uppstå en skillnad mellan det verkliga säkerhetsläget och trygghetskänslan (en fråga som på senare har granskats på en bredare bas som sträcker sig bortom digitaliseringen och där den digitala verksamheten har spelat en roll¹³). Denna klyfta påverkar styrningen av säkerheten och verksamhetskulturen.

¹³ TUOVI-portalen: <https://sisainenturvallisuus.fi/turvallisuuden-tunne-ja-strateginen-viestinta> (FI)

15.11.2022

En effektiv och ändamålsenlig användning av dessa termer innebär att man strävar efter att hitta en balans i hur man på rätt sätt kan hålla sina egna interna och externa intressentgrupper medvetna om vad som sker i omgivningen. Detta kräver att informationen klassificeras och hanteras på ett enhetligt sätt, så att processen och utvecklingsuppföljningen kan genomföras för identifierade fenomen och fenomen under utveckling. Utöver en omfattande granskning kan rätt inriktad forskning och utredningsverksamhet vara strategiskt viktiga för riskhanteringen och för utvecklingen av riskförståelsen.

9.1 Kommunikation och informationsutbyte om risker

Synonym: -

Definition: *kontinuerliga och återkommande processer med vilka organisationen ger, distribuerar eller skaffar information och för en dialog inom organisationen och med sina intressentgrupper om riskhantering och risker*

Anmärkning: Kommunikation och informationsutbyte om risker är en del av den normala riskhanteringsprocessen. Kommunikationen och informationsutbyte kan ske mellan två parter och i olika nätverk. Kommunikationens (inkl. varningar, utbildningar, verksamhetsstyrning osv.) betydelse för riskhanteringen framhävs när man strävar efter att förändra verksamheten.

9.2 Riskrapportering

Synonym: rapportering av risken

Definition: *kommunikation och informationsutbyte om risker i syfte att förmedla information om riskens aktuella tillstånd och hantering till vissa interna eller externa intressentgrupper*

Anmärkning: Rapporteringens djup, detaljrikedom, upprepning och presentationssätt varierar enligt målen för kommunikationen och informationsutbytet om risker samt enligt målgruppen. Till exempel riskbaserat beslutsfattande är beroende av att beslutsprocessen stöds med riskrapportering enligt dess behov.

9.3 Riskuppgifter

Synonym: -

Definition: *uppgifter om en risk*

Anmärkning: Riskuppgifterna skiljer sig från hotuppgifterna så att man i dem behandlar eventuella incidensers inverkan på organisationskontextens mål genom att jämföra och ställa konsekvenserna i relation till resurser, förmågor osv., varmed riskuppgifterna kan avslöja svagheter eller sårbarheter. Riskuppgifterna kan beskriva till exempel sannolikheten för en risk, dess effekter, grundorsaker eller hanteringsåtgärder.

9.4 Riskregister

Synonym: -

15.11.2022

Definition: *register som identifierade risker och bedömningar av dem sparas i*

Anmärkning: I riskregistret kan man spara eller länka till många slags tilläggsuppgifter, till exempel riskanalyser samt uppgifter om planerade och/eller genomförda hanteringsåtgärder. Registrets form har inte definierats i sig och om det har skapats som en separat databas kan det finnas olika riskhanteringsverktyg med vilka uppgifterna i registret behandlas och bl.a. klassificeringar genomförs automatiserat. Riskregistret samlar in riskuppgifterna i en enhetlig och uppdaterbar form, vilket gör det möjligt att följa upp riskerna och skapa en lägesbild över riskerna.

9.5 Hotuppgifter

Synonym: -

Definition: *uppgifter om ett hot*

Anmärkning: Hotuppgifterna skiljer sig från riskuppgifterna i det att de inte relaterar eventuella konsekvenser till målen, resurserna, kontrollerna osv. i organisationskontexten, utan beskriver hotet på ett allmänt plan och främst med dess egna variabler. Till exempel CVSS-bedömning av datasäkerhetshot och tillhörande rapporter är ett sätt att dela hotuppgifter.

9.6 Hotprofil

Synonym: -

Definition: *beskrivning av hotets egenskaper och egenskaperna hos det som orsakade hotet för klassificeringen av hotet*

Anmärkning: Ett hot kan orsakas av en aktör, en grupp aktörer som påverkar varandra eller till exempel ett naturfenomen. En del av de faktorer som påverkar riskerna kan härledas ur de egenskaper som beskrivs i hotprofilerna, såsom hotets läge, motivation och resurser osv. Hotprofiler som har sammanställts av attackerare kallas för attackerarprofiler.

15.11.2022

10 Ämnesområde: Riskhanteringsstrukturer

Begrepp: riskhanteringspolitik, riskhanteringssystem, riskhanteringsverktyg, riskhanteringsprinciper, riskhanteringsramar

Riskhanteringen består av många delar, men i varje organisation är den olika och svarar på olika behov. Genom att specificera dessa strukturer kan man precisera vad som fungerar i riskhanteringen och vad som bör förbättras. Det kan finnas viktningar, men helheten borde ligga på ungefär samma utvecklingsnivå. En del som fungerar på en avvikande mognhetsnivå kan störa en effektiv hanteringsprocess.

Av begreppen på högsta nivå beskriver riskhanteringsramar i stor utsträckning de administrativa resurser som fastställts för att genomföra riskhanteringen och dess ställning i styrningen och säkerställandet av organisationens verksamhet. Begreppet riskhanteringsramar avser en mer omfattande definition än bara en process eller en verksamhetsmodell för genomförandet. Det skiljer sig från den helhet som beskrivs i riskhanteringssystemet i det att riskhanteringssystemet också omfattar den egentliga verksamheten, varvid det omfattar det praktiska genomförandet inom de fastställda ramarna. Den verkliga verksamhetskulturen, de odefinierade gråzonerna och inofficiella tillvägagångssätten kompletterar det övergripande systemet för riskhantering. Då ska systemet alltså uppfattas som en socioteknisk helhet, inte bara som informationssystem.

De som leder, planerar och utvecklar riskhanteringen gör alltså klokt nog när de inser att riskhanteringsramar ska vara tillräckliga med tanke på behovet, men flera faktorer påverkar hur det verkliga genomförandet av riskhanteringssystemet utformas. Man kan sträva efter att påverka genomförandet och utformningen av riskhanteringskulturen med hjälp av riskhanteringsprinciper och en riskhanteringspolitik men man måste komma ihåg att man utöver att dokumentera dessa också ska kommunicera om dem – gärna på ett sätt som mottagaren kan dra fördel av i sin egen verksamhet.

Motvikten till abstraktiviteten hos de föregående begreppen är riskhanteringsverktyget, som ligger närmare det praktiska arbetet. Eftersom riskhanteringsverktyg i dag börjar vara datasystembaserade förväxlas de med riskhanteringssystemen. Skillnaden mellan riskhanteringssystemet och -verktyget är att man med verktyget behandlar och hanterar informationen om riskhanteringen och möjliggör en formbunden process. Verktygen är av många olika slag och en del är avsedda endast för en del av helhetsprocessen, vilket innebär att överföringen av information sker dels med hjälp av ett riskregister, dels med hjälp av en person som ansvarar för genomförandet av processen. Formuläret för anmälningar om avvikelser och gränssnittet för hantering av dessa är ett allmänt exempel på ett verktyg som är en del av helhetsprocessen. Verktyget för avvikelser kan också ha andra syften, men för riskhanteringen är det ett hjälpmedel för insamling av hotuppgifter och kollektiv identifiering av risker. Kanske för att verktyget för många är en av de vanligaste kontakterna till riskhanteringen, likställs dessa verktyg felaktigt med hela riskhanteringssystemet, vilket kan orsaka förvirring.

En effektiv och ändamålsenlig användning av dessa termer innebär att man när man granskar riskhanteringen som helhet kan skilja mellan vad som eftersträvas och vad som är verkligt. Genom planering och dokumentation av strukturer på överordnad nivå skapas en grund för att bygga, upprätthålla och utveckla helheten, men dessa

15.11.2022

frågor måste förankras. Riskhanteringsverktygets har en stor betydelse för hur riskhanteringen uppfattas och man bör kunna forma det – bland annat så att riskhanteringsprinciper och riskhanteringspolitiken kommer fram i verktyget på ett sätt som stöder verksamheten.

10.1 Riskhanteringsens ramar

Synonym: -

Definition: *organisering av riskhanteringen, ansvarsfördelning och preciserad verksamhetsmodell som inom ramen för ledningssystemet gör det möjligt att genomföra riskhanteringsprinciperna i organisationens processer*

Anmärkning: Ramarna för riskhanteringen är de administrativa strukturer som gör det möjligt att ordna riskhanteringen, men ramarna kan också begränsa dess framgång om det finns brister i dem. Till utvecklandet av riskhanteringsramarna hör att inkludera riskhanteringen i organisationens ledningssystem och att planera, genomföra, utvärdera och utveckla riskhanteringen i hela organisationen.

10.2 Riskhanteringssystem

Synonym: -

Definition: *ett hanteringssystem som omfattar riskhanteringspolitiker och mål för riskhanteringen samt processer och eventuella riskhanteringsverktyg med vilka dessa mål uppnås*

Anmärkning: Riskhanteringssystemet är en helhet som består av olika delar och deras funktioner. Helheten motsvarar inte nödvändigtvis det som är avsett, planerat eller nödvändigt, utan den kan vara föråldrad till exempel till följd av förändringar i verksamheten eller verksamhetsmiljön eller otillräcklig på grund av komplexiteten i interaktionsnätverken. Riskhanteringssystemets ändamålsenlighet kan utvärderas i samband med den interna revisionen och/eller av organisationens ledning. Riskhanteringssystemet kan vara en separat helhet, men det ska ha en nära koppling till verksamhetsstyrningen och dess system.

10.3 Riskhanteringsens principer

Synonym: principer för riskhantering

Definition: *riskhanteringsmål och en allmän verksamhetsmodell som inom ramen för ledningssystemet stöder skapandet och bevarandet av organisationens värde*

Anmärkning: Riskhanteringsprinciperna utgör grunden för fastställandet av riskhanteringsramarna och riskhanteringsprocesserna. I standarden ISO 31000 beskrivs de principer som behövs för effektiv riskhantering.

10.4 Riskhanteringspolitik

Synonym: -

15.11.2022

Definition: *organisationsspecifik beskrivning av riskhanteringsprinciperna och de centrala ramarna för riskhanteringen*

Anmärkning: I organisationer där riskhanteringsprinciperna har härletts från rekommendationer eller krav kan man i riskhanteringspolitiken klargöra principernas förhållande till organisationens mål och verksamhet. Vanligtvis dokumenteras riskhanteringspolitiken, men den kan i praktiken bestå av flera dokument. Inom organisationen är riskhanteringspolitiken en central del av ledningskommunikationen. Riskhanteringspolitiken eller delar av den kan publiceras enligt prövning.

10.5 Riskhanteringsverktyg

Synonym: -

Definition: *programvara, blankett eller annat hjälpmedel som leder till att någon del av riskhanteringen genomförs konsekvent enligt vissa modeller eller metoder*

Anmärkning: Organisationen kan ha tillgång till olika separata riskhanteringsverktyg som i bästa fall kompletterar varandra. Till exempel omfattar verktyget för riskbedömningsprocessen endast bedömningsprocessen, och därför kan det vara nödvändigt att ta i bruk verktyg som stöder andra delar av hanteringsprocessen.

15.11.2022

11 Ämnesområde: Uppföljning och lägesbild

Begrepp: lägesbild över risker, lägesbild över riskhanteringen, lägesbild över riskhanteringssystemet, riskuppföljning, uppföljning av riskhanteringen, uppföljning av riskhanteringssystemet

Riskrapporteringen, som togs upp tidigare, och lägesbilden ligger mycket nära varandra, särskilt i talspråket. Det bör dock hållas åtskilda för olika ändamål. Rapporteringen kan anses omfatta mer analys och perspektiv på alternativa framtidsscenarioer, varvid det finns alternativ att lägga fram inför beslutsfattandet. Det finns dock ingen entydig definition av skillnaden mellan begreppen och det uppstår också skillnader om det är fråga om riktad rapportering av engångskaraktär eller allmän, uppreparbar och formbunden rapportering.

Det finns mycket olika definitioner av begreppet lägesbild, om vilka en del anser att uppfattningen om situationen skapas först i mottagarens medvetande. Lägesbilden berättar alltså var man är och eventuellt vart man är på väg (och med vilken säkerhet). En central komponent i utformningen av denna bild är uppföljningen av den historiska utvecklingen, som man kan sträva efter att kombinera med information om framtidsprognoser.

Lägesbilden kan också uppfattas som en aktuell "uppdatering" av situationen vad gäller enskilda risker eller helheten, varvid den kan anses vara lättare i fråga om mängden information än vad man kunde förvänta sig av riskrapporteringen. En sådan hantering av mängden information kan ge alternativ för kommunikationen, varvid en del av behandlingen och granskningen av riskuppgifterna kan göras förenklat till exempel på månadsmöten och genomgången av rapporteringen kan koncentreras till några gånger per år. En begränsad lägesbild kan också kontinuerligt vara synlig i de centrala nyckeltalen i de automatiska rapporter som riskhanteringsverktyget bildar. Man bör dock komma ihåg att nyckeltalen inte utgör själva risken eller riskhanteringen – de är bara ett verktyg för att konstatera förändringar. De gränsvärden som fastställts för dem påminner oss bara om huruvida något ska beaktas, göras eller utredas noggrannare.

I fråga om riskhanteringsstrukturerna lyfte vi fram hur man med riskhanteringssystemet i stor utsträckning avser genomförandet och uppfyllelsen av riskhanteringen. I det sammanhanget fokuserar granskningen inte så mycket på hanteringen av enskilda risker, utan på hur systemet utnyttjas som en del av den övergripande verksamheten. Uppföljningen i anslutning till detta och den syn man skapat sig på lägesbilden är föremål för intresse särskilt för ledningen och den interna revisionen. En central fråga är i vilken utsträckning hela systemet motsvarar den modell som behövs eller eftersträvas och vilken betydelse detta har i strategin. En snävare granskning än så handlar det om i en lägesbild över riskhanteringen och tillhörande uppföljning, där man traditionellt fokuserar på processen och samordningen av dess delar. Genomförandet av riskhanteringen innebär i praktiken hur väl processen följs och om den producerar den information och de hanteringsåtgärder som behövs för såväl normal verksamhetsstyrning som exceptionella situationer. Utöver dessa tillkommer själva riskerna och riskuppgifterna.

En effektiv och ändamålsenlig användning av dessa termer innebär att man vid granskningen av riskhanteringen kan skilja på risker, processen för att hantera dem

15.11.2022

och det mer omfattande systemet kring riskhanteringen. Detta hjälper till att gestalta och administrera helheten, vilket kan äventyras om man endast följer utvecklingen av en del. Till en effektiv lägesbild hör beskrivande och lättbegripliga nyckeltal med vilka man kan följa väsentliga förändringar mellan de mer ingående rapporterna. När resurserna är begränsade är riskhanteringen ett verktyg för att rikta dem rätt och effektivt allteftersom situationer och omständigheter förändras, vilket sparar kostnader genom att man undviker de sämsta konsekvenserna.

11.1 Riskuppföljning

Synonym: uppföljning av riskfaktorer

Definition: *utredning av riskers status och trender*

Anmärkning: Inom ramen för riskuppföljningen observeras vilka konsekvenser förändringar i verksamhetsmiljön och den egna verksamheten har för riskerna, i vilken mån riskerna realiseras och hur man lyckas påverka dem med hanteringsåtgärderna. I riskuppföljningen är det bra att beakta bland annat sårbarheter, sannolikheten för risker och värdet på de objekt som ska skyddas. För uppföljningen av risker bör man använda ett riskregister och upprepa uppföljningsprocessen med lämpliga mellanrum, så att det finns tillräcklig information om eventuella förändringar i rätt tid för nödvändiga nya bedömningar.

11.2 Lägesbild över risker

Synonym: risklägesbild

Definition: *sammanställd beskrivning av resultaten av riskuppföljningen*

Anmärkning: Rapporteringen av uppföljningsresultaten och presentationssättet varierar beroende på organisationskontexten och målgruppen. Lägesbilden ska till sitt innehåll och sin omfattning lämpa sig för sitt användningsändamål, det vill säga oftast som stöd för riskbaserat beslutsfattande eller kommunikation om risker.

11.3 Uppföljning av riskhanteringen

Synonym: -

Definition: *uppföljning av läget hos riskhanteringsprocessen och därmed sammanhängande funktioner*

Anmärkning: Med hjälp av kontinuerlig och/eller regelbunden uppföljning får man information om hur ändamålsenlig och betydelsefull verksamheten är med tanke på de rådande förhållandena och behoven. Syftet med uppföljningen av riskhanteringen är att identifiera hur effektiv processen är och om den producerar rätt information i rätt tid så att den ger nytta. Riskhanteringsprocessens verksamhet kan utvärderas både av den aktör som ansvarar för processen ("andra linjen" i den s.k. trelinjemodellen) och av den interna revisionen ("tredje linjen").

11.4 Lägesbild över riskhanteringen

Synonym: -

15.11.2022

Definition: *sammanställd beskrivning av resultaten av uppföljningen av riskhanteringen*

Anmärkning: Rapporteringen av uppföljningsresultaten och presentationssättet varierar beroende på organisationskontexten och målgruppen.

11.5 Uppföljning av riskhanteringssystemet

Synonym: -

Definition: *observation av sätten att tillämpa riskhanteringssystemet och dess omfattning samt dess förändringshistoria*

Anmärkning: Riskhanteringssystemets ändamålsenlighet kan utvärderas i samband med den interna revisionen och/eller av organisationens ledning.

11.6 Lägesbild över riskhanteringssystemet

Synonym: -

Definition: *sammanställd beskrivning av resultaten av uppföljningen av riskhanteringssystemet*

Anmärkning: Rapporteringen av uppföljningsresultaten och presentationssättet varierar beroende på organisationskontexten och målgruppen.

15.11.2022

12 Ämnesområde: Riskhanterings kontexter och nivåmodeller

Begrepp: bedömningsnivå, hanteringsnivå, informationshanteringsenhet, koordineringsnivå, operativ nivå, organisationskontext, strategisk nivå

Kontexten och en korrekt definition av den är en särskilt viktig faktor för en framgångsrik riskhantering. I ett bredare perspektiv är kontexten med i varje skede av riskhanteringen, i synnerhet av den anledningen att man använder mycket information som anknyter till många olika saker och strävar efter exakthet. Riskhanteringen görs alltid utifrån en granskningskontext, varvid man i regel granskar sina egna risker. Det är organisationer som använder och producerar riskhanteringsprocessen och -strukturerna och därmed kan man tala om en organisationskontext. Därför är det ur riskhanteringssynpunkt ett hasardspel att kopiera någon annans exempel utan närmare granskning.

Definitionen av en organisation är dock inte alltid enkel, eftersom det kan vara fråga om en samverkande grupp som fungerar ihop under mycket fria former. Det kan också vara fråga om en separat avgränsad del av en större organisation eller en grupp bestående av organisationer. Med tanke på riskhanteringen borde det vara viktigt huruvida gruppen själv identifierar sig som en separat aktör och inom sig har avvikande mål (eller begränsningar), i fråga om vilka riskerna borde bedömas. Ofta kan enheternas mål och riskhantering inkluderas i organisationens strategi och övergripande riskhantering.

Informationshanteringsenheten är en särskild organisationskontext. Den ska göra en riskbedömning särskilt i fråga om den egna verksamheten, men också i fråga om kunder i anslutning till den egna verksamheten, eftersom informationshanteringsenheten behandlar bland annat personuppgifter som personuppgiftsansvarig. Lagens krav¹⁴ och definitioner kräver alltså att dessa vissa aktörer beaktar riskerna i en annan kontext som en del av organisationens egen riskhantering, huvudsakligen genom att kommunicera om dem på behörigt sätt.

Ett exempel där kontexten för kunder som använder datanät har lyfts fram som minst lika viktig som organisationens riskkontext är artikel 40.3 i EU-direktivet om en europeisk kodex för elektronisk kommunikation (2018/1972). Enligt artikeln ska det säkerställas att tillhandahållare av allmänna kommunikationsnät och kommunikationstjänster *"informerar de av sina användare som kan komma att påverkas av ett sådant hot om eventuella skydds- eller motåtgärder som användarna kan vidta. Om så är lämpligt ska tillhandahållarna även informera sina användare om själva hotet"*. Detta förutsätter identifiering av hot och risker i olika kontexter.¹⁵

Att beakta andra organisationskontexter kan anses vara ansvarsfull verksamhet med hänsyn till risker, men det kan också utnyttjas för att vidga de egna perspektiven och identifiera möjligheter. Det är bra att vara beredd om kundernas, arbetstagarnas, avtalspartnernas och andra intressentgruppers komplexa risker och i synnerhet

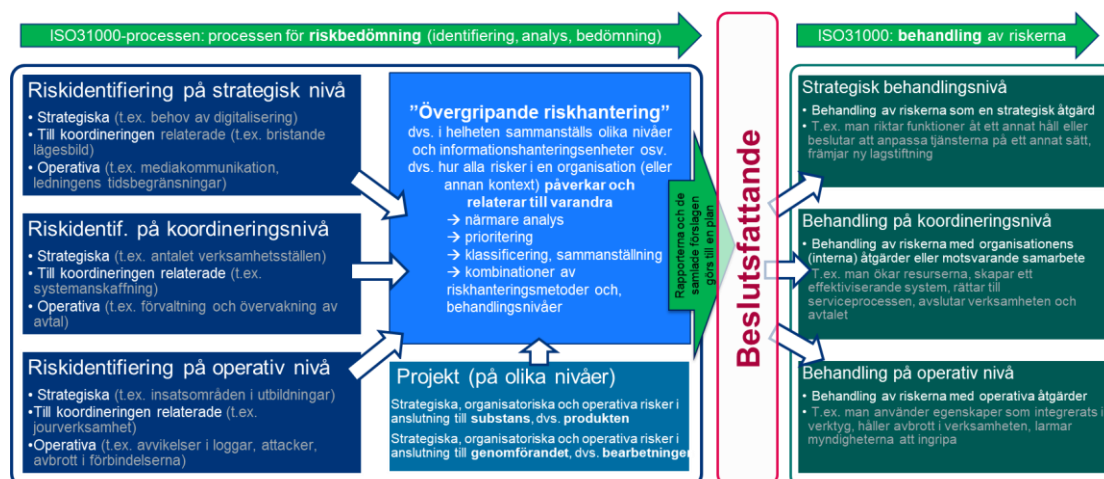
¹⁴ EU förordning (2016/679). Dataombudsmannens byrås anvisning om konsekvensbedömning: <https://ti-etosuoja.fi/sv/hur-gors-en-konsekvensbedomning> och <https://ti-etosuoja.fi/documents/6927448/66036250/TVA+ohje.pdf/ff0b6e1b-5b89-e85e-a2e5-6c4bd4c0ccfc/TVA+ohje.pdf?t=1639729535787> (s. 26, FI)

¹⁵ EU-direktivet om en europeisk kodex för elektronisk kommunikation (2018/1972) <https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A02018L1972-20181217>

15.11.2022

anseenderiskerna förverkligas, eftersom deras effekter kan återspeglas på ett överraskande sätt via kedjor och nätverk.

Om den egna organisationskontexten (vem vi är, vad vi gör, våra mål osv.) och andra bakgrundsantaganden inte definieras tillräckligt noggrant, eller om de har förändrats efter föregående definition, finns det en risk för att riskerna inte identifieras eller bedöms och analyseras på fel sätt. Ofta är det nödvändigt att fastställa på vilken nivå man vill granska riskerna. På så sätt preciseras om man i riskerna strävar efter jämförbarhet, eftersom risker som omfattar hela organisationen, är långvariga och hotar organisationens existens ses på ett annat sätt och beaktas i beslutsfattandet anorlunda än mindre och kortare risker. Bedömningsnivån skiljer sig från hanteringsnivån i och med att riskerna har kunnat identifieras och bedömas på en nivå, men de hanteringsmetoder som skapats för detta kan fördelas på olika nivåer. Det är ganska typiskt att en sårbarhet identifieras på operativ nivå, men korrigeras på operativ nivå och för att förebygga motsvarande skapas en administrativ instruktion eller varning på koordineringsnivå i organisationen. Det är också möjligt att man allteftersom motsvarande risker på operativ nivå ökar dessutom utvecklar en strategi för att beakta dem, vilket i sin tur på koordineringsnivå kan leda till att anskaffningen av ett nytt system och på operativ nivå behovet av utbildning för att använda kontrollen i fråga. Användningen av kontroller på flera nivåer skapar djup och täckning i hanteringen av den digitala säkerheten.



Figur 2: Delarna i riskhanteringsens helhetsprocess – bedömningsprocessen och hanteringsskedet – samt beslutsfattandet mellan dem. Beslutsfattandet grundar sig inte enbart på information som producerats genom riskhantering, utan beaktar också organisationens mål, resurser, verksamhet och annan väsentlig information. Det är viktigt att beakta att riskuppgifterna på olika nivåer kombineras till en övergripande riskhantering, där man utvecklar hanteringsåtgärderna för att genomföra dem på de nivåer som behövs. Behandlingen kan ske på en annan nivå än den nivå där risken har identifierats.

Den strategiska nivån, koordineringsnivån och den operativa nivån jämte synonymer ingår i den allmänna trenivåmodellen¹⁶ som beskriver det faktum att alla hot och

¹⁶ Motsvarande har tidigare presenterats bland annat som en pyramid, men i denna gamla modell har också inkluderats behandlingshierarki samt överföring av information, som inte passar in i alla användningsfall och inte stöder systemisk behandling. I detta sammanhang har också termerna "operativ" och "taktisk", beroende på organisationens bakgrund, blandats ihop från den mellersta och lägsta nivån. Dessutom anses dessa uttryck, som härrör från den militära terminologin inte lämpa sig för alla aktörer. Kommunikationsmässigt har särskilda utmaningar identifierats i anslutning till uttrycket "operativ", som också används i en viss

15.11.2022

risker inte är likadana eller likvärdiga i fråga om hur de påverkar organisationen. I stället för en trenivåmodell kan organisationen vilja använda en annan indelning som passar den bättre, men syftet med en nivåmodell är inte att skilja åt hierarkierna. Det är viktigt att inse att man genom att definiera de olika nivåerna för bedömning och behandling samt gränssnitten mellan dem (den exakta gränsen kan vara problematisk) har bättre förutsättningar att möta, klassificera och hantera riskerna.

Ett tankefel är att man endast identifierar den strategiska nivån, eftersom man i allmänhet börjar skapa planer och anvisningar för organisationer genom att definiera en ledningsstruktur. Då kan det hända att man tänker att "allt annat" finns under denna struktur, utan att närmare definiera dessa aktörer och funktioner. I en sådan konstellation uppstår ingen tydlig process, eftersom det utöver den fastställda genomförandedekedjan saknas en samtalspartner i gränssnittet, med vilken man skapar genomförandet och utbyter information för att omvandla målbilden till handlingar. Den hierarkiska gränsen kan bli för hög i båda riktningarna. Då kan det hända att man försummar att definiera hur de strategiska riktlinjerna för riskhanteringen på det mellersta planet omvandlas till förändringsprojekt inom organisationen och på det lägre planet till praktiska åtgärder. Detta behöver förtydligas i kommunikationen mellan ledningen och sakkunniga, men också i gränssnittet mellan sakkunniga och genomförarna. Även om nivåerna i huvudsak följer hierarkin i beslutsfattandet, kan själva riskerna uppstå på vilken nivå som helst och var som helst i hierarkin. Med andra ord har även "ledningsenheten" sina egna utmaningar i verksamheten och koordineringen, som inte räknas som strategiska för hela organisationskontexten.

Projekt kan också betraktas som en egen kontext. Riskhantering ska göras även i dem. Projekten avviker från en vanlig organisation som genomför processen i och med att de har en livscykel (start och slut), vilket påverkar genomförandet av projektens interna processer och riskernas livscykel. I riskhanteringen glömmer man ofta att utöver de risker som är centrala för projektets genomförande och bearbetning även granska de risker som är förknippade med projektets innehåll och slutresultat, i synnerhet med tanke på fortsättningen. De senare är viktig information för dem som upprätthåller och använder produkten samt för andra intressentgrupper som åtnjuter dess effekter. Den fungerar som input till riskhanteringen - även när den är betydelselös, vilket skingrar ovissheten. När det gäller de system som skapas ska man komma ihåg tillräcklig dataöverföring, eftersom deras olika funktioner och egenskaper tas fram inom vissa gränser, antaganden och krav, varvid de bidrar till ett säkert och önskvärt användningssätt. Allteftersom verksamhetsmiljön och användningssätten förändras kan det uppstå oväntade risker: till exempel äventyras förmågan att handla ofta om antalet ärenden som behandlas snabbt stiger en eller två storleksklasser – oavsett om det är fråga om beställningsmängder, meddelanden, störningar, terabyte eller kundservicemöten. Om projekten ingår i organisationens verksamhet ska de relevanta riskerna också integreras i organisationens övergripande riskhantering. Från ett högre perspektiv i organisationen kan ett projekt också granskas separat som en risk eller riskhanteringsåtgärd utöver de övriga värderingarna.

En lyckad definition, det vill säga en beskrivning av strukturerna, berättar hur väl de funktioner som bildas av olika helheter i organisationen och deras verksamhetsnivåer ses som ett system där funktionerna stöder sig på varandra – eller i värsta fall, hur

klassificering av risktyper där man inte tar ställning till risknivån. Användningen av denna term i sig kan ses som en meningslös, enbart talspråklig skillnad från "strategisk", vilket hör samman med problemet "allt annat" som presenteras nedan.

15.11.2022

slumpmässigt, lösryckt och ineffektivt eller mållöst de fungerar. Det är förvisso bra att påminna om att system som definierats och kopplats ihop alltför strängt inte kan vara flexibla, anpassa sig, utvecklas och reagera vid kriser, dvs. även här ska en balans eftersträvas.

I fråga om alla kontexter och nivåer bidrar ens egen och andras relativa position i dessa strukturer, som skapats för att stöda kontrollen, till att budskapet riktas rätt i kommunikationen. Detta gäller såväl innehållet, utformningen av innehållet, kanalen, tajmningen som andra variabler. Särskild uppmärksamhet ska fästas vid hur riskuppgifter allmänt rör sig mellan nivåer och kontexter. Eftersom riskbedömningarna grundar sig på ett förhållande mellan vissa av organisationens syften, resurser, know-how och andra egenskaper, kan dessa uppgifter inte överföras direkt för att användas i ett annat sammanhang. Dessa uppgifter ska alltid bedömas på nytt (helt och hållet från början eller med hjälp av lämpliga omvandlingsmekanismer) när de passerar olika gränssnitt eller annars kan deras betydelse förvrängas.

En effektiv och ändamålsenlig användning av dessa termer innebär att man kan identifiera både rätt kontext enligt organisation eller en annan bakgrundsgrupp och rätt nivå för att kunna identifiera riskerna på ett heltäckande sätt och förstå deras innebörd rätt. Utöver dessa ska man också komma ihåg andra definierande faktorer, såsom de olika områdena för genomförande av digital säkerhet som perspektiv på riskerna och hanteringen av dem, där man också måste kunna rikta åtgärderna till flera nivåer vid behov. En felaktig definition av kontexten ökar risken för en bristfällig identifiering av riskerna. Behandlingen av risker som en helhet kan vara ineffektiv, förvränga bilden av dem och göra det svårt att skapa en tydlig hanteringshelhet.

12.1 Organisationskontext

Synonym: -

Definition: *den organisation eller del av den vars perspektiv granskningen görs utifrån*

Anmärkning: Varje organisation utför riskhantering utifrån sin egen kontext: vad som identifieras som risker förändras beroende på i vilken organisation man befinner sig – och i vilken del av den. Varje instans i organisationen har till exempel egna mål, resurser och krav inom vilka inställningen till riskerna uppstår. I stora organisationer kan linjeorganisationernas olika verksamhetsenheter eller deras verksamhetsnivåer ha helt olika synvinklar. Även behandlingsnivåerna kan bilda egna kontexter. Ett särskilt exempel på organisationskontext är informationshanteringsenheter som inte nödvändigtvis har en separat organisationsstruktur i bakgrunden, men vars lagstadgade uppgift definierar behovet av riskhantering. Resultaten av de riskbedömningar som olika kontexter producerar inom organisationen bör sammanställas för att producera en heltäckande övergripande riskhantering. När man utbyter riskuppgifter vid ett byte av organisationskontexten – särskilt mellan organisationer – ska antagandena och proportionerna i anslutning till riskerna granskas och omvärderas via ett nytt perspektiv. Organisationen kan ibland vara ovanlig, till exempel inofficiell eller virtuell, varvid även organisationskontexten är av särskild art.

12.2 Informationshanteringsenhet

Synonym: -

15.11.2022

Definition: *en myndighet eller en organisationskontext som består av myndigheter och som är skyldig att ordna sin informationshantering i enlighet med kraven i lagen om informationshantering inom den offentliga förvaltningen 906/2019*

Anmärkning: Informationshanteringsenheter är statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärssärenden, riksdagens ämbetsverk, statliga affärsverk, kommuner, samkommuner, självständiga offentlighetsrättsliga inrättningar, universitet som avses i universitetslagen samt yrkeshögskolor som avses i yrkeshögskolelagen (2 kap. 4 § i informationshanteringslagen 906/2019).

Informationshanteringsenheten är en särskilt definierad organisationskontext för riskhantering som bedömer riskerna i anslutning till den information som den behandlar.

12.3 Bedömningsnivå

Synonym: -

Definition: *nivå ur vars synvinkel risken granskas*

Anmärkning: Risken kan granskas till exempel utifrån den strategiska, koordinerande eller operativ bedömningsnivån, om en sådan nivåindelning används. I granskningen strävar man efter att identifiera riskens betydelse på denna nivå och ställa den i relation till bl.a. verksamheten, målen och påverkningsmöjligheterna på denna nivå.

12.4 Hanteringsnivå

Synonym: -

Definition: *nivå som risken hanteras på*

Anmärkning: Risken kan behandlas till exempel på strategisk, koordinerande eller operativ hanteringsnivå, om en sådan nivåindelning används. I praktiken behandlas samma risk vid behov på flera olika nivåer så att hanteringen av risken inte blir bristfällig.

12.5 Strategisk nivå

Synonym: -

Definition: *beslutsnivå i en organisation där beslut som gäller verksamhetsmiljön och verksamhetens finansiering fattas om hela organisationens verksamhet och utveckling*

Anmärkning: I riskhanteringen kan riskens bedömningsnivå eller hanteringsnivå vara strategisk: På den strategiska bedömningsnivån granskas riskerna med tanke på hela organisationen, och på den strategiska hanteringsnivån behandlas riskerna utifrån detta perspektiv.

12.6 Koordineringsnivå

Synonym: koordinerande nivå, organisatorisk nivå

15.11.2022

Definition: *beslutsnivå i organisationen, på vilken beslut om organisering av enskilda affärsområden och enheter fattas med beaktande av de strategiska besluten*

Anmärkning: Beroende på organisationens storlek och organiseringsätt är det inte nödvändigtvis möjligt eller ändamålsenligt att skilja åt koordineringsnivån från den operativa nivån. Koordineringsnivån för en risk kan utgöras av bedömnings- eller hanteringsnivån inom riskhanteringen: på en koordinerande bedömningsnivå granskas riskerna med tanke på hela affärsområdets eller enheters verksamhet, och på en koordinerande hanteringsnivå behandlas riskerna ur detta perspektiv. När man skiljer åt beslutsnivåer används ofta termerna strategisk, taktisk och operativ nivå, men i synnerhet taktisk och operativ får i olika sammanhang mycket olika betydelser som inte motsvarar den indelning som presenteras här och alltså inte är synonyma till koordineringsnivå och operativ nivå.

12.7 Operativ nivå

Synonym: produktionsnivå

Definition: *beslutsnivå i organisationen, på vilken beslut om genomförande och genomförande fattas med beaktande av den strategiska nivån och koordineringsnivån*

Anmärkning: I riskhanteringen kan riskens bedömningsnivå eller hanteringsnivå vara operativ: på den operativa bedömningsnivån granskas riskerna med tanke på genomförandet och verkställandet, och på den operativa hanteringsnivån behandlas riskerna ur detta perspektiv. När man skiljer åt beslutsnivåer används ofta termerna strategisk, taktisk och operativ nivå, men i synnerhet taktisk och operativ får i olika sammanhang mycket olika betydelser som inte motsvarar den indelning som presenteras här och alltså inte är synonyma till koordineringsnivå och operativ nivå.

15.11.2022

13 Ämnesområde: Betydelser av riskhantering och risker

Begrepp: framförhållning, kritiskhet, kvarstående risk, riskbärkraft, riskmedvetet beslutsfattande, värde för oförverkligad effekt

Ett allmänt syfte med riskhanteringen är att producera förhandsvarningar om eventuella problem så att de kan beaktas i tid. Ur detta perspektiv är riskhanteringen en del av framförhållning i anslutning till forskningen om framtida utvecklingsförlopp. Arbetet med att ta fram prognoser är dock ett mer omfattande uppgiftsområde, eftersom det också behandlar mer allmänna utvecklingsförlopp och dess tidshorisont (eller tidsfönster) i allmänhet ligger betydligt längre fram i framtiden än i riskhanteringen. Riskhanteringen är kortvarigare och tillämpningen av den begränsas i huvudsak lika långt som den nuvarande (och föränderliga) strategiska utsikten.

Framförhållningsarbete görs i huvudsak för att producera information och bakgrund för att skapa nya strategier, det vill säga för vad som ska göras efter de nuvarande strategierna. Syftet är att förstå förändringarna i verksamhetsmiljöerna och deras konsekvenser. De alternativa framtidsbilder som skapats grundar sig i allmänhet på förhållandevis svagare signaler om möjligheterna än vad som vanligen används i riskhanteringen. Perspektivet är ofta ett eller ett par årtionden framåt, men samtidigt belyses i allmänhet också utvecklingsförloppet fram till prognosåret. Framförhållningsarbetet skapar alltså input även för riskhanteringen, så att riskerna kan bedömas i förhållande till kommande förändringar och behov.

När man granskar tidslinjens andra ände, även om man inte kan fastställa någon egentlig nedre gräns, bestämmer den tid som använts för att genomföra riskhanteringsgranskningsprocess – dvs. hur lång tid det tar att upptäcka och behandla olika risker på olika nivåer – nyttan av processen i nuläget. Tiden varierar naturligtvis beroende på hur stort hot det är fråga om. Med tanke på ledningen av riskhanteringen är det viktigt att riskhanteringsprocessen och riskhanteringssystemet är effektiva och snabbcykliska.

Hot som realiseras snabbare än man hinner upptäcka och hantera måste behandlas som en reaktion på den akuta incidensen i stället för framförhållning. Om den framförhållning som riskhanteringen producerar inte är tillräcklig, kan de akuta situationerna utgöra en kris om de överskrider de resurser som reserverats för beredskapen. Detta kan ses både som en brist på observationsförmåga, en risk för otillräcklig riskhantering och som beredskap som vanligen ingår i kontinuitetshanteringen.

När organisationen har tillräcklig förståelse för sitt riskhanteringssystemets förmåga kan man med större tillförsikt acceptera och bära de kvarstående riskerna, eftersom de förknippas med mindre osäkerhet. Allt kan dock inte behandlas eller vara känt: att tolerera osäkerhet och sträva efter att identifiera och förstå de faktorer som orsakar osäkerhet är en del av riskhanteringen och ledningen. Risk kvarstår i praktiken alltid och man måste orka bära den, både psykiskt och som förmågan att vid behov agera till och med om det värsta alternativet förverkligas.

Framförhållning och riskhantering ger information för beslutsfattande som styr organisationen. Som det har påpekats är den information som riskhanteringen producerar endast en del av den information som produceras för beslutsfattandet. Bra riskuppgifter ger en stark grund för åtgärder och i planerna för hanteringsmetoderna borde det finnas alternativ med hjälp av vilka man bäst kan fatta beslut som lämpar sig för andra behov. Detta är ett bra riskmedvetet beslutsfattande på allmän nivå.

15.11.2022

I vissa fall underlättas beslutsfattandet om det ärende som behandlas kan anses vara särskilt viktigt, eftersom valet då är svartvitt. En fördel med ett ärende som på ett tillbörligt sätt identifierats som kritiskt är att man är medveten om det på förhand. Ibland kan man dock understryka vikten av ett riskobjekt genom att på lätta grunder stämpla det som kritiskt. Här bör man kontrollera om ärendet behandlas på en nivå där man talar om konsekvenser som hotar tillvaron eller om konsekvenser som leder till att någon fördel eller egenskap går förlorad, såsom störningar i verksamheten eller förmodligen att på annat sätt agera normalt (jämfört med att man vore tvungen att lägga ned verksamheten).

En närmare granskning kan alltså visa på olika grader av kritiskhet, vilket kan vara skenbart ologiskt med tanke på begreppet i fråga. Även kritiskhet kan underordnas målen, varvid det inte anses vara tillräckligt att enbart klara sig (minimal överlevnad), utan man måste kunna bevara en viss verksamhetsnivå. Förlusten av denna nivå jämföras då med en katastrof. Organisationerna kan (särskilt inom den offentliga förvaltningen) med fog definiera vissa faktorer som möjliggör verksamheten som kritiska, i synnerhet om många andra aktörers handlingsförmåga beror på dem. Grunderna för att definiera kritiskheten bör dock vara tydliga och transparenta.¹⁷

Den andra sidan av de antagna incidenserna är att man genom god riskhantering på förhand kan undvika åtminstone de värsta följderna eller till och med helt och hållet undvika följder. Det är dock ofta omöjligt att konstatera eller hitta en direkt orsak till varför något inte inträffade. Detta gör det utmanande att fastställa ett värde för åtgärderna, eftersom ekonomiska faktorer utgör en betydande del av grunderna för beslutsfattandet. Den centrala tanken är att säkerhetens värde, även inom digitaliseringen, ligger i hur den stöder uppnåendet av målen. Av detta kan man också härleda ett sätt att motivera betydelsen av riskhantering.

Om man vill ge riskerna ett värde i euro finns det två huvudsakliga sätt att göra det på. I det första granskas de potentiella förlusterna om riskscenariot förverkligas och i det andra värdet av de åtgärder (investeringar) som behövs för att förebygga detta. Man ska inte blanda ihop sätten, eftersom de är bedömningar ur olika synvinklar. Båda producerar en siffra, men räknesätten är flera. I sätten bör beaktas att organisationens verksamhetssätt och strukturer för digital säkerhet ska beskrivas i den mån det är möjligt, så att de åtminstone har en indikerande koppling till förvaltningen av området i fråga. Det bör beaktas separat att det finns skillnader i definitionen av värdet på den offentliga och den privata sidan bland annat genom lagliga förpliktelser, vilket också påverkar sättet att bedöma riskerna och kommunicera om dem.

En effektiv och ändamålsenlig användning av dessa termer innebär att man förstår riskhanterings betydelse för beslutsfattandet och ledningen i organisationen. Hanteringen och godkännandet av den kvarstående risken är en central del av detta. Organisationen och dess ansvariga enheter ska vara medvetna om sina egna risker, de kvarstående delarna av riskerna samt riskbärkraften och de faktorer som påverkar den, så att de kan beaktas i verksamheten.

¹⁷ I stödmaterialiet VAHTI God Praxis ingår ett verktyg för bedömning av kritiskheten. Det utvecklas som en efterträdare till de tidigare Palko- och BIA-verktygen. Det är inte nödvändigt att använda verktyget, men identifiering av kritiskheten kan hjälpa till att rikta in riskhanteringen. Kriittisten kohteiden luokittelu (klassificering av kritiska objekt, FI): <https://dvv.fi/digiturvajulkaisut>

15.11.2022

13.1 Framförhållning

Synonym: -

Definition: *bedömning av förändringstrender i organisationen och verksamhetsmiljön samt utredning av förutsättningarna för potentiella utvecklingsförlopp*

Anmärkning: Medan riskhanteringen vanligtvis producerar detaljerad och praktisk information om relativt begränsade ämnen och ur ett relativt kort tidsperspektiv, strävar man genom framförhållning efter att skissa upp långsiktiga trender och trender i omfattande helheter. Genom framförhållning kan man identifiera hot och möjligheter samt sätt att påverka dem, och dessa uppgifter kan utnyttjas vidare i riskhanteringen. Framförhållning är inte alltid övergripande, utan den kan fokusera på till exempel en enskild verksamhet eller ett projekt. I talspråk kan framförhållning innebära inte bara att man producerar bedömningar och utredningar, utan också att man agerar utifrån dem.

13.2 Riskmedvetet beslutsfattande

Synonym: riskbaserat beslutsfattande

Definition: *beslutsfattande där man har beaktat resultatet av riskbedömningsprocessen*

Anmärkning: Riskmedvetet beslutsfattande är inte enbart beslutsfattande som grundar sig på en riskbedömningsprocess, utan i beslutsfattandet ska man alltid beakta även andra uppgifter och perspektiv, såsom målen och den övriga verksamheten. Beslutsfattarna bör ha en uppfattning om ursprunget till och kvaliteten på de riskuppgifter de använder.

13.3 Kvarstående risk

Synonym: -

Definition: *återstående risk efter riskhanteringen*

Anmärkning: Med kvarstående risk kan avses den del av den ursprungliga risken som enligt planerna inte omfattas av hanteringsåtgärderna, varvid man också kan tala om att bevara risken. Å andra sidan kan den kvarstående risken inte alltid elimineras med tillgängliga metoder eller så kan den omfatta en oidentifierad riskdel som kan uppdagas först när risken realiserar. Kvarstående risker som identifierats i riskhanteringsprocessen ska godkännas eller vidarebehandlas. Vid bedömningen av kvarstående risker beaktas riskhanteringsförmågan till exempel med hjälp av de gränsvärden som fastställts för riskerna.

13.4 Riskbärkraft

Synonym: riskhanteringsförmåga, kapacitet att bära risker -

Definition: *organisationens förmåga att anpassa sig till följderna av eventuella risker*

15.11.2022

Anmärkning: Med riskbärkraft avses i allmänhet ekonomisk bärkraft, men följderna kan också granskas till exempel med tanke på organisationens anseende eller personalens välbefinnande. Riskbärkraften bestämmer de gränser inom vilka organisationen kan ta risker. Ingen organisations riskbärkraft är perfekt, men organisationen kan klara av följderna av många slags risker och kombinationer av risker. I synnerhet vid beslut om kvarstående risker är det viktigt att veta vilka risker eller kombinationer av risker som hotar organisationen.

13.5 Kritiskhet

Synonym: -

Definition: *nödvändighet för att uppnå målen eller undvika särskilt skadliga följder*

Anmärkning: Kritiskheten granskas i allmänhet i riskhanteringen med tanke på organisationen, men perspektivet kan också utgöras till exempel av en kund, ett projekt, en process, ett samarbetsnätverk, medborgarna eller samhällsfunktionerna. En kritisk fråga, till exempel ett system som identifierats som kritiskt, svarar mot de centrala behoven med tanke på dess överlevnad och kontinuitet, ur vars synvinkel den är kritisk. För kritiskhet kan man i vissa sammanhang skilja mellan olika typer och nivåer, varvid alla kritiska faktorer inte nödvändigtvis har att göra med hur man klarar sig i sig, utan till exempel med verksamhetens meningsfullhet, bevarandet av vissa förmågor eller förlusten av en central insats.

13.6 Värde för oförverkligad effekt

Synonym: värde för effekt utan incidens

Definition: *omvänt värde för effekten av en undviken risk, med hjälp av vilket man kan beskriva verkningsfullheten i riskhanteringen*

Anmärkning: Med hjälp av värdet för oförverkligad effekt kan man beskriva kostnadseffektiviteten i riskhanteringen och huruvida den motsvarar målen. I det sammanhanget kan man beakta vilket värde de förlorade möjligheterna skulle ha haft. I synnerhet i fråga om indirekta risker är en riktgivande bedömning i allmänhet tillräcklig. Värdet för effekt utan incidens uttrycks inte alltid i pengar, utan kan till exempel ha att göra med anseendet eller en organisations samhälleliga uppdrag.

15.11.2022

14 Ämnesområde: Egenskaper hos riskens uppbyggnad

Begrepp: direkt risk, indirekt risk, kumulativ risk, risk med nätverkslik spridning, överförd risk

Den moderna synen på den digitala verksamhetsmiljön omfattar en socioteknisk struktur, där förutom utrustning och nät även människorna och deras handlingar räknas med i den komplexa helheten. Detta har också beskrivits som en VUCA-tid, som kommer från de engelska orden förändringskänslighet, osäkerhet, komplexitet och tolkningsbarhet (Volatility, Uncertainty, Complexity, Ambiguity). Uttrycket beskriver hur verksamhetsmiljön/-miljöerna kan förändras snabbt och oförutsägbart och därefter påverka genom komplexa ömsesidiga beroenden och mångtydighet. Detta utmanar både riskhanteringen och även i övrigt hur man förutser framtiden. Komplexa konsekvensstrukturer kräver mer för att man ska förstå dem. För den allt snabbare förändringstakten krävs att en ny bedömning görs tillräckligt ofta, vid snabba förändringar måste man upprätthålla förmågan att reagera snabbt. Mångtydigheten ökar behovet av att kunna göra tolkningar av olika kontexters synsätt samt kommunicera med beaktande av dem.

Tydliga omedelbara risker kan ibland betraktas som en självklarhet. De kan fortfarande hamna i toppen av risklistorna, men deras direkta effekter och kontrollmetoderna för normala situationer kan vara vilseledande. Det är också skäl att granska vilka biverkningar och oväntade följder av dem som kan uppstå om en risk realiserar – i synnerhet om det samtidigt uppstår en annan risk. Vid attacker försöker man hitta enkla luckor, eftersom det är svårt att kringgå flera kontroller, men i verkliga situationer är det vanligt att flera risker realiserar samtidigt. Antalet olika kombinationer kan vara för stort för en fullständig granskning, varvid man måste stärka förståelsen för screening av de viktigaste och sannolika kombinationerna för den fortsatta behandlingen.

Dominofenomenet i effektkedjorna kan överföra risker och effekter från andra aktörer eller från system till system på ett oväntat sätt. I synnerhet när externa tjänster används bör det finnas fungerande kommunikationsförbindelser med samarbetsparterna, så att parter är medvetna om varandras betydande risker samt kontroller och riskhanteringsförmåga i anslutning till dem. Mer komplicerade än direkta kedjor är nätverksbaserade effekter, där fenomenen kan påverka på de mest speciella sätt, till exempel genom flera mindre incidenser vars gemensamma effekt är betydligt större. Fenomen som utvecklas oväntat är ofta förknippade med en multiplikatoreffekt eller skalning av en storleksklass som inte kan behandlas inom gränserna för normal beredskap eller gränserna i systemet. Samtidigt bör man i hanteringsmetoderna beakta vilka biverkningar de kan ha i nätverken och hur de kan påverka andra.

En effektiv och ändamålsenlig användning av dessa termer innebär att man förstår hur riskerna kan uppstå på olika sätt och hur konsekvenserna kan överföras på ovanliga sätt. Eftersom varje åtgärd och incidens har biverkningar för den egna eller andras situation, bör man sträva efter att på förhand granska dem för att välja det lämpligaste alternativet. Eftersom förändringar sker kontinuerligt är det skäl att göra en ny bedömning av riskerna och verksamhetsmiljön tillräckligt ofta.

15.11.2022

14.1 Direkt risk

Synonym: omedelbar risk

Definition: *risk vars källa direkt påverkar objektet*

Anmärkning: I organisationen påverkas den omedelbara risken bl.a. av de anställda i organisationen samt av den utrustning och det material som organisationen använder. En direkt risk kan också påverka över organisationsgränserna.

14.2 Indirekt risk

Synonym: -

Definition: *risk vars källa indirekt påverkar objektet*

Anmärkning: Indirekta risker är ofta svårare att identifiera och hantera än direkta risker. Indirekta risker kan bero på kedjor (se överförd risk), nätverk (risk med nätverkslik spridning) eller strukturella förändringar i verksamhetsmiljön.

14.3 Överförd risk

Synonym: -

Definition: *indirekt risk som överförs från ett annat objekt*

Anmärkning: En överförd risk kan likt ett dominofenomen överföras till ett objekt som granskas via många andra objekt. När risken överförs kan sannolikheten för att den realiserar och dess följder förändras.

14.4 Risk med nätverkslik spridning

Synonym: nätverkslik risk, komplex risk

Definition: *indirekt risk som härstammar från ett nätverk av komplexa effektkedjor*

Anmärkning: En risk med nätverkslik spridning är ofta en följd av komplexiteten i verksamhetsmiljön. Till skillnad från en överförd risk kan effekterna av en risk med nätverkslik spridning till exempel förgrenas och kopieras (skalas) och deras ursprung kan sällan identifieras. Det är i de flesta fall omöjligt att helt kunna förutspå hur risker med nätverkslik spridning kommer att bete sig.

14.5 Kumulativ risk

Synonym: tilltagande risk

Definition: *risk vars storlek består av samverkan mellan flera riskfaktorer*

Anmärkning: Effekten av en kumulativ risk kan vara summan av riskfaktorernas följder, men ofta interagerar riskfaktorerna så att samverkan är större. Till exempel är enskilda personuppgifter sammanlagt inte förenade med lika betydande risker som den omfattande databas som består av dessa personuppgifter.

15.11.2022

15 Ämnesområde: Riskpåverkan

Begrepp: kontroll, operativ användbarhet, planerad att ha få risker

Det är viktigt att känna till hoten och identifiera riskerna, men riskhanteringen görs för att man ska kunna hantera riskerna, dvs. vidta åtgärder för att hantera dem. Det finns många olika slags kontroller. Endast ett fåtal av dem utgör i dagens komplexa verksamhetsmiljöer en perfekt match till den risk som är motpart. Kontrollerna kan täcka flera risker på en gång, men också bara omfatta en del av risken och orsaka störningar för den övriga verksamheten. Därför måste man kunna välja en helhet där flera kontroller tillsammans producerar ett tillräckligt omfattande och heltäckande skydd mot konsekvenserna, utan överdriven överlappning. Å andra sidan skapar just överlappningar djup och därmed säkerhet i hanteringsmetoderna.

Kontrollerna bottnar i teoretiska riskhanteringsmetoder som ofta kan kombineras. En risk kan avvärjas genom att avsluta någon verksamhet eller genom att inte inleda någon verksamhet, varvid man inte heller tar någon risk. Den måltavla eller sårbarhet som risken använder som kanal kan elimineras. Sannolikheten för att risken realiserar kan ändras på olika sätt, likaså dess effekter. Risken kan också fördelas eller överföras genom avtal eller försäkringar till en tredje part. Risken kan hållas, tas eller till och med ökas om man i den (eller i de förvaltningsåtgärder som vidtas för den) ser tillräckligt mycket som är användbart och värt att eftersträvas – eventuellt till och med sådant som i sig inte är förknippat med risken. Genom att gå längre än så är ett särskilt tillvägagångssätt bland hanteringsmetoderna att sträva efter att omvandla riskerna till möjligheter och positiva slutresultat. Där kan man skapa nytt och anpassa det som finns från förut. Ju mer man stöder de bredare målen, desto bättre. Då blir den digitala säkerheten till en möjliggörare.

En särskild metod för att hantera riskerna är de principer som tillämpats redan vid förhandsplaneringen, med vilka man strävar efter att producera utrustning och system där man eliminerat centrala riskbildande egenskaper. Det här kallas "säkerhet genom design" (security by design). När man särskilt beaktar dataskyddet har det vid sidan av detta också uppkommit bland annat den motsvarande principen om inbyggt dataskydd (privacy by design) samt principerna om säkerhet som standard och dataskydd som standard (security by default, privacy by default). När man talar om att påverka riskerna i organisationers system bör man i principerna också inkludera till exempel "planerad för hantering och kontroll", så att olika krav kan uppfyllas effektivt, begripligt och säkert.

Flera synvinklar på kontrollerna kunde lyftas fram. En är den operativa användbarheten. Brist på operativ användbarhet kommer fram särskilt i många säkerhetslösningar där användaren inte har beaktats i tillräcklig utsträckning. Dålig operativ användbarhet styr mot felaktig användning och verksamhet, i motsats till vad man eventuellt har försökt förhindra. Allteftersom användargränssnitten blir alltmer komplexa är det till och med möjligt för människan att ignorera säkerhetsåtgärder – särskilt i stressande situationer. Detta kan tolkas genom att användarna är beredda att använda endast begränsat med tid och arbete för att trygga säkerheten. Man kan alltså stöta på att användarna upplever en klyfta mellan de kontrollmetoder som anses nödvändiga och den säkerhet som upplevs som uppnådd.

15.11.2022

Man måste också komma ihåg att oavsett hur säker vår process, vårt system eller våra produkter är, kan en tung eller annars dålig användbarhet göra att de rubbas eller snedvridas. Dessa är indirekt kopplade till kommunikationen. En välplanerad och användbar helhet, vars syfte förstås och som inte medför risker, behöver mindre kommunikation som stöd till exempel i form av instruktioner, förklaringar och motiverande meddelanden. Användarperspektivet har alltså ett värde även för säkerheten.

En effektiv och ändamålsenlig användning av dessa termer innebär att man har förstått de principer som ligger bakom de metoder som utvecklas för att kontrollera riskerna. När man planerar hanteringsåtgärder bör man i första hand sträva efter att beakta genomförandesätt där man för det första inte lämnar något utrymme för riskutveckling, och dessutom använder det säkraste alternativet för olika egenskaper. Dessa egenskaper bör skapas så att det "säkraste" täcker både organisationen och systemet och klientens eller intressentgruppens synpunkter.

15.1 Kontroll

Synonym: hanteringsmetod, hanteringsåtgärd

Definition: *åtgärd genom vilken man strävar efter att ändra eller bevara en risk*

Anmärkning: Kontrollerna kan vara processer, verksamhetsprinciper, utrustning, praxis, engångsåtgärder eller annan typ av verksamhet. Förhandskontroller strävar i allmänhet efter att minska sannolikheten för risker, medan efterkontroller minskar riskernas inverkan. Man kan försöka bevara en risk om den är förknippad med möjligheter eller om man inte vill att den ska ersättas med en annan, eventuellt värre risk. Termen hanteringsmetod används ibland som synonym till kontroll, men ofta hänvisar hanteringsmetod till en helhetslösning (t.ex. identifiering eller god förvaltningssed) som kan innehålla flera konkreta kontroller. Kontrollerna kan granskas enligt typ eller enligt det skyddade objektet, till exempel tillsynsåtgärder, dvs. övervakningskontroller som en egen grupp eller kontroller som skyddar tillgången till information som en helhet.

15.2 Planerad att ha få risker

Synonym: planerad som riskminimerande, inbyggd riskminimering

Definition: *en på förhand planerad egenskap eller metod för en produkt, tjänst eller process där vissa risker som är specifika för den har beaktats*

Anmärkning: I planeringen beaktas i allmänhet risker av någon risktyp, såsom data-skyddsrisker (eng. privacy by design¹⁸) eller säkerhetsrisker i vidare bemärkelse (eng. safety by design, security by design). Till exempel i en enkät kan man undvika frågor vars svar är förknippade med informationssäkerhets- eller dataskyddsrisker, om det inte är nödvändigt att samla in dem. Om man ändå samlar in uppgifter som är förknippade med informationssäkerhetsrisker kan insamlingen genomföras så att alla uppgifter förmedlas som skyddade meddelanden och lagras på ett informationssäkert sätt i stället för att uppgifterna samlas in till exempel i en insamlingslåda av kartong i ett offentligt utrymme. Dessutom kan hanteringen av tillträdes- och nyttjanderätter

¹⁸ Anvisningar om planering och standardvärden i anslutning till dataskydd på Europeiska dataskyddsstyrelsens webbplats: [Guidelines 4/2019 on Article 25 Data Protection by Design and by Default](#)

15.11.2022

planeras så att de medför en låg risk, till exempel så att det krävs samtycke av flera personer för att bevilja vissa rättigheter. Om man på grund av olika behov även måste tillåta alternativ i en produkt eller process där riskerna inte har minimerats, kan en liknande effekt uppnås så att det minst riskfyllda alternativet alltid är standardvärdet (eng. security by default, privacy by default osv.), medan risktagning kräver separata åtgärder.

15.3 Operativ användbarhet

Synonym: -

Definition: *en egenskap hos ett datasystem, en enhet eller en process som visar att det är lätt att lära sig den, dess verksamhetslogik är lätt att komma ihåg, dess funktion stöder de uppgifter som användaren ska utföra med den och den främjar en säker och enkel användning av den*

Anmärkning: Brister i den operativa användbarheten är en svaghet: om det finns brister i den operativa användbarheten kan den öka den felaktiga användningen, vilket i sin tur kan leda till sårbarhet.



15.11.2022

16 Index

Översättningarna grundar sig på VAHTI-riskhanteringsordlistan. När man använder termerna ska man beakta att översättningen inte alltid garanterar rätt betydelse i utländska kontexter.

16.1 Finska

Termit ja synonyymit	Suositeltu	Nro	Sivu
alustava arvio	alustava arvio	7.1.	30
arvio riskien merkityksestä	riskiarvio	7.7.	31
arvio riskien vaikutuksesta	riskiarvio	7.7.	31
arvio riskin merkityksestä	riskiarvio	7.7.	31
arvio riskin vaikutuksesta	riskiarvio	7.7.	31
digiriski	digitaalisen toiminnan riski	4.2.	16
digitaalinen riski	digitaalisen toiminnan riski	4.2.	16
digitaalinen toimintaympäristö	digitaalinen toimintaympäristö	4.1.	16
digitaalinen turvallisuus	digitaalinen turvallisuus	4.3.	16
digitaalinen ympäristö	digitaalinen toimintaympäristö	4.1.	16
digitaalisen toiminnan riski	digitaalisen toiminnan riski	4.2.	16
digitoimintaympäristö	digitaalinen toimintaympäristö	4.1.	16
digiturvallisuus	digitaalinen turvallisuus	4.3.	16
ennakointi	ennakointi	13.1.	54
ensiarvio	alustava arvio	7.1.	30
ensiöarvio	alustava arvio	7.1.	30
epäsuora riski	välillinen riski	14.2.	57
epävarmuus	epävarmuus	6.1.	23
haavoittuvuus	haavoittuvuus	6.3.	24
hallintakeino	kontrolli	15.1.	59
hallintatoimi	kontrolli	15.1.	59
heikkous	heikkous	6.4.	24
hyökkäyksen aiottu kohde	hyökkäyksen aiottu kohde	5.5.	19
hyökkäys	hyökkäys	5.4.	19
häiriö	häiriö	5.3.	19
jatkoarvio	tarkentava arvio	7.2.	30
jatkuvuuden hallinta	jatkuvuudenhallinta	5.6.	20
jatkuvuudenhallinta	jatkuvuudenhallinta	5.6.	20
jäännösriski	jäännösriski	13.3.	54
kasautuva riski	kumulatiivinen riski	14.5.	57
kasantotaso	kasantotaso	12.3.	49
ketjuuntunut riski	ketjuuntunut riski	14.3.	57
kompleksinen riski	verkottunut riski	14.4.	57
kontrolli	kontrolli	15.1.	59
koordinointitaso	koordinointitaso	12.6.	50
koordinoiva taso	koordinointitaso	12.6.	50
kriittisyys	kriittisyys	13.5.	55
kumulatiivinen riski	kumulatiivinen riski	14.5.	57
kybertoimintaympäristö	digitaalinen toimintaympäristö	4.1.	16
kyberturvallisuus	kyberturvallisuus	4.4.	17
käsittelytaso	käsittelytaso	12.4.	50
läpinäkyvyys riskienhallinnassa	läpinäkyvyys riskienhallinnassa	8.3.	36
mahdollisuus	mahdollisuus	6.5.	24
organisaatiokonteksti	organisaatiokonteksti	12.1.	49
organisatorinen taso	koordinointitaso	12.6.	50
osallistavuus riskienhallinnassa	osallistavuus riskienhallinnassa	8.2.	36
poikkeama	poikkeama	5.2.	19



15.11.2022

Termit ja synonyymit	Suosittelut	Nro	Sivu
primääriarvio	alustava arvio	7.1.	30
riskejä koskeva viestintä ja tiedonvaihto	riskejä koskeva viestintä ja tiedonvaihto	9.1.	38
riski	riski	6.6.	25
riskianalyysi	riskianalyysi	7.9.	32
riskiarvio	riskiarvio	7.7.	31
riskien analysointi	riskien analysointi	7.8.	32
riskien arviointi	riskien arviointi	7.6.	31
riskien arviointiprosessi	riskien arviointiprosessi	7.4.	30
riskien arviointiprosessin työkalu	riskien arviointiprosessin työkalu	7.5.	31
riskien luokittelu	riskien luokittelu	7.10.	32
riskien merkityksen arviointi	riskien arviointi	7.6.	31
riskien raportointi	riskiraportointi	9.2.	38
riskien seuranta	riskien seuranta	11.1.	44
riskien tilannekuva	riskien tilannekuva	11.2.	44
riskien vaikutuksen arviointi	riskien arviointi	7.6.	31
riskienarviointijärjestelmä	riskien arviointiprosessin työkalu	7.5.	31
riskienarviointityökalu	riskien arviointiprosessin työkalu	7.5.	31
riskienhallinnan periaatteet	riskienhallintaperiaatteet	10.3.	41
riskienhallinnan puitteet	riskienhallinnan puitteet	10.1.	41
riskienhallinnan seuranta	riskienhallinnan seuranta	11.3.	44
riskienhallinnan tilannekuva	riskienhallinnan tilannekuva	11.4.	44
riskienhallintajärjestelmä	riskienhallintajärjestelmä	10.2.	41
riskienhallintajärjestelmän seuranta	riskienhallintajärjestelmän seuranta	11.5.	45
riskienhallintajärjestelmän tilannekuva	riskienhallintajärjestelmän tilannekuva	11.6.	45
riskienhallintaperiaatteet	riskienhallintaperiaatteet	10.3.	41
riskienhallintapolitiikka	riskienhallintapolitiikka	10.4.	41
riskienhallintatyökalu	riskienhallintatyökalu	10.5.	42
riskikriteerit	riskikriteerit	6.9.	26
riskikäsitys	riskikäsitys	6.7.	25
riskin analysointi	riskien analysointi	7.8.	32
riskin arvio	riskiarvio	7.7.	31
riskin arviointi	riskien arviointi	7.6.	31
riskin elinkaari	riskin elinkaari	6.11.	26
riskin kantokyky	riskinkantokyky	13.4.	54
riskin käsitys	riskikäsitys	6.7.	25
riskin merkityksen arviointi	riskien arviointi	7.6.	31
riskin raja-arvoa välttelevä uhka	riskin raja-arvoa välttelevä uhka	6.10.	26
riskin raportointi	riskiraportointi	9.2.	38
riskin vaikutuksen arviointi	riskien arviointi	7.6.	31
riskinkantokyky	riskinkantokyky	13.4.	54
riskiperusteinen päätöksenteko	riskitietoinen päätöksenteko	13.2.	54
riskiraportointi	riskiraportointi	9.2.	38
riskirekisteri	riskirekisteri	9.4.	38
riskit minimoivaksi suunniteltu	vähäriskiseksi suunniteltu	15.2.	59
riskiteijöiden seuranta	riskien seuranta	11.1.	44
riskitieto	riskitieto	9.3.	38
riskitietoinen päätöksenteko	riskitietoinen päätöksenteko	13.2.	54
riskitilannekuva	riskien tilannekuva	11.2.	44
riskivastuullisuus	riskivastuullisuus	8.1.	35
sekundääriarvio	tarkentava arvio	7.2.	30
sisäänrakennettu riskien minimointi	vähäriskiseksi suunniteltu	15.2.	59
strateginen taso	strateginen taso	12.5.	50
suora riski	välitön riski	14.1.	57
taphtuma	taphtuma	5.1.	18
taphtumattoman vaikutuksen arvo	toteutumattoman vaikutuksen arvo	13.6.	55
tarkentava arvio	tarkentava arvio	7.2.	30



15.11.2022

Termit ja synonyymit	Suosittelut	Nro	Sivu
tiedonhallintayksikkö	tiedonhallintayksikkö	12.2.	49
tietoturva	tietoturvallisuus	4.5.	17
tietoturvallisuus	tietoturvallisuus	4.5.	17
toiminnallinen käytettävyys	toiminnallinen käytettävyys	15.3.	60
toiminnallinen taso	toiminnallinen taso	12.7.	50
toiminnan jatkuvuuden hallinta	jatkuvuudenhallinta	5.6.	20
toisioarvio	tarkentava arvio	7.2.	30
toteutumattoman vaikutuksen arvo	toteutumattoman vaikutuksen arvo	13.6.	55
tuotantotaso	toiminnallinen taso	12.7.	50
uhka	uhka	6.2.	23
uhkaprofiili	uhkaprofiili	9.6.	39
uhkatieto	uhkatieto	9.5.	39
uudelleenarviointi	uudelleenarviointi	7.3.	30
verkostomainen riski	verkottunut riski	14.4.	57
verkottunut riski	verkottunut riski	14.4.	57
vinouma	vinouma	6.8.	25
vähäriskiseksi suunniteltu	vähäriskiseksi suunniteltu	15.2.	59
välillinen riski	välillinen riski	14.2.	57
välitön riski	välitön riski	14.1.	57

16.2 Svenska

Terminologi och synonymer	Rekommendation	Nr	Sida
analys av risken	analys av risker	7.8.	32
analys av risker	analys av risker	7.8.	32
ansvarsfull riskhantering	ansvarsfull riskhantering	8.1.	35
attack	attack	5.4.	19
attackens avsedda mål	attackens avsedda mål	5.5.	19
avvikelse	avvikelse	5.2.	19
bedömning av risken [aktivitet]	bedömning av risker [aktivitet]	7.6.	31
bedömning av riskens betydelse [aktivitet]	bedömning av risker [aktivitet]	7.6.	31
bedömning av riskens betydelse [resultat]	riskbedömning [resultat]	7.7.	31
bedömning av riskens effekt [aktivitet]	bedömning av risker [aktivitet]	7.6.	31
bedömning av riskens effekt [resultat]	riskbedömning [resultat]	7.7.	31
bedömningsnivå	bedömningsnivå	12.3.	49
cybersäkerhet	cybersäkerhet	4.4.	17
cyberverksamhetsmiljö	digital verksamhetsmiljö	4.1.	16
datasäkerhet	informationssäkerhet	4.5.	17
deltagande i riskhantering	deltagande i riskhantering	8.2.	36
digital miljö	digital verksamhetsmiljö	4.1.	16
digital risk	risk för den digitala verksamheten	4.2.	16
digital säkerhet	digital säkerhet	4.3.	16
digital verksamhetsmiljö	digital verksamhetsmiljö	4.1.	16
direkt risk	direkt risk	14.1.	57
fortsatt bedömning	preciserande bedömning	7.2.	30
framförhållning	framförhållning	13.1.	54
första bedömning	preliminär bedömning	7.1.	30
förvrängning	förvrängning	6.8.	25
hantering av verksamhetens kontinuitet	kontinuitetshantering	5.6.	20
hanteringsmetod	kontroll	15.1.	59
hanteringsnivå	hanteringsnivå	12.4.	50
hanteringsåtgärd	kontroll	15.1.	59
hot	hot	6.2.	23
hot som undviker riskens gränsvärden	hot som undviker riskens gränsvärden	6.10.	26





15.11.2022

Terminologi och synonymer	Rekommendation	Nr	Sida
hotprofil	hotprofil	9.6.	39
hotuppgifter	hotuppgifter	9.5.	39
inbyggd riskminimering	planerad att ha få risker	15.2.	59
incidens	incidens	5.1.	18
indirekt risk	indirekt risk	14.2.	57
informationshanteringsenhet	informationshanteringsenhet	12.2.	49
informationssäkerhet	informationssäkerhet	4.5.	17
klassificering av risker	klassificering av risker	7.10.	32
kommunikation och informationsutbyte om risker	kommunikation och informationsutbyte om risker	9.1.	38
kontinuitetshantering	kontinuitetshantering	5.6.	20
komplex risk	risk med nätverkslik spridning	14.4.	57
kontroll	kontroll	15.1.	59
koordinerande nivå	koordineringsnivå	12.6.	50
koordineringsnivå	koordineringsnivå	12.6.	50
kritiskhet	kritiskhet	13.5.	55
kumulativ risk	kumulativ risk	14.5.	57
kvarstående risk	kvarstående risk	13.3.	54
lägesbild över risker	lägesbild över risker	11.2.	44
lägesbild över riskhanteringen	lägesbild över riskhanteringen	11.4.	44
lägesbild över riskhanteringssystemet	lägesbild över riskhanteringssystemet	11.6.	45
möjlighet	möjlighet	6.5.	24
ny bedömning	ny bedömning	7.3.	30
nätverkslik risk	risk med nätverkslik spridning	14.4.	57
operativ användbarhet	operativ användbarhet	15.3.	60
operativ nivå	operativ nivå	12.7.	50
organisationskontext	organisationskontext	12.1.	49
organisatorisk nivå	koordineringsnivå	12.6.	50
osäkerhet	osäkerhet	6.1.	23
planerad att ha få risker	planerad att ha få risker	15.2.	59
planerad som riskminimerande	planerad att ha få risker	15.2.	59
preciserande bedömning	preciserande bedömning	7.2.	30
preliminär bedömning	preliminär bedömning	7.1.	30
primär bedömning	preliminär bedömning	7.1.	30
principer för riskhantering	riskhanteringsprinciper	10.3.	41
produktionsnivå	operativ nivå	12.7.	50
rapportering av risken	riskrapportering	9.2.	38
risk	risk	6.6.	25
risk för den digitala verksamheten	risk för den digitala verksamheten	4.2.	16
risk med nätverkslik spridning	risk med nätverkslik spridning	14.4.	57
riskanalys	riskanalys	7.9.	32
riskbaserat beslutsfattande	riskmedvetet beslutsfattande	13.2.	54
riskbedömning [resultat]	riskbedömning [resultat]	7.7.	31
riskbedömningsprocess	riskbedömningsprocess	7.4.	30
riskbedömningssystem	verktyg för riskbedömningsprocessen	7.5.	31
riskbedömningsverktyg	verktyg för riskbedömningsprocessen	7.5.	31
riskbärkraft	riskbärkraft	13.4.	54
riskens livscykel	riskens livscykel	6.11.	26
riskhanteringsprinciper	riskhanteringsprinciper	10.3.	41
riskhanteringsramar	riskhanteringsramar	10.1.	41
riskhanteringspolitik	riskhanteringspolitik	10.4.	41
riskhanteringssystem	riskhanteringssystem	10.2.	41
riskhanteringsverktyg	riskhanteringsverktyg	10.5.	42
riskkriterier	riskkriterier	6.9.	26
risklägesbild	lägesbild över risker	11.2.	44
riskmedvetet beslutsfattande	riskmedvetet beslutsfattande	13.2.	54
riskrapportering	riskrapportering	9.2.	38



15.11.2022

Terminologi och synonymer	Rekommendation	Nr	Sida
riskregister	riskregister	9.4.	38
riskuppfattning	riskuppfattning	6.7.	25
riskuppföljning	riskuppföljning	11.1.	44
riskuppgifter	riskuppgifter	9.3.	38
sekundär bedömning	preciserande bedömning	7.2.	30
strategisk nivå	strategisk nivå	12.5.	50
störning	störning	5.3.	19
svaghet	svaghet	6.4.	24
sårbarhet	sårbarhet	6.3.	24
tilltagande risk	kumulativ risk	14.5.	57
transparens inom riskhantering	transparens inom riskhantering	8.3.	36
uppfattning av risken	riskuppfattning	6.7.	25
uppföljning av riskfaktorer	riskuppföljning	11.1.	44
uppföljning av riskhanteringen	uppföljning av riskhanteringen	11.3.	44
uppföljning av riskhanteringssystemet	uppföljning av riskhanteringssystemet	11.5.	45
uppskattning av risken	riskbedömning	7.7.	31
verktyg för riskbedömningsprocessen	verktyg för riskbedömningsprocessen	7.5.	31
värde för effekt utan incidens	värde för oförverkligad effekt	13.6.	55
värde för oförverkligad effekt	värde för oförverkligad effekt	13.6.	55
överförd risk	överförd risk	14.3.	57

16.3 Engelska

Terminology and synonyms	Recommended	No.	Page
accumulating risk	cumulative risk	14.5.	57
attack	attack	5.4.	19
bias	bias	6.8.	25
built-in risk minimisation	planned to be low risk	15.2.	59
concatenated risk	concatenated risk	14.3.	57
consequential risk	consequential risk	14.2.	57
continuity management	continuity management	5.6.	20
control (method)	control (method)	15.1.	59
coordinating level	coordination level	12.6.	50
coordination level	coordination level	12.6.	50
criticality	criticality	13.5.	55
cumulative risk	cumulative risk	14.5.	57
cyber operating environment	digital operating environment	4.1.	16
cybersecurity	cybersecurity	4.4.	17
detailed assessment	detailed assessment	7.2.	30
deviation	deviation	5.2.	19
digital activity/operation risk	digital activity/operation risk	4.2.	16
digital environment	digital operating environment	4.1.	16
digital operating environment	digital operating environment	4.1.	16
digital risk	digital activity/operation risk	4.2.	16
digital security	digital security	4.3.	16
direct risk	immediate risk	14.1.	57
disruption	disruption	5.3.	19
event	event	5.1.	18
follow-up assessment	detailed assessment	7.2.	30
foresight	foresight	13.1.	54
immediate risk	immediate risk	14.1.	57
inclusivity in risk management	inclusivity in risk management	8.2.	36
indirect risk	consequential risk	14.2.	57
information management unit	information management unit	12.2.	49
information security	information security	4.5.	17





15.11.2022

Terminology and synonyms	Recommended	No.	Page
information technology security	information security	4.5.	17
initial assessment	preliminary assessment	7.1.	30
intended attack target	intended attack target	5.5.	19
management measure	control (method)	15.1.	59
management method	control (method)	15.1.	59
networked risk	networked risk	14.4.	57
network-like risk	networked risk	14.4.	57
operational availability	operational availability	15.3.	60
operational continuity management	continuity management	5.6.	20
operational level	operational level	12.7.	50
opportunity	opportunity	6.5.	24
organisational context	organisational context	12.1.	49
organisational level	coordination level	12.6.	50
planned to be low risk	planned to be low risk	15.2.	59
planned to minimise risks	planned to be low risk	15.2.	59
preliminary assessment	preliminary assessment	7.1.	30
primary assessment	preliminary assessment	7.1.	30
processing level	processing level	12.4.	50
production level	operational level	12.7.	50
reassessment	reassessment	7.3.	30
residual risk	residual risk	13.3.	54
review level	review level	12.3.	49
risk	risk	6.6.	25
risk accountability	risk accountability	8.1.	35
risk analysis [result]	risk analysis [result]	7.9.	32
risk analysis [activity]	risk analysis [activity]	7.8.	32
risk assessment [result]	risk assessment [result]	7.7.	31
risk assessment [activity]	risk assessment [activity]	7.6.	31
risk assessment process	risk assessment process	7.4.	30
risk assessment process tool	risk assessment process tool	7.5.	31
risk assessment system	risk assessment process tool	7.5.	31
risk assessment tool	risk assessment process tool	7.5.	31
risk classification	risk classification	7.10.	32
risk comprehension	risk comprehension	6.7.	25
risk criteria	risk criteria	6.9.	26
risk factor monitoring	risk monitoring	11.1.	44
risk impact assessment [result]	risk assessment [result]	7.7.	31
risk impact assessment [activity]	risk assessment [activity]	7.6.	31
risk information	risk information	9.3.	38
risk life cycle	risk life cycle	6.11.	26
risk limit value-evading threat	risk limit value-evading threat	6.10.	26
risk management framework	risk management framework	10.1.	41
risk management monitoring	risk management monitoring	11.3.	44
risk management policy	risk management policy	10.4.	41
risk management principles	risk management principles	10.3.	41
risk management situation picture	risk management situation picture	11.4.	44
risk management system	risk management system	10.2.	41
risk management system monitoring	risk management system monitoring	11.5.	45
risk management system situation picture	risk management system situation picture	11.6.	45
risk management tool	risk management tool	10.5.	42
risk monitoring	risk monitoring	11.1.	44
risk register	risk register	9.4.	38
risk reporting	risk reporting	9.2.	38
risk significance assessment [result]	risk assessment [result]	7.7.	31
risk significance assessment [activity]	risk assessment [activity]	7.6.	31



15.11.2022

Terminology and synonyms	Recommended	No.	Page
risk situation awareness/picture	risk situation picture	11.2.	44
risk situation picture	risk situation picture	11.2.	44
risk-based decision making	risk-conscious decision-making	13.2.	54
risk-bearing capacity	risk-bearing capacity	13.4.	54
risk-conscious decision-making	risk-conscious decision-making	13.2.	54
risk-related communications and information exchanges	risk-related communications and information exchanges	9.1.	38
secondary assessment	detailed assessment	7.2.	30
strategic level	strategic level	12.5.	50
threat	threat	6.2.	23
threat information	threat information	9.5.	39
threat profile	threat profile	9.6.	39
transparency in risk management	transparency in risk management	8.3.	36
uncertainty	uncertainty	6.1.	23
value of unrealised impact	value of unrealised impact	13.6.	55
vulnerability	vulnerability	6.3.	24
weakness	weakness	6.4.	24

15.11.2022

Bilaga 1: Allmän definition av helheten för digital säkerhet

Ofta hör man frågan vad olika säkerhetsnivåer är eller hur de definieras. Det finns inget exakt svar, men gestaltningen underlättas till exempel av att man granskar helheten för digital säkerhet eller jämför uppfattningarna om cyber- eller informationssäkerhet. Dessa termer har inte skapats eller definierats i förhållande till varandra och med tiden har de också utvecklats på egen hand. Vid fastställandet av dem har man gjort vissa praktiska gränsdragningar enligt olika aktörers uppgifter. I denna riskhanteringsordlista har termerna behandlats i en begränsad kontext för riskhantering och därmed saknas en hel del olika underbegrepp, förekomster, undantag och egenskaper som knyter an till ämnesområdena.

Helheten för digital säkerhet öppnas när den tolkas via sättet att genomföra den. Syftet med strukturen i definitionssättet är att ge olika begrepp utrymme att leva och utvecklas i takt med verksamhetssätten och tekniken, eftersom perspektiven på säkerhet och digitalisering utvecklas snabbt. Termerna och strukturen grundar sig särskilt på OECD:s definition¹⁹ och på statsrådets principbeslut²⁰.



Figur 3: Helheten för digital säkerhet som en sammanfattning där man betonar den täckning som består av fem centrala genomförandeområden, begränsningar som fastställs enligt behov samt kompletterande genomförande- och betydelseområden. Myndigheten för digitalisering och befolkningsdatas verksamhet inom digital säkerhet fokuserar i denna helhet på utveckling och stöd av hanteringen av centrala delområden, särskilt på strategisk nivå och samordningsnivå.

Digital säkerhet är ett omfattande takbegrepp. Den fokuserar inte bara på den digitala verksamhetsmiljön utan anknyter också till allt som påverkar den och allt som påverkas av den digitala verksamhetsmiljön. Detta kan avse den verkliga världen eller abstraktare betydelsestrukturer, såsom förtroende, politik eller fritid. Således sträcker sig den digitala säkerheten bortom själva det digitala verksamhetsområdet.

Inom den digitala säkerheten kan man behandla flera aspekter på teman och genomförandet av säkerheten. Dessa perspektiv betonar olika saker och i genomförandet

¹⁹ <http://urn.fi/URN:ISBN:978-952-251-790-6> (FI)

²⁰ <http://urn.fi/URN:ISBN:978-952-367-308-3>

15.11.2022

av säkerheten betonar vi dessa olika delområden efter behov. För att uppnå tillräcklig täckning måste man beakta flera aspekter, och dessutom ska man i behandlingen beakta olika nivåer som beror på den granskade kontexten. Tillräcklig täckning behövs för att man ska kunna möta olika typer av utmaningar.

I styrningen av den offentliga förvaltningen har man utsett fem insatsområden som centrala genomförandeområden för digital säkerhet. Tillsammans kan de skapa en trovärdig och kontrollerad digital säkerhet, eftersom deras omfattning hjälper till att möta olika typer av utmaningar och även förenar alla aktörer. Kort sagt:

- **Ledning och riskhantering** kopplar olika delområden till en hanterbar helhet och knyter dem till den övriga ledningen och verksamheten i organisationen på ett mål-inriktat sätt
- **I kontinuitetshanteringen** förbereder man sig på förhand och agerar i störningssituationer för att kontrollera konsekvenserna av dem
- **I cybersäkerheten**, som har många betydelser i talspråket och internationellt, betonas en nätverksmiljö, omfattande fenomen, komplexa effekter samt påverkan i och med hjälp av digitala sammanhang
- **Dataskydd** är integritetsskydd och hantering av personuppgifter - egna och andras
- **Informationssäkerheten** fokuserar traditionsenligt på konfidentialitet, tillgänglighet och integritet i behandlingen av uppgifter och systemen samt till exempel användarbehörigheter och verifiering av obestridlighet

Utöver de ovan nämnda genomförs digital säkerhet även inom andra verksamhetsområden, till exempel genom reglering, standarder, etiska val, kompetensutveckling, frågor som gäller användbarhet, ansvarsaspekten, inom ramen för fysiska fenomen, i kommunikation, tekniska val, programutveckling, förvaltningens strukturer och hos andra motsvarande aktörer som möjliggör genomförandet. Tillämpningen av dessa på digital säkerhet beror på behoven i organisationen (eller någon annan kontext).

Den digitala verksamhetsmiljön är inte exakt avgränsad, eftersom digitalisering kan tillämpas på de flesta saker. Gränsdragningen mellan den digitala miljön och andra verksamhetsmiljöer kan variera i vår komplexa sociotekniska värld. Det finns ingen tydlig definition inom genomförandeområdena heller. De är förknippade med dimensioner som i regel inte räknas som en del av digitaliseringen eller den digitala säkerheten. De begränsar sig alltså inte enbart till digital säkerhet. Exempel på icke-digitala dimensioner i olika områden:

- Ledning och riskhantering görs också i anslutning till andra frågor.
- Det finns också frågor utanför digitaliseringen som det är viktigt att säkerställa kontinuiteten i.
- Till cybersäkerhet kopplas mellanstatliga dimensioner och krigföring, som vanligtvis inte behandlas som ärenden som fokuserar på digital verksamhet, även digitaliseringen utnyttjas i dem.
- Uppgifter på papper är inte digitala (dataskydd och informationssäkerhet).

Gränsdragningen är inte klar och den måste fastställas från fall till fall utifrån målen. Bland annat de papper som nämns i exemplet kan vara en del av den digitala säkerheten när man beaktar de system som skapat informationen, skrivare och dataöverföringen till dem. Flexibiliteten i definitionerna säkerställer att inga frågor blir kvar i gråzonen och beaktar förändringar i tekniken, verksamhetssätten och verksamhetsmiljöerna.

15.11.2022

Exempel 1: Tabell för att gestalta omfattningen av de centrala delområdena

Genomförandeområdena för digital säkerhet kan kombineras med organisationens verksamhetsnivåer för en granskning. I cellerna i tabellen kan man för analysen placera frågor och svar (t.ex. "Hur har vi allokerat resurser för det här?", "Vad i våra system har med detta att göra?", "När har vi senast gjort något åt det här?", "Hur många anmärkningar om detta har vi fått under året?" eller "Vad kan en incidens här innebära?"). Genom granskningen kan man bedöma hur heltäckande området är. Tillämpad på riskhanteringsprocessen kan tabellen klargöra de delområden av identifieringen av risker som är av intresse (i stället för alla delar) eller som inte har granskats.

	Ledning och riskhantering	Kontinuitets-hantering	Cyber-säkerhet	Dataskydd	Informations-säkerhet
Strategisk nivå					
Koordineringsnivå					
Operativ nivå					

Figur 4: Exempel på hur genomförandeområdena för digital säkerhet kan utnyttjas för att fastställa omfattningen eller dela upp en omfattande helhet i delar som ska behandlas. I tabellen ingår de centrala genomförandeområdena på den övre raden och en nivåmodell för dem i den lodräta kolumnen, baserat på tre nivåer (nivåstrukturen beror på kontexten och är därmed riktgivande här).

Man bör komma ihåg att utöver de centrala delområdena kan det finnas andra perspektiv på den egna verksamheten, varvid kompletterande kolumner kan ingå. Dessutom bör man ofta göra en motsvarande granskning av olika intressentgruppers kontext, så att konsekvenserna även för andra omfattas av granskningen. I stora organisationer eller projekt kan man också rikta in sig på mindre helheter, varvid granskningen görs med hänsyn till just den kontexten.

Exempel 2: Hur Julkri kan tillämpas på vissa delområden

Informationshanteringsnämndens rekommendation om kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen²¹ (Julkri) är ett bedömningsverktyg som har skapats för att stöda utvecklingen av informationssäkerheten inom den offentliga förvaltningen. De kan användas som hjälp vid bedömningen av huruvida kraven på informationssäkerhet i informationshanteringslagen, förordningen om säkerhetsklassificering samt delvis även dataskyddsförordningen uppfylls. Kriterierna har grupperats i fem delområden: administrativ säkerhet, fysisk säkerhet, teknisk säkerhet, beredskap och kontinuitetshantering samt dataskydd.

Kriterierna bestämmer alltså perspektivet inom den digitala säkerheten, som systematiskt omfattar informationssäkerheten och dataskyddet till de delar som föreskrivs samt delar av andra genomförandeområden i anslutning till dessa. I bedömningsmodellen har man dessutom på grund av den önskade viktningen särskilt lyft fram den fysiska och tekniska säkerheten inom informationssäkerheten som egna delområden. I kontexten för informationshanteringsenheten gäller granskningen de krav som ställs av organisationens koordineringsnivå och operativa nivå.

²¹ <http://urn.fi/URN:ISBN:978-952-367-264-2>

15.11.2022

Bilaga 2: Riskhanteringstermer i EU:s kommande NIS2-direktiv

NIS2-direktivet²², som är under utveckling inom EU, kommer att ha konsekvenser för den digitala säkerheten och riskhanteringen i synnerhet i anslutning till infrastrukturen. I direktivet hänvisas till riskbaserade termer och andra termer som tagits upp i ordlistan utan att definiera dem uttömmande. Direktivet kan anses komplettera olika sätt att tillämpa uttrycken, särskilt i direktivets egen kontext om cybersäkra nätverk och deras tjänster, och det är bra att vara medveten om dem.

I NIS2-direktivet definieras risk som en mer konkret incidens än den som används i denna riskhanteringsordlista, men incidens behandlas ändå på samma sätt som i denna ordlista och standarderna. NIS2 hänvisar till underkategorin hot, cyberhot, på ett sätt²³ som kompletteras med "betydande cyberhot" (eng. significant cyber threat). En tydlig avvikelse i definitionerna finns endast i begreppen sårbarhet och svaghet: i arbetsversionen av direktivet (i slutet av 2021) definieras de som samma, medan man i denna ordlista identifierar att svagheten inte nödvändigtvis är en sårbarhet eller åtminstone inte ännu har utvecklats till en sådan. Man bör också beakta den definition av tillbud som direktivet tar upp. I ordlistan är ett tillbud ett specialfall av "en incidens" som också kan benämnas farlig situation, men i arbetsversionen av direktivet definieras det endast som en händelse som framgångsrikt hindrades från att få negativa konsekvenser, dvs. ett resultat av genomförda åtgärder.

Ovan nämnda termer utgör en definitionsgrund för riskbaserad bedömning inom beslutsfattande och prioritering vid tillämpning av NIS2. Innehållet i de riskbedömningar som görs som stöd för riskbedömningen fastställs i medlemsstaterna, men innehållet ska i synnerhet omfatta en granskning av indirekta sammanlänkade (och nätverksbaserade) risker med tanke på inbördes beroenden, såsom risker som uppstår i produktionskedjorna. Kriterierna i direktivutkastet för riskbedömning av leveranskedjor omfattar också en tydlig identifiering av kritiska beroendeförhållanden, utredning av tillgången till alternativa produkter och tjänster, planering av motståndskraften mot störningar under hela livscykeln, prognostisering kring systemens framtid samt eventuella specialkrav på produkter från länder utanför EU.

En annan synpunkt som gäller bedömningarna är att man måste kunna ställa saker rätt i relation till bland annat riskens konsekvenser och sannolikheter, aktörernas storlek, (de bästa tillgängliga) hanteringsmetoderna, konsekvenserna och samhället. Riskbaserad verksamhet kan alltså tillämpas både på riskhanteringen och på tillsynen över dessa riskhanteringsåtgärder och på andra åtgärder som gynnas av prioriteringen.

²² https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_SV.html

²³ <https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32019R0881>