Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(44)

<SYSTEM> <VERSION>

INFORMATIONSSÄKERHETSSARKITEKTUR *DEFINIERA* (ITSA)

Innehåll

Mallinformation 18FMV6730-4:1.3

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

Mallinstruktion

Denna mall ska användas för att ta fram IT-säkerhetsarkitekturen, ITSA.

ITSA är en bilaga till ISD-D, och används för att arbeta fram en arkitektur som dels uppfyller informationssäkerhetskraven och dels harmoniserar med SE-arbetet i projektet.

- Det färdigställda dokumentet börjar med kap 1 Basfakta.
- Sidorna innan dess innehåller beskrivningar kring vad ITSA innehåller och att tänka på i arbetet. Dessa sidor tas bort i det färdigställda dokumentet.
- Instruktion om vad som ska stå under varje rubrik i det skarpa dokumentet anges i gul text. Den texten ska raderas innan dokumentet färdigställs.
- Svart text kan användas direkt i det färdigställda dokumentet.
- Ersätt *Systemnamn* med systemets namn och versionsnummer.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av ITSA

Informationssäkerhetsdeklaration *Definiera* (ISD-D) består av ett huvuddokument och tre bilagor;

- Bilaga 1 Analysunderlag *Definiera* (AU-D)
- Bilaga 2 IT-säkerhetsspecifikation *Definiera* (ITSS-D)
- Bilaga 3, IT-säkerhetsarkitektur (ITSA)

Dessa bilagor innehåller detaljer och analysunderlag för informationssäkerhetsdeklarationen där detta dokument utgör bilaga 3.

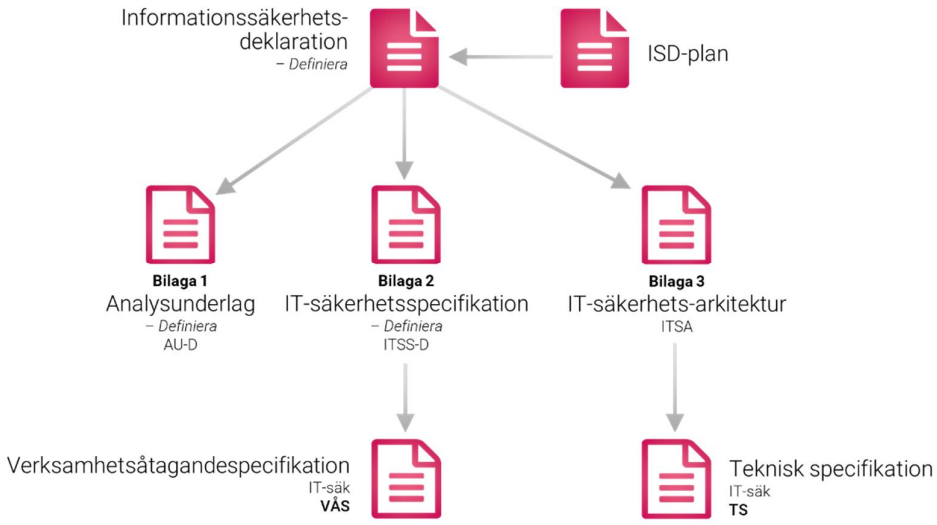
Bilaga 1-AU-D innehåller relevanta analyser avseende informationssäkerhetsaspekten ur ett IT-systemperspektiv. Resultatet från AU-D i form av krav dokumenteras i detta dokument. Kraven och analyserna används för att ta fram IT-säkerhetsarkitektur ITSA.

Figuren nedan visar relationen mellan ISD-D och upphandlingsunderlagen Teknisk specifikation (TS) och VerksamhetsÅtagandeSpecifikation (VÅS). Fasen *Definiera* ska resultera i TS och VÅS.

ITSS-D förser VÅS med krav på IT-säkerhetsarbete och ITSA förser TS med tolkade IT-säkerhetskrav.

ISD-planen, som är en del av genomförandeprojektets projektplan, styr IT-säkerhetsarbetet och är ett viktigt indata till dokumentet ISD-D.

Upphandlingsunderlagen är separata dokument och ingår inte i ISD 3.0.



Dokumentstruktur Informationssäkerhetsunderlag Definiera

ITSA omfattar:

- Kravunderlag (referens till)
- Förutsättningar
- Systembeskrivning

- Säkerhetsarkitektur
- IT-säkerhetsfunktioner
- Kravallokering och -sammanställning

Att tänka på i arbetet med ITSS-D

- Kraven dokumenteras och utvecklas succesivt i IT-säkerhetsspecifikationer i *Identifiera* ITSS-I, *Definiera* ITSS-D, *Realisera* ITSS-R och eventuellt *Vidmakthålla* ITSS-V. Dessa dokument utgör spårbarheten i IT-säkerhetslösningen.
- ITSA dokumenterar säkerhetsarkitekturen med grund i MUST KSF samt verksamhetskraven och utgör den grund som den tekniska specifikationen baseras på.
- ITSA ger tekniska krav till TS.

1 Basfakta

1.1 Giltighet och syfte

Detta kapitel ska entydigt identifiera systemet.

Detta dokument är ITSA för <*System*> version <*version*> inför FMV VHL S3-beslut.

1.2 Revisionshistorik

Detta kapitel ska entydigt identifiera detta dokument.

Datum	Utgåva	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] AU-D	Bilaga 2 till ISD-D <dokumentid., åååå-mm-dd>	<nr>
[3] ITSS-D	Bilaga 2 till ISD-D <dokumentid., åååå-mm-dd>	<nr>
[4] ISD-Plan	<dokumentid., åååå-mm-dd>	<nr>
[5] ISD-Strategi	<dokumentid., åååå-mm-dd>	<nr>
[6] SYD	<dokumentid., åååå-mm-dd>	<nr>
[7] Designregel Härdning av IT-system, utgåva 1.0	18FMV3960-1:1 2018-05-04	1
[8] Krav på loggning i Försvarsmaktens IT-system	FM2016-4365:1, 2016-02-19	1
[9] Designregel Programvaror med underhåll	18FMV3960-2:1, 2018-05-17	1

Tabell 3 - Referenser

2 Inledning

2.1 Syfte

ITSA är en beskrivning/kravställning av arkitekturen som tas fram i syfte att optimera designen avseende informationssäkerhet för att erhålla en ackrediterbar lösning.

ITSA är grunden för kravställning mot leverantör, främst i form av kravställning i Teknisk Specifikation (TS). Krav som identifieras i ITSA kan även vara aktuella för att förtecknas i Verksamhetsåtagandespecifikation (VÅS).

En dokumenterad IT-säkerhetsarkitektur visar hur IT-säkerhetsfunktionerna fördelas (allokeras) och används, hur dessa interagerar med varandra och med systemet samt identifiera säkerhetsrelevanta gränsytor.

2.2 Samverkan med SE

Framtagning av denna ITSA har gjorts i samverkan med övrigt SE-arbete. Syftet är att hitta en optimal systemarkitektur, ur både ett informationssäkerhetsperspektiv och ett funktionellt perspektiv.

Resultatet av både ITSS-D/ITSA-arbetet och SE-arbetet är kravställning i en (eller flera) TS och VÅS.

3 Förutsättningar och systembeskrivning

Informationen i detta kapitel ligger till grund för arkitekturen och allokeringen av säkerhetsfunktioner.

3.1 Informationsklassificering

Systemet kommer att lagra, bearbeta eller transitera information klassad som högst INFOKLASS, enligt REF. Se AU-D för analyser och slutsatser.

Observera att komplexa system kan ha olika informationssäkerhetsklassificering av information i olika systemkomponenter (delsystem). Ange i så fall klassificeringen per systemkomponent.

Observera att även själva komponenten kan vara klassificerad.

3.2 Operativ användning

Information i detta kapitel kan hämtas från användningsfall i AU-D.

3.2.1 Operativ miljö

Ange hur systemet ska användas operativt. Detta innefattar t ex antal instanser, stationärt eller mobilt och nationellt eller internationellt.

OBSERVERA: informationen i detta stycke kan påverka klassificeringen av detta dokument!

3.2.2 Användare

Ange vilka användare det finns i systemet. Beskrivningen ska omfatta användare/operatörer som har skilda rättigheter i system jämfört med administratörer med högre rättigheter.

Ange om det finns behov av root/Administratör/Superuser.

Det ska framgå att det finns olika typer av administratörer (dvs användare med högre rättigheter), såsom behörighetsadministratör, säkerhetsadministratör, säkerhetsloggadministratör och systemadministratör.

OBSERVERA: administratörer är en typ av användare

Information in detta kapitel ska omsättas/överensstämma med behörighetspolicyn.

3.2.3 Exponering

Ange hur och var systemet exponeras, kopplat till respektive användarkategori (HMI). Exponering utgörs av både infologiska och fysiska gränsytor.

Reducering/hantering 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 beställaren. Det kan exempelvis finnas funktionalitet som är ”nice to have” men inte ”need to have”. Avlägsnandet av denna typ av funktioner kan ge fördelar i form av en minskad exponering, men det påverkar verksamhetens behov. Denna förändring kan dock göras, om den är förankrad hos beställaren.

3.2.3.1 Exponering och arkitektur

Att förändra arkitekturen och på så sätt uppnå en lägre exponering av systemet kan göras på olika sätt.

Ett stand alone-system är alltid att föredra ur exponeringssynpunkt (ur ett logiskt perspektiv). Om detta inte är möjligt bör samtliga gränsytor noga definieras och trafik filtreras för att minimera och kontrollera exponering av systemets information.

Uppsäkring och/eller begränsning av informationsutbytet mellan system kan sänka exponeringen, exempelvis genom att kapsla in känslig information eller genom att centralisera systemlösningen och på så sätt uppnå en lägre exponering av systemet som helhet. Antalet behöriga användare är också en faktor som kan vara möjlig att påverka. Ju färre användare desto lägre exponering.

Ytterligare en möjlighet är att skapa ”titthål” in i systemet där läsrättighet ges men inte skrivrättighet. Denna lösning är mest av värde där riktighet eller tillgänglighet är i fokus snarare än sekretess.

3.2.3.2 Exponering och teknisk lösning

Hur förändring av ett systems tekniska lösning i syfte att minska systemets exponering kan göras är något svårare att exemplifiera då den tekniska lösningen inte är fullt lika starkt kopplad till exponeringen som exempelvis arkitekturen. Det finns dock några generella möjligheter.

Att införa kryptering i ett system är ett effektivt sätt att sänka exponeringen. Det bör då genomföras en analys för att se vilka anslutningar och kommunikationsvägar som kan vara mer exponerade än andra och att sedan försöka rikta sina insatser mot dessa.

Att göra ett medvetet val av operativsystem kan också vara ett sätt att reducera exponeringen, framför allt vad gäller skadlig kod, men till viss del även riktade, illvilliga angrepp från icke behöriga individer/system.

3.2.3.3 Exponering och driftmiljö

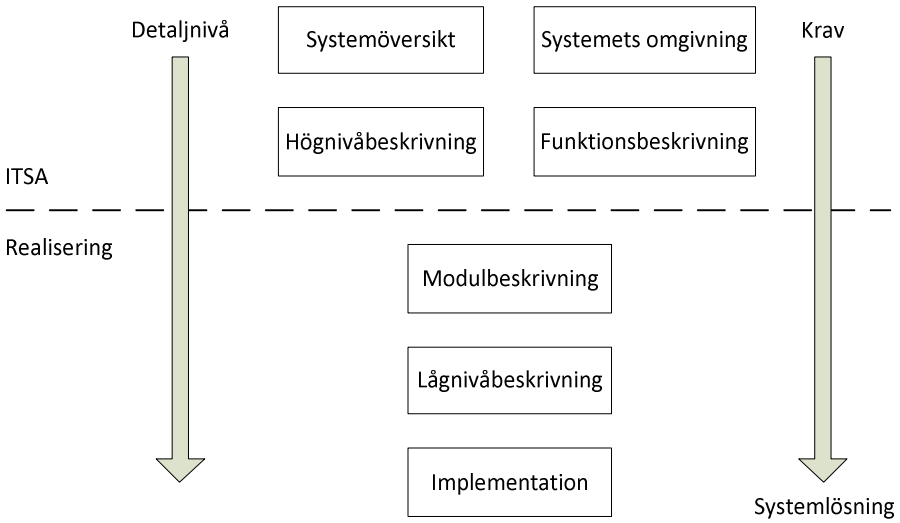
Vad gäller ett systems driftmiljö så finns det en hel del åtgärder som kan vidtas för att sänka systemets exponering. I de fall då systemet ska driftsättas i kontorsmiljö eller motsvarande kan det exempelvis handla om tillträdesbegränsning i de lokaler där systemets hårdvara är placerad. Kanske finns det också möjlighet att drastiskt förändra driftmiljön genom att istället för att driftsätta systemet i kontorsmiljö välja ett bergrum eller annan högsäkerhetsmiljö.

Det är också viktigt att beakta den context i vilket ett system ska driftsättas. Om ackrediteringen innehåller säkerhetskrav i systemets driftmiljö, måste dessa vara uppfyllda för alla miljöer systemet driftsätts i.

Kopplat till driftmiljö finns det också möjlighet att förändra eller begränsa vilka användningsfall som tillåts/möjliggörs. Ett exempel kan vara en verksamhet som har önskemål om att systemet ska kunna användas både på stabsledningsplats (kontrollerad kontorsmiljö) och ute i terrängfordon (betydligt mindre kontrollerad miljö). Frågan kan då ställas om systemet verkligen behöver vara möjligt att använda ute i fält. Om så inte är fallet kan användningsfallen reduceras till att endast omfatta stabsledningsplats och på så sätt har systemets exponering sänkts.

3.3 Systembeskrivning

Följande figur illustrerar olika nivåer på systembeskrivningen. ITSA innehåller FMV målbild avseende systemet som helhet, med viss detaljering på hög nivå. Den faktiska utformningen styrs av systemutvecklaren, som tillsammans med FMV, utformar systemet på en detaljerad nivå.



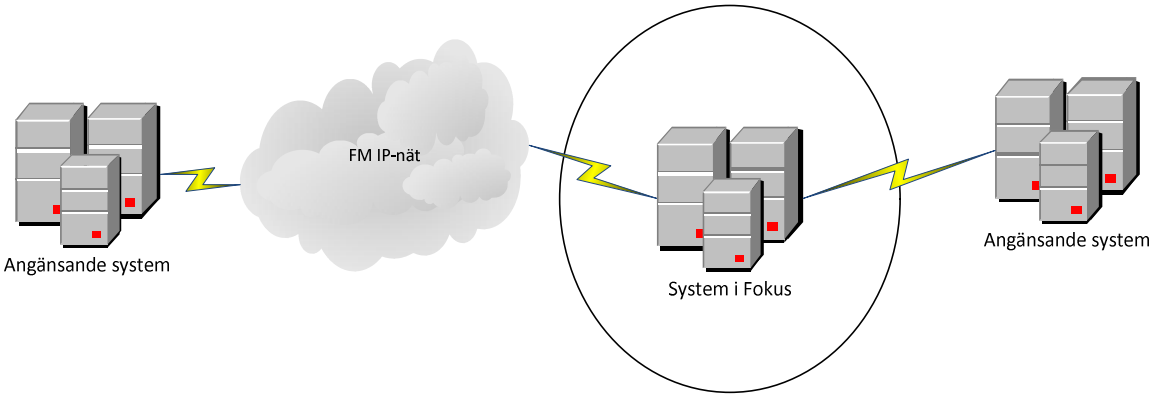
Figur 1 Beskrivningsnivåer

3.3.1 Systemöversikt

Beskriv systemet på en övergripande nivå. Avsikten med detta stycke är att läsaren ska få en bild av vad system är och syftet med detsamma.

3.3.2 Systemets omgivning

Beskriv övergripande hur systemets (System i Fokus, SiF) omgivning ser ut. Visa den övergripande arkitekturen med en bild där externa gränsytor ingår. Beskriv angränsade system och informationsflöden. Exempel på figur:



Figur 2 Systemets omgivning (exempel)

Här ska det även beskrivas om det finns stödjande system, d.v.s system som tillhandahåller säkerhetsfunktioner som System i Fokus är beroende av. Detta kan t ex vara ett underliggande system för administration av användare och behörigheter eller ett system för insamling av säkerhetsloggar.

Vissa system förlitar sig på säkerhetsfunktionalitet som tillhandahålls av komponenter som inte ingår i systemet, exempelvis då systemet utgör en del av ett större system. I dessa fall måste det för varje krav som har ett sådant externt beroende, i IT-säkerhetsspecifikationen (ITSS), tydligt identifieras såväl beroendets art och till vad samt på vilket sätt kravet är tänkt att omhändertas.

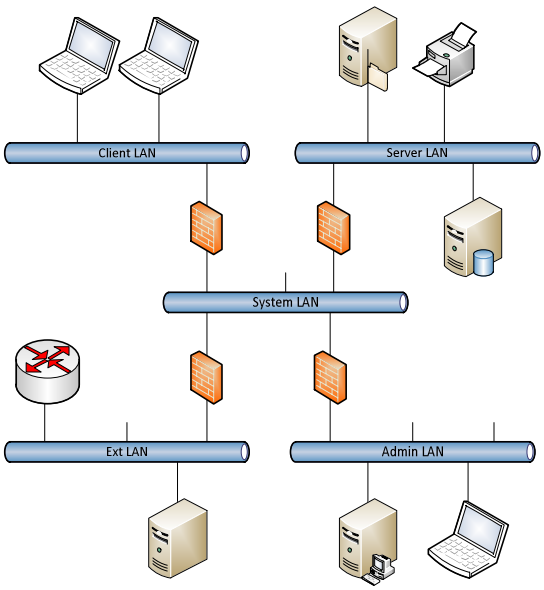
Externa beroenden får endast finnas om den externa komponenten är del av ett ackrediterat system med minst samma nivå av funktionella krav och assuranskrav som det system vilket förlitar sig på den externa komponenten. Detta för att kunna förlita sig på en säkerhetsegenskap i ett annat system. Denna egenskap måste ha utvärderats och överensstämma med vad det förlitande systemet förväntar sig. Kravet på ackreditering avser även tilltron till att den externa komponenten kan skydda sig själv så att egenskaperna bibehålls.

I denna beskrivning kan det också ingå beskrivning av fysiskt skydd och skydd mot obehörig avlyssning och röjande signaler (RÖS och/eller TEMPEST).

Krav på omgivningen kan också finnas i ITSS-D.

3.3.3 Högnivåbeskrivning

I detta avsnitt beskrivs SiF på en hög nivå. Det ska framgå hur systemet är uppbyggt (systemelement) och vilka interna gränsytor som finns. Det är inte möjligt att ge direkta anvisningar om vad som är rätt nivå, då detta är beroende på det aktuella systemet. Syftet med högnivåbeskrivningen är att ge utvecklare, leverantör och/eller granskare en tillräcklig bild över hur systemet är tänkt att se ut. Exempel på figur:



Figur 3 Högnivåbeskrivning (exempel)

Högnivåbeskrivningen ska förteckna olika systemkomponenter, samt interna gränsytor. Beskrivningen ska också innehålla de gränsytor som utgör HMI, dvs där användare och administratörer interagerar med systemet.

4 Säkerhetsarkitektur

Genom uppdelning av ett system kan kostnadsdrivande krav isoleras till egna delsystem och därigenom sänka totalkostnaden för hela systemets skydd.

Skyddet för separationen (dvs kravställningen på skyddsmekanismer) mellan delsystemen skall dock alltid uppfylla delsystemens högsta nivå. Delsystemindelning ger en möjlighet att betrakta det totala system som "flera samverkande delsystem".

4.1 Design- och arkitekturbeslut

4.1.1 ISD Designbeslut

Ange eventuella designbeslut som gäller för systemet. Detta kan exempelvis vara val av systemkomponenter (brandvägg, krypto, diod, kortläsare, osv) eller viss mjukvara (FM Tunnel, antivirus, osv). Källan till dessa beslut kan t ex vara ISD-Strategi eller SYD.

Pos	ISD Designbeslut	Källa/Referens

Tabell 4 – ISD Designbeslut

Om ovanstående designbeslut genererar krav på teknisk lösning, ska detta anges nedan:

Krav	Kravtext

Tabell 5 – Krav härledda ur ISD Designbeslut

4.1.2 Formella designregler

Ange eventuella designregler som gäller systemet. Detta kan exempelvis vara designregler avseende härdning av datorer. Detta avsnitt avser formellt beslutade designregler.

Pos	ISD Designbeslut	Källa/Referens

Tabell 6 – Formella designregler

Om ovanstående formella designregler genererar krav på teknisk lösning, ska detta anges nedan.

Krav	Kravtext

Tabell 7 – Krav härledda ur formella designregler

4.1.3 Användningsfall

Ange eventuell påverkan på arkitekturen utifrån driftsfall i AU-D (ref [XXX]).

Pos	ISD Designbeslut	Källa/Referens

Tabell 8 – Driftfall

Om ovanstående användningsfall genererar krav på teknisk lösning, ska detta anges nedan.

Krav	Kravtext

Tabell 9 – Krav härledda ur driftfall

4.1.4 Arkitekturprinciper

Vid systemutveckling eller framtagning av en IT-tjänst bör följande grundläggande principer beaktas/följas. Dessa arkitekturprinciper följer *best practice* enligt industrin, varför principerna benämns på engelska.

Arkitekturprincip	Beskrivning
Minimalism	Säkerhetsrelevanta funktioner ska inte göra något mer än nödvändigt
Least privilege	Användare och funktioner ska endast ha nödvändiga rättigheter
Redundancy	Funktioner ska ha kapacitet för att hantera hög belastning och systemfel (inklusive fysiska fel)
Defence in depth	Multipla funktioner ska samverka på olika nivåer för att upprätthålla säkerheten
Self-protection	Funktioner ska inte ha onödiga beroende till andra funktioner/domäner
Controlled data flow	Informationsutbyte ska följa väl definierade mönster, som är under central kontroll
Balanced strength	Det ska finnas en balans i styrkan hos säkerhetsfunktionerna i hela systemet
Hardening	Alla funktioner som inte stödjer systemets primära syfte ska vara avstängda/avinstallerade

Tabell 10 – Arkitekturprinciper

Utöver ovanstående principer finns det andra riktlinjer, såsom:

Arkitekturprincip	Beskrivning
Economy of mechanisms	Säkerhetslösningar måste hållas enkla, okomplicerade och begränsade till sin omfattning
Open design	Säkerhetslösningar måste vara öppen i design och implementation och med så få ”hemligheter” som möjligt. Dessutom ska säkerhetslösningar inte förlita sig på skydd från endast kända hot.
Ease of use	Säkerhetslösningar måste vara enkla (användarvänliga) och tillräckligt enkla för att undvika riskabla workarounds. Transparenta säkerhetslösningar bör eftersträvas.

Tabell 11 – Arkitekturprinciper – övriga riktlinjer

4.1.4.1 Minimalism

Principen om minimalism innebär att säkerhetsrelevanta funktioner inte får göra mer än absolut nödvändigt, d.v.s. vara enkel, liten, och fokuserad.

Enkelhet är viktigt eftersom komplexitet tenderar att introducera fel i arkitektur, design, implementation, testning, användning och hantering av informationssäkerhetslösningar.

Komplexitet är svårt att analysera och konkretisera, men ett subjektivt mått . Komplexitet bör således minskas med en söndra och härska strategi (s.k. divide and conquer) samt genom standardisering. Även storleken på en funktion eller en tillgång (asset) kan vara en orsak till problem när det gäller minimalism, det vill säga att alltför många funktioner implementeras i en enskild systemkomponent. Det kan då vara lämpligt att dela upp funktionen eller tillgången till flera funktioner.

Geografisk spridning av dessa funktioner kan också vara ett alternativ.

Principen om minimalism gäller även själva systemet eftersom det inte alltid är lämpligt att skapa ett enda allomfattande system inom en organisation. Vissa komplexa eller äldre funktioner kan användas som distinkta (externa) system snarare än att ingå i det generella systemet. Genom att avskilja komplicerande faktorer kan komplexiteten minskas för helhetslösningen.

Principen om minimalism arbetar vanligtvis tillsammans med principen om Least privilege.

Arkitekturprincip	Hanteras av system på följande sätt
Minimalism	*Ange hur principen om Minimalism beaktas i systemet*

Tabell 12 – Minimalism

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 13 – Krav härledda ur arkitekturprincipen Minimalism

4.1.4.2 Least Privilege

Principen om Least privilege avser att användare och funktioner endast skall tilldelas rättigheter som är absolut nödvändiga. Genom att tillämpa principen minskas den potentiella risken för sårbarheter.

En rättighet här betyder rätt för ett subjekt att utföra en funktion på ett objekt. Subjektet är en användare, eller en funktionell roll, och objektet är typiskt ett dataobjekt, t.ex. en fil. Funktionen kan vara vad som helst, men innebär ofta access, t.ex. läsa, skriva, exekvera, etc. Rättigheter kan vara ovillkorliga eller kräva ett visst sammanhang, t.ex. att de endast är implementerade på vissa terminaler eller under vissa timmar, eller bara vid anrop från vissa applikationer, eller när de tillämpas på vissa objekt.

Med tanke på att en rättighet är en <subjekt, funktion, objekt> -triplett, kan principen om Least privilege främjas genom att minimera subjektet, funktionen och/eller objektet.

- Minimera subjektet -
- Minimera funktionen - Principen om Least privilege är nära besläktad med principen om minimalism när det gäller att minska komplexiteten och storleken på en funktion. Att ha små och väldefinierade funktioner främjar båda principerna.

– Minimera objektet - Minimering av storleken på objektet, det vill säga att öka granulariteten av funktionen, är det konventionella sättet att främja Least privilege. I stället för att en rättighet kontrollerar access till hela objektet, kan flera rättigheter styra accessen till olika delar av objektet.

Att identifiera den minsta uppsättning rättigheter för varje möjlig <subjekt, funktion, objekt> - triplet är en komplex och resurskrävande aktivitet. Standardisering och återanvändning, t.ex. av nod, dator och användarroller, är det mest kostnadseffektiva sättet att identifiera relevanta rättigheter.

Minimering av en funktion genom att ”kosmetiskt” ta bort kommandon från det grafiska användargränssnittet (GUI/HMI) utan också ta bort eller begränsa tillgången till den underliggande funktionaliteten (t.ex. exekverbara filer) är ett exempel på säkerhet genom s.k. security by obscurity. Detta tillvägagångssätt får inte användas om användarna kan åberopa samma funktionalitet från andra, t.ex. lågnivå-gränssnitt eller om de kan importera likvärdig funktionalitet från externa källor, t.ex. genom använd ett USB-minne för att kopiera programmet.

Arkitekturprincip	Hanteras av system på följande sätt
Least privilege	*Ange hur principen om Least privilege beaktas i systemet*

Tabell 14 – Least privilege

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 15 – Krav härledda ur arkitekturprincipen Least privilege

4.1.4.3 Redundancy

Principen om redundancy (redundans) säger att funktionerna ska ha ledig kapacitet för att hantera överbelastningar och fel på utrustningen. I korthet innebär det att viktiga komponenter inte ska äventyras av enkla incidenter, t.ex. genom att ha ”svaga” punkter eller flaskhalsar som hotar tillgängligheten.

Ordet reservkapacitet används i vid bemärkelse och indikerar att systemet inte ska planeras för exakt önskad storlek och effektivitet. Det måste finnas en del planering för det oväntade. Det måste också finnas utrymme för tillväxt och förbättring i händelse av en incident.

I likhet med principen om minimalism, gäller principen om redundans på flera olika abstraktionsnivåer. I ena änden kan ett informationssystem ha en fullt fungerande offline replika redo att snabbt ersätta det ursprungliga systemet. Ingen (akut) återställning av det ursprungliga systemet är då nödvändig. Detta är relevant för små och specialiserade system vilka utför (mycket) kritiska funktioner.

I andra änden kan individuella datorer och nätverksenheter ha redundans av kritiska komponenter, t.ex. nätverksgränssnitt, diskar, processorer och minne.

Ledig kapacitet behöver inte allokeras och/eller vara tillgänglig hela tiden. Standby-resurser kan ge nödvändig kapacitet genom failover eller hot-swap. Säkerhetskopiering och online-reparationer kan ge förnyad kapacitet genom återställning.

Slutligen kan resurskontroller och prioritering säkerställa nödvändig kapacitet där inga oallokerade eller förnybara resurser finns tillgängliga.

Arkitekturprincip	Hanteras av system på följande sätt
Redundancy	*Ange hur principen om Redundanct beaktas i systemet*

Tabell 16 – Redundacy

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 17 – Krav härledda ur arkitekturprincipen Redundancy

4.1.4.4 Defence in depth

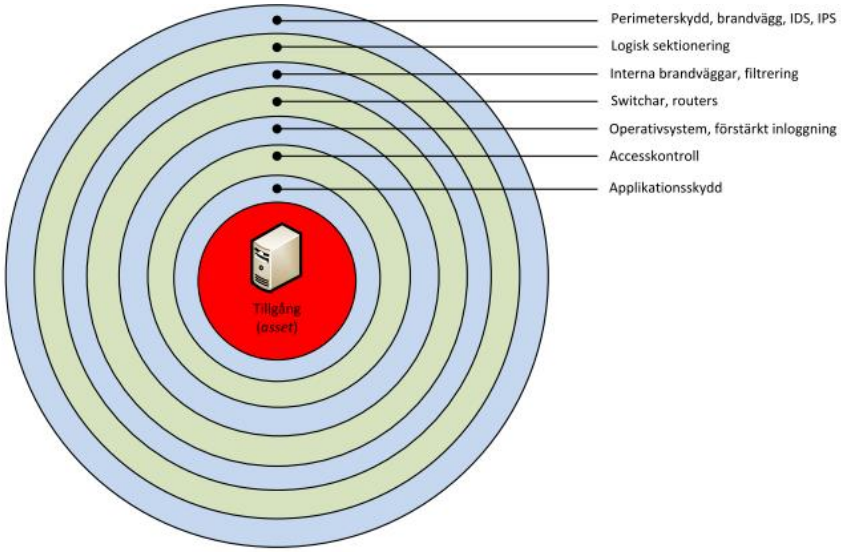
Med principen om defence-in-depth avses att flera funktioner ska behandla samma säkerhetsbehov, t.ex. ska det finnas skiktad säkerhet. Medan principen om redundans främjar funktioner som säkerställer kapaciteten, avser principen om defence-in-depth redundans för funktioner som skyddar och härdar ett IT-system.

Flera överlappande mekanismer är således bättre än en enda mekanism.

En viktig tillämpning av defence-in-depth är att ha flera barriärer framför de resurser som behöver skydd, så att en extern angripare (utan åtkomsträttigheter) måste bryta flera försvar för att få access till skyddsvärda tillgångar. I ett typiskt IT-system kan hindren vara filter och åtkomstkontroller längs nätverksvägarna (t.ex. i routrar och brandväggar) samt datorspecifika kontroller (t.ex. inloggningsrättigheter och tillgång objektkontroller).

En annan viktig tillämpning av defence-in-depth är principen om inneslutning (eng containment), d.v.s. att ha barriärer runt områden där skador kan uppstå för att förhindra eventuella skador från att sprida sig.
I ett typiskt IT-system kan detta vara samma routrar och brandväggar som ovan men att nu styra flödet åt andra hållet.

Följande figur visar ett exempel på defence-in-depth.



Figur 4 Defence-in depth (exempel)

Arkitekturprincip	Hanteras av system på följande sätt
Defence-in-depth	*Ange hur principen om Defence-in-depth beaktas i systemet*

Tabell 18 – Defence-in-depth

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 19 – Krav härledda ur arkitekturprincipen Defence-in-depth

4.1.4.5 Self-protection

Principen om self-protection anger att funktioner inte ska ha onödiga säkerhetsberoenden. Genom att tillämpa principen om self-protection minskar risken för en oönskad händelse att inträffa samt den potentiella omfattningen av skadan.

Principen om self-protection gäller många relationer, till exempel:

- Mellan nationell infrastruktur och utländsk infrastruktur
- Mellan system
- Inom system
  - Mellan interna säkerhetsdomäner och perimeterskydd
  - Mellan management och slutanvändare
  - Mellan interna domäner som utgör olika organisationer/affärsenheter
  - Mellan olika roller, t.ex. datorroller eller användarroller
  - Mellan administratör-, operatör-, och slutanvändarkonton

Kravet på self-protection är starkare på makronivå än mikronivå, det vill säga separation av system är viktigare än separation av delsystem eller roller inom ett system.

Som det kan utläsas från ovanstående lista, kan principen om self-protection både tillämpas enkelriktat och dubbelriktat. Vissa förtroenden (eng trust) är transitiva, medan andra inte är det. Sammantaget kan dessa förtroenden bilda en hierarki av förtroenderelationer.

Kommunikationsvägar får inte undergräva self-protection, t.ex. kommunikation mellan systemnoder ska normalt inte passera andra noder utan hålla sig till ”neutralt” LAN/WAN.

Arkitekturprincip	Hanteras av system på följande sätt
Self-protection	*Ange hur principen om Self-protection beaktas i systemet*

Tabell 20 – Self-protection

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 21 – Krav härledda ur arkitekturprincipen Self-protection

4.1.4.6 Controlled data flow

Principen om controlled data flow avser att informationsutbytet ska följa väldefinierade flödesmönster som är under central (alternativt definierad) kontroll. Principen gäller främst nätverkskommunikation, både mellan system och inom systemen. Målsättningen är att ha en flödeskontroll som är konsekvent och effektiv i hela infrastrukturen.

Från principen om controlled data flow följer att:

- Flow control policies är en systemövergripande fråga. En risk som accepteras av en systemkomponent är en risk som kan påverka många. En enskild komponent i ett system kan inte ensidigt ändra den beslutade policyn och därmed utsätta andra komponenter för ökad risk.
- Flow control policies måste formellt dokumenteras. Tillåtna dataflöden måste formellt överenskommits i avtal om samtrafik och systemspecifik säkerhetsdokumentation.
- Odefinierade policys ska som default vara förbjuden. Alla flöden måste ske i enlighet med policyn. Flöden som inte explicit har överenskommits och därmed är tillåtna är implicit förbjudna.
- Flow control policies behöver en stark samordning och centraliserad tillsyn. Varje organisation behöver central styrning och förvaltning av de gemensamma aspekterna av flödeskontrollpolicyn.

Flow control policies skall inte minska flexibilitet eller systemanslutningar och organisationer bör ha möjligheter att genomföra dagliga operationer inom den beslutade policyn. Det bör också vara möjligt att kunna åsidosätta mekanismer vid eventuella nödsituationer.

Arkitekturprincip	Hanteras av system på följande sätt
Controlled data flow	*Ange hur principen om Controlled data flow beaktas i systemet*

Tabell 22 – Controlled data flow

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 23 – Krav härledda ur arkitekturprincipen Controlled data flow

4.1.4.7 Balanced strength

Principen om en balanced strength bygger på att effektiviteten av säkerhetsfunktionerna skall vara motsvarande starka i hela systemet, enligt principen ”ingen kedja är starkare än sin svagaste länk.

Ordet styrka används här i vid mening och är avsedd att täcka alla relevanta egenskaper av en säkerhetsfunktion, inklusive dess effektivitet avseende att upprätthålla säkerheten. Hot och sårbarheter realiseras inte alltid jämnt över systemet, vilket innebär olika skyddsförmågor för olika delar av systemet.

Det kan till exempel finnas ett behov av mer garantier i vissa funktioner relaterade till perimetersäkerhet och överföring av domändata. Detta bör klargöras genom riskanalyser och ska inte stå i strid med principen om en balanserad styrka. Säkerhetsfunktioner som implementeras mot samma säkerhetsmål skall naturligtvis ha samma styrka.

Principen för balanced strength kan vara lätt att förstå, men svårt att genomföra. Att bedöma styrkan hos en mekanism är inte trivialt, och kan innebära dyra formella utvärderingar och certifieringar, eller komplexa matematiska analyser.

Evaluering enligt Common Criteria (ISO/IEC 15408) är ett utbrett och erkänt sätt att mäta styrkan på säkerhetsfunktioner. En blandning av certifierad och icke certifierad mjuk-/hårdvara för att uppnå en viss säkerhetsnivå är ofta nödvändigt, men kan lätt skapa obalans i säkerheten. Obalansen minskas genom att välja icke certifierad programvara som integrerar med den certifierade programvaran och återanvänder certifierade säkerhetsfunktioner. Att använda icke certifierad/auktoriserad programvara av okänt ursprung, t.ex. vissa typer av public domain programvara, ökar obalansen.

Ofta kan en tillgång nås via olika vägar, vilka är skyddade av olika säkerhetsfunktioner. Ett enkelt exempel är den fysiska sökvägen och den infologiska vägen till en tillgång. Alla sådana vägar måste skyddas av funktioner med motsvarande styrka. Det kan till exempel vara obalanserad säkerhet att bara ha en fyrsiffrig accesskod på fysiska dörrar och ett 15 tecken långt datorlösenord.

Ibland kan flera infologiska vägar leda till samma tillgång. Olika applikationer kan exempelvis processa och publicera samma data. Alla säkerhetsfunktioner på applikationsnivå måste då ha samma styrka som de underliggande säkerhetsfunktionerna för att inte obalans ska uppstå.

Äldre systemen (arv) och dåliga systemkonstruktioner kan införa applikationer som duplicerar säkerhetsfunktioner som redan finns i basplattformen. Alla dubbla säkerhetsfunktioner måste då ha samma styrka som de grundläggande säkerhetsfunktionerna för att inte skapa obalans.

Arkitekturprincip	Hanteras av system på följande sätt
Balanced Strength	*Ange hur principen om Balanced Strength beaktas i systemet*

Tabell 24 – Balanced Strength

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 25 – Krav härledda ur arkitekturprincipen Balanced Strength

4.1.4.8 Hardening

Med härdning avses processen att säkra ett system genom att minska dess exponering av eventuella sårbarheter. Ett system har en större sårbarhetsyta desto fler funktioner den uppfyller; generellt kan sägas att en enda funktion gör systemet säkrare än då flera funktioner exponeras. Metoder för att minska tillgängliga attackvektorer innefattar typiskt avlägsnande av onödiga program, onödiga användarnamn eller inloggningar och inaktivering eller borttagning av ej använda tjänster (services).

Det finns härdningsskript och verktyg som kan inaktivera onödiga funktioner konfigurationsfiler eller utföra diverse andra skyddsåtgärder.

Det finns olika metoder för härdning Unix och Linux-system. Det kan handla om, bland andra åtgärder, med implementation av en patch till kärnan (kernel), såsom t ex Exec Shield eller PaX, stänga öppna nätverksportar och installera intrångsdetektionssystem, brandväggar och intrångsförebyggande system. Motsvarande metoder finns även för Windowsbaserade system.

Härdning omfattas av, men begränsas inte till, följande aktiviteter:

- Definiera systemets syfte och begränsa/minimera mjuk- och hårdvara
- Dokumentera minimikrav avseende mjukvara, hårdvara och tjänster i systemet
- Installera den minsta mängd mjukvara, hårdvara och tjänster som behövs för att uppfylla kravbilden
- Använd en dokumenterad installationsprocess
- Installera nödvändiga patchar
- Installera de nyaste (och mest säkra) versionerna av nödvändiga applikationer
- Konfigurera åtkomstkontroll utifrån principen deny all – grant minimum
- Konfigurera säkerhetsfunktionerna på ett lämpligt sätt
- Aktivera säkerhetsloggning
- Testa systemet för att säkerställa en korrekt konfiguration/installation
- Ändra alla default-lösenord

Arkitekturprincip	Hanteras av system på följande sätt
Hardening	*Ange hur principen om Hardening beaktas i systemet*

Tabell 26 – Hardening

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 27 – Krav härledda ur arkitekturprincipen Hardening

4.1.4.9 Economy of mechanisms

Säkerhetslösningar måste hållas enkla, okomplicerade och begränsade till sin omfattning

Arkitekturprincip	Hanteras av system på följande sätt
Economy of mechanisms	*Ange hur principen om Economy of mechanisms beaktas i systemet*

Tabell 28 –Economy of mechanisms

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 29 – Krav härledda ur arkitekturprincipen Economy of mechanisms

4.1.4.10 Open Design

Säkerhetslösningar måste vara öppen i design och implementation och med så få ”hemligheter” som möjligt. Dessutom ska säkerhetslösningar inte förlita sig på skydd från endast kända hot.

Arkitekturprincip	Hanteras av system på följande sätt
Open Design	*Ange hur principen om Open Design beaktas i systemet*

Tabell 30 –Open Design

Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 31 – Krav härledda ur arkitekturprincipen Open Design

4.1.4.11 Ease of use

Säkerhetslösningar måste vara enkla (användarvänliga) och tillräckligt enkla för att undvika riskabla workarounds. Transparenta säkerhetslösningar bör eftersträvas.

Arkitekturprincip	Hanteras av system på följande sätt
Ease of use	*Ange hur principen om Ease of use beaktas i systemet*

Tabell 32 –Ease of use

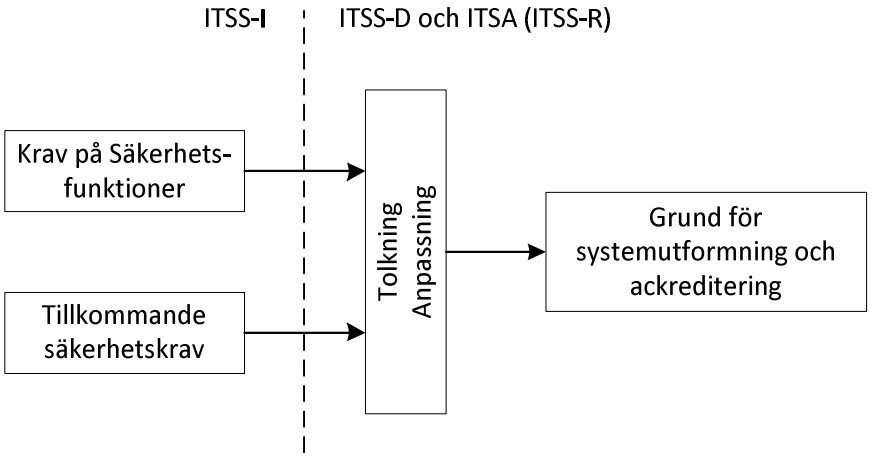
Om ovanstående arkitekturprincip genererar krav på teknisk lösning, ska detta anges nedan.

Krav ID	Kravtext

Tabell 33 – Krav härledda ur arkitekturprincipen Ease of use

4.2 Kravflöde

Kraven som ska allokeras på systemet grundar sig på de tolkade säkerhetskraven i ITSS-D (ref XX), enligt följande kravflöde:



Figur 5 Kravflöde ITSS-I till ITSA

Utöver de tolkade kraven i ITSS-D, kan det även finnas styrande krav i ISD-strategin eller i SYD:en.

ISD-strategin kan t ex innehålla:

- Krav från samverkande system (system-av-system)
- Inriktningar avseende omgivande system/miljö
- Speciella krav avseende gränsytor (internt/externt), i form av t ex format
- Krav på nyttjande av GFE (GOTS/MOTS)
- Krav på nyttjande COTS
- Projektöverskridande säkerhetsfunktioner
- Krav på återbruk av FMV tidigare godkända komponenter

SYD kan t ex innehålla:

- Tjänster som system ska tillhandahålla
- Krav från omgivande system
- Övergripande designbeslut (teknikval)
- Eventuella avvikelser från gällande regelverk

4.3 Säkerhetsfunktioner

4.3.1 Funktionskedjor

Inför kravallokeringen av de tolkade kraven på den tänkta systemarkitekturen, är det viktigt att identifiera systemgemensamma funktionskedjor.

Systemgemensamma funktionskedjor

Exempel på dessa är systemgemensam korrekt tid, säkert tillstånd, behörighetskontrollsystem och säkerhetsloggning.

Funktionskedja	Implementeras i systemet på följande sätt (övergripande beskr.)
Behörighetskontroll	
Säkerhetsloggning	
Säker tid	
Säkert tillstånd	

Tabell 34 – Funktionskedjor

Om ovanstående funktionskedjor genererar krav på teknisk lösning, ska detta anges nedan. Dessa krav kan behöva synkroniseras med de funktionella kraven för respektive säkerhetsfunktion.

Krav ID	Kravtext

Tabell 35 – Krav härledda ur systemövergripande funktionskedjor

4.3.2 SF – Behörighetskontroll

Behörighetskontroll innebär att kunna avgöra vem eller vad som begär åtkomst till systemet eller informationen som behandlas i det och endast medge åtkomst om behörighet har tilldelats.

Behörighetskontroll behövs också för att säkerställa säkerhetsloggning i systemet.
För att kunna implementera en funktionell behörighetskontroll, behövs en Behörighetkontrollpolicy.

Behörighetskontrollpolicy

Beskriv eller hänvisa till behörighetskontrollpolicy.

Beroende på definierad kravnivå, och designval, kan behörighetskontrollen vara låg (t ex en-faktor), förstärkt eller stark. Vissa kategorier av användare (t ex administratörer med mycket höga rättigheter) kan behöva hanteras i särskild ordning.

Följande tabell innehåller verksamhetens krav på behörighetskontroll.

Krav ID	Verksamhetens krav baserade på behörighetspolicy

Tabell 36 – Verksamhetens krav baserade på behörighetspolicy

Observera att det kan förekomma konflikter avseende behörighetskontroll utifrån olika kravkällor, exempelvis FM MUST KSF, verksamhetens krav och krav utifrån flyg- eller sjösäkerhet.

4.3.3 SF – Säkerhetsloggning

Kraven på säkerhetsloggning berör dels själva loggningen och dels analys av insamlade säkerhetsloggar.

För att skydda ett system eller en domän behövs spårbarhet på alla säkerhetsrelaterade händelser i systemet. Detta behövs för att kunna spåra godkända och icke godkända händelser i systemet. I vissa fall behöver systemet även garantera oavvislighet för de åtgärder och händelser som genomförts i systemet.

Säkerhetsrelevanta händelser för säkerhetsloggning

Säkerhetsrelevanta händelser, baserade på verksamhetens krav, framkommer ur AU-D (ref [XX]).

Följande tabell innehåller verksamhetens krav på loggning av säkerhetsrelevanta händelser.

Krav ID	Säkerhetsrelevanta händelser som ska loggas

Tabell 37 – Säkerhetsrelevanta händelser som ska loggas

Möjlighet till analyser av loggar är en grundläggande funktion för att kunna följa händelser och åtgärder genom systemets olika delar.

För att få en ändamålsenlig säkerhetslogg är det viktigt att definiera vilka säkerhetsrelevanta händelser som ska loggas. En grundläggande definition är att dessa ska vara av betydelse för verksamheten. FM MUST KSF förtecknar grundläggande händelser som ska loggas, men de tillkommande säkerhetskraven måste också beaktas. Verksamhetens samlade lista över säkerhetsrelevanta händelser ska vara förtecknade i ITSS-D (ref [XX]) eller AU-D (ref [XX]).

Principer för logganalys (omfattning, frekvens, mm) ska också kravställas i de fall det behövs tekniska funktioner, liksom tekniska system för hantering, analys, back up och export.

Principer för logganalys

Följande tabell innehåller verksamhetens krav på analys säkerhetsloggar.

Krav ID	Verksamhetens krav avseende logganalys

Tabell 38 – Verksamhetens krav avseende logganalys

I ovanstående tabell bör det också framgå var logganalys ska ske, dvs om det är inom systemet (SiF) eller i ett angränsande (externt) system.

I de fall logganalysen genomförs i ett angränsande (extern) system ska det framgå vilket format på loggar som är aktuellt och hur loggar skickas från logproducent till analysenhet.

Utöver krav på säkerhetloggning ställs även krav på oavvislighet (gäller ej KSF Grund-nivå). Syftet med dessa krav är att användare inte ska kunna dölja eller förneka genomförda åtgärder i systemet.

Principer för oavvislighet

Följande tabell innehåller verksamhetens krav oavvislighet.

Krav ID	Verksamhetens krav avseende oavvislighet

Tabell 39 – Verksamhetens krav avseende oavvislighet

4.3.4 SF – Intrångsskydd

För att skydda ett system från intrång behövs säkerhetsfunktioner som kan tillåta behörig kommunikation och samtidigt avvärja icke behörig kommunikation. Detta skydd består av externt perimeterskydd, skydd av kommunikation inom systemet samt skydd av informationsflöden in i eller ut ur systemet.

Perimeterskydd

Perimeterskydd utgörs normalt sett av exempelvis brandväggar. Grundregel för perimeterskydd bör vara ”deny all”.

Följande tabell innehåller verksamhetens krav på intrångsskydd vid externa gränsytor.

Krav ID	Verksamhetens krav avseende perimeterskydd

Tabell 40 – Verksamhetens krav avseende perimeterskydd

Säkerhetsfunktioner mot intrång behövs både i perimetern och inne i systemet. De behövs också på olika nivåer i informationsflödet. Exempelvis behövs både kontroll av enskilda paket i ett kommunikationsflöde och kontroll av vilken information som skickas in i eller ut ur systemet.

Internt intrångsskydd

Internt intrångsskydd utgörs normalt sett av mjukvarubrandväggar. Syftet är att begränsa nätverkstrafik till på kända portar/protokoll.

Följande tabell innehåller verksamhetens krav på internt intrångsskydd.

Krav ID	Verksamhetens krav avseende internt intrångsskydd

Tabell 41 – Verksamhetens krav avseende internt intrångsskydd

Utöver externt och internt intrångsskydd behövs också härdning av systemkomponenter, för att reducera attackytan.

Principer för härdning

Följande tabell innehåller verksamhetens krav på härdning av (främst) operativsystem.

Krav ID	Verksamhetens krav avseende härdning

Tabell 42 – Verksamhetens krav avseende härdning

En grundregel för härdning är att endast inkludera/implementera nödvändiga funktioner/paket, istället för att i efterhand exkludera ej nödvändiga funktioner/tjänster/paket.

4.3.5 SF – Intrångsdetektering

För att skydda ett system från intrång behövs säkerhetsfunktioner som kan upptäcka och varna för icke behörig kommunikation och dataförändringar. Detta skydd består av externt perimeterskydd, skydd av data inom systemet, samt skydd av informationsflöden in eller ut ur systemet.

Nätverksbaserad IDS

Följande tabell innehåller verksamhetens krav på nätverksbaserad intrångsdetektering (NIDS).

Krav ID	Verksamhetens krav avseende nätverksbaserad intrångsdetektering

Tabell 43 – Verksamhetens krav avseende nätverksbaserad intrångsdetektering

Exempel på NIDS är funktioner i DMZ eller dedikerade enheter inne i ett system.

Skyddsåtgärderna behövs både i perimetern och inne i systemet, där intrångsdetekteringen tillsammans med intrångsskyddet utgör en del, och integritetskontroller av applikationer och data utgör en annan del.

Hostbaserad IDS

Intrångsdetekteringen har också möjligheter att utnyttja delar av andra säkerhetsfunktioner, t.ex. säkerhetsfunktionen för säkerhetsloggning, integritetskontroll eller skydd mot skadlig kod för att analysera händelser i systemet.

Följande tabell innehåller verksamhetens krav på intern intrångsdetektering.

Krav ID	Verksamhetens krav avseende intern intrångsdetektering

Tabell 44 – Verksamhetens krav avseende intern intrångsdetektering

4.3.6 SF – Skydd mot skadlig kod

För att skydda ett system behövs säkerhetsfunktioner för att förhindra att systemet påverkas av skadlig kod, t.ex. virus, trojaner, maskar, logiska bomber och liknande. Skyddsåtgärderna behövs både i perimetern och inne i systemet, då hoten från skadlig kod varierar mellan olika typer av IT-system. Olika typer av skadlig kod attackerar också olika typer av gränsytor.

Varken försök att extrahera information eller angrepp avsedda att störa och förstöra den normala funktionen ska kunna genomföras.

Skydd mot skadlig kod

Följande tabell innehåller verksamhetens krav på skydd mot skadlig kod.

Krav ID	Verksamhetens krav avseende skydd mot skadlig kod

Tabell 45 – Verksamhetens krav avseende skydd mot skadlig kod

Säkerhetsfunktionen för skydd mot skadlig kod ska kunna uppdateras för att erbjuda ett adekvat skydd. Inom denna säkerhetsfunktion finns även krav på integritetskontroll.

Integritetskontroll

Följande tabell innehåller verksamhetens krav på integritetskontroll.

Krav ID	Verksamhetens krav avseende integritetskontroll

Tabell 46 – Verksamhetens krav avseende integritetskontroll

4.3.7 SF – Skydd mot obehörig avlyssning

Skyddsvärd information som sänds i elektroniska kommunikationsnät måste skyddas mot obehörig avlyssning, detta sker normalt genom nyttjande av godkända signalskyddssystem. I elektroniska kommunikationsnät där godkänt signalskydd inte används för all kommunikation

måste dess kablar förläggas på ett sätt som inte exponerar dem för inkoppling av utrustning för obehörig avlyssning.

Skydd mot obehörig avlyssning

Följande tabell innehåller verksamhetens krav på skydd mot obehörig avlyssning.

Krav ID	Verksamhetens krav avseende skydd mot obehörig avlyssning

Tabell 47 – Verksamhetens krav avseende skydd mot obehörig avlyssning

4.3.8 SF – Skydd mot röjande signaler

För att skydda ett system från risken att röja information via de elektromagnetiska signaler som skapas i ett IT-system behöver systemet ha ett skydd mot dessa typer av läckage. Skyddet kan realiseras av systemets komponenter, den lokal där systemet befinner sig eller båda i kombination.

Skydd mot Röjande signaler

Skydd mot RÖS hanteras exempelvis genom en kombination av klassad (U-klassad) utrustning, fysiskt skydd och säkerhetsavstånd till okontrollerade områden.

Följande tabell innehåller verksamhetens krav på skydd mot röjande signaler.

Krav ID	Verksamhetens krav avseende skydd mot röjande signaler

Tabell 48 – Verksamhetens krav avseende skydd mot röjande signaler

Skyddet mot RÖS kan även behöva kompletteras med TEMPEST-krav.

TEMPEST

Följande tabell innehåller verksamhetens krav på TEMPEST.

Krav ID	Verksamhetens krav avseende TEMPEST

Tabell 49 – Verksamhetens krav avseende TEMPEST

Observera att TEMPEST-kraven har påverkan på fysisk utformning av system och anläggningar. Krav på TEMEPST kräver ofta en särskild analys, då dessa inte är att direkt jämställa med skydd mot röjande signaler (RÖS).

Observera att kravställningen (SDIP-27, SDIP-28 och SDIP-29) avseende TEMPEST är sekretessbelagda enligt NATO Restricted och NATO Classified.

4.3.9 SF – Integritetsskydd

Utöver krav på integritetskontroll i FM MUST KSF krav på skydd mot skadlig kod, kan det även vara relevant med tillkommande krav på kontroll av integritet.

Integritetskontrollen kan exempelvis omfatta vissa filer eller databaser.

Integritetsskydd

Följande tabell innehåller verksamhetens krav på integritetskontroll.

Krav ID	Verksamhetens krav avseende integritetsskydd

Tabell 50 – Verksamhetens krav avseende integritetsskydd

4.3.10SF – Redundans

Krav avseende redundans härstammar huvudsakligen från tillgänglighet och kan exempelvis röra sig om lastbalansering, dubblering eller hot/cold-swap.

Utöver ovanstående kan även utbytesenheter eller geografisk separation vara aktuellt.

Redundans kan också vara dubblering av kritiska systemfunktioner eller GUI, alternativt uppdelning i normal- respektive nöd-förfarande.

RAID eller motsvarande tekniker är ofta ett exempel på redundans avseende skydd av information.

Redundans

Följande tabell innehåller verksamhetens krav på redundans.

Krav ID	Verksamhetens krav avseende integritetsskydd

Tabell 51 – Verksamhetens krav avseende redundans

4.3.11 SF – Back up

Back up/Restore kan vara ett komplement till både integritetskontroll och redundans. Övriga aspekter på back up är arkivering och kontinuitetsplanering.

Back up

Följande tabell innehåller verksamhetens krav på back up/restore.

Krav ID	Verksamhetens krav avseende back up/restore

Tabell 52 – Verksamhetens krav avseende back up/restore

4.3.12 SF – Säker tid

En gemensam och tillförlitlig tid är viktigt bland annat för:

- Autentisering som förlitar sig på tid för validering av säkerhetsattribut såsom certifikat eller genererade lösenord
- Behörighetskontroller med begränsningar baserade på tid
- Spårbarhet av händelser i systemet

Aspekter på säker tid som bör beaktas är:

- Extern källa
- Intern källa
- Reservförfarande
- Spridning av säker tid
- Stratum-nivåer
- Andra tider (systemtid, speltid, övningstid, o.s.v.)
- Synkronisering med angränsande system

Säker tid

Följande tabell innehåller verksamhetens krav på säker tid.

Krav ID	Verksamhetens krav avseende Säker tid

Tabell 53 – Verksamhetens krav avseende Säker tid

4.3.13 SF – Säkert tillstånd

Fel i säkerhetsfunktioner eller dess styrande data ska upptäckas och systemet eller nödvändiga delar av systemet ska då kunna försättas i ett definierat säkert tillstånd.

Detta innebär att samtliga relevanta säkerhetsfunktioner ska kunna detektera alternativt generera felmeddelande.

Det definierade säkra tillståndet är unikt för varje SiF, och måste analyseras och konkretiseras. Det måste klarläggas i varje enskilt fall vad som utgör ett felsäkert tillstånd, då detta är beroende av bland annat exponeringsnivå och konsekvensnivå.

Det måste också klarläggas att det säkra tillståndet ur en aspekt, t ex sekretess, inte påverkar andra aspekter såsom tillgänglighet. En särskild riskanalys bör genomföras för att klarlägga definition av säkert tillstånd för det aktuella systemet.

Mekanismer som kan bidra till detektering av säkert tillstånd är t.ex. säkerhetsloggning, intrångsdetektering, skydd mot skadlig kod och integritetskontroll.

Säkert tillstånd

Följande tabell innehåller verksamhetens krav på säkert tillstånd.

Krav ID	Verksamhetens krav avseende Säkert tillstånd

Tabell 54 – Verksamhetens krav avseende Säkert tillstånd

4.4 Funktionsallokering

Detta kapitel beskriver principerna för allokeringen av säkerhetsfunktioner i *systemet* (SiF). Allokeringen är beroende av flera aspekter, såsom

- KSF kravnivå
- Tillkommande säkerhetskrav
- Aspekter från SE
- Systemets komplexitet
- Angränsade system

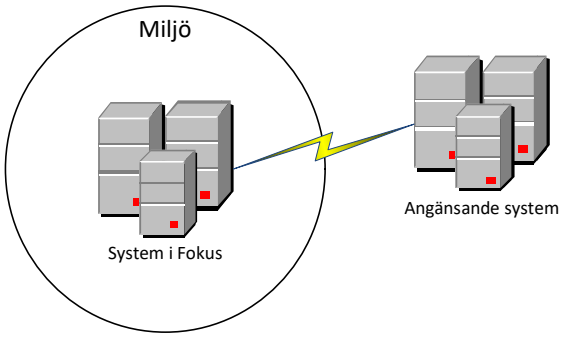
Allokeringen är också beroende på, och styr till viss del, systemets arkitektur. Utöver detta finns det också styrande arkitekturprinciper samt formella designprinciper som påverkar arkitekturen och därmed funktionsallokeringen.

Det är viktigt att allokeringen genomförs på ett genomtänkt sätt, för att reducera komplexitet och kostnader för att införa säkerhetsfunktioner.

4.4.1 Systemarkitektur

I detta kapitel sätts den ursprungliga systemutformningen in i sitt sammanhang avseende omgivande miljö och samverkande system. Den omgivande miljön är både fysisk och funktionell (ur ett IT-säkerhetsperspektiv).

I de fall säkerhetsfunktioner allokeras mot antingen den fysiska miljön eller den omgivande IT-miljön måste dessa funktioner specificeras. De ingår som en del i den totala säkerhetslösningen.

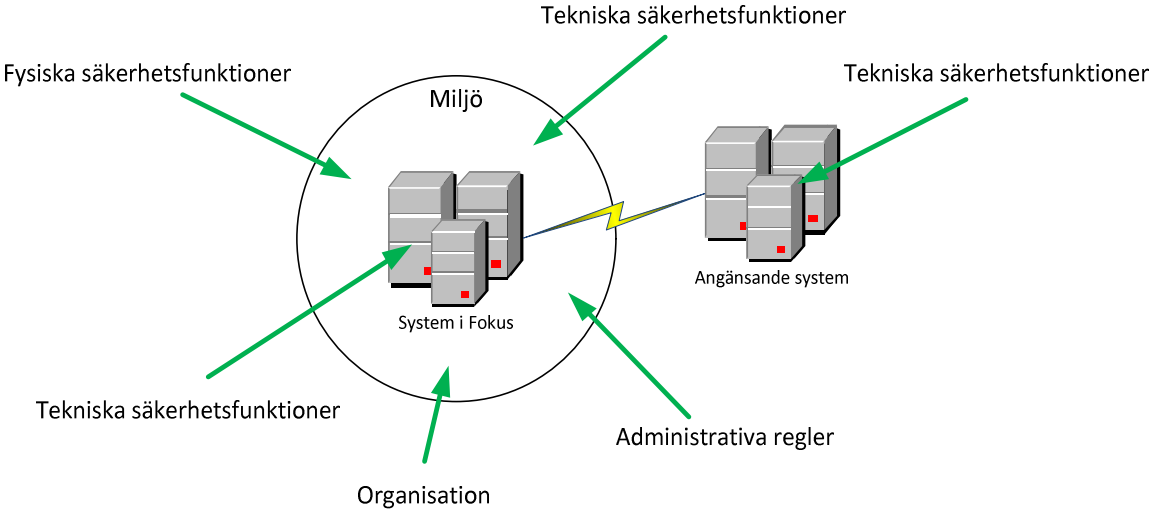


Figur 6 Systemarkitektur HLD

För varje säkerhetsfunktion krävs en analys av var och hur denna funktion ska implementeras på ett så effektivt sätt som möjligt.

4.4.2 Samverkande funktioner

Utöver tekniska lösningar ska det också analyseras om det finns mer effektiva lösningar i t ex fysiskt skydd eller administrativa rutiner/processer.



Figur 7 Samverkande säkerhetsfunktioner

Den övergripande arkitekturprincipen enligt ovan är Defence in depth och Balanced Strength.

Administrativa regler är t ex processer eller rutiner.
Tekniska säkerhetsfunktioner i miljön är t ex övervakningskameror eller larm.
Fysiska säkerhetsfunktioner är t ex skalskydd eller bevakningsåtgärder.

4.4.3 Begränsa exponering

Möjligheterna att begränsa systemets exponering ska också övervägas. Aspekter som kan läggas in här är:

- Externa gränsytor (inkl protokoll)
- HMI
- DMZ
- Kryptering
- Segmentering (intern)

Här kommer också arkitekturprinciper såsom Minimalism, Least Privilag och Ease of Use in.

4.4.4 Reducera konsekvens

Konsekvensen vid informationsförlust eller otillbörlig manipulering av information och radering av information, likväl som otillbörlig exponering som information ska reduceras/minimeras.

Detta gäller även reducering av konsekvens då systemet som sådant inte är tillgängligt.

Ur ett arkitekturperspektiv kan detta reduceras med hjälp av segmentering och/eller separation.

Arkitekturprinciper som gäller här är Redundancy, Defence in Depth, Self-protection, Controlled Data Flow, Hardening och Open Design.

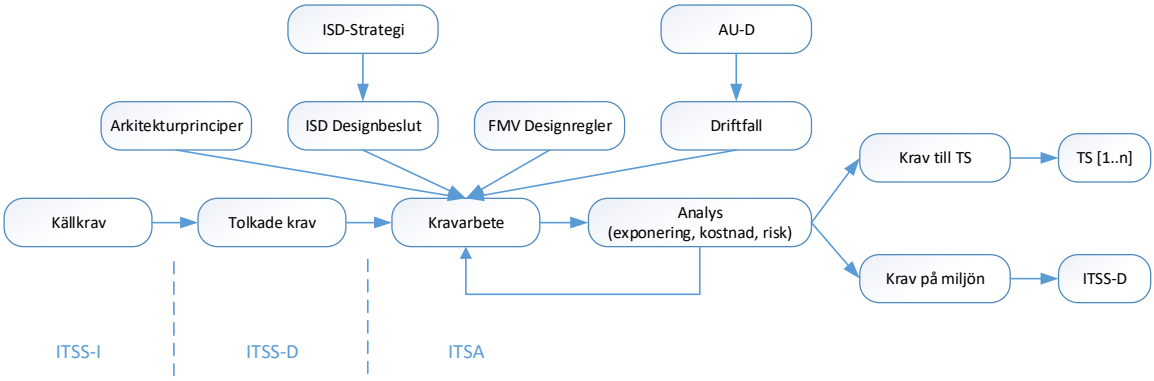
5 Kravsammanställning

Detta kapitel sammanställer samtliga krav avseende säkerhetsfunktioner och arkitektur. Säkerhetskraven baseras på de tolkade kraven i ITSS-D (ref [XX]) samt samtliga krav och analyser i detta underlag.

Kraven i detta kapitel ligger till grund för kravställningen i Teknisk Specifikation (TS) för aktuellt system (SiF).

För varje kravkategori ska följande aspekter sammanvägas, enligt följande figur:

- Tolkade säkerhetsfunktioner, ITSS-D (ref [XX])
- Tillkommande säkerhetsfunktioner, ITSS-D (ref [XX])
- Arkitekturprinciper
- FMV formella Designprinciper
- Designbeslut (ur bl a ISD-strategi, ref XX)
- Driftfall
- Funktionskedjor



Figur 8 Kravarbete

Efter initial kravformulering, bör en riskanalys genomföras. Syftet med denna riskanalys är att identifiera den eventuella risk som vald kravallokering kan ha medfört. En kompletterande exponerings- och konsekvensanalys kan med fördel också göras här.

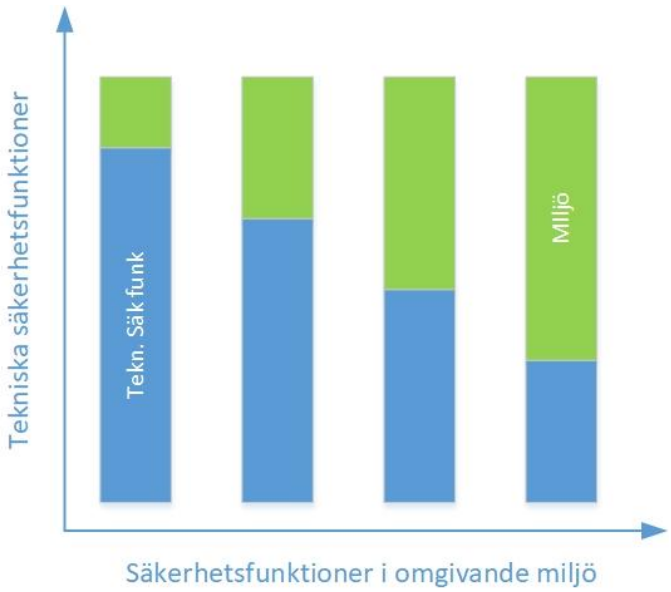
Riskanalysen, och eventuellt exponerings- och konsekvensanalysen, kan dokumenteras här eller i AU-D.

Resultatet från respektive kravkategori är indata till TS. Dessa krav ska också bedömas tillsammans med SE, så att en säker och kostnadseffektiv lösning uppnås.

Observera att ”TS ID” och ”ENV ID” ska vara unikt och att kravformulering i TS och SoW/VÅS ska vara entydig.

Beroende på aktuell driftmiljö är det möjligt att allokera krav på omgivande miljö (ENV ID) istället för det tekniska systemet (TS ID).

Krav på omgivande miljö, vilka uppkommer som en följd av aktuell system- och säkerhetsarkitektur förtecknas i respektive tabell nedan, för att sedan sammanställas i ITSS-D.



Figur 9 Kravuppfyllnad i miljö vs tekniska säkerhetsfunktioner

5.1 Behörighetskontroll

5.1.1 Krav på system

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 55 – TS krav Behörighetskontroll

5.1.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 56 – Krav Behörighetskontroll på miljön

5.2 Säkerhetsloggning

5.2.1 Krav på systemet

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 57 – TS krav Säkerhetsloggning

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

5.2.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 58 – Krav Säkerhetsloggning på miljön

5.3 Intrångsskydd

5.3.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 59 – TS krav Intrångsskydd

5.3.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 60 – Krav Intrångsskydd på miljön

5.4 Intrångsdetektering

5.4.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 61 – TS krav Intrångsdetektering

5.4.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 62 – Krav Intrångsdetektering på miljön

5.5 Skydd mot skadlig kod

5.5.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 63 – TS krav Skydd mot skadlig kod

5.5.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 64 – Krav Skydd mot skadlig kod i miljön

5.6 Skydd mot obehörig avlyssning

5.6.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 65 – TS krav Skydd mot obehörig avlyssning

5.6.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 66 – Krav Skydd mot obehörig avlyssning i miljön

5.7 Skydd mot röjande signaler/TEMPEST

5.7.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 67 – TS krav Skydd mot röjande signaler/TEMPEST

5.7.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 68 – Krav Skydd mot röjande signaler/TEMPEST i miljön

5.8 Integritetsskydd

5.8.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 69 – Krav på Integritetskontroll

5.8.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 70 – Krav på integritetskontroll i miljön

5.9 Redundans

5.9.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 71 – TS krav på redundans

5.9.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 72 – Krav på redundans i miljön

5.10 Back up

5.10.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 73 – TS krav på back-up/restore

5.10.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 74 – TS krav på back-up/restore i miljön

5.11 Säker tid

5.11.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 75 – TS krav på säker tid

5.11.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 76 – TS krav på säker tid i miljön

5.12 Säkert tillstånd

5.12.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 77 – TS krav på säkert tillstånd

5.12.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 78 – TS krav på säkert tillstånd i miljön

5.13 Övriga säkerhetsfunktioner

5.13.1 Krav på systemet

I följande tabell anges de krav som är relevanta för systemet, och som ska överföras till Teknisk Specifikation.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	TS ID	TS Kravtext

Tabell 79 – TS krav på övriga säkerhetsfunktioner

5.13.2 Krav på miljön

I följande tabell anges de krav som avses lösas med omgivande system, administrativa åtgärder, fysiskt skydd alternativt organisatoriska åtgärder.

Pos	Krav från ITSS-D	Design-, arkitektur- eller funktionskrav	Env ID	Kravtext

Tabell 80 – TS krav på övriga säkerhetsfunktioner i miljön