Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(8)

<SYSTEM> <VERSION>

ANALYSUNDERLAG

DEFINIERA (AU-D)

Innehåll

Mallinformation 18FMV6730-4:1.1

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Mall för AU-D	DAOLO

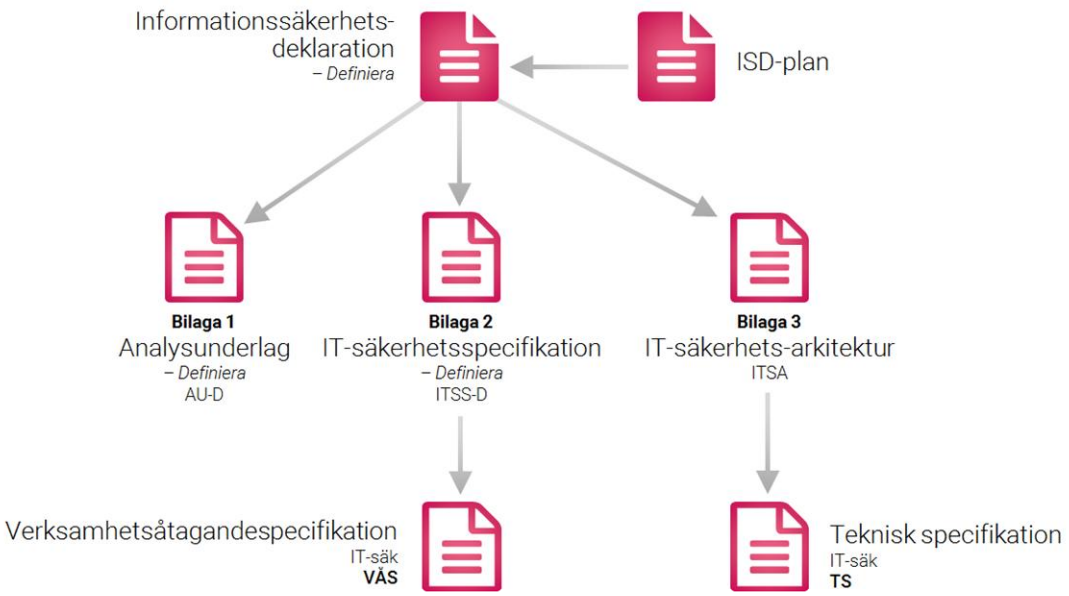
Mallinstruktion och omfattning av Analysunderlag *Definiera*

Sidorna från innehållsförteckning till kapitel 1 Basfakta innehåller hjälp och metodbeskrivning för bilaga 1 till Informationssäkerhetsdeklaration *Definiera*. Dessa ska raderas innan dokumentet färdigställs.

- Instruktionen om vad som ska stå under varje rubrik anges under respektive rubrik. Gulmarkerad text ska raderas innan dokumentet färdigställs.
- Text utan gulmarkering kan användas också i det färdigställda dokumentet.
- Ersätt *Systemnamn* med ackrediteringsobjektets namn.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av Analysunderlag *Definiera*

Informationssäkerhetsdeklaration *Definiera* består av ett huvuddokument nedan benämnt ISD-D och tre bilagor Analysunderlag (AU-D), IT-säkerhetsspecifikation ITSS-D och ITSA – IT-säkerhetsarkitektur. AU-D innehåller relevanta analyser avseende informationssäkerhetsaspekten ur ett systemperspektiv. Denna mall utgör bilaga 1 AU-D.

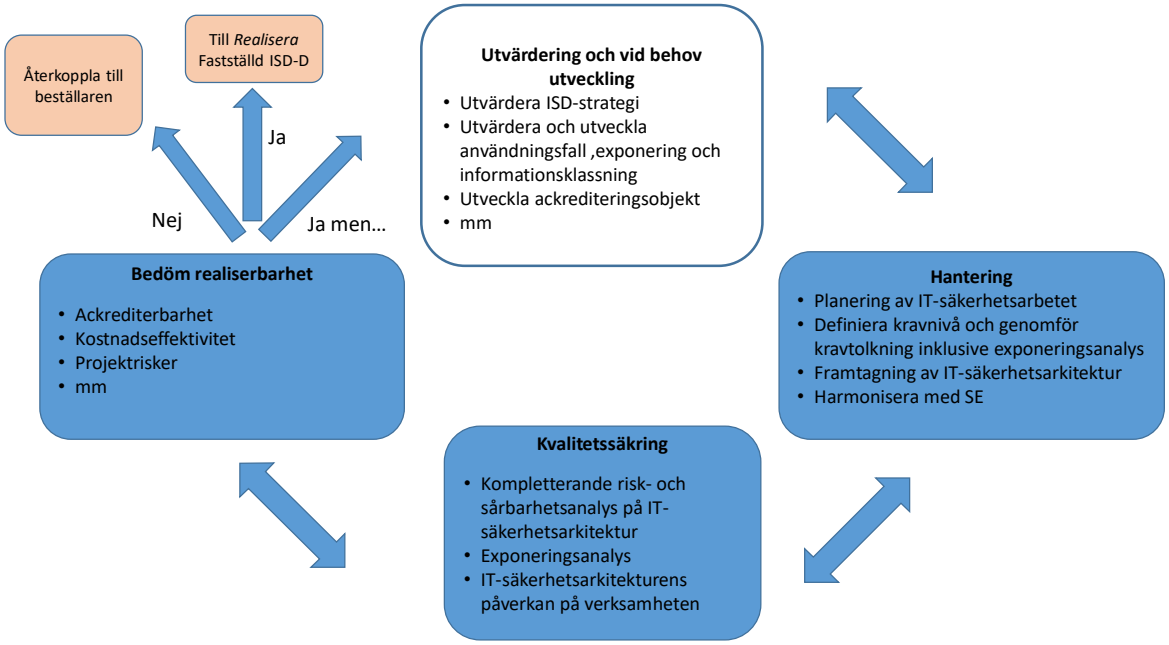


Figur 1 Dokumentstruktur Informationssäkerhetsdeklaration Definiera

I AU-D fördjupas och utvecklas analyserna gjorda i *Identifiera* för att skapa mer detaljer kring det aktuella IT-systemet.

Att tänka på i arbetet med att ta fram Analysunderlag *Definiera*, AU-D

ISD-strategin kommer från *Identifiera* och innehåller inriktningar till genomförandeprojektet.



Figur 2 AU-D:s del av arbetssättet i Definiera

Resultatet från analyserna i form av krav dokumenteras i ITSS-D och slutsatserna dokumenteras i ISD-D.

AU-D omfattar:

- Utvärdering av resultatet från *Identifiera* och utformning av IT-systemet. Vid behov utvecklas och kompletteras användningsfall, informationsklassning och ackrediteringsobjektet.
- Kompletterande hot- och riskanalys
  - I takt med att IT-säkerhetsarkitekturen växer fram genomförs riskanalyser för kvalitetssäkring och för att identifiera kvarvarande risker.
- Kompletterande exponeringsanalys,
  - Exponeringsanalysen beskriver exponering av den information som ska skyddas i verksamheten och det aktuella IT-systemet.

Analyserna från *Identifiera* ska inte göras om utan kompletteras och fördjupas och riktas mot IT-systemet. Resultatet och dokumentet från AU-I kan användas i arbetet med analyserna i *Definiera.* Exponering kan vara antal användare, fysiskt skydd, externa/interna gränsytor mm. Typ av exponering påverkar behov av säkerhetslösning och kan påverka bedömningen av

ackrediterbarhet. I *Definiera* formas IT-systemet med dess säkerhetshetfunktioner där val av IT-säkerhetskomponenter också kan minska exponering.

Beroende på resultatet från analyserna levereras arbetet till *Realisera* och upphandlingen, eller så itereras arbetet ett antal gånger mellan värdering av verksamhetsbehov, kravtolkning av MUST KSF, IT-säkerhetsarkitekturen och risk och sårbarhets- samt exponeringsanalyser.

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är Analysunderlag Definiera (IAU-D) för <System> <version> inför FMV VHL S3-beslut.

Analysunderlaget för *Definiera* (AU-D) har fokus på att utveckla och fördjupa analyserna från *Identifiera* för att kunna genomföra kravtolkning av MUST KSF och fastställa kravnivå inför *Realisera* och upphandling. Analyserna, främst exponeringsanalysen, är av vital betydelse för att iterativt i projektet och, vid behov även med verksamheten, prova olika sätt att hamna rätt i kravnivå. Resultatet dokumenteras som krav i ISD-D bilaga 2, ITSS-D.

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

Följande tabell innehåller specifika begrepp som gäller för detta dokument. En generell lista återfinns i ref [1].

Term (förkortning)	Definition	Källa	Kommentarer/ Anmärkningar
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	

Tabell 2 - Terminologi och begrepp i detta dokument

1.4 Bilageförteckning

Detta dokument har inga bilagor.

1.5 Referenser

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] ISD 3.0 Begrepp och förkortningar	18FMV6730-8:1.1	1
[2] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>
[3] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>

Tabell 3 - Referenser

2 Kompletterande analyser

I detta avsnitt dokumenteras kompletterande analyser med utgångspunkt från resultatet från ISD-I.

2.1 Användningsfall

Resultatet från egna analyser tex exponeringsanalys kan också påverka användningsfallen, och då krävs samverkan med FM.

2.1.1 Informationsflöde och informationsklassning

I detta avsnitt dokumenteras kompletterande analyser avseende informationsklassning och informationsflöde med utgångspunkt från resultatet från ISD-I.

Resultatet från egna analyser tex exponeringsanalys kan också påverka informationsflöde och informationsklassning, och då kan samverkan med FM krävas.

- Konkretiseringen kan ske utifrån aspekter som t.ex. tid och rum. Denna aktivitet är viktig resultatet påverkar kostnader, funktionalitet och tid. Separation av information är ett exempel på designlösning som kan krävas för realisering av IT-systemet.
- Informationsklassningen och flödet i analysunderlaget blir sedan stöd för designfasen.

2.1.2 Risk- och sårbarhetsanalys

Detta avsnitt ska vara en kompletterande hot- och riskanalys som görs då IT-systemet och IT-säkerhetsarkitekturen är framtagen. I ISD-I baserade sig hotanalysen på vilka konsekvenser, avseende informationens tillgänglighet, riktighet och skydd mot oönskad spridning, som IT-systemet ska skydda verksamheten från.

I Definiera görs även sannolikhetsbedömning och fördjupad konsekvensbedömning varav riskerna i lösningen kan identifieras.

2.1.3 Exponeringsanalys

I detta avsnitt dokumenteras kompletterande analyser avseende rätt exponeringsnivåer med utgångspunkt från resultatet från ITSA.

Exponeringsnivå tas fram genom:

- Kravtolkning mot verksamhetsbehov efter exponeringsanalys i ITSA
- Kravtolkning efter designavvägningar i ITSA
- Externa gränsytor med detaljerad information kring tekniska gränsytor.
- Reducering av exponering kan ske på ett antal olika sätt, exempelvis genom att förändra arkitektur eller på annat sätt förändra den tekniska lösningen. Exponeringen kan också reduceras genom att kravställa driftmiljön eller begränsa systemets användning istället för tekniken. Då förändras inte den faktiska systemlösningen men kraven på omgivningen och/eller användarna sänker exponeringen.
- Det är dock viktigt att se till att den förändrade systemlösningen fortfarande uppfyller verksamhetens behov och krav. Om förändringen innebär förändringar av systemets funktionalitet måste detta stämmas av med och accepteras av verksamheten. Det kan exempelvis finnas funktionalitet som är ”nice to have” men inte ”need to have”. Om avlägsnandet av sådan funktionalitet kan ge fördelar i form av en minskad exponering så kan denna typ av förändring göras, så länge det är förankrat i verksamheten.

Resultatet från exponeringsanalysen ligger till grund för kravtolkning av kravnivå MUST KSF.

2.2 Kravnivå

Utifrån definierad informationssäkerhetsklass i kapitel 2.1.1 och exponeringsanalys i kapitel 2.1.3 definieras kravnivån (avseende KSF) för <system> som Grund/Utökad/Hög.

Notera att detta är en iterativ process vilket kan innebära att vald kravnivå kan komma att justeras under systemarbetet.

Det kan också vara olika kravnivåer på olika delar i systemlösningen, vilket då framgår av ITSA.