Datum	Diarienummer	Ärendetyp
2021-06-15	20FMV5903-1:1.3	3.6
	Dokumentnummer	Sida
	3.1.0	1(11)

SYSTGL GRANSKNINGSINSTRUKTION ISD 3.1

Innehåll

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är en generell granskningsinstruktion för rollen SystGL IT-säk (SystemGranskningsLedare IT-Säkerhet) inom ramen för ISD-Processen. Notera att SystG kan genomföra motsvarande granskning på delegat av SystGL. Dokumentet är framtaget för ISD 3.0 men gäller även för ISD 3.1.

Syftet med granskningsinstruktionen är att vara ett stöd till SystGL i samband med anskaffningsprojektets granskning av leverantörerna underlag inför framtagning av ITSS-D och ITSS-R.

ITSS-D tas fram av anskaffningsprojektet inför FMV VHL T3-beslut och ITSS-R tas fram inför FMV VHL T4-beslut.

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Generell granskningsinstruktion SystGL baserad på MUST KSF evalueringsaktiviteter	DAOLO
2021-06-15	1.1	Uppdaterad och anpassad för version 3.1.0 av ISD processen	ULCHR

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

En lista över begrepp och förkortningar återfinns i referens [1].

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] Krav på IT-säkerhetsförmågor hos IT-system v3.1	FM skr 2014-06-13, FM2014-5302:1	n/a

Tabell 2 - Referenser

2 Inledning

2.1 Syfte med evaluering

Syftet med SystGL granskning är att få förtroende för att systemets IT-säkerhetsspecifikation (ITSS-D) är lämplig som specifikation för en systemevaluering. Detta sker genom granskning;

- om ITSS-D på ett korrekt sätt tillämpat KSF säkerhetsmodell för att bestämma nivån på säkerhetskraven
- att ITSS-D är tekniskt sund, icke motsägelsefull och har gjort en riktig tolkning av säkerhetskraven.

Huruvida systemet kan uppfylla dessa säkerhetskrav tas om hand av alla andra assuranskrav.

Syftet med SystGL evaluering av ITSS-R i *Realisera* är att få förtroende för att systemet uppfyller de IT-säkerhetsförmågor som definierats i ITSS-D.

2.2 SystGL uppgifter

SystGL har i ISD 3.1 sin huvudsakliga uppgift i D- och R-faserna, där målet med granskningarna är att säkerställa innehåll och kvalitet i systemets IT-säkerhetsspecifikation.

Samtliga aktiviteter i denna instruktion härstammar från KSF v3.1 (referens [2]).

SystGL kan även granska övriga underlag i *Definiera* (ISD-plan, ISD-I, AU-I samt ISTA), underlag i *Realisera* (ISD-R, AU-R samt VMH-R) men också underlag i *Identifiera* (ISD-Strategi, ISD-I, AU-I samt ITSS-I). Denna granskningsinstruktion omfattar däremot endast aktiviteter riktade mot ITSS-D och ITSS-R.

Under *Vidmakthålla* kan denna instruktion aven användas för att granska ITSS-V där fokus ligger på de förändringar som skett från ITSS-R.

Följande uppgifter ingår i SystGL ska granskning:

- Granska ITSS-D/R kapitel *Inledning* för att säkerställa att inledning entydigt identifierar en viss version av ITSS, och refererar till en specifik version av system och version av KSF, samt att den innehåller en övergripande och korrekt högnivåbeskrivning av systemet.
- Granska ITSS-D/R kapitel *Systembeskrivning* för att säkerställa att systembeskrivningen ger en detaljerad beskrivning av systemet och att den information som användas för att fastställa kravnivå utifrån KSF säkerhetsmodellen finns dokumenterad.
- Granska ITSS-D/R kapitel *Sammanställning av säkerhetskrav* för att säkerställa att alla säkerhetskrav som gäller för systemet är identifierade korrekt utifrån KSF-modellen eller utifrån tillkommande säkerhetskrav.
- Granska ITSS-D/R kapitel *Säkerhetskrav på omgivningen* för att säkerställa att alla säkerhetskrav för systemets miljö är identifierade och beskrivna.
- Granska ITSS-D/R kapitel *Tolkning av säkerhetskrav* för att säkerställa att beskrivningen visar en komplett kravbild för systemet och ange kravtolkningen utifrån de krav som identifierades i ITSS kapitlet *Sammanställning av säkerhetskrav*.

- Granska ITSS-R kapitel *Uppfyllande av säkerhetskrav* för att säkerställa att alla funktionella säkerhetskrav som identifierats hanteras av systemet.

2.3 Redovisning av granskningsaktiviteter

Dokumentation av granskningsaktiviteterna redovisas i en kopia av detta dokument eller i en separat rapport.

ISM eller PL ska söka SystGL samråd innan T4-beslut, där SystGL redovisar utfallet från oberoende granskning av ITSS-R, i ISD-R inför framtagning av ISD (deklarationen)

3 Granskningsaktiviteter

3.1 Granskning av ITSS Inledning

Inledning ska innehålla en övergripande och korrekt beskrivning av systemet som omfattar följande:

- En referens som identifierar ITSS.
- En referens som identifierar systemet och som visar att ITSS på ett acceptabelt sätt representerar KSF-krav och andra kravdokument som systemet uppfyller.
- En systemöversikt som kortfattat beskriver systemets användning, arkitektur och säkerhetsfunktioner.

Nr	Aktivitet	Källkrav
Inl.1	SystGL ska verifiera att informationen i ITSS kapitel **Inledning** möter alla krav på innehåll och presentation.	SASS_INL.E1

Tabell 3 – SystGL aktiviteter för granskning av ITSS Inledning

3.1.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Inl.2	Inledningen ska bestå av ITSS-referens, systemreferens och systemöversikt.		SASS_INL.C2
Inl.3	ITSS referensen ska entydigt identifiera ITSS.		SASS_INL.C3
Inl.4	IT-systemreferens ska entydigt identifiera systemet IT-systemreferens ska identifiera versionen på KSF-krav, samt vilken kravnivå, som ITSS anger att systemet ska uppfylla.		SASS_INL.C4
Inl.5	IT-systemreferens ska identifiera styrande dokument, internationella standarder samt andra säkerhetsrelaterade dokument som ITSS anger att systemet ska uppfylla.		SASS_INL.C5
Inl.6	IT-systemreferens ska visa vilka säkerhetskrav i den aktuella kravsamlingen som systemet och dess komponenter ska uppfylla.		SASS_INL.C6
Inl.7	Systemöversikt ska beskriva systemets användning och säkerhetsmekanismer i systemet på en hög nivå		SASS_INL.C7

Tabell 4 –ITSS Inledning – krav på innehåll och presentation

3.2 Granskning av ITSS Systembeskrivning

Systembeskrivningen ska beskriva systemet på ett sådant sätt att man ur systembeskrivningen kan identifiera vilka KSF-krav som gäller, men också att man förstår hur systemet ska användas och hur det ska samverka med sin omgivning. Därmed måste förutsättningar för systemet, dess arkitektur, gränsytor och säkerhetsförmågor beskrivas.

Nr	Aktivitet	Källkrav
Sys.1	SystGL ska verifiera att informationen i ITSS kapitel **Systembeskrivning** möter alla krav på innehåll och presentation.	SASS_SYS.E1

Tabell 5 – SystGL aktiviteter för granskning av ITSS Systembeskrivning

3.2.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Sys.2	Systembeskrivningen ska beskriva vilken information som hanteras i systemet samt konsekvenserna som skulle uppstå vid förlust av denna information.		SASS_SYS.C1
Sys.3	Systembeskrivningen ska beskriva systemets exponering.		SASS_SYS.C2
Sys.4	Beskrivning av information, konsekvens och systemets exponering ska ske med termer som KSF använder och som möjliggör att KSF-kraven kan baseras på dessa faktorer.		SASS_SYS.C3
Sys.5	Systembeskrivningen ska beskriva systemets tänkta användning, användare av systemet och information som ska lagras, bearbetas, överförs i eller utförs ut ur systemet.		SASS_SYS.C4
Sys.6	Systembeskrivningen ska beskriva systemets fysiska avgränsning, och alla externt åtkomliga gränsytor.		SASS_SYS.C5
Sys.7	Systembeskrivningen ska beskriva syfte och användningssätt för alla externt åtkomliga gränsytor.		SASS_SYS.C6
Sys.8	Systembeskrivningen ska beskriva systemets arkitektur och design och ska identifiera de komponenter som systemet består av.		SASS_SYS.C7
Sys.9	Systembeskrivningen ska tydligt identifiera de komponenter som är säkerhetsrelevanta.		SASS_SYS.C8
Sys.10	Systembeskrivningen ska för alla externt åtkomliga gränsytor innehålla en beskrivning av vilka individuella komponenter som utgör gränsytan.		SASS_SYS.C9
Sys.11	Systembeskrivningen ska beskriva systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller		SASS_SYS.C10
Sys.12	Beskrivningen av systemets förmågor ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS.		SASS_SYS.C11

Tabell 6 –ITSS Systembeskrivning – krav på innehåll och presentation

3.3 Granskning av ITSS Sammanställning av säkerhetskrav

Sammanställningen av systemets alla säkerhetskrav identifieras utifrån KSF säkerhetsmodell och andra analyser som måste genomföras. Den ska visa att KSF säkerhetsmodell tillämpats i enlighet med kapitlet Systembeskrivning och att alla funktionella säkerhetskrav och assuranskrav identifierats och dokumenterats. Den ska även visa inte bara att alla säkerhetskrav identifierats, utan även att all säkerhetskrav antingen grundas i KSF-modellen eller har identifierats genom andra analyser och kravställningar.

Nr	Aktivitet	Källkrav
Krv.1	SystGL ska verifiera att informationen i ITSS kapitel **Sammanställning av säkerhetskrav** möter alla krav på innehåll och presentation.	SASS_KRV.E1

Tabell 7 – SystGL aktiviteter för granskning av ITSS Sammanställning av säkerhetskrav

3.3.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Krv.2	Sammanställningen av säkerhetskrav ska identifiera de krav som kommer från KSF och de krav som är tillkommande säkerhetskrav		SASS_KRV.C1
Krv.3	Sammanställningen av KSF-krav ska beskriva kravnivån för alla krav, alla därav gällande kravkomponenter, både de som uppfylls av systemet och de som ska uppfyllas av systemets omgivning.		SASS_KRV.C2
Krv.4	Sammanställningen av KSF-krav ska beskriva kravnivå för assuranskrav och alla gällande kravkomponenter.		SASS_KRV.C3
Krv.5	Tillkommande säkerhetskrav ska identifiera alla säkerhetsmål som identifierades under andra analyser som genomförts (såsom obligatoriska verksamhetsanalys, säkerhetsanalys, hot-, risk- och sårbarhetsanalys, och författningsanalys)		SASS_KRV.C4
Krv.6	Beskrivningen av KSF-krav och tillkommande säkerhetskrav ska identifiera vilka krav som ska uppfyllas av systemet och vilka som ska uppfyllas av systemets omgivning.		SASS_KRV.C5
Krv.7	Beskrivningen av KSF-krav och tillkommande funktionella krav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS.		SASS_KRV.C6

Tabell 8 –ITSS Sammanställning av säkerhetskrav – krav på innehåll och presentation

3.4 Granskning av ITSS Säkerhetskrav på omgivningen

Vissa säkerhetskrav för systemet är tänkt att vara helt eller delvis uppfyllda genom att utnyttja systemets miljö. Dessa säkerhetskrav måste dokumenteras hur och till vilken grad de är tänkt att uppfyllas med hjälp av säkerhetskrav på omgivningen, med en detaljnivå motsvarande säkerhetskravens kravkomponenter.

Granskningen ska visa att alla nödvändiga förutsättningar på systemets miljö är identifierade och att alla säkerhetskrav som gäller för systemets miljö identifierats och dokumenterats. Dessa förutsättningar ska formuleras som säkerhetskrav på omgivningen i VMH-R (bilaga 3 till ISD-R) så att de entydigt kan omsättas i systemets miljö.

Nr	Aktivitet	Källkrav
Omg.1	SystGL ska verifiera att informationen i ITSS kapitel S**äkerhetskrav på omgivningen** möter alla krav på innehåll och presentation.	SASS_OMG.E1

Tabell 9 – SystGL aktiviteter för granskning av ITSS Säkerhetskrav på omgivningen

3.4.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Omg.2	Säkerhetskraven på omgivningen ska identifiera och beskriva alla förutsättningar på systemets miljö som är nödvändiga för att systemet ska kunna uppfylla sina säkerhetskrav.		SASS_OMG.C1
Omg.3	Säkerhetskraven på omgivningen ska beskriva fysiska, administrativa samt organisatoriska åtgärder i systemets miljö som helt eller delvis uppfyller säkerhetskraven för systemets miljö		SASS_OMG.C2

Nr	Krav på innehåll	Utlåtande	Källkrav
Omg.4	Säkerhetskraven på omgivningen ska identifiera säkerhetskrav och de funktionella säkerhetskrav för systemet som härrör från KSF och de helt eller delvis omhändertas av systemets miljö		SASS_OMG.C3
Omg.5	Beskrivningen av säkerhetskraven för systemets miljö ska tydligt visa vilka krav som uppfylls av systemet och vilka som uppfylls av systemets miljö		SASS_OMG.C4
Omg.6	Beskrivningen av säkerhetskraven för systemets miljö ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS		SASS_OMG.C5

Tabell 10 –ITSS Säkerhetskrav på omgivningen – krav på innehåll och presentation

3.5 Granskning av ITSS Tolkning av säkerhetskrav

Säkerhetskraven för systemet måste tolkas (nedbrytas) på ett systemspecifikt sätt så att de konkret kan omsatts av systemet. Då de funktionella säkerhetskraven i KSF är formulerade på en allmän nivå som gör dem generellt användbara, måste man precisera dessa säkerhetskrav för varje system för att kunna beskriva en sammanställd kravbild för systemet. Tolkningen av säkerhetskraven ska vara så entydig att den kan användas som grund för en systemdesign. Tolkningen av säkerhetskrav innebär att visa att KSF-kraven preciseras.

Detta innebär att SystGL måste verifiera om det preciserade KSF-kravet är mer strikt än det ursprungliga KSF-kravet.

Det kan vara så att vissa funktionella krav uppfylls till viss del av systemet och till viss del av dess omgivning, eventuell i samverkan mellan systemet och dess omgivning. De tolkade kraven måste vara så att de entydigt identifierar vilka krav som gäller för systemet och vilka krav som gäller dess omgivning.

Nr	Aktivitet	Källkrav
Tol.1	SystGL ska verifiera att informationen i ITSS kapitel **Tolkning av säkerhetskrav** möter alla krav på innehåll och presentation.	SASS_TOL.E1

Tabell 11 – SystGL aktiviteter för granskning av ITSS Tolkning av säkerhetskrav

3.5.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Tol.2	Tolkningen av säkerhetskrav ska beskriva tolkningen av alla säkerhetskrav för systemet.		SASS_TOL.C1
Tol.3	Tolkningen av säkerhetskrav ska precisera funktionella säkerhetskrav så att de tolkade kraven är testbara och att en design kan verifieras mot tolkningen av kravet.		SASS_TOL.C2
Tol.4	Tolkningen av säkerhetskraven måste vara lika strikt eller mer strikt än de ursprungliga kraven, oavsett om kraven kommer från KSF eller är tillkommande säkerhetskrav.		SASS_TOL.C3
Tol.5	Beskrivningen av tolkningen av KSF-krav och tillkommande säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS.		SASS_TOL.C4

Tabell 12 –ITSS Tolkning av säkerhetskrav – krav på innehåll och presentation

3.6 Granskning av ITSS Uppfyllande av säkerhetskrav

Nr	Aktivitet	Källkrav
Upf.1	SystGL ska verifiera att informationen i ITSS kapitel **Uppfyllande av säkerhetskrav** möter alla krav på innehåll och presentation.	SASS_UPF.E1

Tabell 13 – SystGL aktiviteter för granskning av ITSS Uppfyllande av säkerhetskrav

Notera att gransknings av uppfyllande av säkerhetskraven endast görs för ITSS-R.

3.6.1 Krav på innehåll och presentation

Nr	Krav på innehåll	Utlåtande	Källkrav
Upf.2	Uppfyllande av säkerhetskrav ska visa hur alla säkerhetskrav i kapitlet Tolkning av säkerhetskrav har uppfyllts av systemets säkerhetsfunktioner.		SASS_UPF.C1
Upf.3	Uppfyllande av säkerhetskrav ska visa att alla krav fullständigt uppfylls av systemet.		SASS_UPF.C2
Upf.4	Uppfyllande av säkerhetskrav ska för varje krav visa att hela kravet har uppfyllts av systemet.		SASS_UPF.C3
Upf.5	Beskrivningen av uppfyllandet av säkerhetskrav ska vara tydlig, konsekvent och överensstämma med andra delar av ITSS		SASS_UPF.C4

Tabell 14 –ITSS Uppfyllande av säkerhetskrav – krav på innehåll och presentation