**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*Materielsystem/Projekt***   
Granskningsplan

*Mall för Oberoende granskning: Granskningsplan*

*Huvudsyftet med granskningsplanen är at**t specificera hur granskningsuppdrag, såsom detta definierats i tidigare uppdragsplan, ska realiseras i form av utvärderingsaktiviteter, organisation, dokumentation, tidplan etc.*

*Blå text utgör instruktion och bör tas bort när eget dokument skapas.*

*Information i denna mall syftar i att utgöra ett stöd för eget resonemang. Utformningen är vägledande, inte styrande, och innehåll kan ändras vid behov. Med hänsyn till exempelvis granskningens omfattning, sekretess etc. kan således rubriker läggas till och tas bort, tillvägagångssätt modifieras etc. Detta under förutsättning att ISD-metodik för oberoende granskning [] fortfarande åtföljs, vilken omfattar ISD-processens senare del avseende produktion/leverans och utvärdering av en produkts eller ett systems informationssäkerhet med hänsyn till given kravbild. Tillämpning av aktuell mall förutsätter inblick i denna metodik*

INNEHÅLL

[1 Inledning 5](#_Toc476308564)

[1.1 Bakgrund 5](#_Toc476308565)

[1.2 Syfte 5](#_Toc476308566)

[1.3 Förutsättningar 5](#_Toc476308567)

[1.4 Omfattning 5](#_Toc476308568)

[2 Basfakta 6](#_Toc476308569)

[2.1 Giltighet 6](#_Toc476308570)

[2.2 Informationssäkerhetsklass 6](#_Toc476308571)

[2.3 Revisionshistorik 6](#_Toc476308572)

[2.4 Referenser 6](#_Toc476308573)

[2.5 Definitioner 7](#_Toc476308574)

[3 Granskningsobjekt 8](#_Toc476308575)

[3.1 Översiktlig systembeskrivning 8](#_Toc476308576)

[3.2 Säkerhetsuppbyggnad och granskningspåverkande systemaspekter 8](#_Toc476308577)

[4 Utvärderingsaktiviteter 9](#_Toc476308578)

[4.1 Härledning av utvärderingsaktiviteter 9](#_Toc476308579)

[4.2 Beskrivning av utvärderingsaktiviteter 11](#_Toc476308580)

[4.2.1 Utvärderingsaktivitet Vulnerability scanning 11](#_Toc476308581)

[4.2.2 Utvärderingsaktivitet Penetrationstest 11](#_Toc476308582)

[4.2.3 Utvärderingsaktivitet Dokumentanalys 11](#_Toc476308583)

[4.2.4 Utvärderingsaktivitet Kodgranskning 11](#_Toc476308584)

[4.2.5 Utvärderingsaktivitet Kryptoverifiering 11](#_Toc476308585)

[4.2.6 Utvärderingsaktivitet Funktionstest 11](#_Toc476308586)

[4.2.7 Utvärderingsaktivitet Fuzz-test 11](#_Toc476308587)

[5 Bedömning och avvikelsehantering 12](#_Toc476308588)

[5.1 Bedömningsnivåer. 12](#_Toc476308589)

[5.2 Avvikelsehantering 12](#_Toc476308590)

[6 Organisation 13](#_Toc476308591)

[6.1 Roller 13](#_Toc476308592)

[6.1.1 Utvärderande organisation 13](#_Toc476308593)

[6.1.2 Beställare 13](#_Toc476308594)

[6.1.3 Mottagare 13](#_Toc476308595)

[6.1.4 Utvecklare 14](#_Toc476308596)

[6.1.5 Annan part 14](#_Toc476308597)

[6.2 Kompetens 14](#_Toc476308598)

[6.3 Oberoende 14](#_Toc476308599)

[7 Koordinering av arbete 15](#_Toc476308600)

[7.1 Statusrapporter 15](#_Toc476308601)

[7.2 Avstämningsmöten 15](#_Toc476308602)

[7.3 Arbetsmöten med Utvecklare 15](#_Toc476308603)

[7.4 Projektintern koordinering 15](#_Toc476308604)

[8 Leverans 16](#_Toc476308605)

[8.1 Statusrapporter och mötesprotokoll 16](#_Toc476308606)

[8.2 Granskningsrapport 16](#_Toc476308607)

[9 Tidplan 17](#_Toc476308608)

[10 Assurans och risker 18](#_Toc476308609)

# Inledning

*Allmän beskrivning av, alt. generella uppgifter om, den oberoende granskningen.*

## Bakgrund

*Redogörelse av bakgrund till projektet med hänvisning till Beställares uppdragsplan. Vad ska utföras/levereras, vilka aktörer är involverade etc. Det ska framgå att granskningsuppdraget följer framtagen Metodbeskrivning för oberoende granskning vilken omfattar ISD-processens senare del avseende produktion/leverans och utvärdering av en produkts eller ett systems informationssäkerhet med hänsyn till given kravbild.*

## Syfte

*Beskrivning av syftet med den oberoende granskningen för aktuellt materielsystem/projekt samt vilka resultat/slutsatser som förväntas. Granskningsplanens syfte och innehåll ska presenteras och dess betydelse för granskningsuppdraget tydliggöras. Det ska vidare framgå att planen utgör underlag för Beställaren att ta ställning till inför beslut om granskningsgenomförande.*

## Förutsättningar

*Eventuella beroenden till andra aktiviteter och/eller överordnat projekt noteras här, liksom styrande dokumentation/direktiv för granskningsuppdragets genomförande, såsom uppdragsplan och Metodbeskrivning för oberoende granskning. Normalt omfattar uppdragsplanen samtliga förutsättningar som styr granskningen genom att beskriva granskningens omfattning och syfte samt identifiering av gällande systembeskrivningar, granskningsunderlag, källor till den uppsättning krav som granskningen omfattar/bemöter – t.ex. upprättad Säkerhetsmålsättning och/eller KSF – etc. Om Utvärderare gör kompletteringar av dessa styrande förutsättningar genom egna bedömningar och antaganden ska dessa redogöras för här.*

## Omfattning

*Tydliggörande av granskningsuppdragets/projektets omfattning och avgränsningar. Detta kan exempelvis innefatta systemavgränsningar, begränsningar i granskningsaktiviteter, tänkbara hotagenter/scenarion att beakta etc.*

# Basfakta

*Redogörelse av dokumentuppgifter.*

## Giltighet

*Beskrivning av de yttre villkor som är styrande för granskningsplanens giltighet i form av t.ex. tillgång till överenskommet granskningsunderlag, uppfyllande av åtaganden enligt avsnitt Organisation, eventuellt överenskomna villkor för avbrytande av uppdrag etc. Det ska tydliggöras att granskningsplanen är giltig då den har godkänts av Beställaren och om det under granskningsgenomförandets fortskridande skulle identifieras faktorer som medför att planen ej längre bör följas ska Utvärderaren initiera uppdatering av planen i enlighet med beslut avstämt med Beställaren. Mindre förändringar i tidplanen undantages.*

## Informationssäkerhetsklass

## Revisionshistorik

*Ändringar ska vara spårbara genom att ange status och ändringsbeskrivning i en revisionshistorik. Denna ska omfatta de fastställda utgåvorna av det specifika dokumentet samt de senaste preliminära utgåvorna om dokumentet fortfarande anses vara under omarbetning. Revisionshistoriken ska specifikt tydliggöra om en uppdatering har föranletts av att man under granskningsgenomförandet har identifierat faktorer som medfört att tidigare version ej längre ska följas.*

|  |  |  |
| --- | --- | --- |
| **VERSION** | **DATUM** | **BESKRIVNING** |
|  |  |  |
|  |  |  |
|  |  |  |

## Referenser

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REF.NR** | **BENÄMNING** | **DOK.ID** | **VERSION** | **DATUM** |
| *1* | *Metodbeskrivning för oberoende granskning* | 13FMV5921-11:2 | 2.1 | 20140530 |
| *3* | *Uppdragsplan* |  |  |  |
| *4* | *Systemdokumentation* |  |  |  |
| *5* | *Säkerhetsmålsättning el. motsv.* |  |  |  |
| *6* | *…* |  |  |  |

## Definitioner

| **Term** | **Innebörd/lydelse** |
| --- | --- |
| *Assurans* | *Tillit till att ett systems eller en produkts säkerhetsfunktioner uppfyller specificerade säkerhetskrav* |
| *Hot* | *”Möjlig, oönskad händelse med negativa konsekvenser för verksamheten. (SIS HB 550 Utgåva 3 – ”Hot”)*  *Ett hot är således en källa vilken kan orsaka en oönskad händelse med en negativ konsekvens och därmed generera en risk.* |
| *Informationssäkerhet* | *Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet och spårbarhet.* |
| *ISD* | *Informationssäkerhetsdeklaration* |
| *Oberoende granskning* | *Avser i detta sammanhang utvärdering av en produkts eller ett systems informationssäkerhet med hänsyn till given kravbild.* |
| *Risk* | *”En kombination av sannolikheten för att en händelse skall inträffa och dess konsekvens. (ISO/IEC Guide 73:2002 – ”Risk”)*  *I FM riskhanteringssammanhang innebär risk en systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala.* |
| *Säkerhetsmålsättning* | *Verksamhetens behov av säkerhetsfunktioner* |
| *…* | *…* |

# Granskningsobjekt

*Beskrivning av aktuellt granskningsobjekt.*

## Översiktlig systembeskrivning

*Här ges en översiktlig beskrivning av det materielsystem som utgör föremål för den oberoende granskningen samt hänvisningar till systembeskrivningar/-specifikationer. Även användningsområde, användare/roller och operativ miljö ska beskrivas.*

## Säkerhetsuppbyggnad och granskningspåverkande systemaspekter

*Ange förutsättningar/antaganden avseende:*

* *fysiskt skydd, organisatoriskt skydd, kommunikationsskydd*
* *ev. godkända systemdelar/komponenter*
* *design, källkod*
* *säkerhetsarkitektur, säkerhetsfunktioner*
* *extra granskningsvärda aspekter, kritiska funktioner och gränssnitt*
* *relevanta hotagenter/attackerare, verktyg och kompetens*
* *hot-/riskanalys, säkerhetsmålsättning och/eller KSF eller motsvarande mot vilka granskningen ska genomföras.*
* *relevanta kända sårbarheter*

# Utvärderingsaktiviteter

*Beskrivning av granskningsuppdragets utvärderingsaktiviteter.*

## Härledning av utvärderingsaktiviteter

*Se tabell nästa sida.*   
*Aktuella utvärderingsaktiviteter ska redogöras för med spårbarhet till den uppsättning krav som granskningen omfattar/bemöter, angivna i exempelvis upprättad Säkerhetsmålsättning eller motsvarande. Varje ursprungligt mål/krav ska brytas ned så pass långt så att en bedömning av lämplig uppsättning granskningsaktiviteter är möjlig och eventuella beroenden mellan granskningsaktiviteter och/eller krav ska noteras liksom prioriteter. På detta sätt ska det tydliggöras VARFÖR granskningskraven finns (genom spårbarhet till ursprungliga mål/krav) samt HUR de avses granskas (i form av utvärderingsaktiviteter).*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **UTVÄRDERINGSAKTIVITETER** | | | | | | | |  |
| **URSPRUNGLIGT MÅL/ KRAV** | **FUNKTION FÖR GRANSKNING** | *Vulnerability  scanning* | *Penetrationstest* | *Fuzz-test* | *Dokumentations- analys* | *Funktionstest* | *Kryptoverifiering* | *Kodgranskning* | *…* | **KOMMENTAR** |
| *M1: …* | *K1: ….* | *X* |  |  |  |  |  |  |  |  |
|  | *K2: ….* | *X* |  | *X* |  |  |  |  |  | *OCH-villkor mellan utvärderingsaktiviteter* |
|  | *….* |  |  |  | *X* |  |  |  |  |  |
| *M2: …* | *KX: …* |  | *X* |  |  |  |  |  |  |  |
|  | *KX+1. …* |  |  |  |  | *X* |  |  |  |  |
|  | *…* |  |  |  |  |  |  |  |  |  |
| *M3: …* | *K2: (enligt ovan)* | *X* |  | *X* |  |  |  |  |  | *Koppling till krav … genom…* |
|  | *KX: (enligt ovan)* |  | *X* |  |  |  |  |  |  |  |
|  | *KX+2: …* | *X* | *X* |  |  |  | *X* |  |  |  |
|  | *…* |  |  |  |  |  |  |  |  |  |

## Beskrivning av utvärderingsaktiviteter

*Beskrivning av de utvärderingsaktiviteter som har härletts enligt avsnitt 4.1.*

### Utvärderingsaktivitet Vulnerability scanning

*Beskrivning av utvärderingsaktiviteten i allmänhet och med hänsyn till aktuellt granskningsuppdrag i synnerhet. Följande bör anges:*

* *Hänvisning till avsnitt 3.1 avseende vilka granskningskrav aktiviteten avser granska samt eventuella beroenden mellan dessa och/eller andra utvärderingsaktiviteter.*
* *Målsättning/förväntat resultat, med hänsyn till bakomliggande krav och ursprungsmål/-krav samt beskrivning av händelser som kan bedömas utgöra avvikelser från detta förväntade resultat.*
* *Granskningsmiljö, granskningsverktyg och eventuellt andra resurser.*
* *Omfattning/avgränsning av granskning.*
* *Villkor/kriterium för avslutande av granskning.*

### Utvärderingsaktivitet Penetrationstest

*Enligt ovan.*

### Utvärderingsaktivitet Dokumentanalys

*Enligt ovan.*

### Utvärderingsaktivitet Kodgranskning

*Enligt ovan.*

### Utvärderingsaktivitet Kryptoverifiering

*Enligt ovan*

### Utvärderingsaktivitet Funktionstest

*Enligt ovan*

### Utvärderingsaktivitet Fuzz-test

*Enligt ovan*

# Bedömning och avvikelsehantering

*Beskrivning av gällande bedömningsnivåer för granskningsuppdraget samt hantering vid avvikelser från förväntat/önskat resultat. Om inget annat överenskommits gäller bedömningsnivåerna enligt nedan.*

## Bedömningsnivåer.

De bedömningsnivåer som tillämpas vid säkerhetsgranskningsuppdrag är följande:

Ok / OK – Godkänt/*Pass.*

Observation (O) – Brist/synpunkt som inte påverkar säkerhetsrelaterad funktionalitet. Förändring är inte nödvändig ur säkerhetssynpunkt. Ger inte ett underkännande som resultat från säkerhetsgranskningen./ *Observation or remark that does not have for the security functionality any impact. Updates are not necessary for security reasons. A fail is not given as the result for the security review.*

Minor Remark (Mi) / Mindre Anmärkning – Brist som kan påverka säkerhetsrelaterad funktionalitet, men som bedöms som ej exploaterbar/ mindre kritisk. Förändring rekommenderas. Ger inte enskilt ett underkännande, men ett flertal kan tillsammans ge ett underkännande som resultat från säkerhetsgranskningen./ *A minor remark is a shortage that has for the security functionality some minor impact or a vulnerability that is evaluated as minor and not exploitable. Updates are recommended but not necessary for security reasons. A fail is not normally given as the result for the security review.*

Major Remark (Ma) / Större Anmärkning – Brist som direkt påverkar säkerhetsrelaterad funktionalitet. Förändring krävs. Ger alltid ett underkännande som resultat från säkerhetsgranskningen. */ A major remark is a shortage that has impact for the security functionality or a vulnerability that is evaluated as major and/or exploitable. Updates are necessary for security reasons. A fail is always given as the result for the security review.*

Det sammanfattande resultatet från genomförd säkerhetsgranskning ges enligt:

Godkänt/*Pass*

Underkänt/*Fail*

## Avvikelsehantering

*Beskrivning av hur händelser enligt ovanstående bedömningsnivåer ska hanteras. Händelser bedömda enligt Större Anmärkning bör lämpligtvis rapporteras snarast möjligt till FMV. Om eventuella villkor för avbrytande av granskningsuppdrag baserat på granskningsresultat har definierats ska även detta beskrivas, liksom hantering av eventuella omgranskningar. I övrigt ska granskningsresultat i allmänhet men avvikelser i synnerhet dokumenteras i slutlig granskningsrapport med en tydlig beskrivning av vari skillnaden mellan verkligt och förväntat resultat består i, bedömd risk och hur denna skulle kunna nyttjas samt resulterande säkerhetspåverkan och eventuella förslag på hantering.*

# Organisation

*Beskrivning av granskningsuppdragets organisation och ansvariga personer för aktuella roller. Detta omfattar utöver Utvärderande organisation även Beställare, Mottagare och eventuellt Utvecklare och/eller annan part. För Utvärderande organisation ska specifikt oberoende/obundenhet redogöras för liksom kompetens hos samtliga involverade.*

## Roller

### Utvärderande organisation

*Samtliga involverade personer inom den utvärderande organisationen ska presenteras. Det ska specifikt framgå vem som ytterst ansvarar för att granskningen genomförs i enlighet med denna plan samt vem/vilka som utgör kontaktperson(-er) vid avstämningsmöten eventuella tekniska diskussioner etc.*

### Beställare

*Kontaktperson(-er) vid avstämningsmöten, eventuella tekniska diskussioner etc. ska anges. Därtill ska ansvarig för Beställarens åtagande enligt nedan anges:*

* *Godkännande av granskningsplan samt initiering av granskningsgenomförande enligt denna.*
* *Involvering av Mottagare då så är lämpligt, t.ex. vid utvärdering/godkännande av granskningsplan, avstämningsmöten etc.*
* *(Vid behov) involvering av Utvecklaren för tekniskt stöd till Utvärderaren, erhållande av systemdokumentation, utvecklingsmiljö etc.*
* *Tillhandahållande av erforderligt granskningsunderlag i form av t.ex. uppdragsplan, systemdokumentation, säkerhetsmålsättning eller motsvarande och, om överenskommet, även tillhandahållande av granskningsmiljö, verktyg och andra resurser.*
* *Beslutande avseende avbrytande av granskningsuppdrag eller uppdatering av granskningsplan, enligt villkor i granskningsplan och avstämning med Utvärderare.*

### Mottagare

*Om direktkontakt mellan Mottagare och Utvärderare är överenskommet och avstämt med Beställaren ska detta beskrivas här och kontaktperson anges. I övrigt bör Mottagares åtagande- i dialog med Beställare – omfatta avstämning av granskningsplan och granskningsresultat, deltagande vid avstämningsmöten och framförande av eventuella synpunkter som påverkar granskningsuppdragets omfattning eller genomförande till. Kontaktperson/ansvarig ska, om identifierat, namnges.*

### Utvecklare

*Utvecklarens eventuella deltagande i granskningsuppdraget ska presenteras, liksom kontaktperson. Sådant deltagande kan bestå i att tillhandahålla Utvärderaren granskningsunderlag och/eller tillgång till gransknings-/utvecklingsmiljö samt bistå med teknisk kompetens.*

### Annan part

*Vid eventuellt deltagande av annan part i granskningsuppdraget ska dennes roll och ansvar beskrivas och kontaktperson anges.*

## Kompetens

*Kompetens hos samtliga involverade inom den granskande organisationen ska redogöras för. Utöver eventuella specifika krav ska redovisad kompetens vara motiverad utifrån granskningskompetens, granskningsobjektet och dess teknikområde, kompetens avseende de eventuella verktyg och granskningsmiljöer som är aktuella etc.*

## Oberoende

*Redogörelse av den granskande organisationens oberoende till utvecklingen av granskningsobjektet.*

# Koordinering av arbete

*Beskrivning av extern koordinering i form av regelbundna/överenskomna avstämningar och projektmöten med beställare samt arbetsmöten med utvecklare och intern koordinering mellan granskningsprojektets olika aktiviteter.*

## Statusrapporter

*Beskrivning av den statusrapportering som Utvärderaren ansvarar för och som överenskommits med Beställaren. Vid identifiering av faktorer som kan innebära att granskningsplan ej längre bör följas eller identifiering av allvarliga brister eller andra villkor för avbrytande av uppdrag ska detta rapporteras snarast möjligt.*

## Avstämningsmöten

*Beskrivning av de avstämningsmöten som överenskommits med Beställaren och eventuellt Mottagaren, till vilka Utvärderaren kallar och protokollför. Ytterligare avstämningsmöten kan efter överenskommelse med Beställaren bli aktuella, t.ex. vid identifiering av faktorer som kan ha påverkan på granskningsuppdragets fortskridande. Beslut i form av exempelvis uppdateringar av granskningsplan och/eller avbrytande av uppdrag ska dokumenteras.*

## Arbetsmöten med Utvecklare

*Om arbetsmöten med Utvecklare planeras ska dessa beskrivas här.*

## Projektintern koordinering

*Här beskrivs de aktiviteter som Utvärderaren avser utföra i syfte att koordinera de olika utvärderingsaktiviteterna och säkerställa att samtliga granskningsresultat beaktas vid ställningstagande avseende granskningsuppdragets fortskridande och granskningsobjektets säkerhet.*

# Leverans

*Redogörelse för vilka dokument som kommer tas fram och levereras i granskningsuppdraget samt mottagare, sekretesskrav, hantering och ägande av resultat. Det skall vidare framgå att framtagen dokumentation utformas i enlighet med Metodbeskrivning för oberoende granskning och eventuella avvikelser ska motiveras. Granskningsuppdraget bör utöver granskningsplanen minst omfatta leverans av statusrapporter/mötesprotokoll samt granskningsrapport.*

## Statusrapporter och mötesprotokoll

*Beskrivning av de statusrapporter och mötesprotokoll som avses levereras i enlighet med avsnitt 6.1-6.2. Det ska framgå om dessa rapporter/protokoll är av informativt syfte eller om respons från Beställare förväntas, samt i vilken form leveranser av dessa avses ske (t.ex. via e-post). För syfte och innehåll hänvisas till avsnitt 6.1-6.2.*

## Granskningsrapport

*Beskrivning av granskningens slutrapport, i vilken fullföljandet av granskningsarbetet enligt denna plan redogörs för och de slutsatser som kan dras angående granskningsobjektets säkerhet presenteras. Såväl objektiva resultat som Utvärderarens bedömning av granskningsresultaten i sin helhet ska redogöras för, liksom eventuella rekommendationer. Det ska här framgå i vilken form granskningsrapporten avses levereras samt förväntad respons från Beställare.*

# Tidplan

*Ange tidsplan för såväl definierade aktiviteter som in-/utleveranser, och med beaktande av samtliga rollers åtagande.*

# Assurans och risker

*Diskussion kring assurans och granskningsbarhet utifrån bl.a. de prioriteringar som gjorts avseende utvärderingsaktiviteter, granskningsobjektets säkerhetsuppbyggnad, erhållet granskningsunderlags kvalitet, förutsättningar i form av säkerhetsmålsättning eller bakomliggande risk- och sårbarhetsanalys, verksamhetsanalys etc. Om alternativ för genomförande har identifierats ska dessa framgå med indikation på dess säkerhetsrelaterade påverkan på granskningsresultat, liksom dess påverkan på granskningsuppdragets omfattning. Denna information ska vara Beställaren behjälplig vid validitetsbedömning och ställningstagande till genomförande av granskning enligt upprättad granskningsplan.*