Instruktion granskning systemsäkerhet och HFI Led

Innehåll

[Instruktion granskning systemsäkerhet och HFI Led 1](#_Toc163809211)

[Allmänt 2](#_Toc163809212)

[Granskningsanvisningar 2](#_Toc163809213)

[Anvisning för granskning 2](#_Toc163809214)

[Värdering av kommentarer 3](#_Toc163809215)

[Rekommendation kring behov av ny granskning 4](#_Toc163809216)

[Stödjande information 4](#_Toc163809217)

[Checklista 4](#_Toc163809218)

# Allmänt

Föreliggande instruktion är en del av TC Led designsäkringssystem. Dokumentet utgör en instruktion och en checklista för granskning av systemsäkerhetsunderlag, inklusive HFI, inom ramen för OSG (Oberoende Systemgranskningsfunktion) vid LedM. Dokumentet kan även användas som ett stöd vid framtagning av systemsäkerhetsunderlag.

# Granskningsanvisningar

## Anvisning för granskning

För rätt förståelse av denna instruktion erfordras kännedom om innehållet i Teknisk Chef Ledningssystem Handlingsregler (TC Led HR) inom området.

* Granskaren (SystG/Systemgranskare eller SystGL/Systemgranskningsledare) ska kunna hävda ett oberoende vid granskning
* Granskaren ska presentera sitt granskningsutlåtande i en Granskningsrapport.
* Granskaren ska i rapporten tydligt ange vilket underlag som är granskade. Åtminstone huvuddokumentet ska vara angivet med följande om tillgängligt: titel, dokument/diarienummer, datum, version/utgåva.
* Granskaren ska i rapporten ange att arbetet är utfört inom ramen för OSG (Oberoende systemgranskningsfunktion) systemsäkerhet Led.
* Granskaren ska i rapporten kort beskriva det granskade systemet.
* Granskaren ska i utlåtandet ange en kort övergripande beskrivning kring det granskade underlaget, exempelvis ange om processen följs, huvudsakligen/delvis eller inte följs eller annat som är lämpligt i en kort sammanfattning.
* Granskaren ska i utlåtandet ange granskningskommentarer över funna brister eller sådant som granskaren anser vara värt att notera.
* Kommentar ska vara så utformade att mottagaren ska kunna förstå brister som föranleder respektive kommentar. Sådana kommentarer kan ha bristbeskrivningar som börjar med ”Bristen är ….”
* Granskaren får inte bestämma någon särskild lösning i respektive kommentar. Samtidigt kan granskaren, om lämpligt, stödja med förslag på möjliga handlingsvägar för åtgärder. Granskningskommentarer bör så långt som möjligt utformas så att det blir förståeligt vad som kan vara en eller flera acceptabla åtgärder.
* Granskaren ska i utlåtandet ange för vilka kommentarer som åtgärder förordas eller rekommenderas. Detta kan göras separat för respektive kommentar eller generellt. Skrivningen ska ha följande innebörd: Åtgärdande av kommentarer rekommenderas regelmässigt för åtminstone nivå ”Störande” samt ”Allvarlig” i av FMV framtagna underlag samt nivå ”Allvarlig” i av leverantör framtagna underlag. Övriga identifierade brister, t.ex. sådana som klassats som ”Störande” i underlag från leverantör till FMV, har lägre krav på åtgärd (bör åtgärdas).
* Rätt terminologi för åtgärd, ”ska” respektive ”bör”, ska användas kopplat till kommentarens klassning (”Allvarlig”, ”Störande” respektive ”Skönhetsfel”).
* Granskaren ska i slutgiltig version av rapporten ange lämpligt dokumentnummer, sin funktion (SystG), namn, organisation samt skriva under. Signerad rapport skickas till SystGL, enligt av denne anvisad plats, normalt via e-post i digitalt format.
* Anvisningarna i denna checklista kan tillfälligt eller permanent ändras av SystGL. Ändringarna framförs då normalt skriftligen till godkända SystG.
* Granskaren ska använda checklista under avsnitt 3 som stöd vid granskning. Ifylld checklista kan men behöver inte följa med en granskningsrapport ifrån SystG, om inte SystGL särskilt begär en sådan vid initiering av granskning.

## Värdering av kommentarer

Granskaren ska värdera sina kommentarer med bedömd allvarlighetsgrad, i tre steg: ”Skönhetsfel”, ”Störande”, ”Allvarlig” eller som en ”Notering”.

Följande övergripande ledning ges för värdering av granskningskommentarer.

* *"Allvarlig"* – Kritiska delar saknas, eller har så allvarliga brister att underlaget inte anses kunna accepteras utan åtgärd. TC Led inriktning är att dessa normalt åtgärdas oavsett om de finns i dokument från FMV eller leverantör.  
  Exempel på ”Allvarlig” brist: Otydlighet gällande risker. Beskrivning av grundläggande förutsättningar som t.ex. användningsmiljö eller gränsytor saknas i underlaget. Avsaknad av kravställt underlag.
* *"Störande"* – Icke försumbara brister, har kännbar negativ påverkan men är inte kritiska eller allvarliga. TC inriktning är att dessa normalt ändras i dokument som fastställs av FMV. I dokument som fastställts av leverantör får det övervägas från fall till fall om FMV ska kräva ändring; om inte ska anmärkningen beaktas i framtida arbete.  
  Exempel på ”Störande” brist: Otydlighet vad gäller giltighet. Bristande spårbarhet, t.ex. gällande DoC.
* *”Skönhetsfel”* – Brister som har minimal negativ påverkan, exempelvis stavfel. TC Led inriktning är att dessa åtgärdas normalt på dokument som FMV fastställer. Om det kräver mycket arbete kan dock anmärkningar på nivån "Skönhetsfel" lämnas utan åtgärd, men ska beaktas i framtida arbete.
* *”Notering”* – Något som granskaren vill kommentera, lyfta fram, men där uppenbara behov av åtgärd inte föreligger.

## Rekommendation kring behov av ny granskning

Granskaren ska ange en rekommendation om hur denne bedömer behovet av en förnyad oberoende granskning, efter ett eventuellt åtgärdande av kommentarer. Vägledning:

* *Ingen ny oberoende granskning rekommenderas.* Detta kan rekommenderas där inga eller endast mindre brister har upptäckts i underlaget. Bristerna ska vara av den art att beslutande instans, utan djupare HFI- och systemsäkerhetskunskap, enkelt kan följa upp eventuella åtgärder.
* *Ny oberoende granskning rekommenderas efter eventuell felrättning om beslutande instans så önskar* (normalt TC/CCB). Detta är en medelnivå, där det i underlaget finns brister som behöver åtgärdas och där åtgärderna kan följas upp av beslutande instans utan djupare HFI- och systemsäkerhetskunskap, dock inte med lätthet.
* *Ny oberoende granskning rekommenderas.* Sådana brister är funna i underlaget att beslutande instans (normalt TC/CCB) skulle behöva ha en djupare HFI- och systemsäkerhetskunskap samt utföra en omfattande granskning för att kunna bedöma underlaget efter åtgärd. Exempel kan vara brist på ett helt dokument, avsaknad av viktiga delar av ett dokument, stor mängd brister generellt, icke sammanhängande underlag och dylikt.

## Stödjande information

Som ett stöd för mottagare av granskningsutlåtanden ska granskaren i sin granskningsrapport införa följande text som beskriver nästkommande processteg:

”Följande information är avsedd som stöd för vidare hantering av ärendet. Observera att detta endast är en sammanfattning; för fullständig och senast uppdaterad information hänvisas till gällande processbeskrivningar.

Denna granskningsrapport anger en rekommendation på vilka förhållanden som minst bör rättas inför ett fastställande. När en förnyad granskning av OSG inte erfordras, är nästa steg i processen normalt att:

* Rätta dokumentationen enligt kommentarer och rekommendation i denna granskningsrapport.
* Beskriva varje rättning på en lagom nivå och sammanställa detta i en separat rättningsrapport. Detta krävs för att CCB skall få ett tydligt uttalande från projektet samt snabbt kunna bilda sig en uppfattning om vilka granskningskommentarer som är åtgärdade och hur det är gjort.
* Lämna in underlaget, OSG granskningsrapport samt rättningsrapport till CCB. Relevant signering ska vara utförd. De delar av underlaget som ska skrivas under av TC Led ska skickas in i pappersoriginal med enkelsidig utskrift i färg.

FMV LedM CCB e-mailadress: ledm-ccb.fmv@fmv.se. Funktionsbrevlåda kopplad till e-mailadressen: FMV LedM CCB (finns i FMV adresskatalog). Postfack: FMV LedM CCB, postställe XXX (kontakta SystGL för aktuell adress).

Dylik obligatorisk information kan med fördel integreras som en del av granskningsrapportens inledande instruktion.

# Checklista

Följande är en checklista för granskaren att använda vid granskning. Granskaren kommenterar normalt respektive punkt. I granskningsrapporten behöver dock inte hela checklistan presenteras.

| Granskningsmoment specifika underlag | Granskarens kommentar |
| --- | --- |
| **Systemsäkerhetsdeklaration (SSD)**  Har TC Led HR nr 102 följts avseende SSD innehåll?  Vid ev. brist på risknivåer från HKV, är det tydligt angivet att FMV har antagit risknivåer?  Kontrollera bland annat att beskrivning av användningsmiljö, användare och gränsytor är tillfyllest exempelvis inomhus, utomhus, temp, fukt mm. är angivet. Att systemsäkerhetsmål samt mål för HFI i form av risknivåer är angivna eller hänvisade till.  Annat? |  |
| **Acceptansbeslut av riskhantering**  I eget dokument eller i ett annat fastställt dokument ska det klart framgå ett acceptansbeslut för hantering av samtliga risker. Det ska för varje enskild risk framgå att den är accepterad, vem som fattar beslutet, personens organisatoriska tillhörighet samt underskrift.  Annat? |  |
| **PHL (Riskkällelista)**  Normalt ska Led PHL instruktion/mall användas, enligt TC Led HR 102. Kontrollera bland annat rimligheten i riskkällebedömning, att beskrivning av användningsmiljö, användare och gränsytor är tillfyllest exempelvis inomhus, utomhus, temp, fukt mm. är angivet. Kontrollera att alla riskkällor är bedömda och att kommentarer finns där sådana kravställts (\*3, \*3b).  Om bedömning av vägval 1-6, analysera utförd bedömning, att det finns bakomliggande kriterier samt rimligheten att dessa uppfylls.  Annat? |  |
| **SCA och SAR**  Är underlaget underskrivet och av rätt instans? Finns det ett tydligt uttalande att systemets säkerhet är acceptabel med hänsyn till gällande lagstiftning samt ställda systemsäkerhetskrav?  Annat? |  |
| **Risklogg**  Kontrollera rimligheten i riskbedömningar, rimliga åtgärder vid riskminskning, saknas det uppenbara risker? Är alla riskkällor som kräver riskbedömning i PHL hanterade som risker i riskloggen? Är HFI och systemsäkerhetsmål komplett angivna, per (antal) system och tidsenhet (kan vara i annan bilaga eller SSD)?  Annat? |  |

| Granskningsmoment generellt | Granskarens kommentar |
| --- | --- |
| **Är materialet konsistent?**  Granskaren granskar i en av denne ansedd rimlig omfattning. |  |
| **Beskrivs samma sak på samma sätt överallt?**  Granskaren granskar i en av denne ansedd rimlig omfattning. |  |
| **Finns det motsägelser mellan olika delar?**  Kontrollera bland annat att risker, stämmer till exempel nummer och allvarlighetsgrad mellan olika tabeller. Kontrollera att olika delar av riskmatriserna/kravställningarna är samstämmiga med varandra. Annat? |  |
| **Fullständighet**  Alla relevanta underlag ska granskas. Finns alla underlag som anges ska finnas?  Är det rätt sammansättning av underlag mot gällande regelverk? Kontrollera bland annat mot TC Led Hr nr 102 samt SSMP och SSPP om tillämpligt.  Normalt ska minst SSD, SCA, SAR, PHL, RL och riskacceptans finnas (se även avsnitt 3).  Annat? |  |
| **Har alla systemsäkerhetskrav beaktats?**  Granskas i en rimlig omfattning. |  |
| **Har alla användningsområden beaktats?**  Granskas i en rimlig omfattning. |  |
| Har man beskrivit användningsområdet på ett bra sätt? |  |
| Är användningsområdet rimligt – kan man med rimlig säkerhet säga att systemet inte kommer att användas på ett annat sätt (utan ett nytt systemsäkerhetsarbete)? |  |
| Är användarbeskrivningarna utformade så att mottagaren kan får en rimlig bild av tillåtna användare?  Är det rimligt att inga andra användare än de angivna kommer att använda systemet? |  |
| Är användarmiljön tydligt angiven? Det ska tydligt framgå inom vilka miljöer som systemet är tillåtet att användas inom. Detta är avgörande information för att bedöma systemets risker samt att minimera risken för felanvändning. |  |
| **Användare**  Är alla användargrupper beskrivna som rimligen kan använda systemet?  Är användarbeskrivningarna utformade så att läsaren bedöms få en bra uppfattning? |  |
| **Finns relevanta styrande dokument redovisade?**  Granskas i en rimlig omfattning. |  |
| **Är rätt styrande dokument utnyttjade**  Exempelvis HR 102. Granskas i en rimlig omfattning. |  |
| **Systemsäkerhetskrav och -mål**  Har alla systemsäkerhetskrav (specifikt uttryckta krav) samt systemsäkerhetsmål (riskmatriser) från styrande dokument beaktats?  Granskas i en rimlig omfattning. |  |
| **Underskrifter**  Kontroll om rätt funktion och person står för underskrift. Kontroll om underlag är underskrivna. Om det med rimlighet kan antas att underlaget skrivs under efter granskning, ges detta som en notering och/eller som en del av granskningsrapportens inledande instruktion (se kap **Fel! Hittar inte referenskälla.** ovan). |  |
| **Riskhantering**  Är systemsäkerhetsmålen, dvs den risknivå som det kravställs emot rimlig för det granskade systemet?  Är riskmatriser utformade på så sätt att det finns en rimlig möjlighet att ta fram system utan att få risker i kategorin ET (Ej Tillåtna)? Exempelvis en riskmatris måste åtminstone ha en riskkategori T eller BT för dödsfall, även om tillåtna frekvensen kan vara mycket låg. |  |
| Verkar antalet risker rimligt för systemet, samt är den antagna systemsäkerhetsnivån för dessa rimlig? |  |
| Är risker för alla områdena beaktade, det vill säga människa, miljö och egendom samt HFI? Ekonomiska skador bör vara angivna med antagna värden i pengar. Frekvenserna bör inte vara angivna med siffervärden, exempelvis (1-10 ggr per år), om inte det finns välgrundade beräkningar, statistik eller motsvarande. |  |
| Är definitionerna rätt utformade för konsekvens samt frekvens? Är sannolikhets/frekvensbedömningar komplett angivna, per (antal) system och tidsenhet? |  |
| Om flera sätt att presentera sannolikhets/frekvenskrav är samtidigt angivna, stämmer dessa mot varandra? Se HSS22 bild 14.3. |  |
| Är alla risker bedömda mot alla skadeklasser? |  |
| Är det för egendomsskador (del i ekonomiska skador) medräknat skador på eget system såväl som skador som det egna systemet kan orsaka på annan utrustning eller annan egendom? |  |
| Framgår det vem som ansvarar/stänger riskhantering i de angivna risknivåerna? (Normalt T=Leverantör, BT=FMV, ET=FM.) |  |
| **Restriktioner**  Stämmer eventuellt angivna restriktioner med definitionen enligt TC Led HR nr 102? |  |
| **Formalia**  Kontroll att rätt nomenklatur används. |  |
| Kontrollera att mindre kända förkortningar finns utskrivna |  |
| Kontroll att rätta identifikationer samt beteckningar används. |  |
| Kontroll om det förekommer eventuella tvetydigheter i underlaget, även mellan olika dokument. |  |
| Kontroll om det förekommer eventuella felstavningar eller felaktigheter i meningsuppbyggnad. Kommenteras särskilt om de kan föranleda missförstånd. |  |
| Kontroll om det finns olämpliga ordval. |  |

FÖRSVARETS MATERIELVERK

*(Digitalt fastställd i Platina/AN)*

Adam Narel

SystGL Systemsäkerhet och HFI Led

Sändlista:

Arkiv