Myndigheten för samhällsskydd och beredskap

FORSKNING

VISKA

Verktygsstöd för anpassningsbar informationsklassning

VISKA Verktygsstöd för anpassningsbar informationsklassning

Tidsperiod: 2022–2024
Utförare: Tekniska Högskolan i Jönköping AB
Ansvarig: forskare/författare Erik Bergström

Kort sammanfattning Projektet har syftat till att insamla kunskap kring de egenskaper som gör informationsklassning anpassningsbar från olika intressegrupper. Resultatet inkluderar bland annat en kunskapsöversikt över befintliga verktyg som stödjer informationsklassningen, vad som behöver dokumenteras under klassningen samt designprinciper som stödjer ett anpassningsbart verktygsstöd.

MSB:s Kontaktpersoner: Tove Wätterstam, 010-240 4182,
Erik Sundström, 010-240 5371

Foto omslag: AI-genererat i DALL-E
Text: Erik Bergström
Produktion: Advant

Publikationsnummer: MSB2524 – december 2024
ISBN: 978-91-7927-584-6

MSB har beställt och finansierat genomförandet av denna forskningsrapport.
Författarna är ensamma ansvariga för rapportens innehåll.

Förord

Informationsklassning är en central del av det systematiska informationssäkerhets-arbetet och syftar till att säkerställa att information får rätt skyddsnivå baserat på dess betydelse för organisationen. Processen bedömer säkerhetsaspekter som konfidentialitet, riktighet och tillgänglighet och ligger till grund för identifiering och införande av säkerhetsåtgärder. Klassningen fungerar även som ett viktigt ingångsvärde till riskanalysen, vilket ytterligare understryker vikten av en korrekt utförd klassning. Trots sitt centrala syfte möter många organisationer utmaningar med att implementera informationsklassning i praktiken, ofta på grund av bristfälligt stöd från standarder och ramverk.

Ett återkommande problem är den subjektivitet som präglar informationsklassning, vilket kan leda till inkonsekventa bedömningar beroende på individuella tolkningar och organisatoriska kontexter. För att minska subjektiviteten kan verktygsstöd användas, men det saknas fortfarande mycket kunskap om hur dessa bör utformas och hur de effektivt kan bidra till att minska subjektiviteten.

Denna studie har samlat in en stor mängd data genom en enkät, intervjuer samt verktygsdemonstrationer för att skapa en förståelse av vilka verktyg som används för att stödja informationsklassningen. Studien fann att en bred flora av verktyg används, men att majoriteten använder enklare verktygsstöd baserade på Office-programvaror. Vidare framkom att de flesta upplevde att verktygen inte uppfyllde deras behov på ett acceptabelt sätt. Projektet har även undersökt vad som behöver dokumenteras under klassningsprocessen när denna utförs på ett strukturerat sätt. Att strukturera dokumentationsprocessen är viktigt då det ger ett tydligare flöde genom klassningen och ger också bättre stöd för att säkerställa att inga aspekter missas. Det möjliggör dessutom ett bättre underlag för framtida omklassning. Slutligen har även designprinciper för verktygsstöd formulerats.

Jönköping, 2024-11-30

Erik Bergström

PhD, Avdelningen för datateknik och informatik
Tekniska Högskolan i Jönköping

Innehåll

1 Introduktion

Att arbeta med informationsklassning är en självklar del av det systematiska informationssäkerhetsarbetet i alla typer av organisationer. Tyvärr finns det dock utmaningar med att både utforma och använda informationsklassning som metod, exempelvis eftersom klassningsbeslut ofta bygger på subjektiva bedömningar. Detta projekt utgick från att undersöka hur subjektiviteten kan minskas samt hur verktygsstöd kan bidra till att underlätta och förbättra klassningsbeslut.

1.1 Varför ett informationsklassningsprojekt?

För att på ett systematiskt sätt hantera en organisations tillgångar använder sig många organisationer, både inom offentlig och privat sektor, av informationsklassning som syftar till att säkerställa att information får en lämplig skyddsnivå i enlighet med dess betydelse för organisationen (ISO/IEC 27002:2022, 2022). I praktiken görs detta genom att alla informationstillgångar bedöms utifrån säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

Informationsklassning beskrivs i flera standarder, ramverk, nationella riktlinjer och metoder som föreslagits av forskare, men tyvärr har alla dessa brister när det gäller att ge tillräckligt stöd för praktisk implementation och användning (Bergström, 2020). Detta resulterar i att många organisationer har svårt att framgångsrikt implementera informationsklassning.

I Sverige ska svenska myndigheter säkerställa att informationssäkerhetsarbetet är systematiskt och riskbaserat genom att *”klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få (informationsklassning)”* (MSBFS 2020:6, 2020, p. 3). Informationsklassningen ligger sedan tillsammans med en riskbedömning till grund för både identifikationen av behovet av ändamålsenliga och proportionella säkerhetsåtgärder och för införandet av desamma. Flertalet studier, exempelvis Shedden et al. (2016) och Webb et al. (2014), har påvisat att brister i informationsklassningen leder till att resultaten i kommande aktiviteter i säkerhetsarbetet brister, vilket kan leda till att informationstillgångar inte skyddas på ett korrekt sätt. Trots att informationsklassning är så centralt i det systematiska informationssäkerhetsarbetet har befintliga metoder tonat ned informationsklassningens roll och hur den implementeras i organisationer (Wangen m. fl., 2018).

Informationsklassning har beskrivits som ett underforskat område av många, exempelvis Oscarson and Karlsson (2009) och Shedden et al. (2016). Trots detta finns det studier som påvisar ett antal grundläggande utmaningar som påverkar informationsklassning på ett negativt sätt, vilket leder till att det blir svårare att

genomföra klassningar. Informationsklassning handlar exempelvis om att göra subjektiva bedömningar vilket kan leda till inkonsekventa klassningar (Kaarst-Brown & Thompson, 2015). Detta är allvarligt eftersom två klassningar som genomförs med olika individer kan leda till olika resultat som i sin tur kan leda till att informationen inte får rätt skyddsnivå. Ett antal aspekter spelar in när information klassas, såsom sociala och kulturella perspektiv samt en persons medvetenhet om organisatoriska, ekonomiska, juridiska och sociala sammanhang. Detta är något som i slutändan skapar en spänning mellan klassificeringsschemat, säkerhetsåtgärder, policy och de beslut anställda fattar (Kaarst-Brown och Thompson, 2015). Andra utmaningar inom informationsklassningsområdet är exempelvis ordningen mellan aktiviteter i det systematiska informationssäkerhetsarbetet och hur det kan påverka informationsklassningen (se t.ex. Parker (2007) samt Coles-Kemp (2009)). För en mer utförlig genomgång av utmaningar, se Bergström (2020).

Ett sätt att minska subjektiviteten är att använda ett verktygsstöd. Befintliga verktyg kan vara utformade som kalkylblad, dokumentmallar eller programvara som är inriktad på att stödja hela eller delar av ledningssystemet för informationssäkerhet (Wangen et al., 2018). Gritzalis et al. (2018) har gjort en jämförelse av tio populära riskbedömningsmetoder och konstaterade att de flesta har någon typ av verktyg som stödjer metoden. De enklare verktygen bygger på kalkylblad som beskrivs som *”begränsande och ofördelaktiga,”* men även de mer avancerade verktygen kunde innehålla oflexibla egenskaper såsom förutbestämda nivåer av konsekvenser. Gritzalis et al. (2018) konstaterar också att de flesta av de undersökta metodernas verktyg krävde expertkunskaper inom riskbedömning av användarna. Andra genomgångar av verktyg har skett t.ex. av Europeiska unionens cybersäkerhetsbyrå (ENISA) som upprätthåller en lista över verktyg för riskhantering/riskbedömning (ENISA, 2024b). Gemensamt för de flesta av dessa verktyg är att de är utformade för att överensstämma med specifika standarder och det gör att deras respektive aktiviteter beskrivs i en serie steg som ska följas (Gritzalis m. fl., 2018). Både standarder och verktygsstöd saknar ofta svar på grundläggande frågor som hur olika moment ska utföras, vad som räknas som kritiska och icke-kritiska tillgångar, och hur sannolikheten för ett hot kan uppskattas (Shameli-Sendi et al., 2016). I slutändan beror ofta klassningsresultatet på hur verktygsstödet används samt på den indata som fångas upp och tillhandahålls av användaren. Denna indata baseras ofta på användarens förståelse av exempelvis definitioner och krav – något som visat sig vara alltför tekniskt eller tvetydigt för användare med begränsad erfarenhet (Wangen, 2017).

1.2 Syfte och mål

Som framgår i bakgrunden finns det problem för organisationer att framgångsrikt implementera och använda informationsklassning. Dessutom finns det ett gap mellan hur organisationer arbetar med informationsklassning och de befintliga verktygsstöden som erbjuds för detta ändamål. Projektets syfte har därför varit att öka kunskapen om verktygsstöd för informationsklassning och att föreslå designprinciper som stödjer utvecklingen av anpassningsbara verktyg. För att uppnå detta syfte har fyra mål (M) formulerats:

M1. Att upprätta en kunskapsöversikt över befintliga verktyg och designprinciper som stödjer anpassningsbar informationsklassning.

M2. Att upprätta en kunskapsöversikt bland svenska myndigheter över befintliga informationsklassningsverktygsstöd.

M3. Att insamla kunskap kring de egenskaper som gör informationsklassning anpassningsbar från olika intressegrupper såsom nybörjare och experter.

M4. Att utveckla designprinciper som stödjer ett anpassningsbart verktygsstöd för informationsklassning baserat på M1–M3.

2 Genomförande och resultat

Denna del av rapporten är uppdelad i tre delar. Först en del som redovisar den data som samlats in som en del av VISKA, de resultat som framkommit samt de publikationer som författats som en del av projektet.

2.1 Datainsamling

Som en del av denna studie har en mängd data samlats in. Tabell 1 innehåller en översikt över den insamlade data som skett under projektet.

VISKA inleddes med att en scoping-studie utfördes som lade grunden för att identifiera forskningsfronten inom området. Som det beskrivits i inledningen, så bekräftades bilden av att informationsklassning tyvärr ofta är en förbisedd aktivitet jämfört med andra informationssäkerhetsaktiviteter, såsom riskanalys. Litteraturen inom området kan beskrivas som relativt grund och fragmentarisk. Scoping-studien användes för att ta fram en enkät som skickades till alla svenska myndigheter via e-post och för att fungera som bas för insamling av intervjudata. Intervjuer genomfördes i en svensk kontext med fokus på seniora roller inom säkerhets-området på myndigheter. För att studien skulle få högre validitet samlades data även in i en europeisk kontext med personer i liknande roller som de svenska respondenterna, där samtliga hade erfarenhet av att använda verktygsstöd i sitt systematiska informationssäkerhetsarbete. Detta verktygsstöd liknar i stor utsträckning de hjälpmedel eller verktyg som finns tillgängliga i MSBs metodstöd, med skillnaden att det europeiska verktyget i större utsträckning bygger på ISO/IEC 27005 (2018), men har i grund samma syfte och mål, nämligen att förenkla det systematiska informationssäkerhetsarbetet.

Vidare har VISKA samlat in data om 13 olika befintliga kommersiella verktygsstöd. Denna insamling har skett genom att granska information om verktygen på tillverkarnas hemsidor samt genom att delta i demonstrationer av verktygen, där fokus har varit på klassning, den data som samlas in i samband med klassning, samt hur klassningen samverkar med övriga aktiviteter i informationssäkerhetsarbetet. I samtliga fall har verktygen demonstrerats av en representant för verktygstillverkaren. Alla verktyg har varit avsedda antingen för den svenska eller europeiska marknaden.

Tabell 1. Översikt av den datainsamling som skett under projektet VISKA.

Typ av datainsamling	Omfattning
Scoping-studie	Datainsamlingen startade med en så kallad scoping-studie för att upprätta en kunskapsöversikt inom området, vilken även fungerade som grund för enkäten och intervjuerna. Datainsamlingen inkluderade både vetenskaplig och annan litteratur från området för informationsklassning.
Enkät till alla[1] svenska förvaltningsmyndigheter samt statliga affärsverk	Enkäten skickades till 207 myndigheter, och efter två påminnelser stängdes insamlingen. 139 myndigheter svarade (en svarsfrekvens på 67 %). Enkäten innehöll 15 frågor som främst var utformade för att samla in kvalitativa data.
Intervjuer i en svensk kontext	17 intervjuer genomfördes (de flesta intervjuade hade rollen som Chief Information Security Officer (CISO) eller liknande, exempelvis informationssäkerhetsspecialist eller säkerhetschef). Alla intervjuer varade cirka 1–1,5 timmar.
Intervjuer i en europeisk kontext	19 intervjuer genomfördes (rollerna inkluderade exempelvis CISOs, IT-säkerhetschefer och säkerhetsingenjörer). Samtliga deltagare hade erfarenhet av att använda verktygsstöd i sitt systematiska informationssäkerhets-arbete. Alla intervjuer varade cirka en timme.
Verktygsdemonstrationer	13 olika verktyg har undersökts som en del av studien. Verktygen har i alla fall demonstrerats för användning. I de flesta fall har denna demonstration med frågestund varat runt en timme.
Valideringar	Tre valideringar med experter har genomförts, och ytterligare två valideringar är planerade för att granska de sista resultaten i projektet.

Källa: Datainsamlingen är den övergripande data som samlats in som en del av författandet av publikationerna med hög relevans som är listade under 2.3.

2.2 Resultatöversikt

Denna studie är en av de första som presenterar en översikt över vilka verktyg som används för att stödja informationsklassningen och det övergripande LIS-arbetet i praktiken. Resultaten visar att de flesta av de undersökta organisationerna använder Microsoft Office-produkter som stöd för sin informationsklassning eller andra LIS-relaterade aktiviteter (ledningssystem för informationssäkerhet). Resten av de verktyg som används är en blandning av dedikerade LIS/GRC-verktyg (governance, risk och compliance) och andra lösningar. För en detaljerad översikt av verktyg som används i klassningsarbetet, se Tabell 2. Ett flertal organisationer använder även en kombination av verktyg för att hantera informationsklassningen. Studien undersökte också anledningar till varför organisationerna valt sina verktyg. De vanligaste orsakerna var att verktygen var lättanvända, lättillgängliga och att de upplevdes som tillräckligt bra för att lösa uppgiften. En öppen fråga inkluderades också för att undersöka hur väl klassificeringsverktygen uppfyllde organisationernas behov. Analysen av dessa textsvar delades in i tre kategorier (inte acceptabelt, marginellt och acceptabelt) baserat på en skala inspirerad av SUS (Brooke, 1996). Färre än 20 % ansåg att verktygen uppfyllde deras behov på ett acceptabelt sätt.

[1] Vid utskick av enkäten fanns det 255 svenska förvaltningsmyndigheter samt statliga affärsverk, men 48 saknade egen administration eller hade noll anställda vilket gjorde att 207 ingick i studiens urval.

Tabell 2. Översikt över de verktyg som används för att stödja informationsklassificering enligt svar i enkäten. Kolumnen för typ av verktyg beskriver hur utvecklaren beskriver verktyget.

Typ av datainsamling	Antal	Omfattning
Microsoft – Excel	75	Kalkylprogram
Microsoft – Word	26	Ordbehandlingsprogram
VisAlfa – VisAlfa	8	Processbaserad informationskartläggning
MSB – Infosäkkollen	4	Uppföljning, baselining
Atlassian – Confluence	2	Wiki (Knowledge management, samarbete)
Microsoft – Sharepoint	2	Content management system, samarbete, intranät
Omegapoint – Ciso	2	Processhantering/modellering - Uttryckligt klassningsstöd
2c8 – 2c8 Apps	1	System för att modellera verksamhets-processer och stötta ledningssystem
Addsystems – ADD	1	Ledningssystem (ärendehanteringssystem, processhantering, dokumenthantering)
Egenutvecklat system	1	Ärendehantering och diarieföring
Formpipe Software – Platina	1	Dokument- och ärendehanteringssystem
Ida Infront - iipax case	1	Ärendehanteringssystem
Microsoft – PowerPoint	1	Presentationsprogram
Microsoft – Visio	1	Diagramprogram
OpenText – Documentum D2	1	Enterprise content management
Software AG – ARIS Enterprise	1	Enterprise management system
Stratsys – GRC management	1	Styrning & ledning, risk, kontroll, rapportering. Uttryckligt klassningsstöd
SKR – Klassa	1	Informationsklassning och handlingsplan

Källa: Verktygsöversikten är hämtad från Bergström (2023).

Dessutom framkom det att en stor andel organisationer använder sina verktyg enbart för att det inte finns några bättre alternativ, och vissa som inte använder verktyg förlitar sig på manuellt arbete eftersom de inte hittar några lämpliga verktyg som stödjer deras behov på ett effektivt sätt.

Flera verktyg var varken dedikerade säkerhetsrelaterade verktyg eller tillhörde Office-programmen. Dessa verktyg hjälpte organisationerna på andra sätt i säkerhetsarbetet. Baserat på de typer av verktyg som nämns och svaren i

fritextfrågorna kan några behov identifieras. Det finns ett behov av att stödja hela livscykeln för informationsklassning. Indata till informationsklassningen kommer ofta från en process, och om processkartläggning/modellering/hantering finns i ett annat verktyg, stödjer det även klassificeringen. Detta kan förklara varför respondenterna inkluderade användningen av programvara för processhantering eller motsvarande. På samma sätt, efter en klassning, kommer ett ifyllt kalkylblad eller ett annat dokument att innehålla dokumentation som måste lagras någonstans. Att respondenterna nämner ärendehanteringssystem, dokumenthanteringssystem och arkiveringsprogram pekar därför på ett behov av dokumentationsstöd. Att ha ett bredare livscykelperspektiv för klassificering är inte en ny uppfattning, men hur det tillämpas i praktiken är fortfarande oklart.

En sak att reflektera över i resultatet är användningen av kalkylblad och andra typer av dokument som används som mallar, t.ex. i metodstödet. Det finns en risk att organisationer som använder metodstödet inte uppfattar dessa mallar som exempel (som dessutom måste anpassas till egna organisationer) utan ser dem som verktyg. Denna studie ger inget svar på om det är så, men flera undersökta myndigheter använder exempelvis konsekvenskriterierna och klassningsmatrisen utan förändringar från de exempel som ges i metodstödet, vilket indikerar att detta kan vara fallet. Det finns också en uppenbar risk att tillgången till mallar och andra rudimentära verktyg, som snarare exemplifierar funktionalitet, ses som ett fullfjädrat verktyg, vilket kan hämma användningen av mer avancerade verktyg.

Även vad som ska dokumenteras som en del av klassningen har undersökts. Startpunkten för detta arbete har varit att utgå från modellen som tagits fram som en del av metoden i Bergström et al. (2021). Dokumentationen har delats in i de steg som passeras under en klassning och som är kompatibla med ISO/IEC 27002 och därigenom MSBs metodstöd. Stegen är att beskriva den identifierade informationstypen, externa krav, interna krav, klassningsbeslutet utifrån konfidentialitet, riktighet och tillgänglighet (samt eventuellt andra säkerhetsaspekter om så önskas). Att strukturera dokumentationsprocessen är viktigt eftersom det ger ett tydligare flöde genom klassningen och gör att de som genomför klassningen får bättre stöd för att inga aspekter missas. Det ger också ett bättre underlag att ta fram vid framtida omklassning. Eftersom den publikation som tagits fram som resultat av kartläggningen av vad som behöver dokumenteras under klassning ännu inte är publicerad, ges här ett antal exempel från kategorin beskrivning av den identifierade informationstypen: Ägare, process/system, lagringsplats, allmän handling, gallring, personuppgift, personuppgiftsbiträde, samt typ av känslig personuppgift.

En annan aspekt som undersökts är klassningens roll i förhållande till riskanalys och val av säkerhetsåtgärder. Tidigare studier (t.ex. Lundgren och Bergström (2019)) har indikerat att det funnits en direkt relation mellan klassning och säkerhetsåtgärder utan att däremellan genomföra riskanalysen. Som en del av detta projekt har även riskanalysen beaktats eftersom resultatet av en klassning kan påverkas av vad som är nästa steg i arbetet. Projektet har undersökt *när*, *var* och *hur* riskanalysen utförs. Resultaten visade att det finns tillfällen när riskanalysen inte genomförs på det traditionella sättet, exempelvis för att deltagarna efter klassningen inte bedömer

att det behövs. Detta kan bero på att de vid den organisationsövergripande riskanalysen redan bedöms ha identifierat tillräckligt med risker och att det därmed inte bedömdes ge något ytterligare värde, utan lämpliga säkerhetsåtgärder kunde väljas ändå.

Designprinciper har formulerats som en del av VISKA och för att få en struktur på designprinciperna så har de formulerats baserat på 3U-modellen, där 3U står för *user*, *usage* och *usability* (användare, användning och användbarhet). Denna rapport är för kort för att kunna redovisa alla designprinciper (som dessutom ännu inte är officiellt publicerade), så här redovisas ett par exempel på framtagna designprinciper. Under usage finns det ett tekniskt krav att *verktyg måste stödja omklassning*. Det innebär i sin tur att det finns funktionella krav som måste uppfyllas, exempelvis tidsstämpling, historik och påminnelser. Andra exempel på designprinciper är att *verktyg måste kunna ge en översiktsbild*, att *verktyg måste kunna ge en nulägesbild*, *verktyget måste kunna vägleda fram klassningsbeslutet, verktyget måste ha ett "startstöd"* (för att kunna starta diskussioner, ge grunddata etc.), *kunna migrera data* samt att *verktyget måste vara anpassningsbart* (exempelvis stödja byte av terminologi inom en organisation).

Slutligen har även konsekvenskriteriers användning vid klassning undersökts som en del av projektet. Konsekvenskriterier nämns inte explicit i till exempel ISO/IEC 27002, men utgör ett intressant tillägg som har en möjlighet att minska subjektiviteten. Denna studie har samlat in data kring användningen av konsekvenskriterier, men alla data är ännu inte analyserad utan resultat kan väntas under kommande år.

2.3 Publikationer

Som en del av detta projekt har ett antal vetenskapliga publikationer författats. Tyvärr är kan ledtiderna vara ganska långa när vetenskapliga bidrag är under granskning och revison och postdoktorala projekt är tidsbegränsade till en kortare period. Därför är alla bidrag ännu inte publicerade, men det finns en plan för att publicera dessa under 2025.

Publikationer med hög relevans för projektet

Följande publikationer med hög relevans har publicerats som en del av VISKA.

- Bergström, E., Andersson, S., & Lundgren, M. (2025). To risk analyse, or not to risk analyse: That's the question. IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024), Skövde, Sweden.
- Bergström, E. (2023). Tools Supporting Information Security Risk Management in Practice. The 9th International Conference on Socio-Technical Perspectives in IS (STPIS'23) 27.-28.10, Portsmouth, UK.
- Bergström, E., Lundgren, M., Bernsmed, K., & Bour, G. (2023). "Check, Check, Check, We Got Those" – Catalogue Use in Information Security Risk Management. Human Aspects of Information Security and Assurance, Kent, UK.

Följande manuskript med hög relevans är under granskning eller författas som en del av VISKA. Dessa artiklar beräknas vara publicerade under 2025.

- Andersson, S., Bergström, E., and Lundgren, M. (2025) "Doing it on paper is not the best" - Why We Need Risk Management Tools. Submitted to Journal of Information Systems Security.
- Bergström, E., Andersson, S. and Grosse, C. (2025) Information Classification Design Principles, International Journal of Information Security, Springer.
- Andersson, S., and Bergström, E. (2025) What goes where? - Documentation practices in Information Classification, Information and Computer Security, Emerald.
- Andersson, S., and Bergström, E. (2025) The use of Consequence criteria in Information Classification, Information and Computer Security, Emerald.

Utöver de bidrag som har hög relevans så har projektet nämnts i ett antal andra informationssäkerhetsrelaterade publikationer som en del av VISKA.

Publikationer med låg relevans för projektet

Publikationer med låg relevans som har publicerats som en del av VISKA.

- Kävrestad, J., Bergström, E., Stavrou, E., & Nohlberg, M. (2025). Useful but for Someone Else - An Explorative Study on Cybersecurity Training Acceptance. In N. Clarke & S. Furnell, Human Aspects of Information Security and Assurance Cham.
- Bergström, E., Kävrestad, J., Gustafsson, J. H., & Jonsson, H. (2024). Factors influencing the adoption of awareness-raising activities in SMEs. The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) 16.-17.8, Jönköping Sweden.
- Kävrestad, J., Bergström, E., & Johansson, S. (2024). Using tabletop exercises to raise cybersecurity awareness of decision-makers. Critical Information Infrastructures Security. CRITIS 2024, Rome, Italy.
- Kävrestad, J., Bergström, E., & Johansson, S. (2024). Using TTX to raise cybersecurity awareness of decision-makers: A research agenda and early results IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024), Skövde, Sweden.
- Johansson, K., Paulsson, T., Bergström, E., & Seigerroth, U. (2022). Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry. SPS2022: Proceedings of the 10th Swedish production symposium, Skövde, Sweden.

Följande manuskript med låg relevans är under granskning eller författas som en del av VISKA. Dessa artiklar beräknas vara publicerade under 2025.

- Kävrestad, J., Bergström, E., Gunnarsson, R., Mazeh, A. and Stenlund, L. (2025). Deciding on Cybersecurity Awareness Initiatives: Insights from the Public Sector. Applied Sciences, MDPI.
- Kävrestad, J., Bergström, E., Seigerroth, U., Mulshine, T., and Berkemar, L. (2025) "Learning by doing is the best really": Competence development of the cybersecurity workforce. IEEE Computer.

3 Reflektioner och förslag på framtida studier

Det finns ett flertal saker att reflektera över angående denna studie och vad den har medfört. Det finns även ett antal spår kvar att utforska inom klassningsområdet där framtida forskning behövs. Nedan presenteras dessa reflektioner samt förslag på framtida forskningsinriktningar.

3.1 Reflektioner

Det finns flera saker som jag har upplevt som oväntade under studiens gång. Det första är det stora intresset från inte enbart offentlig sektor utan även privat sektor, som letar efter lösningar som kan underlätta deras klassningsarbete. Detta drivs säkerligen av ökat tryck på kraven att jobba systematiskt med informationssäkerhetsarbetet. Det är lätt att tro att detta främst gäller organisationer som inte har kommit så långt i sitt säkerhetsarbete, men det finns även intresse från vad som skulle kunna betonas som mogna organisationer. Uppenbart är det så att många organisationer vill ha ett bättre verktygsstöd, inte enbart för klassningen utan mer holistiskt för allt deras informationssäkerhetsarbete. Detta arbete har satt luppen på detta behov och även lagt några pusselbitar i detta pussel.

En annan reflektion är att projektet har varit mycket viktigt från ett miljöbyggande perspektiv. VISKA har inneburit att Tekniska Högskolan i Jönköping (JTH) har kunnat anställa ytterligare lektorer, vilket har möjliggjort att vi har nått en kritisk massa avseende både utbildning och forskning inom området. Under projektets gång har vi därför kunnat starta ett nytt magisterprogram i Cybersäkerhet (startade hösten 2024). Att få ut fler på arbetsmarknaden med kunskaper inom området är viktigt för Sverige på så många sätt, framförallt om man väger in den geopolitiska situationen. Vidare listar t.ex. ENISA i sin senaste hotrapport just kompetensbrist som det näst största hotet 2030 (ENISA, 2024a), vilket ytterligare visar på vikten av att vi fokuserar på denna typ av utbildning. Projektet (och anställningarna som kommit som en konsekvens av det) har även lett till skapandet av en forskningsgrupp, Cybersecurity and Privacy Research group (CPR), som i sin tur har agerat som en bas för att söka ytterligare forskningsanslag. Hittills har CPR fått två ansökningar beviljade: Identifying Cybersecurity Awareness Needs and Perceptions of User Groups (ICANP) (projektstart 2024, MSB) och RECAP: Regional Cybersecurity Awareness for SMEs in Production (projektstart 2025, KK-stiftelsen). Vidare har vi ansökt om forskningsanslag från Horizon (EU), KK-stiftelsen samt Familjen Kamprads Stiftelse, som alla tre lämnar besked under vintern 2024 och våren 2025.

3.2 Framtida studier

Sammantaget kan det sägas att syfte och mål har uppfyllts i projektet, men det finns givetvis många aspekter kvar att undersöka när det gäller verktygsstöd för informationsklassning. Många möjliga forskningsinriktningar har potential att påverka både teori och praktik. Eftersom mycket inom området handlar om att på olika sätt minska subjektiviteten vid klassningstillfället, så spelar hur detta kan ske egentligen mindre roll, utan alla tillvägagångssätt eller kombinationer av tillvägagångssätt är viktiga. Som konstaterats i resultatdelen är det inte informationsklassningsverktyg som fristående verktyg som efterfrågas, utan klassningsstöd ska bakas in som en del i en mer omfattande programvara. Exakt vad som ska inkluderas är oklart från denna studie. VISKA indikerar dock att verktygen bör stödja processhantering och dokumenthantering, dvs. ett lite bredare perspektiv än den traditionella livscykelsynen som beskrivs i standarder.

Verktygsstöd kan minska subjektiviteten genom att stötta dokumentation, automatisera eller ge beslutsstöd vid klassning. Ett beslutsstöd kan föreslå klassningsnivå baserat på information i en process eller system, men detta innebär säkerhetsrisker eftersom det krävs stora rättigheter för analysen. Ett alternativ är att utveckla beslutsstöd baserat på tidigare klassningsdeltagares kunskap.

Hur dokumentation ska genomföras på ett effektivt sätt under klassning samt vad som ska dokumenteras är ett intressant och viktigt område som är i princip outforskat. VISKA har tagit ett första steg inom detta område, men fler studier behövs. Likaså är de flesta aspekter av hur konsekvenskategorier implementeras och används okända ur ett forskningsperspektiv. Även här behövs fler studier, t.ex. hur matriserna kan visualiseras, vilka kriterier som bör beaktas, hur olika kriterier påverkar gruppsammansättningen av de som utför klassningen.

Ett generellt problem inom forskning i informationssäkerhetsområdet är hur mätning av resultat kan göras på ett tillförlitligt sätt. Exempelvis skulle det vara intressant med studier som gör bidrag kring metoder för hur effektiviteten av olika förändrade arbetssätt kan mätas. Konkret skulle detta kunna vara att mäta hur olika typer av konsekvenskriterier påverkar klassningen, hur vissa typer av verktygsstöd påverkar, hur förändrad dokumentationsprocess påverkar osv. Detta är i sig ett väldigt svårt problem då både mätmetoder och själva mätningen kan vara svår (exempelvis avseende att hitta jämförbara grupper att mäta på).

Tittar man ännu bredare så är det generellt för litet fokus på forskning som innefattar människan och dess roll inom säkerhetsområdet. Tyvärr sker mycket forskning enbart på nya tekniker där de mänskliga aspekterna utelämnas, ibland för att det finns en tro att man kan automatisera bort de mänskliga aspekterna om bara tillräckligt bra teknik utvecklas. Det finns exempelvis många aspekter att undersöka gällande hur medvetenhetshöjande åtgärder implementeras, anpassas, görs effektiva etc. Mycket resurser läggs på detta område i organisationer, men forskningen är mycket begränsad.

Referenser

Bergström, E. (2020). *Supporting Information Security Management: Developing a Method for Information Classification* University of Skövde]. Skövde, Sweden. http://his.diva-portal.org/smash/record.jsf?pid=diva2%3A1458263&dswid=-5603.

Bergström, E. (2023). Tools Supporting Information Security Risk Management in Practice. The 9th International Conference on Socio-Technical Perspectives in IS (STPIS'23) 27.-28.10, Portsmouth, UK.

Bergström, E., Andersson, S., & Lundgren, M. (2024). To risk analyse, or not to risk analyse: That's the question. IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024), Skövde, Sweden.

Bergström, E., Andersson, S., & Lundgren, M. (2025). To Risk Analyse, or Not to Risk Analyse: That's the Question. In N. Clarke & S. Furnell, *Human Aspects of Information Security and Assurance* Cham.

Bergström, E., Karlsson, F., & Åhlfeldt, R.-M. (2021). Developing an Information Classification Method. *Information and Computer Security*, *29*(2), 209–239. https://doi.org/10.1108/ICS-07-2020-0110.

Bergström, E., Kävrestad, J., Gustafsson, J. H., & Jonsson, H. (2024). Factors influencing the adoption of awareness-raising activities in SMEs. The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) 16.-17.8, Jönköping Sweden.

Bergström, E., Lundgren, M., Bernsmed, K., & Bour, G. (2023, 2023). "Check, Check, Check, We Got Those" – Catalogue Use in Information Security Risk Management. Human Aspects of Information Security and Assurance, Kent.

Brooke, J. (1996). SUS-A quick and dirty usability scale. *Usability evaluation in industry*, *189*(194), 4–7.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report*, *14*(4), 181–185. http://dx.doi.org/10.1016/j.istr.2010.04.005.

ENISA. (2024a). *Foresight Cybersecurity Threats For 2030 - Update 2024: Extended report*. ENISA. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report.

ENISA. (2024b). *Inventory of Risk Management / Risk Assessment Tools*. Retrieved 2024-11-25 from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools.

Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the Risk Assessment Maze: A Meta-Survey. *ACM Comput. Surv.*, *51*(1), 1–30. https://doi.org/10.1145/3145905.

ISO/IEC 27002:2022. (2022). Information security, cybersecurity and privacy protection – Information security controls. In: ISO/IEC.

ISO/IEC 27005. (2018). Information technology – Security techniques – Information security risk management. In: ISO/IEC.

Johansson, K., Paulsson, T., Bergström, E., & Seigerroth, U. (2022, 2022). Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry. SPS2022: Proceedings of the 10th Swedish production symposium, Skövde, Sweden.

Kaarst-Brown, M. L., & Thompson, E. D. (2015). Cracks in the Security Foundation: Employee Judgments about Information Sensitivity. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, California, USA.

Kävrestad, J., Bergström, E., & Johansson, S. (2024a). Using tabletop exercises to raise cybersecurity awareness of decision-makers. Critical Information Infrastructures Security. CRITIS 2024, Rome, Italy.

Kävrestad, J., Bergström, E., & Johansson, S. (2024b). *Using TTX to raise cybersecurity awareness of decision-makers: A research agenda and early results* IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024), Skövde, Sweden.

Kävrestad, J., Bergström, E., Stavrou, E., & Nohlberg, M. (2024). Useful but for someone else - an explorative study on cybersecurity training acceptance. IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2024), Skövde, Sweden.

Kävrestad, J., Bergström, E., Stavrou, E., & Nohlberg, M. (2025). Useful but for Someone Else - An Explorative Study on Cybersecurity Training Acceptance. In N. Clarke & S. Furnell, *Human Aspects of Information Security and Assurance* Cham.

Lundgren, M., & Bergström, E. (2019). Dynamic Interplay in the Information Security Risk Management Process. *International Journal of Risk Assessment and Management*, *22*(2), 212–230.

MSBFS 2020:6. (2020). Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter [The Swedish Civil Contingencies Agency's Regulations on Government Agencies Security Information Security]. https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf.

Oscarson, P., & Karlsson, F. (2009). *A National Model for Information Classification* AIS SIGSEC Workshop on Information Security & Privacy (WISP2009), Phoenix, AZ, USA.

Parker, D. B. (2007). Comparison of Risk-Based and Diligence-Based Idealized Security Reviews. *EDPACS*, *36*(3–4), 1–12. https://doi.org/10.1080/07366980701804805.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems*, *39*(1), 15.

Wangen, G. (2017). Information Security Risk Assessment: A Method Comparison. *Computer*, *50*(4), 52–61. https://doi.org/10.1109/mc.2017.107.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness [journal article]. *International Journal of Information Security*, *17*(6), 681–699. https://doi.org/10.1007/s10207-017-0382-0.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1–15. https://doi.org/10.1016/j.cose.2014.04.005.

Myndigheten för samhällsskydd och beredskap

I samarbete med:

JÖNKÖPING UNIVERSITY
School of Engineering

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2524 – december 2024 ISBN 978-91-7927-584-6