**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*Materielsystem/Projekt***   
Granskningsrapport

*Mall för Oberoende granskning: Granskningsrapport*

*Huvudsyftet med granskningsrapporten är att redogöra för fullföljandet av granskningsarbete enligt tidigare upprättad granskningsplan. Erhållna resultat presenteras liksom de slutsatser som utifrån dessa har kunnat dras angående granskningsobjektets säkerhet. Rekommendationer presenteras avseende hantering av granskningsresultat men även säkerhetshöjande rekommendationer avseende granskningsobjektet kan vara aktuella.*

*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 Metodbeskrivning för oberoende granskning [13FMV5921-11:2] fortfarande åtföljs, vilken omfattar ISD-processens senare del avseende produktion/leverans och utvärdering av en produkts eller ett systems IT-säkerhet med hänsyn till given kravbild. Tillämpning av aktuell mall förutsätter inblick i denna metodik*

# SAMMANFATTNING

*Här återges en kort sammanfattning av hela granskningsuppdraget. Sammanfattningen ska omfatta en kortfattad beskrivning av följande:*

* *granskningsobjektet*
* *syfte med granskningsuppdraget*
* *involverade parter i granskningsuppdraget*
* *beskrivning av utförda utvärderingsaktiviteter*
* *identifierade faktorer som har haft påverkan på granskningsgenomförandets fortskridande med hänsyn till ursprunglig granskningsplan*
* *granskningsresultat och eventuella avvikelser*
* *slutsatser avseende granskningsobjektets säkerhet*
* *rekommendationer avseende hantering av granskningsresultat och eventuella säkerhetshöjande rekommendationer avseende granskningsobjektet*

INNEHÅLL

[SAMMANFATTNING 3](#_Toc476301247)

[1 Inledning 5](#_Toc476301248)

[1.1 Syfte 5](#_Toc476301249)

[2 Basfakta 6](#_Toc476301250)

[2.1 Giltighet 6](#_Toc476301251)

[2.2 Informationssäkerhetsklass 6](#_Toc476301252)

[2.3 Granskare 6](#_Toc476301253)

[2.4 Revisionshistorik 6](#_Toc476301254)

[2.5 Referenser 6](#_Toc476301255)

[3 Granskningsgenomförande 8](#_Toc476301256)

[3.1 Genomförda utvärderingsaktiviteter 8](#_Toc476301257)

[3.1.1 Utvärderingsaktivitet Vulnerability scanning 8](#_Toc476301258)

[3.1.2 Utvärderingsaktivitet Penetrationstest 8](#_Toc476301259)

[3.1.3 Utvärderingsaktivitet Dokumentationsanalys 8](#_Toc476301260)

[3.1.4 Utvärderingsaktivitet Kodgranskning 8](#_Toc476301261)

[3.1.5 Utvärderingsaktivitet Kryptoverifiering 8](#_Toc476301262)

[3.1.6 Utvärderingsaktivitet Funktionstest 8](#_Toc476301263)

[3.1.7 Utvärderingsaktivitet Fuzz-test 8](#_Toc476301264)

[3.2 Genomförda arbetsmöten med Utvecklare 8](#_Toc476301265)

[3.3 Genomförd projektintern koordinering 8](#_Toc476301266)

[4 Resultat 9](#_Toc476301267)

[4.1 Resultat från genomförda utvärderingsaktiviteter 9](#_Toc476301268)

[4.1.1 Utvärderingsaktivitet Vulnerability scanning 9](#_Toc476301269)

[4.1.2 Utvärderingsaktivitet Penetrationstest 9](#_Toc476301270)

[4.1.3 Utvärderingsaktivitet Dokumentationsanalys 9](#_Toc476301271)

[4.1.4 Utvärderingsaktivitet Kodgranskning 9](#_Toc476301272)

[4.1.5 Utvärderingsaktivitet Kryptoverifiering 9](#_Toc476301273)

[4.1.6 Utvärderingsaktivitet Funktionsgranskning 9](#_Toc476301274)

[4.1.7 Utvärderingsaktivitet Fuzz-test 9](#_Toc476301275)

[4.2 Sammanställning resultat 9](#_Toc476301276)

[5 Genomförda avstämningar med Beställare 11](#_Toc476301277)

[5.1.1 Statusrapportering 11](#_Toc476301278)

[5.1.2 Avstämningsmöten 11](#_Toc476301279)

[6 Slutsatser 12](#_Toc476301280)

# Inledning

*Här ges en kortfattad beskrivning av aktuellt granskningsobjekt och granskningsuppdrag.   
med hänvisning till tidigare upprättad granskningsplan i vilken granskningens syfte, bakgrund, förutsättningar, organisation, planerade utvärderingsaktiviteter etc. beskrivits detaljerat. Granskningsrapportens syfte, giltighet, revisionshistorik och referenser ska dock presenteras utförligare enligt nedanstående avsnitt.*

## Syfte

*Beskrivning av granskningsrapportens syfte och innehåll. Detta syfte består i såväl redogörelse av fullföljandet av granskning enligt upprättad granskningsplan som presentation av de granskningsresultat, slutsatser och rekommendationer som granskningen resulterat i. Det ska vidare framgå att granskningsrapporten utgör underlag för Beställares/Mottagares slutgiltiga ställningstagande avseende Granskningsobjektets säkerhet.*

# Basfakta

*Redogörelse av dokumentuppgifter.*

## Giltighet

*Det ska här framgå att granskningsrapporten är giltig då den har godkänts av Beställaren.*

## Informationssäkerhetsklass

## Granskare

*Det ska framgå vem/vilka som genomfört granskningen samt tillhörande företag.*

## 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.*

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

## Referenser

| **REF.NR** | **BENÄMNING** | **DOK.ID** | **VERSION** | **DATUM** |
| --- | --- | --- | --- | --- |
| *1* | *Metodbeskrivning för genomförande Oberoende granskning* | 13FMV5921-11:3 | 1.1 |  |
| *2* | *Granskningsplan* |  |  |  |
| *3* | *Uppdragsplan* |  |  |  |
| *4* | *Utvärderares granskningsspecifikationer eller motsvarande med detaljerad planering av resp. utvärderingsaktivitet.* |  |  |  |
| *5* | *Utvärderares granskningsprotokoll eller motsvarande med detaljerad information avseende utförd granskningsaktivitet och erhållna resultat.* |  |  |  |
| *7* | *Statusrapporter* |  |  |  |
| *8* | *Mötesprotokoll* |  |  |  |
| *…* | *…* |  |  |  |

# Granskningsgenomförande

*Här redogörs för fullföljandet av granskning enligt upprättad granskningsplan.*

*Granskningsgenomförandet ska beskrivas kortfattat och med avsikt att komplettera upprättad granskningsplan snarare än att upprepa vad som redan angivits i denna. Om skillnader i faktiskt granskningsgenomförande gentemot gällande granskningsplan föreligger, t.ex. då granskningsgenomförande påbörjats i enlighet med tidigare version av granskningsplan ska detta framgå.*

## Genomförda utvärderingsaktiviteter

*Beskrivning av utförda utvärderingsaktiviteter och om dessa bedöms ha uppfyllt sitt syfte. För detaljerad information kan hänvisning göras till Utvärderares eventuella granskningsspecifikationer eller motsvarande där detaljer avseende respektive aktivitets genomförande framgår.*

### Utvärderingsaktivitet Vulnerability scanning

*Enligt ovan.*

### Utvärderingsaktivitet Penetrationstest

*Enligt ovan.*

### Utvärderingsaktivitet Dokumentationsanalys

*Enligt ovan.*

### Utvärderingsaktivitet Kodgranskning

*Enligt ovan.*

### Utvärderingsaktivitet Kryptoverifiering

*Enligt ovan.*

### Utvärderingsaktivitet Funktionstest

*Enligt ovan.*

### Utvärderingsaktivitet Fuzz-test

*Enligt ovan.*

## Genomförda arbetsmöten med Utvecklare

*Beskrivning av de eventuella arbetsmöten med Utvecklare som ägt rum.*

## Genomförd projektintern koordinering

*Beskrivning av de aktiviteter som Utvärderaren har utfört i syfte att koordinera de olika utvärderingsaktiviteterna och säkerställa att samtliga granskningsresultat beaktats vid ställningstagande avseende granskningsuppdragets fortskridande och granskningsobjektets säkerhet.*

# Resultat

*Beskrivning av de granskningsresultat som erhållits vid respektive utvärderingsaktivitet med spårbarhet till granskningsuppdragets ursprungliga mål/krav.*

*Identifierade avvikelser ska beskrivas med en tydlig redogörelse av vari skillnaden mellan verkligt och förväntat resultat består i, en bedömning enligt de bedömningsnivåer som definierats i granskningsplan avseende resulterande säkerhetspåverkan samt eventuella säkerhetshöjande rekommendationer. Om olika utvärderingsaktiviteter påvisar olika resultat avseende ett och samma krav som varit föremål för granskning, ska detta uppmärksammas och analyseras. Likaså ska resultaten för ett granskat krav, vilket har en uttalad koppling till ett annat krav, beaktas även vid analys av detta senare kravs resultat. För mer detaljerad information om avvikelsen hänvisas lämpligen till Utvärderarens testprotokoll eller motsvarande.*

## Resultat från genomförda utvärderingsaktiviteter

### Utvärderingsaktivitet Vulnerability scanning

*Enligt ovan.*

### Utvärderingsaktivitet Penetrationstest

*Enligt ovan.*

### Utvärderingsaktivitet Dokumentationsanalys

*Enligt ovan.*

### Utvärderingsaktivitet Kodgranskning

*Enligt ovan.*

### Utvärderingsaktivitet Kryptoverifiering

*Enligt ovan.*

### Utvärderingsaktivitet Funktionsgranskning

*Enligt ovan.*

### Utvärderingsaktivitet Fuzz-test

*Enligt ovan.*

## Sammanställning resultat

*Se tabell nästa sida.*   
*Erhållna resultat sammanställs i tabellform för tydliggörande av spårbarhet till och påverkan på granskningsuppdragets ursprungliga mål/krav. Bedömningsnivåer enligt granskningsplan nyttjas: OK, O (Observation), Mi (Minor remark/Mindre anmärkning), Ma (Major remark/Större anmärkning).*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **UTVÄRDERINGSAKTIVITETER** | | | | | | | |  |
| **URSPRUNGLIGT MÅL/ KRAV** | **FUNKTION FÖR GRANSKNING** | *Vulnerability  scanning* | *Penetrationstest* | *Fuzz-test* | *Dokumentations- analys* | *Funktionstest* | *Kryptoverifiering* | *Kodgranskning* | *…* | **KOMMENTAR** |
| *M1: …* | *K1: ….* | *OK* |  |  |  |  |  |  |  |  |
|  | *K2: ….* | *OK* |  | *Mi* |  |  |  |  |  | *Olika utvärderingsaktiviteter påvisar olika resultat!* |
|  | *….* |  |  |  | *OK* |  |  |  |  |  |
| *M2: …* | *KX: …* |  | *OK* |  |  |  |  |  |  |  |
|  | *KX+1. …* |  |  |  |  | *OK* |  |  |  |  |
|  | *…* |  |  |  |  |  |  |  |  |  |
| *M3: …* | *K2: (enligt ovan)* | *Mi* |  | *OK* |  |  |  |  |  | *Tidigare identifierad koppling till krav … varför denna mindre avvikelse bör beaktas även vid analys av detta krav!* |
|  | *KX: (enligt ovan)* |  | *Ma* |  |  |  |  |  |  | *Större avvikelse identifierad!* |
|  | *KX+2: …* | *O* | *OK* |  |  |  | *OK* |  |  |  |
|  | *…* |  |  |  |  |  |  |  |  |  |
| *…* | *…* |  |  |  |  |  |  |  |  |  |

# Genomförda avstämningar med Beställare

*Beskrivning av den statusrapportering som har gjorts och de avstämningsmöten som ägt rum under granskningsuppdragets fortskridande. Hänvisningar till avsnitt 1.7 Referenser där samtliga upprättade statusrapporter/mötesprotokoll anges tillämpas lämpligen.*

### Statusrapportering

*Händelser som har haft betydande påverkan på granskningsuppdragets fortskridande och/eller identifierade avvikelser av sådan grad att de har redovisats i dessa rapporter bör kortfattat beskrivas.*

### Avstämningsmöten

*Beslut som har haft betydande påverkan på granskningsuppdragets fortskridande och som dokumenterats i dessa rapporter bör kortfattat beskrivas.*

# Slutsatser

*Beskrivning av de slutsatser som kan dras utifrån erhållna granskningsresultat samt Utvärderarens egen bedömning i sin helhet avseende granskningsobjektets säkerhet, utifrån bedömningsnivåer angivna i granskningsplan (Godkänt/Pass respektive Underkänt/Fail).*

*Rekommendationer till Beställare avseende hantering av resultaten ska presenteras. Sådana rekommendationer kan t.ex. vara att Beställare/Mottagare utifrån utfört granskningsuppdrag bör kunna dra slutsatsen att aktuellt granskningsuppdrag uppfyller alt. ej uppfyller gällande säkerhetskrav eller att viss granskning bör fördjupas innan Beställares/Mottagares slutgiltiga ställningstagande avseende granskningsobjektets säkerhet görs.*