



REKTORS KANSLI

2023-03-13

Dnr C2023/267

Riktlinjer för normskala vid Karlstads universitet

Syfte

Riktlinjernas syfte är att beskriva Karlstads universitets normskala vid arbete med riskanalyser enligt exempelvis Förordning (2007:603) om intern styrning och kontroll, MSB:s föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6), Förordning (1995:1300) om statliga myndigheters riskhantering samt Dataskyddsförordningen (EU) 2016/679.

Målet är även att normskalan ska kunna användas vid andra riskanalyser som genomförs vid universitetet, såsom till exempel konsekvensbedömningar enligt dataskyddsförordningen (EU) 2016/679.

Vid framtagande av dessa riktlinjer har jämförelse gjorts mellan de rekommenderade arbetssätt som förespråkas av bland annat MSB:s metodstöd för riskanalyser samt de regelverk som styr riskanalys enligt förordning om intern styrning och kontroll.

Riktlinjerna är även ett av de underdokument som kompletterar styrdokumentet Informationssäkerhetspolicy vid Karlstads universitet.

Det huvudsakliga arbetet med att ta fram riktlinjerna har utförts av informationssäkerhetsansvarig och verksamhetscontroller i samråd med dataskyddsombudet, chefsjurist, kommunikationschef, internrevisionschefen, säkerhetschefen, biträdande HR-chef samt IT-chefen vid Karlstads universitet.

Beslut:	RB 42/23	Dnr:	C2023/267	Ersätter:	-	Dnr:	-
Giltighet fr.o.m:	2023-03-13	t.o.m:	Tills vidare	Handläggare:	Niklas Nikitin		

1 Inledning

Nya regelverk, interna förändringar samt kontinuerliga omvärldsförändringar ställer universitetet inför nya risker och förnyade krav på verksamheten. För ett lärosäte med höga ambitioner att bedriva en effektiv verksamhet är det dock inte alltid ändamålsenligt att i alla avseenden minimera alla risker. Även en hög risknivå kan i vissa undantagssituationer motiveras ifall den är accepterad av behörig beslutsfattare och hanteras på ett ändamålsenligt sätt. Det centrala är att riskerna identifieras och värderas utifrån sannolikhet och konsekvens, att ändamålsenliga åtgärder vidtas och att verksamheten bedrivs inom en säkerställd miljö.

Hur normskalan ska användas samt hur riskerna ska hanteras inklusive eventuella val av riskhanteringsåtgärder, ska ske i enlighet med Karlstads universitets olika beslutade styrdokument för riskanalyser. Även de vägledningar som återfinns i föreskrivande myndigheters reglering och handledande dokumentation ska beaktas.

2 Omfattning

Det finns flera förordningar och föreskrifter som reglerar att riskanalyser ska genomföras inom olika områden. Några exempel:

- Förordning (2007:603) om intern styrning och kontroll
- MSB:s föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)
- Förordning (1995:1300) om statliga myndigheters riskhantering
- Dataskyddsförordningen (EU) 2016/679

Regelverken har olika utgångspunkter och syften och innehållet kan skilja sig åt en del. Det som samtliga riskanalyser har gemensamt är dock att de bedrivs enligt någon riskanalysmodell samt att riskerna identifieras och värderas utifrån en normskala.

Denna normskala utgör det ramverk som universitetet så långt det är möjligt ska utgå ifrån vid genomförandet av olika riskanalyser. I detta dokument fastställs definitioner för viktiga begrepp som förekommer i de olika regelverken samt universitetets tolkningar och ställningstaganden av begreppen.

3 Definitioner

Ekonomisk påverkan: Minskade intäkter, ökade kostnader eller en kombination av minskade intäkter och ökade kostnader. Exempelvis minskade anslag eller externa intäkter, stora investeringar, skadestånd eller viten, skada på tillgångar, exempelvis vid intrång i IT-system, brand, vattenläcka, stöld.

Enskild person: Fysiska personer som kan påverkas av Karlstads universitets verksamhet. Denna definition omfattar bland annat anställda, studenter och forskningspersoner (medverkande i studier).

Extern intressent: Kan utgöras av såväl enskild näringsidkare som juridisk person, såsom myndighet, företag eller organisation med någon form av relation till Karlstads universitet.

GDPR: Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter

och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Hot: möjlig, önskad händelse med negativa konsekvenser för verksamheten.

Integritetskänsliga personuppgifter: Även känt som extra eller särskilt skyddsvärda personuppgifter. Några exempel som Integritetsskyddsmyndigheten anger: personnummer, kreditkortsuppgifter, uppgifter från medarbetarsamtal, löneuppgifter med mera. Denna definition omfattar även uppgifter om lagöverträdelser (artikel 10 GDPR).

Känsliga personuppgifter: Uppgifter som avslöjar ras¹ eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (artikel 9 GDPR).

Operativ verksamhet: Till exempel utbildning, forskning, administration samt att universitetet ska fungera som en myndighet. Notera att brister i stödsystem som exempelvis IT-system kan innebära att universitets operativa verksamhet påverkas.

Ordinära personuppgifter²: Namn, födelsedatum, kontaktuppgifter till arbetet och till studenter med mera.

Personskada: Delas upp enligt nedan.

- *Lindrig personskada*, kan till exempel innebära sår, stukning, finger- eller näsfraktur.
- *Måttlig personskada*, kan vara hjärnskakning med medvetslöshet < 1 timme eller okomplicerade frakturer.
- *Allvarlig personskada*, kan betyda hjärnskakning med medvetslöshet 1-6 timmar, lårbensbrott, blödning i hjärnan, amputering av ben eller skada på kroppspulsådern.

Sekretess: Uppgifter som är sekretessreglerade i offentlighets- och sekretesslag (2009:400), till exempel företagshemligheter, persons hälsotillstånd, urvalstester vid anställning, anställdas bostadsadress och privata telefonnummer, samt uppgifter hos studenthälsan eller studie- och yrkesvägledning med mera. För mer information se Policy för hantering av allmänna handlingar.

4 Riskvärdering

Det finns risker med nästan allt som händer eller existerar. Riskbegreppet utgår från sannolikheten att ett hot inträffar, se Bilaga A, och konsekvensen av om hotet inträffar, se Bilaga B. Då blir risken den samlade bedömningen av sannolikheten för ett hot och konsekvensen om hotet skulle inträffa.

Bedömningen av sannolikheten ska enbart grundas på hur troligt det är att hotet inträffar, på samma sätt ska bedömningen av hotets konsekvens enbart grundas på

¹ I dataskyddsförordningen används ordet ras, men det står också att det inte innebär att EU godtar teorier om att det skulle finnas skilda människoraser.

² Är även känd som harmlösa personuppgifter.

den påverkan som hotet har om den inträffar. Bedömningarna av sannolikhet respektive konsekvens ska inte påverka varandra.

Det gäller att få grepp om de viktigaste riskerna för organisationer samt att riskerna värderas på ett enhetligt sätt. Resurser för att åtgärda risker är begränsade i tid och pengar och det gäller att identifiera väsentliga risker samt sätta in ändamålsenliga åtgärder där de gör bäst nytta.

4.1 Hantering av risker

Vid hantering av risker görs en bedömning av varje identifierad risk. Risker kan accepteras, reduceras, elimineras eller överföras.

För att kunna prioritera hantering av risker ska man för varje risk ta fram ett riskvärde. Riskvärdet är en produkt av varje risks sannolikhet samt dess konsekvens.

Risk = Sannolikhet * Konsekvens

Riskerna graderas i allvarlighetsgraden i enlighet med det metodstöd som används för den aktuella riskanalysen. Detta möjliggör enkel visualisering av olika riskers riskvärde i matrisform, med sannolikhet på ena axeln och allvarlighetsgrad konsekvens på den andra. Ju högre riskvärde desto allvarligare risk. Detta ger en grafisk bild avseende vilka risker som måste prioriteras avseende hantering.

4.2 Acceptera, reducera, eliminera eller överföra en risk

För att reducera eller eliminera en risk ska man ta fram riskhanteringsåtgärder. Riskhanteringsåtgärder kan kopplas till de bakomliggande orsakerna. En bakomliggande orsak kan kräva flera olika åtgärder, både tekniska och administrativa. Dessa åtgärder ska vara konkreta, realistiska och möjliga att genomföra inom accepterad tidsram.

Man kan också välja att överföra en risk, exempelvis till ett försäkringsbolag.

Slutligen kan man också välja att acceptera risken. Detta efter en noggrann värdering av konsekvens, sannolikhet och övriga eventuella omgivningsfaktorer.

Bilaga A. Sannolikhetsnivåer i tabellformat

Tabell 1 visar de beskrivna sannolikhetsnivåerna sammanställda i tabellform. Varje hot ska bedömas utifrån hur stor sannolikheten är att hotet ska inträffa.

Sannolikhetsnivå	Bedömningsgrunder
Stor sannolikhet 4	• Hotet kan inträffa när som helst eller har redan inträffat. • Vi vet att detta kommer att hända. • Det är vanligt förekommande. • Det är mycket troligt att fel uppstår. • Inträffar en eller flera gånger i veckan.
Sannolikt 3	• Det finns flera kända fall av händelsen. • Det finns möjlighet för att fel ska uppstå. • Det finns tydliga tecken på att hotet är reellt idag. • Inträffar en till ett par gånger i månaden.
Liten sannolikhet 2	• Hotet har inträffat vid enstaka tillfällen och är ganska ovanligt. • Det finns få kända fall av händelsen. • Det finns tecken på att hotet är reellt idag. • Inträffar en till ett par gånger om året.
Osannolikt 1	• Hotet inträffar sällan och under ovanliga eller exceptionella förhållanden. • Händelsen har inträffat vid något enstaka tillfälle, eller inte inträffat alls tidigare. • Det finns få eller inga tecken på att hotet är reellt idag. • Inträffar inte alls eller högst en till ett par gånger på ett årtionde.

Tabell 1, Sannolikhetsnivåer i tabellformat.

Bilaga B. Konsekvensnivåer i tabellformat

Tabell 2 visar de olika konsekvensnivåerna sammanställda i tabellform och varje hot ska bedömas utifrån hur allvarlig konsekvensen riskerar att bli om ett hot inträffar. Det räcker att ett av exemplen nedan kan inträffa. Om flera av exemplen är aktuella för ett identifierat hot så väljs den högsta konsekvensnivån bland de exempel som uppfylls.

Exempel Konse- kvens nivå	Negativ påverkan på, eller avbrott i den operativa verksamheten	Ekonomisk påverkan för myndigheten	Juridiska aspekter	Förtroendeskada eller skadat varumärke	Externa intressenter	Påverkan på enskild person
Allvarlig 4	Allvarliga avbrott i en eller flera kritiska verksamheter som är längre än godtagbart. Omfattande omprioriteringar av verksamheten. Allvarliga störningar i verksamheten.	Allvarligt ekonomisk påverkan i form av exempelvis missade intäkter, skadestånd eller konsultkostnader. 2 mnkr och uppåt.	Hot om avsked, uppsägning, fängelse eller skadestånd för anställd efter brott mot lagar, förordningar eller avtal. Höga viten, sanktionsavgifter eller skadestånd för myndigheten.	Ihållande drev i rikstäckande medier, eller av organiserade grupperingar i sociala medier. Ej endast enskilda personer pekas ut, utan även organisationens grundläggande kultur. Allvarlig förtroendeskada för universitetet eller ledningen med en debatt som förs externt och med stor negativ påverkan på arbetsgivarvarumärket.	Allvarlig inverkan för externa intressenter. Påverkan enligt vad som beskrivs för övriga kategorier för allvarlig då någon av dessa drabbar externa intressenter.	Minst en enskild stöter på allvarliga eller till och med oåterkalleliga konsekvenser. Alternativt att ett större antal enskilda stöter på konsekvenser enligt konsekvensnivå 3. Allvarlig personskada, kan innefatta både fysisk och psykisk ohälsa. Allvarligt hot mot enskild i syfte att skada personen fysiskt, till exempel dödshot. Allvarlig ekonomisk skada. Integritetskränkning genom att sekretessreglerade uppgifter eller känsliga personuppgifter som riskerar att leda till allvarlig skada eller men för enskild sprids till obehöriga. Allvarlig systematisk diskriminering eller kränkande särbehandling.

Exempel Konse- kvens nivå	Negativ påverkan på, eller avbrott i den operativa verksamheten	Ekonomisk påverkan för myndigheten	Juridiska aspekter	Förtroendeskada eller skadat varumärke	Externa intressenter	Påverkan på enskild person
Kännbar 3	Kännbart avbrott i en kritisk verksamhet som är längre än godtagbart. Stora omprioriteringar av verksamheten.	Kännbar ekonomisk påverkan i form av exempelvis missade intäkter, skadestånd eller konsultkostnader. 500 tkr – 2 mnkr.	Arbetsrättsliga konsekvenser (till exempel varning) för anställd. Vite eller varning för myndigheten efter brott mot lagar, förordningar eller avtal.	Nyheter i både riks- och lokalmedia och i organiserade grupperingar i sociala medier. Missnöjet är dock begränsat till enskilda händelser eller enskilda personers agerande. Visst missnöje med universitetets ledning och begränsad extern spridning.	Kännbar negativ inverkan för externa intressenter. Påverkan enligt vad som beskrivs för övriga kategorier för kännbar då någon av dessa drabbar externa intressenter.	Minst en enskild kan stöta på kännbara konsekvenser som är hanterbara om än med svårigheter. Alternativt att en större mängd enskilda kan stöta på konsekvenser enligt konsekvensnivå 2. Måttlig personskada, kan innefatta både fysisk och psykisk ohälsa. Hot mot enskild om fysisk skada eller mot enskilds egendom, samt till exempel olaga förföljelse. Kännbar ekonomisk skada. Integritetskränkning genom att känsliga personuppgifter sprids till obehöriga. Systematisk diskriminering eller kränkande särbehandling.

Exempel Konse- kvens nivå	Negativ påverkan på, eller avbrott i den operativa verksamheten	Ekonomisk påverkan för myndigheten	Juridiska aspekter	Förtroendeskada eller skadat varumärke	Externa intressenter	Påverkan på enskild person
Lindrig 2	Lindriga avbrott i en eller flera verksamheter som inte är kritiska men som är längre än godtagbart. Mindre omprioriteringar av verksamheten.	Lindrig ekonomisk påverkan i form av exempelvis missade intäkter, skadestånd eller konsultkostnader. 20 tkr – 500 tkr.	Arbetsrättsliga konsekvenser (till exempel erinran) för anställd. Varning eller erinran för myndigheten efter försumlighet mot lagar, förordningar eller avtal.	Enstaka missnöjda individer som uttalar sig i sociala medier, eller en mindre notis i lokalpress. Internt missnöje med enstaka beslut eller enstaka ledningspersoner, debatten förs internt.	Lindrig negativ inverkan för externa intressenter. Påverkan enligt vad som beskrivs för övriga kategorier för lindrig då någon av dessa drabbas av externa intressenter.	Minst en enskild kan stöta på vissa konsekvenser som är hanterbara. Alternativt att en större mängd enskilda kan stöta på konsekvenser enligt konsekvensnivå 1. Lindrig personskada, kan innefatta både fysisk och psykisk ohälsa. Önskade kontakter via till exempel sociala medier, e-post eller fysiskt. Lindrig ekonomisk skada. Integritetskränkning genom att integritetskänsliga personuppgifter sprids till obehöriga. Upprepad diskriminering, dock ej systematisk. Upprepad kränkande särbehandling som riktar sig mot en eller flera medarbetare.

Exempel Konse- kvens nivå	Negativ påverkan på, eller avbrott i den operativa verksamheten	Ekonomisk påverkan för myndigheten	Juridiska aspekter	Förtroendeskada eller skadat varumärke	Externa intressenter	Påverkan på enskild person
Försumbar 1	Försumbara avbrott i verksamheten och/eller inga omprioriteringar av verksamheten.	Försumbar ekonomisk påverkan. 20 tkr eller lägre.	Ingen eller marginell försumlighet eller brott mot lagar, förordningar eller avtal.	Ingen eller försumbar negativ uppmärksamhet. Inget eller försumbart missnöje internt med enstaka beslut, ingen påverkan på förtroendet.	Försumbar negativ inverkan för externa intressenter.	De enskilda kan stöta på försumbara konsekvenser som kan hanteras utan problem eller kommer inte att påverkas. Försumbar personskada. Försumbar ekonomisk skada. Försumbar integritetskränkning genom att ordinära personuppgifter sprids till obehöriga. Enskilt fall av diskriminering eller omedveten diskriminering eller kränkande särbehandling.

Tabell 2 Konsekvensnivåer i tabellformat.