Verksamhetsanalys

Genomförande och betydelse för säkra IT-system

Henrik Karlzén, Ove Jansson, Johan Bengtsson,
Caroline Bildsten, Christian Valassi

FOI-R--4857--SE

December 2019

FOI

Henrik Karlzén, Ove Jansson, Johan Bengtsson, Caroline Bildsten, Christian Valassi

Verksamhetsanalys

Genomförande och betydelse för säkra IT-system

Titel	Verksamhetsanalys – Genomförande och betydelse för säkra IT-system
Title	Business process modelling – Implementation and significance for secure IT systems
Rapportnr/Report no	FOI-R--4857--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	60
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E72778
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: Shutterstock, thodonal88

Sammanfattning

Verksamhetsanalyser genomförs för befintliga eller planerade verksamheter och utgör grunden för riskbedömningar. Resultatet av verksamhetsanalyser utgörs av verksamhetsbeskrivningar. Denna rapport syftar till att skapa bättre förutsättningar att utföra och redovisa de verksamhetsanalyser som genomförs i Försvarsmakten vid framtagandet av nya IT-system eller vid förändring av befintliga IT-system. Rapporten beskriver därför vad verksamhetsanalyser kan bidra med i ett informationssäkerhetsperspektiv, hur analyserna bör genomföras och vilka informationsmängder som bör ingå.

Arbetet baseras på litteratur från Försvarsmakten, Försvarets materielverk, civila myndigheter, akademiska forskningsartiklar samt på intervjuer med personer som utfört eller granskat verksamhetsanalyser. Någon utvärdering av faktiska genomförda verksamhetsanalyser har däremot inte gjorts.

Verksamhetsanalyser är en viktig grund för säkerhetsarbetet vid framtagande av IT-system. Analyserna kan också stödja utvärdering av huruvida systemen är realiserbara eller ens önskvärda.

Att använda mallar för verksamhetsanalyser kan göra arbetet mer kostnadseffektivt och enhetligt, men samtidigt ger de en risk att analytikerna inte tänker tillräckligt vitt och brett. Informationskällorna har olika åsikt om detta.

Kommunikation är en viktig del vid genomförandet av en verksamhetsanalys. Med hjälp av kommunikation kan missförstånd minskas, fler komma till tals och viktig information som inte står med i styrande dokument kan inhämtas.

Nyckelord: verksamhetsanalys, verksamhetsbeskrivning, riskbedömning, säkerhetsanalys, säkerhetsmålsättning, informationssäkerhet, IT-säkerhet, cybersäkerhet, IT-system, intervjustudie, litteraturanalys

Summary

Business process modelling is performed on current or planned businesses, and is the foundation of risk assessments. The result is a thorough description of the business. This report aims to generate a better basis to conduct and report the business process modelling that is performed within the Swedish Armed Forces (SwAF) in the context of new (or changes in current) IT-systems. This was performed by studying what business process modelling may achieve for information security, how business process modelling should be performed, and what information is needed for the modelling.

This work is based on documents from the SwAF, the Swedish Defence Materiel Administration, civil authorities and scientific papers, as well as interviews with people having experiences of conducting and validating business process models. However, no evaluation of actual business analyses has been carried out.

Business process modelling is an important basis for the security work when developing IT systems. The modelling can also support evaluation of whether the systems are feasible or even desirable.

Using templates for business process modelling can make the work more cost-effective and uniform, while at the same time risking that the modellers do not think widely and freely enough. The information sources have different views on this.

Communication is an important part of conducting business process modelling. With the help of communication, misunderstandings can be reduced, more people can be heard, and important information that is not included in governing documents can be obtained.

Keywords: business process modelling, enterprise architecture, business process architecture, business process management, business analysis, risk assessment, risk analysis, information security, IT security, cyber security, IT systems, interview study, literature review.

Innehållsförteckning

1. Inledning

Kunskap om verksamheten är en avgörande faktor för att säkerhetsrisker ska kunna identifieras, bedömas och reduceras (J. Hallberg, Bengtsson, & Sommestad, 2012). En gedigen verksamhetsanalys är därmed en förutsättning för genomförandet av Försvarsmaktens säkerhetsanalyser, där risker identifieras och bedöms samt skydd föreslås (Försvarsmakten, 2013a). Resultatet av en verksamhetsanalys är en verksamhetsbeskrivning som innehåller information om vad som är viktigt för verksamheten och varför (Försvarsmakten, 2013a).

Denna rapport har skrivits på uppdrag av Försvarsmakten och syftet med rapporten är att skapa bättre förutsättningar att utföra och redovisa verksamhetsanalyser inför framtagandet av nya IT-system i Försvarsmakten.

Tidigare FOI-forskning påtalade behovet av att viderutveckla Försvarsmaktens instruktioner för hur verksamhetsanalyser ska genomföras (J. Hallberg m.fl., 2012). Rapporten gav även förslag på mer strukturerat genomförande och återanvändning av befintliga verksamhetsbeskrivningar. Dessutom beskrevs ett antal förslag på framtida forskningsfrågor. Dessa förslag bedöms fortfarande vara relevanta och ligger tillsammans med beställningen till grund för denna rapports frågeställningar:

1. Vad kan verksamhetsanalyser bidra med i ett informationssäkerhetsperspektiv?
2. Hur bör verksamhetsanalyser genomföras?
3. Vilka informationsmängder bör ingå i verksamhetsanalyser?

1.1 Målgrupp

Rapporten har skrivits på uppdrag av Försvarsmakten och målgruppen för rapporten utgörs därför främst av de inom Försvarsmakten som

- utför verksamhetsanalyser
- använder verksamhetsbeskrivningar
- tar fram metoder och verktyg för verksamhetsanalyser
- genomför säkerhetsanalyser för planerade IT-system.

Försvarsmakten är dock inte ensam om att behöva utföra verksamhetsanalyser som underlag för att förbättra säkerheten. Nya säkerhetsskyddslagen medför att fler organisationer inryms inom sfären för Sveriges säkerhet (Regeringskansliet, 2018). Således är denna rapport tillämplig för en bredare krets än enbart Försvarsmakten.

1.2 Läsanvisning

Avsnitt 1.3 beskriver relaterad forskning som utförts på FOI inom närliggande områden.

Kapitel 2 beskriver forskningsområdets mognad.

Kapitel 3 beskriver den metod som användes för att besvara rapportens frågeställningar. Metoden baseras på försvarsmaktslitteratur, litteratur från FMV, akademisk litteratur och litteratur från civila myndigheter samt på intervjuer med personer som har inblick i ämnet.

Kapitel 4–7 beskriver resultat från litteraturstudierna.

Kapitel 8 beskriver resultatet av intervjuerna.

Kapitel 9 beskriver analys och diskussion av de olika resultaten som helhet och skillnader i resultat mellan litteraturtyperna och intervjuerna.

Kapitel 10 utgör rapportens slutsatser med bland annat förslag kring utformning av handböcker och mallar för genomförande av verksamhetsanalyser.

Rapporten innehåller även en bilaga som återger intervjufrågorna, en bilaga som innehåller en informationsmängdstabell och en bilaga som förklarar informationsmängderna.

1.3 Relaterad FOI-forskning

På FOI har det, utöver vad som redan nämnts, genomförts flera studier som anknyter till verksamhetsanalyser. Nedan ges en kort sammanfattning av några av de dokument som beskriver sådana studier:

- **Kravhantering för FMA**
  Rapporten beskriver en kravhanteringsprocess som består av de tre delprocesserna verksamhetsanalys, behovsanalys och kravanalys. Verksamhetsanalysens roll i kravhanteringsarbetet beskrivs som det första utvecklingsstadiet för krav, vars resultat utgörs av behovsunderlag. Behovsunderlaget innefattar information om den aktuella verksamheten och intressenternas krav på systemet. I rapporten ges det förslag på aktiviteter som bör genomföras under verksamhetsanalysen. (N. Hallberg, Lindell, Pilemalm, Andersson, & Ericson, 2004)

- **Verksamhetsmodell Ledningsplats**
  Rapporten beskriver en verksamhetsmodellering av verksamhet som genomförs inom en ledningsplats. Modellen utgör grund för att identifiera och beskriva de ledningsaktiviteter som genomförs liksom de aktiviteter som sker för att samordna och möjliggöra varje ledningsaktivitet. (Stenius, 2006)

- **Tjänstebaserad krishantering för lokalsamhället**
  Rapporten beskriver ett underlag för utveckling av en ledningsfunktion för tjänstebaserad distribuerad krishantering på lokal samhällsnivå. Resultatet består bland annat av en beskrivning av medverkande krishanteringsaktörer med tillhandahållna tjänster, en modell över hur tjänster ska beskrivas samt ett scenario för hur tjänstebaserad krishantering skulle kunna utföras. (N. Hallberg m.fl., 2008)

- **Tankar kring tillämpning av MODAF i Försvarsmakten**
  Ett memo som sammanfattar tankar kring tillämpningen av brittiska ramverket *Ministry of Defence Architecture Framework* (MODAF). MODAF anges vara lämpligt att använda vid beskrivning av verksamhet och för tekniska system som fungerar över organisatoriska gränser. (Sparf & Sparf, 2012)

- **Informationsbehov vid säkerhetsanalyser**
  Rapporten beskriver att en central svårighet i säkerhetsanalyser inför framtagande av IT-system är att avgöra vilken information som ska ligga till grund för analyserna. Det kan lätt bli dyrt att samla in information och normalt måste prioriteringar göras angående vilken information som ska samlas in. En slutsats är att de metoder som finns främst efterfrågar information om verksamheten snarare än informationen systemet ska behandla, vilka beteenden som är tänkbara rörande systemet eller vilka tekniska lösningar som ska finnas. En annan slutsats är att Försvarsmakten bör fundera på hur detaljerade analyserna behöver vara jämfört med att mer standardiserade analyser utförs (Sommestad, Bengtsson, & Hallberg, 2013).

- **Översikt av verksamheters informationsbehov för bedömningar av informationssäkerhetsrisker**[1]
  En akademisk forskningsartikel som beskriver en jämförelse av informationsbehoven hos tolv olika etablerade riskbedömningsmetoder. Dessutom undersöks hur väl informationsbehoven täcks in av ramverket Archimate som delar in information i olika lager såsom teknisk infrastruktur, verksamhet och intressenter. En indelning gjordes också av om informationen som behövdes var av mer passiv art (såsom objekt) eller mer av aktiv art (såsom processer) (Korman, Ekstedt, Sommestad, Hallberg, & Bengtsson, 2014).

[1] Fritt översatt av eng. *Overview of Enterprise Information Needs in Information Security Risk Assessment*.

2. Forskningsområdets mognad

Forskningslitteraturen pekar på att en del forskning kvarstår att utföra, både vad gäller den teoretiska grunden och empirisk utvärdering av teoribildningar. Forskningsområdet har sitt ursprung i flera olika andra forskningsområden som i sig är ganska unga:

- Studier av system dök upp först på 60-talet (Alotaibi & Liu, 2017).
- Fokus på verksamhetsprocesser kom först på 1990-talet (Aguilar-Saven, 2004; Röhrig, 2003).
- Affärsmodeller fick ett större fokus först i början av 2000-talet (Wirtz, Göttel, & Daiser, 2016).

Området betraktas nu som moget och populärt, även om området ofta kritiseras av en del forskare (Klang, Wallnöfer, & Hacklin, 2014; Recker & Mendling, 2016; van der Aalst, La Rosa, & Santoro, 2016). Det finns dessutom ett betydande avstånd mellan forskningsfronten och praxis (van der Aalst m.fl., 2016). Många forskningsartiklar handlar om formella koncept (Recker & Mendling, 2016) och föreslår nya modelleringsspråk. Ett exempel är CySeMoL som kan användas för att formellt modellera organisationers systemarkitekturer och därefter utvärdera systemets säkerhet (Sommestad, Ekstedt, & Holm, 2013). Å andra sidan förpassas många av dessa språk till bokhyllan utan att användas i praktiken (van der Aalst, 2013). På så vis sker mycket av forskningen i olika stuprör (Zott, Amit, & Massa, 2011). På senare år har visserligen forskningsfältet vuxit ihop något (Wirtz, Pistoia, Ullrich, & Vincent, 2015), men fortfarande saknas gemensam terminologi och ensade definitioner (Lambert & Davidson, 2013; Massa, Tucci, & Afuah, 2017; Saint-louis, Morency, & Lapalme, 2017; Zott m.fl., 2011) och den teoretiska grunden behöver förstärkas (Nurmi, Pulkkinen, Seppänen, & Penttinen, 2019).

Mycket av forskningen handlar om att föreslå nya formella koncept vilket ger en rigorös grund, men å andra sidan har mer empiriska studier fått stå tillbaka (Burkhart, Krumeich, Werth, & Loos, 2011; Recker & Mendling, 2016). Av de 50 studier som analyserades i en systematisk genomgång hade enbart sex empiriskt stöd för sina påståenden (Tamm, Seddon, Shanks, & Reynolds, 2011). Vidare är de som arbetar med verksamhetsanalyser ofta självlärda, vilket gör att det finns en risk att den praktiska användningen inte är konsekvent (Recker, 2010).

3. Metod

Studien som redovisas i denna rapport baseras på genomgång av litteratur (avsnitt 3.1) och intervjuer med personer som genomfört eller på annat sätt kommer i kontakt med verksamhetsanalyser (avsnitt 3.2).

3.1 Litteraturstudie

Potentiell litteratur av Försvarsmakten, Försvarets Materielverk (FMV) och andra civila myndigheter granskades av en till fem av rapportens författare och information från dokumenten som var kopplat till verksamhetsanalyser (innehåll, genomförande eller användning) sammanställdes. När samtlig litteratur granskats genomfördes flera arbetsmöten för att se till att forskargruppen hade en samstämmig uppfattning.

Kort efter sammanställningen av den akademiska litteraturen användes den för att skapa kategorier (med tillhörande aspekter), vilka ämnade ge en överblick över verksamhetsanalysers informationsbehov. Baserat på dessa kategorier och aspekter granskades och kategoriserades sedan den sammanställda litteraturen från Försvarsmakten, FMV och civila myndigheter, vilket sedan jämfördes med den akademiska sammanställningen och den totala uppsättningen kategorier och aspekter uppdaterades.

Hur dokumenten identifierades beskrivs i avsnitten 3.1.1–3.1.4. Därefter följer ett avsnitt (3.1.4) som beskriver hur litteraturen analyserades.

3.1.1 Försvarsmaktslitteratur

Eftersom *Militära underrättelse- och säkerhetstjänsten* (MUST) står bakom de dokument som reglerar Försvarsmaktens användning av verksamhetsanalyser (inom ramen för säkerhetsanalyser) utgick litteratursökningen från MUST:s lista på relevanta bestämmelser och riktlinjer (Försvarsmakten, 2018b). De dokument som baserat på titel bedömdes vara relevanta lästes igenom och allt som uttryckligen rörde verksamhetsanalys noterades.[2]

[2] Det kan även finnas andra utsagor som påverkar hur verksamhetsanalyser ska utföras och beskrivas. Exempelvis kan ett dokument säga att verksamhetsanalyser ska dokumentera resurserna (en inkluderad utsaga) medan ett annat dokument förtydligar vad Försvarsmakten menar med resurser, men utan att uttryckligen nämna verksamhetsanalyser (därför en exkluderad utsaga).

Relevant information identifierades i nio dokument: en föreskrift[3], en intern bestämmelse, fyra handböcker och tre skrivelser. Några ytterligare dokument hittades inte i vidare sökningar.

3.1.2 Litteratur från Försvarets Materielverk

Litteratur från Försvarets Materielverk (FMV) har inkluderats i litteraturstudien i form av dokumentation av processen för it-säkerhetsdeklaration (ISD-processen) (FMV, 2018). Litteraturgenomgången för FMV-dokument har därför inte varit uttömmande.

3.1.3 Akademisk litteratur

Sökningen efter akademisk litteratur gjordes på engelska och inleddes med några sökningar för att komma fram till vilka begrepp på engelska som motsvara svenskans *verksamhetsanalys*. De söktermer som slutligen nyttjades var:

- business analysis
- business description
- business process
- business model
- business process modelling
- process model/-ling
- business process management
- process architecture
- business architecture
- business process architecture
- enterprise architecture

För var och en av söktermerna gjordes sökning i databasen *Scopus* för att hitta forskningsartiklar som innehöll respektive söktermen i titel, sammanfattning eller som nyckelord. För vissa av söktermerna erhölls ett stort antal artiklar. Då inkluderades enbart de artiklar som erhållit många citeringar samt artiklar som utgjorde genomgångar av andra artiklar (eng. review eller survey). Särskilda sökningar gjordes också med tillägget *security* till de övriga söktermerna. Bedömning av vilka av artiklarna som bedömdes vara relevanta gjordes av en av rapportens författare och denne författare läste sedan igenom artiklarna och

[3] Föreskriften (FFS 2015:2) som pekades ut av MUST:s övergripande dokument uppdaterades kort efter att det övergripande dokumentet utgivits. Den uppdaterade versionen av föreskriften (dvs. FFS 2019:2) inkluderades.

noterade utsagor om verksamhetsanalys. För de artiklar där många, eller särskilt intressanta utsagor hittades, undersöktes även relevanta artiklarnas referenser efter fler relevanta artiklar. Totalt inkluderades 19 intressanta forskningsartiklar som kan besvara rapportens forskningsfrågor.

Utöver Scopus gjordes även sökningar (på svenska efter verksamhetsanalys eller verksamhetsbeskrivning) i forsknings- och studentdatabasen *DIVA*[4], men där hittades inga intressanta dokument.

3.1.4 Litteratur från civila myndigheter

Relevant svensk litteratur från civila myndigheter identifierade genom sökningar på myndigheternas webbplatser och utsagor som gick att koppla till verksamhetsanalyser noterades. Sådana utsagor hittades i ett dokument utgivet av *Säkerhetspolisen* och ett utgivet av *Myndigheten för Samhällsskydd och Beredskap* (MSB). Relevant information hittades också på webbplatsen Informationssakerhet.se som MSB står bakom. Vad gäller internationell myndighetslitteratur gjordes sökningar som enbart resulterade i två extra källor. Det ena dokumentet var utgivet av amerikanska National Institute of Standards and Technology (NIST), medan det andra var utgivet av Internationella standardiseringsorganisationen (ISO).

3.1.5 Analys av litteraturen

För varje typ av litteratur delades de identifierade relevanta utsagorna (per källa) in i kategorier och aspekter som bedömdes vara lämpliga. Detta gjordes i likhet med tematisk analys (Braun & Clarke, 2006) är utsagorna användes för att skapa kategorier och aspekter (teman). De olika kategoriseringarna från de fyra olika typerna av litteratur jämfördes sedan med varandra, likheter och skillnader analyserades.

Utifrån den akademiska litteraturen kategoriserades information som resultatet från verksamhetsanalyser bör innehålla. Kategoriseringen användes sedan som stöd vid granskning av övrig litteratur för att se om det finns överlapp mellan Försvarsmakten, FMV, civila myndigheter och akademin gällande hur verksamhetsanalyser utförs och vad de innehåller.

Förutom att svara på rapportens frågeställningar användes resultaten från litteraturstudien som stöd för att generera relevanta intervjufrågor till personer

[4] DIVA är ett digitalt arkiv som samlar forskningsartiklar och studentuppsatser från Sveriges olika universitet och högskolor.

som aktivt arbetar med att göra verksamhetsanalyser eller är mottagare av dessa. Hur intervjuerna genomfördes beskrivs i avsnitt 3.2.

3.2 Intervjustudie

Intervjuer genomfördes med fyra personer som tagit fram eller varit mottagare av verksamhetsanalyser. Syftet med intervjuerna var att erhålla ytterligare insikter gällande hur verksamhetsanalyser utförs i praktiken och att jämföra riktlinjer från litteraturen med erfarenheter från praktiskt genomförande.

Intervjupersonerna kategoriserades in fyra stereotyper:

- Riskhanteringsexperten
- Cybersäkerhetskonsulten
- Informationsvärderaren
- Säkerhetsansvarige

Intervjuerna genomfördes med en semistrukturerad metodik där frågorna som konstruerats på förhand baserades på intervjuexempel från (Arvola, 2014). Dessa intervjuexempel innehåller ett antal olika synvinklar såsom *vem*, *vad*, *när* och *hur*. Utifrån synvinklarna och forskningsområdet konstruerades de specifika frågor som var relevanta. Den kompletta frågelistan återfinns i Bilaga A. Frågorna användes som stöd vid intervjuerna och avslutades med att deltagaren fick lämna öppna tankar och åsikter samt ställa frågor till intervjuledarna om studien.

4. Försvarsmaktslitteratur

Försvarsmaktens verksamhetsanalyser (Försvarsmakten, 2013a) utgör grunden för:

- Regelverksanalys, där det analyseras vilka lagar, förordningar, föreskrifter, bestämmelser och andra regler som IT-systemet och dess information omfattas av.
- Säkerhetsanalys, där risker identifieras och bedöms samt skydd föreslås.

Försvarsmaktens dokument beskriver inte i någon större omfattning hur verksamhetsanalys ska utföras. Det föreskrivs dock att:

- Verksamhetsanalysen ska genomföras av den eller de med ansvar för verksamheten (Försvarsmakten, 2013a).
- För mindre system kan verksamhetsanalysen utföras i ett steg gemensamt med regelverksanalys och säkerhetsanalys (Försvarsmakten, 2013b).
- Tillgångar kan delas in på olika sätt i verksamhetsanalysen (Försvarsmakten, 2013a).

Enligt tidigare mallar för genomförande av verksamhetsanalys (MAACK[5]), står det att användningsfall ska användas eftersom de ger en intuitiv beskrivning av verksamheten. Vidare beskrivs att verksamhetsanalysen bör revideras då verksamhet, system eller informationsinnehåll förändrats. Intervjuer och gruppövningar anges som lämpliga metoder (Försvarsmakten, 2006).

Det framgår också att verksamhetsanalysen ska utgå ifrån de aspekter av verksamheten som beskrivs i Tabell 1. Aspekterna utgår från de som identifierades i den akademiska litteraturen och för varje aspekt anges i tabellen vilka dokument (kolumner a–i) som nämner aspekten. Aspekterna är indelade i fyra kategorier. Nedan följer kortare beskrivningar av kategorierna och deras aspekter (kursiverade):

- Styrning avser hur verksamheten styrs, exempelvis i form av *inriktning*, *uppgifter* och *mål*. Dessutom inkluderas hur medarbetarna regleras med tanke på *behörigheter* och *författningar*[6] samt vilka *beroenden* som finns mellan olika delar av verksamheten och vad *konsekvenserna*

[5] Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten.

[6] I Försvarsmaktens process sker regelverksanalys efter verksamhetsanalys. Viss uppfattning om regelverken är dock nödvändig redan i verksamhetsanalysen, varför författningar inkluderats som en informationsmängd för verksamhetsanalyser.

skulle bli om någon del av verksamheten skadas, förstörs, försenas, uteblir eller röjs.

- Innehav berör vad verksamheten innehar, både i form av fysiska ting såsom *materiel* och *resurser*, men även *processer* och *funktioner*. Även *information* är inkluderad som en aspekt under kategorin innehav och har delats upp i de tre delaspekterna konfidentialitet, riktighet och tillgänglighet.
- Människor inkluderar bland annat olika aspekter av *intressenter*.
- Externt tar upp faktorer som *samarbete* (över nationsgränsen), *geografisk plats* (miljön och om IT-systemet ska användas utanför Försvarsmaktens objekt, lokaler, områden och om det ska användas internationellt) samt *tillstånd* (huruvida det är kris, krig, fred, eller gråzon).

Aspekterna kan ytterligare förklaras av de citat som finns i Bilaga C.

Tabell 1: Kategoriserade aspekter för verksamhetsanalyser och verksamhetsbeskrivningar och vilka av källorna som nämner aspekterna.

Kategori	**Aspekt**	**Delaspekt**	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
Styrning	Inriktning				●					●	
	Uppgifter					●					
	Behov				●				●		
	Mål				●			●			
	Behörigheter						●				
	Författningar			●			●				●
	Beroenden		●				●				
	Konsekvenser				●	●					
Innehav	Processer							●			
	Funktioner				●						
	Informations-överföring		●				●				
	Metoder									●	
	Anläggningar					●					
	Materiel					●				●	

Kategori	Aspekt	Delaspekt	a	b	c	d	e	f	g	h	i
	Resurser						●			●	
	Brister				●						
	Information	Konfidentialitet		●		●	●		●	●	
	Information	Riktighet	●			●	●				
	Information	Tillgänglighet	●		●	●	●				
	Skydd		●								
Människor	Förmågor och kompetenser				●					●	
	Ansvar					●	●	●			
	Personal					●				●	
	Intressenter				●						
	Roller				●	●	●				
Externt	Samarbete						●				
	Arbetsmiljö				●						
	Geografisk plats	Externarbete					●				
	Geografisk plats	Nationellt/inter-nationellt					●				
	Tillstånd		●				●				
	Tidsramar							●			

Tabellens källor: a = FFS 2019:2 säkerhetsskydd (2019), b = FIB 2015:1 skydd för utrikes- och sekretessklassificerade uppgifter och handlingar (2015), c = H KIS (2018a), d = H Säk grunder (2013a), e = H Säk infosäk (2013b), f = H Säk skydd (2007), g = KSF 3.1 (2014), h = Riktlinjer avseende säkerhetstjänstens bedrivande under större övningar (2009), i = Säkerhetskrav på IT-system som är avsedda för behandling av personuppgifter (2013c).

5. Litteratur från Försvarets materielverk

FMV har tagit fram en process som kallas för ISD[7] (FMV, 2018). Processen används då FMV tar fram IT-system till Försvarsmakten. Information från Försvarsmakten är indata till processen, där sedan vidare analyser utförs för att komma fram till en design som kan ackrediteras hos Försvarsmakten. I de fall indata från den verksamhetsanalys som utförs i säkerhetsmålsättningen inte är tillräcklig genomförs en kompletterande analys.

De informationsmängder som lyfts fram som viktiga återges i Tabell 2.

Tabell 2: Kategoriserade aspekter för verksamhetsanalyser och verksamhetsbeskrivningar och kommentarer för aspekterna (i förekommande fall).

Kategori	**Aspekt**	**Kommentar**
Styrning	Uppgifter	
	Behov	Som verksamheten har.
	Regelverk	
Innehav	Användningsfall	
	Tillgångar	Som är skyddsvärda.
	Brister	
	Information	Både i form av information som flödar i användningsfallen och som informationssäkerhetsklassificering och utmaningar med sådana klassificeringar.
	Teknik	I form av system av system.
	Exponering	Såsom antal användare, fysiskt skydd och externa/interna gränsytor.
Externt	Kontext	

[7] Informationssäkerhetsdeklaration.

Informationen från verksamhetsanalysen används för flera steg i ISD-processen, bland annat för att bedöma realiserbarheten och den ekonomiska aspekten. Ett syfte med att identifiera användningsfall som lyfts fram är att ge en rimlig uppfattning om aktuella driftmiljöer, hot och regelverkspåverkan. Användningsfallen kan även ge information om vilka säkerhetsdomäner som passeras och om det finns risk för att information med olika informationssäkerhetsklass möts. Vidare ger de en övergripande beskrivning av verksamhetens syfte.

6. Akademisk litteratur

I följande avsnitt beskrivs vad forskningen säger om verksamhetsanalysers syfte (6.1), hur analyserna ska genomföras (6.2) och vad analyserna ska utgå ifrån för information (6.3).

6.1 Verksamhetsanalysers syfte

Forskningslitteraturen beskriver tre övergripande syften med att göra verksamhetsanalyser: nuläge, önskat tillstånd samt bättre IT och ökad säkerhet.

6.1.1 Nuläge

De syften med verksamhetsbeskrivningar som är återkommande i litteraturen är att beskrivningarna ger:

- En enhetlig och informativ modell av verksamheten (Carnaghan, 2006; Oda, Fu, & Zhu, 2009; Tamm m.fl., 2011).
- Ökad situationsuppfattning (Alotaibi & Liu, 2017; Recker, 2010; Tamm m.fl., 2011).
- Ökad kunskap (Alotaibi & Liu, 2017; Recker, 2010).
- Dekonstruktion av den organisatoriska komplexiteten (Recker, 2010).

Dessutom möjliggör verksamhetsbeskrivningar:

- Gemensam förståelse (Aguilar-Saven, 2004; Tamm m.fl., 2011).
- Delad kunskap (Koubarakis & Plexousakis, 2002).
- Bättre kommunikation (Tamm m.fl., 2011).
- Koordinering mellan olika roller (Kaisler, Armour, & Valivullah, 2005).
- Klargörande av ansvarsfördelningen (Kaisler m.fl., 2005).

Det lyfts också fram att genomförandet av verksamhetsanalys kan vara lärorikt för analytiker och andra inblandade (Koubarakis & Plexousakis, 2002; Tamm m.fl., 2011).

6.1.2 Önskat tillstånd

Det finns brett stöd i forskningslitteraturen för att verksamhetsanalyser förutom att visa på ett nuläge också kan användas för att förbättra verksamheten genom att definiera ett önskat verksamhetstillstånd (Aguilar-Saven, 2004; Kaisler m.fl., 2005; Pavlovski & Zou, 2008; Tamm m.fl., 2011). Verksamhetsanalyser kan då leda till:

- Förbättringar såsom ökad interoperabilitet och standardisering mellan processer (Tamm m.fl., 2011).
- Eliminering av redundans (Oda m.fl., 2009; Tamm m.fl., 2011).
- Eliminering av processer som inte bidrar till verksamhetens mål (Röhrig, 2003).
- Ökad effektivitet (Koubarakis & Plexousakis, 2002).
- Mer renodlade processer och roller (Röhrig, 2003).
- Ökad prestanda (Kaisler m.fl., 2005).

Tamm m.fl. (2011) noterade att vilket värde en organisation kan erhålla av en verksamhetsanalys beror på kontexten för organisationen, där större värde exempelvis fås av en organisation som har mer redundans, större behov av standardisering och en högre grad av separation mellan organisationsdelar. Kaisler m.fl. (2005) framförde behovet av att verksamhetsbeskrivningen (av nuläget) hålls korrekt under tiden verksamheten förändras (till det önskade läget).

6.1.3 Bättre IT och ökad säkerhet

Det finns ett antal forskningsartiklar som specifikt påtalar verksamhetsanalysers betydelse för att erhålla bättre IT-system och ökad säkerhet. Angående IT-system kan verksamhetsanalyser göra det möjligt att utifrån övergripande verksamhetsmål ta fram IT-mål (Alotaibi & Liu, 2017) och i övrigt stödja och förbättra IT-satsningar (Oda m.fl., 2009; Tamm m.fl., 2011). Vad gäller säkerheten underlättar verksamhetsanalyser identifiering av risker (Röhrig, 2003) samt identifiering och utvärdering av säkerhetsmekanismer (Pavlovski & Zou, 2008; Röhrig, 2003). Dessutom kan verksamhetsanalyser leda till ökad regelefterlevnad (Tamm m.fl., 2011), förenkla kommunikation mellan säkerhetsexperter och chefer (Röhrig, 2003) samt i övrigt leda till ökad säkerhet (Alotaibi & Liu, 2017; Tamm m.fl., 2011).

6.2 Verksamhetsanalysers genomförande

Den akademiska litteraturen beskriver hur verksamhetsanalyser ska genomföras och hur resultatet ska beskrivas, vad gäller metodval, intressenter och roller samt vidmakthållande.

6.2.1 Metodval

Enligt Aguilar-Savén (2004) finns det ett stort antal sätt att utföra verksamhets-analyser och det är svårt att avgöra hur valet bland dessa ska genomföras. Analysen kan inledas från en översiktlig nivå och sedan brytas ner till mindre

delar, eller börja med de mindre, specifika delarna och sedan kombinera dessa för att bygga upp den översiktliga nivån (Alotaibi & Liu, 2017). Enligt Dijkman m.fl. (2014) är det vanligast att återanvända delar av tidigare genomförda analyser och anpassa dessa för den nya kontexten. Lund m.fl. (2011a) lyfte också fram att resultaten från tidigare genomförda verksamhetsanalyser bör utgöra underlag för framtida verksamhetsanalyser vilket sparar tid. Studier har också visat att användandet av en konsekvent verksamhetsanalysmetod över tid ger bättre möjligheter att upprätthålla korrekta verksamhetsbeskrivningar snarare än att byta eller förändra den metod som används för varje nytt system som ska införas (Fox & Gruninger, 1998). Samtidigt lyfter Kaisler m.fl. (2005) fram att varje verksamhetsbeskrivning är unik och att valet av metod är den största utmaningen för verksamhetsanalysarbetet. I den akademiska litteraturen kan det urskiljas ett antal faktorer som bör beaktas vid valet av metod:

- **Vad metoden ursprungligen togs fram för**
  Många metoder togs inte ursprungligen fram för att genomföra verksamhetsanalyser utan exempelvis för att studera enskilda IT-system (Carnaghan, 2006). Vidare är vissa metoder bättre för vissa tillämpningar (Aguilar-Saven, 2004) och det kan vara lämpligt att välja en metod som används av organisationer som har likheter med den egna (Kaisler m.fl., 2005). Vidare kan det vara lämpligt att ha en enklare organisationsövergripande verksamhetsbeskrivning som varje projekt använder som utgångspunkt för att ta fram en mer specifik beskrivning (Kaisler m.fl., 2005). Detta ställer krav på att den allmänt hållna verksamhetsbeskrivningen kan delas till övriga i organisationen (Fettke, Loos, & Zwicker, 2005).

- **Hur enkel och förståelig metoden är**
  Detta inkluderar användbarhet (Fettke m.fl., 2005) och om metoden har verktygsstöd (Fettke m.fl., 2005; Green & Ould, 2005). Kaisler m.fl. (2005) noterade exempelvis att verktyg ofta saknar tidsaspekten för processer, medan Koubarakis och Plexousakis (2002) lyfte fram ett särskilt behov av verktygsstöd för mer formella och svårförståeliga metoder. Generella slutsatser i litteraturen är att det är svårt att använda metoderna och att gå från verksamhetsövergripande verksamhetsbeskrivningar till något som är lämpat för IT-system (Alotaibi & Liu, 2017). En ytterligare slutsats är svårigheten att avgöra var en process börjar och var en annan tar vid samt att avgöra hur detaljerad verksamhetsbeskrivningarna behöver vara (Dijkman m.fl., 2014).

- **Hur uttryckbar metoden är**
  Koliadis et al. (2008) noterade att vissa metoder inte rymmer mål på alla möjliga nivåer och att det ofta saknas möjlighet att uttrycka hur väl

verksamhetsprocesserna fungerar. Metoder tar dessutom ofta inte hänsyn till var i organisationen något görs eller vilka skydd som finns (Carnaghan, 2006). Kaisler m.fl. (2005) presenterade en sexgradig skala för hur väl den resulterande verksamhetsbeskrivningen stämmer överens med verkligheten.

- **Hur resultatet (verksamhetsbeskrivningen) ska se ut**
  Carnaghan (2006) formulerade en grundläggande forskningsfråga med avseende på om det är bättre att resultatet visas med någon av de många grafiska varianter som finns eller textbaserat. Fettke m.fl. (2005) noterade att resultatet inte får bli otympligt stort.

6.2.2 Intressenter och roller

En verksamhetsanalys måste väga in intressenter och roller (Alotaibi & Liu, 2017; Lund m.fl., 2011a). Detta är viktigt för att ensa verksamhetsbehov och IT-behov samt integrera säkerheten i analysen (Alotaibi & Liu, 2017). Alotaibi och Liu (2017) lyfte fram tre grupper av intressenter:

- Verksamhetsnära: De som utför verksamhetsanalysen eller designar och implementerar system.
- Användarstöd: De som ger stöd till användare.
- Utbildare: De som utbildar analytiker och tar fram nästa generations metoder.

För att de olika intressenternas perspektiv ska kunna beaktas behövs god kommunikation intressenterna emellan. Exempelvis kan intervjuer med, eller observationer av, intressenter utföras (Pavlovski & Zou, 2008). Lund m.fl. (2011a) lyfte fram att kommunikation mellan intressenter kräver att intressenterna enas om en gemensam terminologi som leder till förenklad kommunikation och minskar risken för missförstånd.

6.2.3 Vidmakthållande

Litteraturen beskriver behov av att kunna göra om delar av verksamhetsanalysen i takt med förändringar av omgivningen (Alotaibi & Liu, 2017; Lund, Solhaug, & Stølen, 2011b) eller verksamheten (Kaisler m.fl., 2005). Detta ställer krav på att förändringarna har uppfattats och förståtts samt att verksamhetsanalysen kan göras snabbt nog (Green & Ould, 2005; Kaisler m.fl., 2005). Kaisler m.fl. (2005) noterade att det är svårt att avgöra när en ny analys behöver göras och forskningen ger bara begränsat stöd vad gäller förändringarna.

6.3 Verksamhetsanalysers informationsbehov

I den akademiska litteraturen uttrycks att verksamhetsanalyser ska utgå ifrån de aspekter som återges i Tabell 3, indelat i fyra kategorier. Nedan följer några kortare beskrivningar av kategorierna och deras aspekter:

- *Styrning* innehåller bland annat aspekten *uppdrag* (eng. mission), vilket är den övergripande anledningen till att organisationen finns. *Mål* är mer detaljerade (nedbrutna) varianter av uppdrag. *Vision* beskriver var verksamheten ska vara i framtiden och *strategi* beskriver vägen dit. *Koordinering och beroenden* handlar om att andra aspekter beror på varandra och måste koordineras. *Beslutsmodell* beskriver hur och var beslut tas i organisationen.
- *Innehav* rör aspekter om vad verksamheten innehar, både i form av fysiska ting såsom *resurser och tillgångar* samt *teknik*, men också sådant som *processer* och *funktioner*. Dessutom inkluderas *information*.
- *Människor* inkluderar *intressenter och roller*, *personal*, deras *förmågor och kompetenser* samt hur de passar in i organisationens struktur.
- *Externt* tar upp externa faktorer som *kunder* och *leverantörer*, *rykte*, *kontext* och *tidsramar*.

Tabell 3: Kategoriserade aspekter för verksamhetsanalyser och verksamhetsbeskrivningar och vilka av källorna som nämner aspekterna.

Kategori	**Aspekt**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**
Styrning	Uppdrag	●					●		
	Vision						●		
	Behov						●		
	Mål		●	●	●	●	●	●	
	Strategi		●	●					
	Beslutsmodell		●						
	Policyer			●					●
	Riktlinjer, vägledningar och standarder		●						
	Koordinering och beroenden					●			
	Ekonomi	●							

Kategori	Aspekt	j	k	l	m	n	o	p	q
Innehav	Processer	●	●	●	●		●		●
	Funktioner				●				
	Resurser och tillgångar	●			●		●	●	
	Information		●	●	●	●	●		
	Teknik		●			●	●		●
Människor	Organisatorisk struktur		●		●		●		
	Förmågor och kompetenser	●							
	Personal				●		●		●
	Intressenter och roller		●	●		●	●	●	●
Externt	Avtal och kontrakt								●
	Kunder	●							
	Leverantörer	●		●					
	Konkurrenter	●							
	Rykte	●							
	Kontext			●					
	Geografisk plats					●	●		
	Tidsramar			●					

Tabellens källor: j = (Shafer, Smith, & Linder, 2005), k = (Youseef & Liu, 2012) l = (Oda m.fl., 2009), m = (Fox & Gruninger, 1998), n = (Röhrig, 2003), o = (Kaisler m.fl., 2005), p = (Lund m.fl., 2011b), q = (Lund m.fl., 2011a).

7. Litteratur från civila myndigheter

Enligt den civila myndighetslitteraturen leder verksamhetsanalys till en verksamhetsbeskrivning som beskriver ett nuläge av en verksamhet och som kan användas för att illustrera verksamhetsmålens betydelse och vilka problem som

finns inom en verksamhet (Andersson m.fl., 2011)[8]. En verksamhetsbeskrivning visar också på verksamhetens ansvar och vilka övergripande processer verksamheten består av (Säkerhetspolisen, 2018). Dessutom åskådliggör en verksamhetsbeskrivning vilken kontext verksamhetens informationssäkerhetsrisker finns i, såsom huruvida informationssäkerhetsavdelningen lyder under IT-avdelningen eller under högre ledning (ISO, 2018).

Inom civila myndighetslitteratur beskrivs flera olika sätt att utföra verksamhetsanalyser. Eftersom det kan vara ett omfattande arbete att starta ett analysarbete från ett blankt ark är rekommendationen att, om möjligt, utgå från tidigare genomförda analyser (Informationssäkerhet.se, u.å.). Dock kan tidigare genomförda analyser behöva omstruktureras för att passa sitt nya syfte (Andersson m.fl., 2011).

Analysarbetet kan inledas med att studera verksamheten på en övergripande nivå och sedan bli mer detaljerad. Ett alternativ är att börja med den lägre och mer konkreta nivån för att sedan lägga samman delarna och nå den övergripande nivån som bättre beskriver helheten. Exempelvis går det att utgå från informationstillgångarna och undersöka vilka mål som ska uppnås med dessa, vad som skulle ske om en tillgång saknas och vilka processer som stöds av den. En annan möjlighet är att utgå från processer och informationsflöden för att komma fram till vilka tillgångar som behövs (Andersson m.fl., 2011).

En närliggande fråga är vilket omfång analysen behöver ha. Exempelvis kan en del tillgångar inte vara så centrala i sammanhanget varför de kan ignoreras (Informationssäkerhet.se, u.å.). Omfånget kan också begränsas baserat på vilka organisationsnivåer eller verksamhetsprocessnivåer som ska inkluderas, om bara det enskilda IT-systemet ska beaktas eller även kontexten samt vilket tidsspann analysen ska gälla för (NIST, 2012).

Om intressenter har olika uppfattning om hur verksamheten fungerar, så är det nödvändigt att genomföra gruppdiskussioner eller seminarium för att ena uppfattningarna (Andersson m.fl., 2011).

Tabell 4 redogör för vilka kategorier och aspekter som identifierats i den civila myndighetslitteraturen, indelat i fyra kategorier.

[8] Detta dokument är utgivet av MSB.

Tabell 4: Kategoriserade aspekter för verksamhetsanalyser och verksamhetsbeskrivningar och vilka av källorna som nämner aspekterna.

Kategori	**Aspekt**	**r**	**s**	**t**	**u**
Styrning	Uppdrag	●		●	●
	Affärsidé och värdegrund	●			●
	Vision	●			
	Mål	●	●		●
	Strategi		●		●
	Policyer		●		●
	Författningar	●			●
	Riktlinjer, vägledningar och standarder		●		●
	Beroenden				●
	Ekonomi				●
	Ägarförhållanden	●	●		
Innehav	Processer		●	●	●
	Funktioner			●	●
	Kommunikation		●	●	●
	Resurser och infrastruktur		●	●	●
	Fysiska tillgångar	●			
	Information	●	●	●	●
	Teknik				●
	Programvara	●		●	●
Människor	Organisatorisk struktur		●		●
	Förmågor och kompetenser	●	●		●
	Personal			●	●
	Ansvar		●		●
	Kultur		●		●
	Intressenter och roller		●		●

Kategori	Aspekt	r	s	t	u
Externt	Avtal och kontrakt	●			●
	Leverantörer				●
	Tjänster (ex värme, el)	●		●	●
	Konkurrenter				●
	Rykte	●		●	●
	Kontext				●
	Tillstånd (ex kris, politiskt klimat)				●
	Bransch	●			
	Geografisk plats (i allmänhet)		●		●
	Geografisk plats (nationellt/internationellt)				●
	Tidsramar				●

Tabellens källor: r = (Andersson m.fl., 2011) utgiven av MSB, s = (Informationssäkerhet.se, u.å.), t = (NIST, 2012), u = (ISO, 2018).

8. Intervjuer

Fyra intervjuer genomfördes och dessa beskrivs i de kommande avsnitten. Först följer dock en kort beskrivning av varje intervjuperson tillsammans med ett sammanfattande namn.

- **Riskhanteringsexperten**
  Den första intervjupersonen hade erfarenhet av genomförande av verksamhetsanalys kopplat till risk- och sårbarhetsanalyser inom den civila sektorn och hade erfarenhet av att arbeta med både kommuner och statliga myndigheter.
- **Cybersäkerhetskonsulten**
  Den andra intervjun genomfördes med en person med erfarenhet av både verksamhetsanalyser och säkerhetsmålsättning inom ramen för sin roll som cybersäkerhetsexpert inom den militära och civila domänen.
- **Informationsvärderaren**
  Den tredje intervjun genomfördes med en person med koppling till värdering av information. Personen har erfarenhet av att arbeta inom den militära domänen och har innehaft samordningsansvar för komplexa verksamhetsanalyser.
- **Säkerhetsansvarige**
  Den fjärde intervjun genomfördes med en person som innehar en roll som säkerhetsansvarig. Personen innehar erfarenhet inom den militära domänen och har arbetat med säkerhet i relation till affärssystem.

8.1 Intervju 1 – Riskhanteringsexperten

Från intervjun framkom att de verksamhetsanalyser som genomförs ofta sker explorativt. Arbete inleds med att ta reda på vad verksamheten har för krav och åtaganden. Analys sker sedan av vilka funktioner som krävs för åtagandena. Från funktionerna går analysen sedan ner på detaljnivå för att identifiera exakt vad som krävs för att verksamheten ska fungera (t.ex. personer, nätverksförbindelser och drivmedel). För att göra detta uppgav riskhanteringsexperten att både top-down- och bottom-up-perspektiv fungerar. Riskhanteringsexperten använde själv en kombination av båda perspektiven.

Det viktigaste vid genomförandet av en verksamhetsanalys är enligt Riskhanteringsexperten att ”*strunta i vad som står i beskrivande handböcker och policydokument*”. En person som genomför verksamhetsanalyser måste fokusera på praktiken och vad som verkligen sker i organisationer snarare än vad som beskrivs i dokument. Handböcker ska endast användas som inspiration och inte som checklistor då det annars kan leda till en blindhet inför hur verksamheten

ser ut med dess förutsättningar och begränsningar. Handböcker och checklistor ska endast användas för att ge kreativa inslag i en process och inte explicit skriva vad som ska göras. För en lyckad process ställs krav på erfarenhet och kunskap hos de som analyserar verksamheten. Genomförandet av verksamhetsanalysen måste vara explorativ och spegla hur verksamheten fungerar. Det som säkerställer att en verksamhetsanalys är bra är kompetensen att genomföra den och erfarenhet av domänen.

Riskhanteringsexperten ansåg att det är positivt att det inte finns en konkret handbok för genomförandet av analyser. Samtidigt upplevs det dock som viktigt att det finns riktlinjer som beskriver hur en verksamhetsanalytiker bör agera och tänka. Exempelvis bör riktlinjerna inte säga vilken information som behöver tas hänsyn till utan hur analytikern bör tänka för att ta reda på vilken information som behövs. Vidare poängterades att en handbok bör notera att olika roller ger tillgång till olika typer av insikter i verksamheten. Detta innebär att det är viktigt att prata både med individer i chefsroller (generalister) och med mer operativa roller (specialister).

Det poängterades av riskhanteringsexperten att granskare av verksamhetsanalyser helst ska ha varit med i processen för att förstå arbetet och dess innebörd, men att externa granskare har möjlighet att ge tillgång till perspektiv som annars riskerar att missas. Externa granskare (vilket inkluderar individer från andra delar av verksamheten) bär med sig fördelen att de inte är investerade i det genomförda arbetet varför de troligtvis inte drar sig för att ställa frågor och rikta kritik. Riskhanteringsexperten uppgav att detta ifrågasättande ofta är något interna granskare missar på grund av att de har alltför starka anknytningar till verksamheten som analyseras. Oavsett om granskaren är en extern part eller har starka anknytningar till verksamhetsanalysen är det viktigt att se till kompetensen hos mottagaren. Om inte nödvändig kompetens som krävs för att förstå den genomförda verksamhetsanalysen finns, så kan detta leda till missförstånd kring använda begrepp eller att viktiga detaljer saknas. Det är därför viktigt att förstå kompetensen hos den som är mottagare av verksamhetsanalysen.

När riskhanteringsexperten fick ta del av projektets tabell (se Bilaga B) över viktiga informationsmängder enligt befintlig litteratur och handböcker såg riskhanteringsexperten vissa paralleller till sitt arbete. Följande aspekter angav riskhanteringsexperten som mest relevanta (utan specifik prioriteringsordning):

- Avtal och kontrakt (som kritiskt beroende)

- (Brister) och skydd[9]
- Funktioner
- Förmågor och kompetenser (som resurs)
- Koordinering och beroenden
- Leverantör
- Organisatorisk struktur (med fokus på arbetet i praktiken)
- Personal (som resurs)
- Resurser och tillgångar
- Rykte (i form av konsekvensanalys)
- Samarbetspartner
- Teknik
- Uppdrag (det allra viktigaste att bygga arbetet mot)

Riskhanteringsexperten framhöll också att vissa aspekter *inte* skulle inkluderas:

- Mål
- Strategi
- Beslutsmodell
- Policyer
- Riktlinjer, vägledningar och standarder

Riskhanteringsexperten upprepade sedan att sådana listor är farliga att använda då fokus lätt tappas på det eget uppdraget (hur verksamheten faktiskt fungerar) och genom dessa förbiser viktiga delar i verksamheten.

8.2 Intervju 2 – Cybersäkerhetskonsulten

Enligt intervjupersonen, cybersäkerhetskonsulten, är inledningsvis det största arbetet att reda ut vilken del av verksamheten som är i fokus och hur denna verksamhet är beroende av andra. Detta sker i huvudsak med en genomgång av det som är dokumenterat och genom att komplettera detta med intervjuer. Kompletteringen behövs eftersom dokumenten oftast inte innehåller allt nödvändigt, vilket exempelvis kan bero på att det som saknas ses som uppenbart eller att vissa personer ogillar att dokumentera. Det upplevs som att den mest relevanta informationen inhämtas genom att prata med användare i verksamheten eftersom dessa oftast vet hur verksamheten fungerar i praktiken och därmed utgör en källa för att ta reda på de konkreta behoven. Vid förändringar av verksamheter är det viktigt att dessa förändringar bygger på

[9] Intervjupersonen såg skydd som en viktigare aspekt än brister, därav parentesen.

praktisk information som är baserad på användarnas kontext. Det är också viktigt att se till att kommunikationen fungerar mellan de parter som ingår i verksamhetsanalysen för att säkerställa att de olika parterna använder samma definitioner och termer så att analysen inte bygger på eller bidrar till missförstånd.

Det finns enligt cybersäkerhetskonsulten ingen universalmetod att nyttja för verksamhetsanalyser. Det viktiga är istället att känna till målet och att arbetet hela tiden styrs mot detta mål. Mallar och handböcker bör endast användas som stöd för att viktiga aspekter inte ska förbises. Dessutom kan mallar och handböcker användas som inspirationskälla och förklara hur utföraren bör tänka och varför. Att istället använda mallar och handböcker strikt kan göra att utföraren låser in sig i ett för snävt perspektiv, vilket i sin tur leder till att viktiga aspekter i verksamhetsanalysen förbises.

Det är inte ovanligt att en verksamhetsanalys måste expandera och även täcka in andra verksamheter. Detta är ofta problematiskt då en analytiker sällan har direkt tillgång till dessa verksamheter. I dessa situationer finns det förhoppningsvis väl beskrivna verksamhetsanalyser av dessa verksamheter som analytikern kan ta del av.

Cybersäkerhetskonsulten gav uttryck för att mottagare förstår vad som vill förmedlas med verksamhetsanalyser, men att det ibland ställs krav på utveckling av analysen. Detta medför att det är bra om några representanter från verksamheten som kan vara med i hela processen, från verksamhetsanalys till säkerhetsmålsättning.

För cybersäkerhetskonsulten har genomförandet av en verksamhetsanalys alltid varit grund till genomförandet av en säkerhetsanalys. Det har också hänt att cybersäkerhetskonsulten fått en redan genomförd verksamhetsanalys att använda som underlag för en säkerhetsanalys. I sådana situationer har cybersäkerhetskonsulten upplevt att det i verksamhetsanalyser är lätt att vara blind för det uppenbara. Cybersäkerhetskonsulten uppgav att det kan vara värdefullt med en extern granskare av analysen som kan kontrollera att det som oftast tas för givet faktiskt finns med.

När personen fick ta del av projektets sammanställda tabell över kategorier och aspekter markerade denne tio aspekter som extra viktiga, även om ingen aspekt ansågs vara onödig. Nedanstående lista presenteras utan specifik prioritetsordning:

- Information
- Intressenter och roller
- Kontext
- Mål

- Riktlinjer, vägledningar och standarder
- Resurser och tillgångar
- Strategi
- Organisatorisk struktur
- Personal

8.3 Intervju 3 – Informationsvärderaren

För intervjupersonen, informationsvärderaren, var verksamhetsanalysernas huvudsakliga syfte att fånga in hela flödet av den givna informationen (en bottom-up-process). Verksamhetsanalysen ska inkludera var informationen kommer att finnas likväl vem som är ansvarig. Processer och organisationsstruktur kommer i andra hand. För att genomföra detta måste verksamhetsanalysen ske iterativt och agilt, eftersom verksamheterna har hög komplexitet och det är vanligt att viktiga detaljer missas.

Informationsvärderaren påpekade att det ofta inträffar att verksamheter interagerar med varandra. Detta medför att arbetsgruppen som genomför analyserna bör bestå av representanter från de olika verksamheterna. Det är även viktigt att dessa representanter har kunskaper om hur verksamheterna fungerar snarare än expertkunskap inom genomförandet av analyser (även om det kan behjälpligt).

Ett tydligt krav som framkom i intervjun är att de berörda verksamheterna har en förståelse för vikten av att intervjua verksamhetsrepresentanter för analysens resultat. En sådan förståelse leder troligtvis till att deras representanter ges den tid och de verktyg som behövs. Det är dock ofta svårt att få alla representanter på plats samtidigt eftersom verksamheterna ska genomföra sin ordinarie verksamhet parallellt.

Vid analysarbetets uppstart är det vanligt att det uppstår problem med kommunikationen då de olika verksamheterna ”använder olika språk”. Det är därför viktigt att ett gemensamt begreppsspråk etableras i arbetsgruppen för att undvika missförstånd. Det kan ta flera arbetsmöten innan gruppens medlemmar förstår varandra fullt ut.

Vid genomförandet av verksamhetsanalysen finns det en mall att tillgå. Informationsvärderaren förordar fritt arbete då mallar kan leda till ett tänkande som hämmar kreativitet. Det uttrycktes dock att mallar eventuellt kan fungera som stöddokument för nybörjare, men att dessa inte får användas som facit.

I analysarbetets avslutande faser är det den verksamhetsansvariga som har ansvar över analysens korrekthet. Det inträffar dock att mottagaren av analysen

inte har den förståelsen som krävs för att tolka resultatet vilket innebär att analysgruppen måste revidera resultatet.

När informationsvärderaren fick granska projektets framtagna tabell gällande information som bör ingå i en verksamhetsanalys bedömde informationsvärderaren alla listans aspekter som relevanta. Specifikt skulle aspekten *information* betonas som den viktigaste aspekten i informationsvärderarens eget arbete.

8.4 Intervju 4 – Säkerhetsansvarige

Den fjärde intervjudeltagaren genomför inga verksamhetsanalyser själv utan tar emot analyser i sin roll som säkerhetsansvarig. Det största problemet som uppgavs är att det är väldigt sällan som verksamhetsanalyser faktiskt genomförs. Detta är problematiskt då verksamhetsbeskrivningar ska agera som underlag för Militära underrättelse- och säkerhetstjänsten (MUST) och för att säkerställa att verksamheten ska kunna ställa krav. Verksamhetsbeskrivningen kan ses som ett sätt för verksamheten att kommunicera.

Även om verksamhetsanalyser sällan genomförs finns det vissa återkommande problem. Ofta är det vanligt att ”inte prata samma språk” vid genomförandet av säkerhetsanalyser. Det är också viktigt att de personer som genomför verksamhetsanalyserna faktiskt förstår hur dessa fungerar, men det är svårt att frigöra tid för alla deltagare som behövs. Detta är ett problem eftersom det är väldigt viktigt att få med rätt personer från början och att de kan vara med i hela processen (inte bara verksamhetsanalysen). Det kan också vara så att en given verksamhet påverkas eller påverkar en annan verksamhet och att vissa förändringar inte kan göras då dessa påverkar överlappande verksamheter. Rätt personer kan även innebära extern expertkompetens, exempelvis så föreslogs att jurister är med under regelverksanalysen, eftersom det krävs expertkunskap för att förstå regelverkstexterna.

Det är vanligt att verksamhetsanalyser inte genomförs vilket kan beror på bristande stöd. Av detta skäl förordar den säkerhetsansvarige användningen av mallar eller att utgå från H Säk InfoSäk (Försvarsmakten, 2013b) för att få inspiration. Mallar är dock inte alltid nödvändigtvis bra, men de ger en inriktning över vad som måste genomföras.

Genomförandet av verksamhetsanalysen ska ses som ett agilt arbete. Vid säkerhetsanalysarbetet kan exempelvis information framkomma som påverkar verksamhetsanalysen så den behöver revideras.

När den säkerhetsansvarige fick se tabellen med sammanställda data från litteraturstudien gällande vad som bör ingå i en verksamhetsanalys såg intervjupersonen följande saker som mer viktiga än andra:

- I kategorin *styrning* ansåg den säkerhetsansvarige att *vision*, *behov* och *mål* var viktigast. *Strategi*, *beslutsmodell* och *policyer* och *ekonomi* bör ej ingå i en verksamhetsanalys.
- I kategorin *innehav* ansåg den säkerhetsansvarige att *processer*, *teknik* och *information* var det viktigaste. *Brister och skydd* är inkluderat i en annan analys.
- I kategorin *människor* var *intressenter* och *roller* viktigast. *Organisatorisk struktur* samt *förmågor* och *kompetenser* var inte viktigt. *Organisatorisk struktur* ändras hela tiden och därför är det bättre att hoppa över den.
- I kategorin externt var *tid* extra viktigt (med tanke på att uppdrag och uppgifter genomförs inom satta tidsramar). *Avtal* och *kontrakt* är inte viktigt och *konkurrenter*, *rykte* och *geografisk plats* inkluderas på andra sätt.

9. Analys och diskussion

Detta kapitels första avsnitt (9.1) lägger samman resultaten från litteraturstudiens genomgång av försvarsmaktslitteratur, litteratur från FMV, akademisk litteratur och litteratur från civila myndigheter. Därefter ger avsnitt 9.2 vilka nya insikter intervjuerna gett utöver vad som framkommit i litteraturstudien. Avslutningsvis ger avsnitt 9.3 en beskrivning av begränsningarna med det arbete som beskrivs i rapporten.

9.1 Litteraturen

I de följande avsnitten beskrivs de olika typerna av litteratur som helhet indelat i *verksamhetsanalysers syfte*, *verksamhetsanalysers genomförande* och *verksamhetsanalysers informationsbehov*, vilka kopplar till frågeställningarna:

1. Vad kan verksamhetsanalyser bidra med i ett informationssäkerhetsperspektiv? (avsnitt 9.1.1)

2. Hur bör verksamhetsanalyser genomföras? (avsnitt 9.1.2)

3. Vilka informationsmängder bör ingå i verksamhetsanalyser? (avsnitt 9.1.3)

Huvudsakligen återges enbart litteraturens innehåll, men avsnitt 9.1.3 innehåller en diskussion om varför de olika typerna av litteratur skiljer sig åt.

9.1.1 Verksamhetsanalysens syfte

Dokument från Försvarsmakten lyfter fram vikten av verksamhetsanalys som en del i säkerhetsarbetet. Den övriga litteraturen bekräftar vikten av verksamhetsanalyser för ökad säkerhet, men framhåller också att verksamhets-analyser har andra användningsområden. Både den akademiska och den civila myndighetslitteraturen framhåller att verksamhetsanalyser leder till en verksamhetsbeskrivning som ger en bild av verksamhetens nuläge, vilket ger ökad kunskap och förbättrade kommunikationsmöjligheter. Den akademiska litteraturen lyfter också fram att verksamhetsanalyser kan användas för att förbättra verksamheten genom att bland annat definiera och nå ett önskat verksamhetstillstånd med mer interoperabilitet, mindre redundans och onödiga processer och mer renodlade roller. Dokumentation från FMV lyfter fram att verksamhetsanalysen behövs för att analysera kring systemets realiserbarhet, krav och säkerhetsåtgärder.

9.1.2 Verksamhetsanalysens genomförande

Både den akademiska och den civila myndighetslitteraturen identifierade att en verksamhetsanalys antingen kan genomföras från detaljnivå till en högre abstraktionsnivå som visar verksamheten i ett större perspektiv, eller brytas ner från en högre nivå. Oavsett vilket angreppssätt som väljs framgår det också från litteraturen att det är viktigt att en verksamhetsanalys täcker in hela kedjan så att systemets samtliga aspekter fångas. Det är mycket möjligt att en förändring i ett system inte påverkar detaljnivån, men har stora konsekvenser för den övergripande organisationen. Detta ställer även hårdare krav på vem som gör verksamhetsanalysen.

Forskningslitteraturen beskriver behov av att kunna göra om delar av verksamhetsanalysen i takt med förändringar av omgivningen eller verksamheten. Det är dock svårt att avgöra när en ny analys behöver göras och forskningen ger bara begränsat stöd för detta. Den civila myndighetslitteraturen framhåller också att det är tidsödande att utföra verksamhetsanalyser varför en rekommendation är att utgå från tidigare genomförda analyser om sådana finns. Dock är det viktigt att vara medveten om att tidigare genomförda analyser kan behöva omstruktureras för att passa sitt nya syfte.

Den akademiska litteraturen och den civila myndighetslitteraturen tar båda upp vikten av kommunikation vid genomförandet av en verksamhetsanalys. Anledningen till att kommunikation anses viktigt är för att säkerställa användning av samma terminologi och för att minska sannolikheten för missförstånd för hur verksamhetens olika delar interagerar med varandra, vilket går bortom det som står i föreskrifter (exempelvis vissa beteenden som är till följd av en organisationskultur). En svårighet med kommunikationen är att de personer som har god kunskap om verksamheten är väldigt efterfrågade och därför svåra att få tid att prata med. Kommunikation lyftes däremot inte fram i försvarsmaktslitteraturen. Närliggande kommunikation är att se till att granskare ställer kritiska frågor. Det är då viktigt att granskarna inte varit direkt involverade i arbete med analysen.

I försvarsmaktslitteraturen finns det exempel på vad som bör ingå i en verksamhetsanalys, men väldigt lite information om genomförandet. I FMV:s dokument beskrivs att verksamhetsanalysen behöver kompletteras i de fall det finns behov av ytterligare information om verksamheten. Ett förslag till arbetsgång föreslås, men det ges inga detaljer kring genomförandet.

9.1.3 Verksamhetsanalysens informationsbehov

I Tabell 5 återges de kategorier och aspekter som identifierades som den information vilken verksamhetsanalyser bör utgå ifrån i de olika litteraturtyperna. I vissa fall återfinns en aspekt i en viss typ av litteratur, men en viss skillnad mot hur aspekten är definierad. Detta markeras då särskilt och förklaras i tabellen.

Dokumenten från Försvarsmakten och FMV lyfter till skillnad från den akademiska litteraturen och den civila myndighetslitteraturen inte fram *vision*. Detta kan vara rimligt då det inte finns någon poäng med att vid framtagandet av ett IT-system veta vad *visionen* är när beslut om införande av systemet redan tagits. Eftersom behovet av ett system redan framkommit så är det förmodligen baserat på den *vision* Försvarsmakten innehar. Detta kan jämföras med urvalet av akademisk litteratur som i högre grad berör verksamhetsförbättring än specifika system, varför *visionen* är mer relevant. Vad gäller den civila myndighetslitteraturen inkluderas *vision*, men inte *behov*. En möjlighet är att *behoven* ses som ingående i *visionen*. Ett annat alternativ till att dokumentation om *behov* saknas är att behovsanalyser oftast är kostsamma och tidskrävande, samtidigt som de kan leda till konflikter inom en organisations ledning. Ledningen kan ha stora *visioner* över vad som ska ske i en verksamhet, men under behovsanalysen är det möjligt att få insikten att *behovet*, som *visionen* skulle bygga på, saknas. Avsaknaden av behovsanalyser kan vara en anledning till att beslut som fattas på högre nivå i en verksamhet inte uppskattas på en lägre nivå i verksamheten.

Försvarsmaktslitteraturen nämner till skillnad från den civila myndighetslitteraturen inte *kultur* som en del av aspekten *personal* (åtminstone inte uttryckligen). Det skulle kunna bero på att exempelvis Försvarsmaktens *säkerhetskultur* är grundläggande i Försvarsmakten som inte ytterligare behöver behandlas i dokument som rör verksamhetsanalys. Det är rimligt att anta att Försvarsmakten har en stark hierarkisk *kultur*, exempelvis med ordergivning. På samma sätt kanske *beslutsmodellen* i Försvarsmakten är uppenbar. Alternativt ger *beslutsmodellen* avtryck i Försvarsmaktens process för framtagande av IT-system med tydliga beslutssteg och vem som ska fatta besluten. Liknande resonemang gäller troligen för *organisationsstruktur* (som också saknas i försvarsmaktslitteraturen).

I försvarsmaktslitteraturen nämns inte *ekonomi* i samband med verksamhetsanalys. Det är möjligt att *ekonomi* är en aspekt senare i processen, angående kostnad för skyddsåtgärder. I FMV:s beskrivning av verksamhetsanalyser ingår inte *ekonomi* men däremot tas det i deras ISD-process fram ett utlåtande kring realiserbarheten och den ekonomiska aspekten.

En annan förklaring till att *ekonomi* inte nämns i försvarsmaktslitteraturen är att processens (och MUST:s) fokus är att systemets säkerhet ska vara bra nog och att säkerheten därmed måste nå en viss nivå, oavsett kostnad. Det är möjligt att det är av samma skäl som *avtal och kontrakt, leverantörer* samt *kunder* saknas i försvarsmaktslitteraturen.

Försvarsmaktslitteraturen har ofta ett fokus på *information* och då ur CIA-triadens perspektiv[10], med tonvikt på konfidentialitet. Detta är rimligt eftersom Försvarsmakten, till skillnad från forskningen, har tydligt säkerhetsfokus och CIA-triaden återspeglar detta. Närliggande är att det är naturligt att Försvarsmakten ofta nämner informationsöverföring som en viktig *funktion.* Av samma skäl är det inte konstigt att försvarsmaktslitteraturen till skillnad från övriga urval tar upp *brister* och *skydd*. Dessutom tar försvarsmaktslitteraturen upp *konsekvenser,* medan den akademiska litteraturen istället använder begrepp som *koordinering* och *beroenden* (enbart *beroenden* i den civila myndighetslitteraturen). Det bör dock noteras att försvarsmaktslitteraturen inte nämner *konkurrenter* i detta sammanhang, vilket i och för sig är naturligt eftersom det ungefär motsvarar hot, vilka beaktas senare i Försvarsmaktens process.

Tabell 5: Kategoriserade aspekter för verksamhetsanalyser och verksamhetsbeskrivningar och vilka av de fyra typerna av litteratur som nämner aspekterna. Akad. = akademisk litteratur. Civil mynd. = civil myndighetslitteratur. Δ (deltatecken) innebär att typen av källa har aspekten men på ett lite annat sätt. - (minustecken) innebär att typen av källa inte har en viss del av aspekten. + (plustecken) innebär att typen av källa har aspekten plus mer som också passar in i aspekten.

Kategori	**Aspekt**	**Akad.**	**FM**	**FMV**	**Civil mynd.**
Styrning	Uppdrag	●	Δ istället *uppgifter* och *inriktning*	Δ istället *uppgifter*	+ *affärsidé* och *värdegrund*
	Vision	●			●
	Behov	●	●	●	
	Mål	●	●		●
	Strategi	●			●
	Beslutsmodell	●			

[10] CIA-triaden utgörs av informationssäkerhetsegenskaperna konfidentialitet (eng. confidentiality), riktighet (eng. integrity) och tillgänglighet (eng. availability) (Bishop, 2003).

Kategori	Aspekt	Akad.	FM	FMV	Civil mynd.
	Policyer	●	Δ istället *författningar* och *behörighet*		+ *författningar*
	Riktlinjer, vägledningar och standarder	●		Δ regelverk	●
	Koordinering och beroenden	●	- *beroenden* + *konsekvenser*		Δ bara *beroenden*
	Ekonomi	●			+ *ägar-förhållanden*
Innehav	Processer	●	●		●
	Funktioner	●	+ *information-söverföring* och metoder	Δ användnings-fall	+ *kommunikation*
	Resurser och tillgångar	●	- tillgångar[11] + *materiel* och *anläggningar*	- resurser	Δ istället *resurser* och *fysiska tillgångar* och *infrastruktur*
	Information	●	Δ nämner ofta *information* ur perspektivet CIA	Δ nämner informations-flöde och informations-säkerhets-klassifi-ceringar	●

[11] I H Säk Grunder nämns dock att om verksamhetsanalysen genomförts på rätt sätt är tillgångar i allt väsentligt redan identifierade. Det nämns också att tillgångar kan delas in i kategorier som ”personal, materiel, information, anläggningar och verksamhet”, vilket täcker in flera aspekter här.

Kategori	Aspekt	Akad.	FM	FMV	Civil mynd.
	Teknik	●		Δ system av system	+ *programvara*
	Brister och skydd		●	Δ i form av exponering (inkl. skydd)	
Människor	Organisatorisk struktur	●			●
	Förmågor och kompetenser	●	●		●
	Personal	●	+ *ansvar*		+ *ansvar* och *kultur*
	Intressenter och roller	●	●		●
Externt	Avtal och kontrakt	●			●
	Kunder	●			
	Leverantörer	●			+ *tjänster* (som värme och el)
	Samarbetspartner internationellt		●	Δ samverkan internationellt	
	Konkurrenter	●			●
	Rykte	●	Se fotnot.[12]		●
	Kontext	●	Δ istället *tillstånd* (som fred, kris, eller krig) och *arbetsmiljö*	●	+ *bransch* och *tillstånd* (som kris och politiskt klimat)

[12] H Säk Hot pratar om anseende som ett exempel på skyddsvärd tillgång (och FFS 2019-2 s3 föreskriver att verksamhetsbeskrivning ska beskriva bland annat skyddsvärden)

Kategori	Aspekt	Akad.	FM	FMV	Civil mynd.
	Geografisk plats	●	Δ specificeras som externarbete och nationellt eller internationellt		Δ specificeras som miljö och nationellt eller internationellt
	Tidsramar	●	●		●

9.2 Intervjuerna

I intervjuerna framkom sådant som inte beskrivits i litteraturen. I vissa fall stod intervjupersonernas rekommendationer i stark kontrast till det som återfanns i litteraturen.

Riskhanteringsexperten, cybersäkerhetskonsulten och informationsvärderaren framhöll att förlita sig på listor över informationsmängder som bör ingå i verksamhetsanalyserna kan göra att fokus förloras, vilket kan leda till att viktiga delar i den specifika verksamheten förbises. Listor och handböcker ska med fördel vara utformande så att de ger en förklaring av vikten av analysarbetet och de ska användas som inspiration för att komma vidare i processen. Säkerhetsansvarige poängterade att verksamhetsanalyser sällan genomförs. Handböcker som tydligt visar på vikten av verksamhetsanalyser kan göra att fler inser att de behöver utföras.

I intervjuerna med riskhanteringsexperten, cybersäkerhetskonsulten och informationsvärderaren poängterade intervjupersonerna hur viktigt det är att vara kreativ och inte strikt följa handböcker och mallar. Detta skiljde sig markant från intervjun med säkerhetsansvarige där mallar sågs som positivt och efterfrågat. Detta skulle kunna förklaras av hur nära intervjupersonerna är det operativa arbetet gällande att genomföra verksamhetsanalyser. Från den säkerhetsansvariges perspektiv kan mallar ses som positivt för att säkerställa ett väl genomfört arbete. Detta står i direkt konflikt med synpunkterna i de andra intervjuerna, vilket måste beaktas vid framtagning av handböcker och riktlinjer.

Stöddokument i form av exempelvis handböcker och mallar bör fokusera på att stödja hur analytikern bör tänka för att genomföra och komma vidare i sin analys, snarare än vilken information analytikern bör ta hänsyn till i analysen. Säkerhetskonsulten ansåg i detta att mallar kan riskerar att göra analyser för statiska, vilket kan resultera i att viktiga delar missas då viktiga aspekter av verksamheter riskerar att hamna utanför mallarna. Mallar bör istället användas som stöd för att säkerställa att inte uppenbara delar förbises eller som

inspirationskälla som kan förklara hur analytikern bör tänka och varför. Intresset av att använda mallar finns dock främst på nivån ovanför de som tar emot verksamhetsanalyser och beskrivningar. Om anledningen till detta är att mallar fungerar eller om anledningen är att säkerställa att arbetet faktiskt blir genomfört låter vi dock vara osagt. Intervjun med säkerhetsansvarige pekar på att det finns ett stort problem med att verksamhetsanalyser inte blir genomförda. Mallar bör beskriva vikten av att genomföra verksamhetsanalyser, snarare än bara hur genomförandet ska gå till, vilket är koherent med de andra intervjuerna.

Riskhanteringsexperten uppgav att individer med stark anknytning till verksamheten som analyseras ofta förbiser värdefull information cybersäkerhetskonsulten och informationsvärderaren lyfte fram att det är bra om det finns representanter från verksamheten som kan vara med i hela processen från verksamhetsanalys till säkerhetsmålsättning. På så sätt blir analyserna mer lättförståeliga för dessa representanter. Cybersäkerhetskonsulten noterade också att det i verksamhetsanalyser är lätt att vara ”blind för det uppenbara”. I relation till det uppgav cybersäkerhetskonsulten att det kan vara värdefullt med en extern granskare av resultaten som kan kontrollera att information som ofta tas för given faktiskt inkluderats. Riskhanteringsexperten poängterade att det är svårt att förstå analysernas resultat om personen inte själv varit med i processen och att analysresultatet bör utformas olika beroende på mottagarens kompetens. Relaterat till detta är den information som framkom under intervjun med cybersäkerhetskonsulten och informationsvärderaren, där dessa personer uppgav att det ibland händer att mottagare av analysen inte förstår innehållet, vilket gör att analysen måste revideras.

Samtliga intervjupersoner beskrev att det inte är ovanligt att verksamhetsanalyserna inkluderar flera verksamheter. Från intervjun med riskhanteringsexperten och cybersäkerhetskonsulten framkom att en analytiker i en verksamhet inte nödvändigtvis har tillgång till information om de andra verksamheterna. En framgångsrik verksamhetsanalys ställer därför krav på kommunikation mellan verksamheter och att det går att hantera konfidentialitet över verksamhetsgränserna.

Även om intervjupersonerna såg mallar och checklistor som potentiellt farliga formulerade de att vissa informationsbehov var särskilt viktiga för verksamhetsanalyser:

- Information
- Uppdrag
- Mål
- Resurser och tillgångar
- Teknik
- Organisatorisk struktur

9.3 Begränsningar

Forskningslitteraturen på området framstår som omogen och att det som beskrivs om verksamhetsanalyser sällan rör specifikt säkerhet. Dessutom är forskningslitteraturen inte så inriktad på framtagande av IT-system utan mer på verksamhetsförbättring och då hur verksamheter beskrivs ur ett allmänt perspektiv (med ett nuläge eller börläge). Detta medför att forskningslitteraturen måste tolkas med försiktighet när den sätts i perspektivet IT-säkerhet. Mycket av det som framkom i forskningslitteraturen framkom även i den litteratur som har IT-säkerhetsfokus, det vill säga litteraturen från Försvarsmakten och den civila sidan.

En begränsning med rapporten är att den i huvudsak utgår från litteratur snarare än hur verksamhetsanalyser genomförs i praktiken. De intervjuer som genomfördes kompenserade delvis för detta. Det faktum att intervjuerna faktiskt kontrasterade mot litteraturen på flera punkter indikerar dock en möjlighet att det finns fler delar i litteraturen som skulle motsägas om ett större antal intervjuer hade genomförts. Av samma skäl vore det relevant att studera faktiskt genomförda verksamhetsanalyser. En sådan studie har dock inte varit möjlig, bland annat på grund av svårigheter rörande konfidentialitet.

Även om informationen från intervjuerna är samstämmig hade ett större antal intervjuer stärkt studiens validitet. En informationskälla som skulle kunna ge ytterligare insikter är utländska försvarsmakters processer. Här existerar dock samma svårigheter gällande konfidentialitet och möjligtvis även vad gäller språk.

Det är också av vikt att ta hänsyn till intervjudeltagarnas kompetensnivåer. Riskhanteringsexperten, cybersäkerhetskonsulten och informationsvärderaren hade längre erfarenhet av att genomföra verksamhetsanalyser och det är möjligt att de åsikter de framfört inte speglar de åsikter personer med mindre erfarenhet skulle framfört. Exempelvis kanske en novis ser större nytta med färdiga mallar och mer vägledning, medan experter känner att sådant gör analysen stel och ofri.

10. Slutsatser

I detta kapitel presenteras studiens slutsatser indelade efter om de berör verksamhetsanalysens syfte (avsnitt 10.1), genomförande (10.2) eller informationsbehov (10.3). Detta motsvarar studiens frågeställningar och dessa upprepas först i varje avsnitt.

10.1 Verksamhetsanalysers syfte

Vad kan verksamhetsanalyser bidra med i ett informationssäkerhetsperspektiv?

Verksamhetsanalyser är en viktig grund för säkerhetsarbetet vid framtagande av IT-system. Dessutom kan verksamhetsanalyser stödja utvärdering av huruvida systemen är realiserbara eller ens önskvärda, vilket i slutändan påverkar säkerhetsbudgeten.

10.2 Verksamhetsanalysers genomförande

Hur bör verksamhetsanalyser genomföras?

Källorna som använts i denna rapport är av olika åsikt om i vilken utsträckning verksamhetsanalyser ska baseras på mallar. Mallar kan göra arbetet mer kostnadseffektivt och enhetligt men samtidigt ger dem en risk att analytikerna inte tänker tillräckligt vitt och brett.

Kommunikation är en viktig del vid genomförandet av en verksamhetsanalys. Med hjälp av kommunikation kan missförstånd minskas, fler komma till tals och viktig information som inte står med i styrande dokument kan inhämtas.

10.3 Verksamhetsanalysers informationsbehov

Vilka informationsmängder bör ingå i en verksamhetsanalys?

Informationsbehoven för verksamhetsanalyser är stora. Vilka aspekter som bör ingå i en verksamhetsanalys beror därför på vilken prioritering den enskilda organisationen gör. Exempelvis inkluderar Försvarsmakten synnerligen många säkerhetsmässiga aspekter samtidigt som aspekterna e*konomi* och *vision* inte inkluderas. Försvarsmakten inkluderar inte heller *kultur, organisationsstruktur* eller *beslutsmodell* som aspekter i analysen. Kanske är dessa aspekter tillräckligt homogena i Försvarsmakten för att behöva analyseras särskilt.

Även om litteraturen identifierar olika kategorier och aspekter som bör ingår i en verksamhetsanalys, är ett viktigt resultat från intervjuerna att det är farligt att

begränsa analyserna till en viss uppsättning aspekter eftersom det riskerar att låsa in den som genomför verksamhetsanalyser i tankemönster som i värsta fall gör att viktiga delar av verksamheten inte fångas upp. Intervjupersonerna lyfte dock fram vissa aspekter som särskilt viktiga informationsbehov. Det gällde aspekterna *information, uppdrag, mål, resurser och tillgångar, teknik* samt *organisatorisk struktur*.

11. Referenser

Aguilar-Saven, R. S. (2004). Business process modelling: Review and framework. *International Journal of Production Economics*, *90*(2), 129–149. Hämtad från https://econpapers.repec.org/RePEc:eee:proeco:v:90:y:2004:i:2:p:129-149

Alotaibi, Y., & Liu, F. (2017). Survey of business process management: challenges and solutions. *Enterprise Information Systems*, *11*(8), 1119–1153. https://doi.org/10.1080/17517575.2016.1161238

Andersson, H., Andersson, J.-O., Björck, F., Eriksson, M., Eriksson, R., Lundberg, R., … Starkerud, K. (2011). *Verksamhetsanalys. Ramverket för informationssäkerhet*.

Arvola, M. (2014). *Interaktionsdesign och UX : om att skapa en god användarupplevelse*. Studentlitteratur AB.

Bishop, M. (2003). *Computer security: art and science*. Addison-Wesley.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 163–186.

Burkhart, T., Krumeich, J., Werth, D., & Loos, P. (2011). *Analyzing the business model concept - A comprehensive classification of literature*. (January).

Carnaghan, C. (2006). Carnaghan, C.: Business process modeling approaches in the context of process level audit risk assessment: An analysis and comparison. *International Journal of Accounting Information Systems*, *7*, 170–204. https://doi.org/10.1016/j.accinf.2005.10.005

Dijkman, R., Vanderfeesten, I., & Reijers, H. A. (2014). Business process architectures: overview, comparison and framework. *Enterprise Information Systems*, *10*(2), 129–158. https://doi.org/10.1080/17517575.2014.928951

Fettke, P., Loos, P., & Zwicker, J. (2005). Business Process Reference Models: Survey and Classification. *Proceedings of the Workshop on Business Process Reference Models (BPRM)*.

FMV. (2018). *ISD-Processen 3.0*. Hämtad från http://isd.fmv.se/

Försvarsmakten. (2006). *Metodik verksamhetsanalys - Bilaga till MAACK – Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten*. Försvarsmakten.

Försvarsmakten. (2007). *Handbok - Säkerhetstjänst säkerhetsskyddstjänst*.

Försvarsmakten. (2009). *Riktlinjer avseende säkerhetstjänstens bedrivande under större övningar*.

Försvarsmakten. (2013a). *Handbok - Säkerhetstjänst grunder*.

Försvarsmakten. (2013b). *Handbok - Säkerhetstjänst informationssäkerhet*.

Försvarsmakten. (2013c). *Säkerhetskrav på IT-system som är avsedda för behandling av personuppgifter*.

Försvarsmakten. (2014). *Krav på IT-säkerhetsförmågor hos IT-system (KSF v3.1)*.

Försvarsmakten. (2015). *FIB 2015-1 - Försvarsmaktens interna bestämmelser om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar*.

Försvarsmakten. (2018a). *Handbok - Kravhantering för informationsystem*.

Försvarsmakten. (2018b). *Sammanställning över bestämmelser och riktlinjer för säkerhetstjänsten (SAMSÄK) 2019*.

Försvarsmakten. (2019). *FFS 2019-2 - Försvarsmaktens föreskrifter om säkerhetsskydd*.

Fox, M. S., & Gruninger, M. (1998). Enterprise Modeling. *AI Magazine Volume 19 Number 3. American Association for Artificial Intelligence.*

Green, S., & Ould, M. (2005). A framework for classifying and evaluating process architecture methods. *Software Process: Improvement and Practice*, *10*(4), 415–425. https://doi.org/10.1002/spip.244

Hallberg, J., Bengtsson, J., & Sommestad, T. (2012). *Verktygsstöd för hot-, risk- och sårbarhetsanalyser – Realiseringsförslag*.

Hallberg, N., Jungert, E., Andersson, R., Ölvander, C., Hallberg, J., Pilemalm, S., & Timpka, T. (2008). *Tjänstebaserad krishantering för lokalsamhället: verksamhetsanalys och initial arkitektur*.

Hallberg, N., Lindell, P.-O., Pilemalm, S., Andersson, M., & Ericson, L. (2004). *Kravhantering för FMA*.

Informationssäkerhet.se. (u.å.). Stöd för systematiskt arbete med informationssäkerhet i organisationer. Hämtad från https://www.informationssakerhet.se/metodstod-for-lis/identifiera-och-analysera/#verksamhetsanalys

ISO. (2018). *ISO/IEC 27005. Information technology — Security techniques — Information security risk management.*

Kaisler, S. H., Armour, F., & Valivullah, M. (2005). Enterprise Architecting: Critical Problems. *Proceedings of the 38th Hawaii International Conference on System Sciences*.

Klang, D., Wallnöfer, M., & Hacklin, F. (2014). The business model paradox - A systematic review and exploration of antecedents. *International Journal of Management Reviews*, *16*, 454–478. https://doi.org/10.1111/ijmr.12030

Koliadis, G., Ghose, A. K., & Padmanabhuni, S. (2008). Towards an enterprise

business process architecture standard. *IEEE Congress on Services*, 239–246. https://doi.org/10.1109/SERVICES-1.2008.60

Korman, M., Ekstedt, M., Sommestad, T., Hallberg, J., & Bengtsson, J. (2014). Overview of Enterprise Information Needs in Information Security Risk Assessment. *IEEE EDOC – Enterprise Computing Conference*. https://doi.org/10.1109/EDOC.2014.16

Koubarakis, M., & Plexousakis, D. (2002). A Formal Framework for Business Process Modelling and Design. *Inf. Syst.*, *27*(5), 299–319. https://doi.org/10.1016/S0306-4379(01)00055-2

Lambert, S. C., & Davidson, R. A. (2013). Applications of the business model in studies of enterprise success , innovation and classification - An analysis of empirical research from 1996 to 2010. *European Management Journal*, 668–681. https://doi.org/http://dx.doi.org/10.1016/j.emj.2012.07.007

Lund, M. S., Solhaug, B., & Stølen, K. (2011a). *Model-Driven Risk Analysis.The CORAS Approach*. https://doi.org/10.1007/978-3-642-12323-8

Lund, M. S., Solhaug, B., & Stølen, K. (2011b). Risk analysis of changing and evolving systems using CORAS. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 231–274. https://doi.org/10.1007/978-3-642-23082-0_9

Massa, L., Tucci, C. L., & Afuah, A. (2017). A critical assessment of business model research. *Academy of Management Annals*, *11*(1), 73–104. https://doi.org/https://doi.org/10.5465/annals.2014.0072

NIST. (2012). *NIST Special Publication 800-30. Revision 1. Guide for Conducting Risk Assessments.*

Nurmi, J., Pulkkinen, M., Seppänen, V., & Penttinen, K. (2019). *Systems approaches in the enterprise architecture field of research : a systematic literature review*. (January). https://doi.org/10.1007/978-3-030-06097-8_2

Oda, S. M., Fu, H., & Zhu, Y. (2009). Enterprise information security architecture a review of frameworks, methodology, and case studies. *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 333–337. https://doi.org/10.1109/ICCSIT.2009.5234695

Pavlovski, C. J., & Zou, J. (2008). Non-functional requirements in business process modeling. *Conferences in Research and Practice in Information Technology Series*, *79*.

Recker, J. (2010). Opportunities and constraints: the current struggle with BPMN. *Business Process Management Journal*, *16*(1), 181–201. https://doi.org/10.1108/14637151011018001

Recker, J., & Mendling, J. (2016). The state of the art of business process

management research as published in the BPM conference - recommendations for progressing the field. *Business & Information Systems Engineering*, *58*(1), 55–72. https://doi.org/10.1007/s12599-015-0411-3

Regeringskansliet. (2018). *Säkerhetsskyddslag (2018:585)*.

Röhrig, S. (2003). *Using Process Models to Analyse IT Security Requirements*.

Saint-louis, P., Morency, M. C., & Lapalme, J. (2017). Defining enterprise architecture - a systematic literature review. *IEEE 21st International Enterprise Distributed Object Computing Conference Workshops*. https://doi.org/10.1109/EDOCW.2017.16

Säkerhetspolisen. (2018). *Sex frågor, sex steg– svaren som krävs i en säkerhetsskyddsanalys*.

Shafer, S. M., Smith, H. J., & Linder, J. C. (2005). The power of business models. *Business Horizons*, *48*(3), 199–207. https://doi.org/https://doi.org/10.1016/j.bushor.2004.10.014

Sommestad, T., Bengtsson, J., & Hallberg, J. (2013). *Informationsbehov vid säkerhetsanalyser: En systematisk genomgång av etablerade metoder*.

Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language : A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, *7*(3), 363–373. https://doi.org/10.1109/JSYST.2012.2221853

Sparf, M., & Sparf, A. (2012). *Tankar kring tillämpning av MODAF i Försvarsmakten*.

Stenius, J. (2006). *Verksamhetsmodell Ledningsplats*.

Tamm, T., Seddon, P. B., Shanks, G., & Reynolds, P. (2011). How Does Enterprise Architecture Add Value to Organisations? *Communications of the Association for Information Systems*, *28*, 141–168. https://doi.org/10.17705/1CAIS.02810

van der Aalst, W. M. P. (2013). *Business Process Management : A Comprehensive Survey*. *2013*. https://doi.org/http://dx.doi.org/10.1155/2013/507984

van der Aalst, W. M. P., La Rosa, M., & Santoro, F. M. (2016). *Business process management - Don't forget to improve the process! 58*(1), 1–6. https://doi.org/10.1007/s12599-015-0409-x

Wirtz, B. W., Göttel, V., & Daiser, P. (2016). *Business Model Innovation: Development, Concept and Future Research Directions*. Journal of Business Models 4(2), 1-28.

Wirtz, B. W., Pistoia, A., Ullrich, S., & Vincent, G. (2015). Business models : Origin , development and future research perspectives. *Long range planning*, 1–19. https://doi.org/10.1016/j.lrp.2015.04.001

Youseef, A., & Liu, F. (2012). A New Framework to Model a Secure E-Commerce System. *World Academy of Science, Engineering and Technology. nternational Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *6*(1), 6–12.

Zott, C., Amit, R. H., & Massa, L. (2011). The Business Model : Recent Developments and Future Research The Business Model : Recent Developments and Future Research. *Journal of Management*. https://doi.org/http://dx.doi.org/10.1177/0149206311406265

Bilaga A – Intervjufrågor

Introduktion

- Vilken roll och jobbtitel har du?
- Utför du säkerhetsanalyser (eller verksamhetsanalyser) som en del i säkerhetsmålsättningsarbete för IT-system?
    - Har du någon specifik roll eller specifikt ansvarsområde?
    - Hur många gånger per år genomför du typiskt säkerhetsanalyser/verksamhetsanalyser?

Vad och Varför

- Vad är en verksamhets-/säkerhetsanalys för dig?
- Vad är det huvudsakliga syftet med att genomföra en säkerhetsanalys/verksamhetsanalys?
    - Hur används verksamhetsbeskrivningen i säkerhetsanalysarbetet?
    - Om du tar del av en verksamhetsbeskrivning som underlag för säkerhetsanalysen, vad innehåller den vanligen?
- Vilken information behöver du från en verksamhetsbeskrivning för att kunna genomföra ditt arbete i säkerhetsanalysen?
    - Till vad använder du den informationen?
- Anser du att dagens typiska verksamhetsbeskrivning är ett bra underlag för säkerhetsanalysen?
    - Om det saknas information, hur hanterar du det?
    - Förbättringar?
    - Bör utformningen vara på något speciellt sätt?
- Vem ser du som den typiska användaren av den verksamhetsanalys/säkerhetsanalys som du tar fram?
    - Vem kvalitetssäkrar/granskar resultatet?
    - Vem godkänner resultatet?
- Upplever du att den typiske mottagaren av verksamhetsanalys/säkerhetsanalysen har förståelse för innehållet?

Hur

- Hur ser arbetsgången typiskt ut när du genomför en verksamhets/säkerhetsanalys?
    - Jobba själv, grupparbete eller workshop?

        - Vilka andra roller är inkluderade om det inte är självständigt arbete?
    - Vilka arbetsmoment ingår?
- Har du tillgång till någon typ av verktyg som stödjer genomförandet av verksamhets/säkerhetsanalysen?
- Har du någon specifik metod som ni följer?
- Hur många arbetstimmar läggs typiskt på att genomföra en verksamhets/säkerhetsanalys?
    - Händer det att du inte blir klara inom utsatt tid? Vad händer då?
- Hur mycket kalendertid finns typiskt tillgänglig för att genomföra en verksamhets/säkerhetsanalys?
- Vilket är det mest tidskrävande momentet vid genomförandet av en verksamhets/säkerhetsanalys?
- När ni genomför verksamhetsanalyser, genomförs dem genom en top-down- eller en bottom-up-approach?
    - Styrkor och svagheter inom given approach?
- När du analyserar verksamhetens olika delar, kommunicerar ni med olika aktörer (interna eller externa) som kommer att beröras av given förändring?
- När du genomför verksamhetsanalyser, är fokus på verksamhetens vision, eller är det grundat i verksamhetens behov?
- Hur avgör du vad som ska ingå i en verksamhetsanalys? Vilken information som den skall innehålla? Markera gärna på tillhörande tabell[13]

Summering

- Hur upplever du att din verksamhetsanalysprocess fungerar?
- Avslutande tankar eller frågor?

[13] Se Bilaga B

Bilaga B – Informationsmängdstabell

Kategori	Aspekt	Forsk.	Försvarsmakten	Civilt
Styrning	Uppdrag	●	Δ istället *uppgifter* och *inriktning*	+ *affärsidé* och *värdegrund*
	Vision	●		●
	Behov	●	●	
	Mål	●	●	●
	Strategi	●		●
	Beslutsmodell	●		
	Policyer	●	Δ istället *författningar* och *behörighet*	+ *författningar*
	Riktlinjer, vägledningar och standarder	●		●
	Koordinering och beroenden	●	- *beroenden* + *konsekvenser*	Δ bara *beroenden*
	Ekonomi	●		+ *ägarförhållanden*
Innehav	Processer	●	●	●
	Funktioner	●	+ *informationsöverföring* och metoder	+ *kommunikation*
	Resurser och tillgångar	●	- inte tillgångar[14] + *materiel* och *anläggningar*	Δ istället *resurser* och *fysiska tillgångar* och *infrastruktur*

[14] I H Säk Grunder nämns dock att om verksamhetsanalysen genomförts på rätt sätt är tillgångar i allt väsentligt redan identifierade. Det nämns också att tillgångar kan delas in i kategorier som ”personal, materiel, information, anläggningar och verksamhet”, vilket täcker in flera aspekter här.

Kategori	**Aspekt**	**Forsk.**	**Försvarsmakten**	**Civilt**
	Information	●	Δ nämner ofta *information* ur perspektivet CIA	●
	Teknik	●		+ *programvara*
	Brister och skydd		●	
Människor	Organisatorisk struktur	●		●
	Förmågor och kompetenser	●	●	●
	Personal	●	+ *ansvar*	+ *ansvar* och *kultur*
	Intressenter och roller	●	●	●
Externt	Avtal och kontrakt	●		●
	Kunder	●		
	Leverantörer	●		+ *tjänster* (som värme och el)
	Samarbetspartner internationellt		●	
	Konkurrenter	●		●
	Rykte	●	Se fotnot.[15]	●
	Kontext	●	Δ istället *tillstånd* (som fred, kris, eller krig) och *arbetsmiljö*	+ *bransch* och *tillstånd* (som kris och politiskt klimat)
	Geografisk plats	●	Δ specificeras som externarbete och nationellt eller internationellt	Δ specificeras som miljö och nationellt eller internationellt

[15] H Säk Hot pratar dock om anseende som ett exempel på skyddsvärd tillgång (och FFS 2019-2 s3 säger att verksamhetsbeskrivning ska beskriva bland annat skyddsvärden)

Kategori	Aspekt	Forsk.	Försvarsmakten	Civilt
	Tid	●	●	●

Bilaga C – Förklaringar av aspekterna

Tabell 6: Förklaringar av aspekterna.

Kategori	Aspekt (delaspekt)	Exempel	Källa
Styrning	Inriktning	Vilket direkt bidrag till Försvarsmaktens … strategiska inriktning ger en lösning?	c
	Uppgifter	Vilken eller vilka uppgifter ska lösas?	d
	Behov	Vad behöver … intressenterna …?	c
	Mål	Vilka faktorer i form av bl a mål … påverkar verksamheten?	f
	Behörigheter	Finns begränsningar av vem som får behandla uppgifter i IT-systemet?	e
	Författningar	Försändelser med utrikesklassificerade handlingar till och från utlandet?	b
	Beroenden	Vilka andra verksamheter eller organisationsenheter är beroende av den verksamhet som IT-systemet ska stödja?	e
	Konsekvenser	Hur klarar sig verksamheten om det inte kan tillhandahållas någon lösning som hanterar problemen eller tillvaratar möjligheten?	c
Innehav	Processer	Vilka faktorer i form av bl a … medel [och] metoder … påverkar verksamheten?	f
	Funktioner	… hur bearbetas [information] av intressenterna då de utför sina arbetsuppgifter?	c
	Informations-överföring	… kommunikation till andra IT-system?	e
	Metoder	Vad som är skyddsvärt inom ramen för övningen? Det kan omfatta … metoder …	h
	Anläggningar	Vilka anläggningar krävs för att genomföra verksamheten?	d

Kategori	Aspekt (delaspekt)	Exempel	Källa
	Materiel	Vilken materiel krävs för att genomföra verksamheten?	d
	Resurser	Vilka resurser finns för att skydda IT-systemets delar och informationen i dessa?	e
	Brister	Vilka problem eller brister finns i befintliga tjänster och system?	c
	Information (konfidentialitet)	Vilka konsekvenser får det för verksamheten om informationen … röjs …?	d
	Information (riktighet)	… verksamhetens krav på … riktighet …	a
	Information (tillgänglighet)	… krav på tillgänglighet till informationssystemet, och de uppgifter som behandlas i det …	a
	Skydd	Dokumentationen ska beskriva … de skyddsåtgärder som avser systemet …	a
Människor	Förmågor och kompetenser	Vad som är skyddsvärt inom ramen för övningen? Det kan omfatta … egen förmåga …	h
	Ansvar	Vem eller vilka ansvarar för vilken verksamhet?	d
	Personal	Vilken personal eller enhet genomför verksamheten?	d
	Intressenter	Vad behöver och förväntar sig intressenterna för stöd …?	c
	Roller	Vem ska utföra arbetsuppgifterna?	c
Externt	Samarbete	Kommer personal från en annan stat eller mellanfolklig organisation använda IT-systemet?	e
	Arbetsmiljö	I vilken miljö utförs verksamheten?	c
	Geografisk plats (externarbete)	Är IT-systemet avsett för användning utanför Försvarsmaktens objekt, lokaler och områden?	e

Kategori	Aspekt (delaspekt)	Exempel	Källa
	Geografisk plats (nationellt/inter-nationellt)	Vilken verksamhet ska IT-systemet stödja? Nationellt – internationellt?	e
	Tillstånd	Vilken verksamhet ska IT-systemet stödja? Fred – kris – krig?	e
	Tidsramar	Vilka faktorer i form av bl a tid påverkar verksamheten?	f

Tabellens källor: a = FFS 2019:2 säkerhetsskydd (2019), b = FIB 2015:1 skydd för utrikes- och sekretessklassificerade uppgifter och handlingar (2015), c = H KIS (2018a), d = H Säk grunder (2013a), e = H Säk infosäk (2013b), f = H Säk skydd (2007), h = Riktlinjer avseende säkerhetstjänstens bedrivande under större övningar (2009).

Verksamhetsanalyser genomförs för befintliga eller planerade verksamheter och utgör grunden för riskbedömningar. Resultatet av verksamhetsanalyser utgörs av verksamhetsbeskrivningar. Denna rapport syftar till att skapa bättre förutsättningar att utföra och redovisa de verksamhetsanalyser som genomförs i Försvarsmakten vid framtagandet av nya IT-system eller vid förändring av befintliga IT-system. Rapporten beskriver därför vad verksamhetsanalyser kan bidra med i ett informationssäkerhetsperspektiv, hur analyserna bör genomföras och vilka informationsmängder som bör ingå.

Arbetet baseras på litteratur från Försvarsmakten, Försvarets materielverk, civila myndigheter, akademiska forskningsartiklar samt på intervjuer med personer som utfört eller granskat verksamhetsanalyser. Någon utvärdering av faktiska genomförda verksamhetsanalyser har däremot inte gjorts.

Verksamhetsanalyser är en viktig grund för säkerhetsarbetet vid framtagande av IT-system. Analyserna kan också stödja utvärdering av huruvida systemen är realiserbara eller ens önskvärda.

Att använda mallar för verksamhetsanalyser kan göra arbetet mer kostnadseffektivt och enhetligt, men samtidigt ger de en risk att analytikerna inte tänker tillräckligt vitt och brett. Informationskällorna har olika åsikt om detta.

Kommunikation är en viktig del vid genomförandet av en verksamhetsanalys. Med hjälp av kommunikation kan missförstånd minskas, fler komma till tals och viktig information som inte står med i styrande dokument kan inhämtas.

FOI

ISSN 1650-1942

www.foi.se