Datum	Diarienummer	Ärendetyp
2018-11-08	18FMV6730	3.6
	Dokumentnummer	Sida
	18FMV6730-8:1.2	1(14)

ISE GRANSKNINGSINSTRUKTION
ISD 3.0

Innehåll

1 Basfakta

1.1 Giltighet och syfte

Detta dokument är en generell granskningsinstruktion för ISD-rollen ISE (Information Security Evaluator).

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

ITSS-R tas fram av anskaffningsprojektet inför FMV VHL S4-beslut.

1.2 Revisionshistorik

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Generell granskningsinstruktion ISE baserad på MUST KSF evalueringsaktiviteter	DAOLO

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

En över begrepp och förkortningar lista 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 evaluering är att få förtroende för att systemet uppfyller de IT-säkerhetsförmågor som definierats i ITSS-D.

Detta uppnås genom att försäkra sig om:

- förtroende för systemutvecklaren och dennes utvecklingsprocesser
- förtroende för arkitekturen, designen och implementation av säkerhetsfunktionerna
- förtroende för att drift- och förvaltningsdokumentation är korrekt och fullständig
- genom sårbarhetsanalys och riskanalys påvisa att systemet, för den tänkta användningen, har tillräckliga IT-säkerhetsförmågor.

Evalueringen har två moment:

- Först krävs underlag från systemutvecklaren som beskriver design, verifieringsaktiviteter, tester och administrativa rutiner, samt underlag som visar att dessa rutiner tillämpas och att tester har utförts.
- Därefter granskas detta underlag av ISE som kontrollerar om underlaget är fullständigt, tydligt och icke motsägelsefullt. Systemet analyseras genom bl.a. verifieringsaktiviteter och testning, för att hitta eventuella sårbarheter. Eventuella kvarstående risker identifieras och beskrivs, så att de vid en ackreditering kan bedömas vara acceptabla eller ej.

2.2 ISE uppgifter

ISD-rollen ISE, Information Security Evaluator, har sin huvudsakliga uppgift i R-fasen. Uppgiften består bland annat av att granska leverantörens (leverantörernas) system- och assuransunderlag och med hjälp av dessa verifiera kravuppfyllnaden samt genomföra olika analyser.

Följande uppgifter ingår i detta arbete, där omfattningen beror på vald kravnivå:

- Granska leverantörens underlag (innehåll och kvalité)
- Verifiera att regler och rutiner är implementerade och efterföljs.
- Analysera säkerhetsarkitekturen
- Upprepa, vid behov, leverantörens tester
- Genomföra egna kompletterande tester
- Genomföra oberoende sårbarhetsanalyser
- Genomföra restriskanalys

Samtliga ISE-aktiviteter ska dokumenteras i AU-R.

Samtliga krav i ITSS-D ska granskas, dvs både de krav som härstammar från KSF v3.1 (referens [2]) och de tillkommande säkerhetskraven som kommer från övriga källor.

Granskningsaktiviteterna grundar sig på de assuranskrav som ställs på evalueraren i KSF 3.1, vilket innebär att de listade aktiviteterna är en generisk förteckning. Den faktiska omfattningen kan dels styras via ISD-Strategi och ISD-plan, dels via tolkning av KSF krav i ITSS-D.

De tillkommande säkerhetskraven, som härrör från andra källor (t ex verksamhetsanalys och risk- och sårbarhetsanalys), kan innebära att andra typer av ISE-aktiviteter behöver genomföras.

2.3 Redovisning av granskningsaktiviteter

Dokumentation av granskningsaktiviteterna redovisas i AU-R och ITSS-R. I AU-R redovisas kravuppfyllnad av assuranskrav och i ITSS-R redovisas IT-systemets kravuppfyllnad.

3 Granskningsaktiviteter

3.1 Kravnivå Grund

ISE ska för kravnivå Grund minst genomföra följande aktiviteter (referens [2]).

3.1.1 Dokumentgranskning

Nr	Aktivitet	Källkrav
D.1	ISE ska verifiera att informationen i dokumentation som beskriver **rutiner och mekanismer för IT system- och komponentleveranser** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_LEV.C1-C2*	SALC_LEV.E1
D.2	ISE ska verifiera att dokumenterade **procedurer för hantering av säkerhetsrelevanta brister** i systemet möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.3	ISE ska verifiera att erforderliga **avtal och processer för att få information kring säkerhetsrelevanta brister** i systemet och ingående komponenter finns och används. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.4	ISE ska verifiera att **installationsdokumentation som beskriver förberedande åtgärder** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_INS.C1-C3*	SAOP_INS.E1
D.5	ISE ska verifiera att **drift- och förvaltningsdokumentation** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_DOK.C1-C8*	SAOP_DOK.E1
D.6	ISE ska verifiera att **instruktioner som möjliggör för drift- och förvaltningsorganisationen att utföra bevakning av brister samt bristkorrigering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_BRK.C1-C8*	SAOP_BRK.E1
D.7	ISE ska verifiera att dokumenterade **administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ÅTK.C1-C5*	SARU_ÅTK.E1
D.8	ISE ska verifiera att **dokumenterade administrativa rutiner för kontroll av kvaliteten på säkerhetsattribut som används för autentisering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ATT.C1-C7*	SARU_ATT.E1
D.9	ISE ska verifiera att dokumenterade **administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_INT.C1-C7 och C10*	SARU_INT.E1
D.10	ISE ska verifiera att dokumenterade **administrativa rutiner för att utföra regelbundna säkerhetsuppdateringar av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UPD.C1-C7*	SARU_UPD.E1
D.11	ISE ska verifiera att dokumenterade **administrativa rutiner för att genomföra konfigurationsstyrning av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_KFG.C1-C3*	SARU_KFG.E1

Nr	Aktivitet	Källkrav
D.12	ISE ska verifiera att **underlag för utbildning** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UTB.C1-C5*	SARU_UTB.E1
D.13	ISE ska verifiera att **analys av testtäckningen för funktionella- och angripartester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_TTK.C1*	SATS_TTK.E1
D.14	ISE ska verifiera att **testdokumentationen avseende funktionella tester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_FUN.C1-C5 och SATS_EVL.C1*	SATS_FUN.E1 SATS_EVL.E1
D.15	ISE ska verifiera att **testdokumentationen avseende utvecklarens angreppstester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_ANG.C1-C5 och SATS_EVL.C1*	SATS_ANG.E1 SATS_EVL.E1
D.16	ISE ska verifiera att **avvikelseanalysen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARA_AVV.C1-C5*	SARA_AVV.E1
D.17	ISE ska verifiera att **informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys** av hela systemet. *Krav på innehåll framgår av SARA_SBH.C1*	SARA_SBH.E1

Tabell 3 – ISE aktiviteter för kravnivå Grund – Dokumentgranskning

3.1.2 Utvecklingssäkerhet

Ingen granskning av leverantörens utvecklingssäkerhet är nödvändig för kravnivå Grund.

3.1.3 Analys

Nr	Aktivitet	Källkrav
A.1	ISE ska använda tillgängliga källor för att **komplettera leverantörens dokumentation**, t.ex. publik sårbarhetsinformation.	SARA_SBH.E2
A.2	ISE ska **analysera**, med hjälp av leverantörens dokumentation och övrig tillgänglig information, systemets komponenter och gränsytor och kartlägga deras beroenden i syfte att **identifiera attackytor** och **eventuella svagpunkter** i arkitekturen.	SARA_SBH.E3
A.3	ISE ska genomföra en **oberoende sårbarhetsanalys** av systemet baserad på arkitektur- och designinformationen, drift- och förvaltningsdokumentation och avvikelseanalysen för att identifiera potentiella sårbarheter i systemet.	SARA_SBH.E4
A.4	ISE ska genomföra **restriskanalys** för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor.	SARA_RRA.E2

Tabell 4 – ISE aktiviteter för kravnivå Grund – Analys

3.1.4 Test

Nr	Aktivitet	Källkrav
T.1	ISE ska, om denne finner det nödvändigt, **upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall överensstämmer med testspecifikationen.**	SATS_EVL.E2

Tabell 5 – ISE aktiviteter för kravnivå Grund - Test

3.1.5 Kontroll

Ingen kontrollaktivitet än normalt nödvändig för kravnivå Grund.

3.1.6 Egenkontroll

Nr	Aktivitet	Källkrav
E.1	ISE ska verifiera att alla andra **evalueringsaktiviteter** är genomförda med godkänt resultat.	SARA_RRA.E1
E.2	ISE ska dokumentera resultatet av **restriskanalysen** i en form och med ett språkbruk som är tydligt och ger den avsedda mottagaren rätt underlag inför beslut om ackreditering.	SARA_RRA.E3

Tabell 6 – ISE aktiviteter för kravnivå Grund - Egenkontroll

3.2 Kravnivå Utökad

ISE ska för kravnivå Utökad minst genomföra följande aktiviteter (referens [2]).

3.2.1 Dokumentgranskning

Nr	Aktivitet	Källkrav
D.1	ISE ska verifiera att informationen i **Systemutvecklingsdokumentationen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_UTV.C1-C4*	SALC_UTV.E1
D.2	ISE ska verifiera att informationen i **dokumentation som beskriver konfigurationsledningssystemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_KFG.C1-C9*	SALC_KFG.E1
D.3	ISE ska verifiera att informationen i dokumentation som beskriver **rutiner och mekanismer för IT system- och komponentleveranser** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_LEV.C1-C3*	SALC_LEV.E1
D.4	ISE ska verifiera att informationen i dokumentation som beskriver **livscykelmodellen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_LCM.C1.C8*	SALC_LCM.E1
D.5	ISE ska verifiera att dokumenterade **procedurer för hantering av säkerhetsrelevanta brister** i systemet möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.6	ISE ska verifiera att erforderliga **avtal och processer för att få information kring säkerhetsrelevanta brister** i systemet och ingående komponenter finns och används. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.7	ISE ska verifiera att **beskrivningen av systemets gränsytor** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_GRÄ.C1-C4*	SADE_GRÄ.E1
D.8	ISE ska verifiera att **beskrivning av systemets säkerhetsarkitektur** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_ARK.C1-C3*	SADE_ARK.E1
D.9	ISE ska verifiera att **dataflödesanalysen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_DFA.C1-C4*	SADE_DFA.E1
D.10	ISE ska verifiera att **designdokumentation** för systemet möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_DES.C1-C1-C5*	SADE_DES.E1
D.11	ISE ska verifiera att **installationsdokumentation som beskriver förberedande åtgärder** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_INS.C1-C4*	SAOP_INS.E1

Nr	Aktivitet	Källkrav
D.12	ISE ska verifiera att **drift- och förvaltningsdokumentation** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_DOK.C1-C8*	SAOP_DOK.E1
D.13	ISE ska verifiera att **instruktioner som möjliggör för drift- och förvaltningsorganisationen att utföra bevakning av brister samt bristkorrigering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_BRK.C1-C8*	SAOP_BRK.E1
D.14	ISE ska verifiera att dokumenterade **administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ÅTK.C1-C7*	SARU_ÅTK.E1
D.15	ISE ska verifiera att **dokumenterade administrativa rutiner för kontroll av kvaliteten på säkerhetsattribut som används för autentisering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ATT.C1-C7*	SARU_ATT.E1
D.16	ISE ska verifiera att dokumenterade **administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_INT.C1-C10*	SARU_INT.E1
D.17	ISE ska verifiera att dokumenterade **administrativa rutiner för att utföra regelbundna säkerhetsuppdateringar av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UPD.C1-C8*	SARU_UPD.E1
D.18	ISE ska verifiera att dokumenterade **administrativa rutiner för att genomföra konfigurationsstyrning av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_KFG.C1-C5*	SARU_KFG.E1
D.19	ISE ska verifiera att **underlag för utbildning** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UTB.C1-C5*	SARU_UTB.E1
D.20	ISE ska verifiera att **analys av testtäckningen för funktionella- och angripartester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_TTK.C1-C3*	SATS_TTK.E1
D.21	ISE ska verifiera att **testdokumentationen avseende funktionella tester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_FUN.C1-C5 och SATS_EVL.C1*	SATS_FUN.E1 SATS_EVL.E1
D.22	ISE ska verifiera att **testdokumentationen avseende utvecklarens angreppstester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_ANG.C1-C5 och SATS_EVL.C1*	SATS_ANG.E1 SATS_EVL.E1
D.23	ISE ska verifiera att **avvikelseanalysen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARA_AVV.C1-C5*	SARA_AVV.E1
D.24	ISE ska verifiera att **informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys** av hela systemet. *Krav på innehåll framgår av SARA_SBH.C1*	SARA_SBH.E1

Tabell 7 - ISE aktiviteter för kravnivå Utökad - Dokumentgranskning

3.2.2 Utvecklingssäkerhet

Nr	Aktivitet	Källkrav
S.1	ISE ska verifiera om **systemutvecklingsdokumentationens säkerhetsåtgärder tillämpas**.	SALC_UTV.E2
S.2	ISE ska verifiera om **konfigurationsledningssystemets säkerhetsåtgärder tillämpas.**	SALC_KFG.E2
S.3	ISE ska verifiera om **livscykelmodellen tillämpas**.	SALC_LCM.E2

Tabell 8 - ISE aktiviteter för kravnivå Utökad – Utvecklingssäkerhet

3.2.3 Analys

Nr	Aktivitet	Källkrav
A.1	ISE ska analysera **beskrivningen av systemets säkerhetsarkitektur** och **verifiera att det inte går att kringgå systemets säkerhetsfunktioner**.	SADE_ARK.E2
A.2	ISE ska använda tillgängliga källor för att **komplettera leverantörens dokumentation**, t.ex. publik sårbarhetsinformation.	SARA_SBH.E2
A.3	ISE ska **analysera**, med hjälp av leverantörens dokumentation och övrig tillgänglig information, systemets komponenter och gränsytor och kartlägga deras beroenden i syfte att **identifiera attackytor** och **eventuella svagpunkter** i arkitekturen.	SARA_SBH.E3
A.4	ISE ska genomföra en **oberoende och metodisk sårbarhetsanalys** av systemet baserad på all tillgänglig information och erfarenhet för att identifiera potentiella sårbarheter i systemet.	SARA_SBH.E5
A.5	ISE ska genomföra **restriskanalys** för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor.	SARA_RRA.E2

Tabell 9 - ISE aktiviteter för kravnivå Utökad - Analys

3.2.4 Test

Nr	Aktivitet	Källkrav
T.1	ISE ska, om denne finner det nödvändigt, **upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall överensstämmer med testspecifikationen.**	SATS_EVL.E2
T.2	ISE ska **analysera systemutvecklarens testfall** och **komplettera** dessa testfall med egna testfall.	SATS_EVL.E3
T.3	ISE ska **genomföra de egna testfallen,** dokumentera resultatet och bekräfta att systemet fungerar enligt specifikation.	SATS_EVL.E4
T.4	ISE ska genomföra **praktiska tester av systemet** för att avgöra om de potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet.	SARA_SBH.E7

Tabell 10 - ISE aktiviteter för kravnivå Utökad - Test

3.2.5 Kontroll

Nr	Aktivitet	Källkrav
K.1	ISE ska **tillämpa åtgärderna i installationsdokumentation** för att verifiera att systemet kan mottagas och installeras på ett säkert sätt genom att **följa beskrivningen** av dem.	SAOP_INS.E2

Tabell 11 - ISE aktiviteter för kravnivå Utökad – Kontroll

3.2.6 Egenkontroll

Nr	Aktivitet	Källkrav
E.1	ISE ska verifiera att alla andra **evalueringsaktiviteter** är genomförda med godkänt resultat.	SARA_RRA.E1

Nr	Aktivitet	Källkrav
E.2	ISE ska dokumentera resultatet av **restriskanalysen** i en form och med ett språkbruk som är tydligt och ger den avsedda mottagaren rätt underlag inför beslut om ackreditering.	SARA_RRA.E3

Tabell 12 - ISE aktiviteter för kravnivå Utökad - Egenkontroll

3.3 Kravnivå Hög

ISE ska för kravnivå Hög minst genomföra följande aktiviteter (referens [2]).

3.3.1 Dokumentgranskning

Nr	Aktivitet	Källkrav
D.1	ISE ska verifiera att informationen i **Systemutvecklingsdokumentationen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_UTV.C1-C2 och C5-C6*	SALC_UTV.E1
D.2	ISE ska verifiera att informationen i **dokumentation som beskriver konfigurationsledningssystemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_KFG.C1-C10*	SALC_KFG.E1
D.3	ISE ska verifiera att informationen i dokumentation som beskriver **rutiner och mekanismer för IT system- och komponentleveranser** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_LEV.C1-C3*	SALC_LEV.E1
D.4	ISE ska verifiera att informationen i dokumentation som beskriver **livscykelmodellen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_LCM.C1-C10*	SALC_LCM.E1
D.5	ISE ska verifiera att dokumenterade **procedurer för hantering av säkerhetsrelevanta brister** i systemet möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.6	ISE ska verifiera att erforderliga **avtal och processer för att få information kring säkerhetsrelevanta brister** i systemet och ingående komponenter finns och används. *Krav på innehåll framgår av SALC_BRK.C1-C10*	SALC_BRK.E1
D.7	ISE ska verifiera att **beskrivningen av systemets gränsytor** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_GRÄ.C1-C4*	SADE_GRÄ.E1
D.8	ISE ska verifiera att **beskrivning av systemets säkerhetsarkitektur** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_ARK.C1-C3*	SADE_ARK.E1
D.9	ISE ska verifiera att **dataflödesanalysen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_DFA.C1-C5*	SADE_DFA.E1
D.10	ISE ska verifiera att **designdokumentation** för systemet möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SADE_DES.C1-C6*	SADE_DES.E1
D.11	ISE ska verifiera att **installationsdokumentation som beskriver förberedande åtgärder** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_INS.C1-C4*	SAOP_INS.E1

Nr	Aktivitet	Källkrav
D.12	ISE ska verifiera att **drift- och förvaltningsdokumentation** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_DOK.C1-C8*	SAOP_DOK.E1
D.13	ISE ska verifiera att **instruktioner som möjliggör för drift- och förvaltningsorganisationen att utföra bevakning av brister samt bristkorrigering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SAOP_BRK.C1-C8*	SAOP_BRK.E1
D.14	ISE ska verifiera att dokumenterade **administrativa rutiner för tilldelning och återkallning av åtkomsträttigheter** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ÅTK.C1-C9*	SARU_ÅTK.E1
D.15	ISE ska verifiera att **dokumenterade administrativa rutiner för kontroll av kvaliteten på säkerhetsattribut som används för autentisering** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_ATT.C1-C7*	SARU_ATT.E1
D.16	ISE ska verifiera att dokumenterade **administrativa rutiner för att upptäcka och spåra intrång och missbruk i systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_INT.C1-C10*	SARU_INT.E1
D.17	ISE ska verifiera att dokumenterade **administrativa rutiner för att utföra regelbundna säkerhetsuppdateringar av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UPD.C1-C8*	SARU_UPD.E1
D.18	ISE ska verifiera att dokumenterade **administrativa rutiner för att genomföra konfigurationsstyrning av systemet** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_KFG.C1-C5*	SARU_KFG.E1
D.19	ISE ska verifiera att **underlag för utbildning** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARU_UTB.C1-C5*	SARU_UTB.E1
D.20	ISE ska verifiera att **analys av testtäckningen för funktionella- och angripartester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_TTK.C1-C5*	SATS_TTK.E1
D.21	ISE ska verifiera att **testdokumentationen avseende funktionella tester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_FUN.C1-C5 och SATS_EVL.C1*	SATS_FUN.E1 SATS_EVL.E1
D.22	ISE ska verifiera att **testdokumentationen avseende utvecklarens angreppstester** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SATS_ANG.C1-C5 och SATS_EVL.C1*	SATS_ANG.E1 SATS_EVL.E1
D.23	ISE ska verifiera att **avvikelseanalysen** möter alla krav på innehåll och presentation. *Krav på innehåll framgår av SARA_AVV.C1-C5*	SARA_AVV.E1
D.24	ISE ska verifiera att **informationen i leverantörens dokumentation är tillräcklig för att utföra en grundlig sårbarhetsanalys** av hela systemet. *Krav på innehåll framgår av SARA_SBH.C1*	SARA_SBH.E1

Tabell 13 - ISE aktiviteter för kravnivå Utökad - Dokumentgranskning

3.3.2 Utvecklingssäkerhet

Nr	Aktivitet	Källkrav
S.1	ISE ska verifiera om **systemutvecklingsdokumentationens säkerhetsåtgärder tillämpas**.	SALC_UTV.E2
S.2	ISE ska verifiera om **konfigurationsledningssystemets säkerhetsåtgärder tillämpas.**	SALC_KFG.E2
S.3	ISE ska verifiera om **livscykelmodellen tillämpas**.	SALC_LCM.E2

Tabell 14 - ISE aktiviteter för kravnivå Utökad – Utvecklingssäkerhet

3.3.3 Analys

Nr	Aktivitet	Källkrav
A.1	ISE ska analysera **beskrivningen av systemets säkerhetsarkitektur** och **verifiera att det inte går att kringgå systemets säkerhetsfunktioner**.	SADE_ARK.E2
A.2	ISE ska använda tillgängliga källor för att **komplettera leverantörens dokumentation**, t.ex. publik sårbarhetsinformation.	SARA_SBH.E2
A.3	ISE ska **analysera**, med hjälp av leverantörens dokumentation och övrig tillgänglig information, systemets komponenter och gränsytor och kartlägga deras beroenden i syfte att **identifiera attackytor** och **eventuella svagpunkter** i arkitekturen.	SARA_SBH.E3
A.4	ISE ska genomföra en **oberoende, metodisk och semiformell sårbarhetsanalys** av systemet baserad på all tillgänglig information och erfarenhet för att identifiera potentiella sårbarheter i systemet.	SARA_SBH.E6
A.5	ISE ska genomföra **restriskanalys** för att identifiera kvarvarande osäkerheter kring systemets IT-säkerhetsförmågor.	SARA_RRA.E2

Tabell 15 - ISE aktiviteter för kravnivå Utökad - Analys

3.3.4 Test

Nr	Aktivitet	Källkrav
T.1	ISE ska, om denne finner det nödvändigt, **upprepa ett representativt antal av systemutvecklarens tester och bekräfta att systemutvecklarens testresultat för dessa testfall överensstämmer med testspecifikationen.**	SATS_EVL.E2
T.2	ISE ska **analysera systemutvecklarens testfall** och **komplettera** dessa testfall med egna testfall.	SATS_EVL.E3
T.3	ISE ska **genomföra de egna testfallen,** dokumentera resultatet och bekräfta att systemet fungerar enligt specifikation.	SATS_EVL.E4
T.4	ISE ska genomföra **praktiska tester av systemet** för att avgöra om de potentiella sårbarheterna kan utnyttjas i den tänkta användningen av systemet.	SARA_SBH.E7

Tabell 16 - ISE aktiviteter för kravnivå Utökad - Test

3.3.5 Kontroll

Nr	Aktivitet	Källkrav
K.1	ISE ska **tillämpa åtgärderna i installationsdokumentation** för att verifiera att systemet kan mottagas och installeras på ett säkert sätt genom att **följa beskrivningen** av dem.	SAOP_INS.E2

Tabell 17 - ISE aktiviteter för kravnivå Utökad – Kontroll

3.3.6 Egenkontroll

Nr	Aktivitet	Källkrav
E.1	ISE ska verifiera att alla **evalueringsaktiviteter** är genomförda med godkänt resultat.	SARA_RRA.E1

Nr	Aktivitet	Källkrav
E.2	ISE ska dokumentera resultatet av **restriskanalysen** i en form och med ett språkbruk som är tydligt och ger den avsedda mottagaren rätt underlag inför beslut om ackreditering.	SARA_RRA.E3

Tabell 18 - ISE aktiviteter för kravnivå Utökad - Egenkontroll