RIKSREVISIONEN

FÖRSVARETS MATERIELVERK (FMV)
115 88 STOCKHOLM

DNR: 3.1.2-2016-0454
BESLUT: 2017-04-18

Försvarets materielverk (FMV)

Granskning av generella IT-kontroller för PLS-systemet vid Försvarets materielverk (FMV)

Som ett led i granskningen av årsredovisningen med syfte att göra uttalanden om denna har Riksrevisionen även granskat rutiner och kontroller inom IT. Granskningen har omfattat systemet PLS som är ett projektledningssystem.

Riksrevisionen har utfört en kartläggning och testning av generella IT-kontroller i och kring systemet som av Riksrevisionen bedöms vara väsentligt för såväl verksamhet som finansiell redovisning. Granskningen har omfattat rutiner och kontroller för systemförändringar och behörighetshantering.

De punkter som är upptagna i denna revisionsrapport är sådana som Riksrevisionen vill fästa ledningens uppmärksamhet på. Iakttagelserna avser endast rutiner och kontroller för det system som har granskats, men eftersom granskningen avser generella IT-kontroller kan iakttagelserna och rekommendationerna vara aktuella att beakta även för andra system inom FMV.

Riksrevisionen önskar information senast 2017-05-22 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

Projektredovisningssystemet PLS är ett verksamhetskritiskt system som är väsentligt för den finansiella redovisningen, resultatredovisningen och för verksamhetens fortlöpande drift. Det är därför viktigt att det finns god intern kontroll i samtliga rutiner kring PLS och även i FMV:s övriga verksamhetskritiska IT-system.

Riksrevisionen bedömer att FMV bör verka för att rutiner för programförändringar är enhetliga och tillämpas med god intern kontroll för samtliga verksamhetskritiska IT-system samt att om möjligt separera åtkomst till utvecklings- och produktionsmiljö.

Riksrevisionen bedömer även att det finns behov av att förbättra FMV:s hantering av behörigheter i PLS både vad gäller rutiner för tilldelning, borttag och uppföljning av

behörigheter samt att ytterligare anpassa systemets behörigheter till att bättre avspegla verksamhetens ansvarsstruktur och behov.

1. Brister i rutiner för programförändringar

1.1 Myndighetsgemensam rutin för programförändringar är inte känd inom myndigheten

Riksrevisionen har under granskningen noterat att det finns en generell ”change process” samt IT-säkerhetskrav framtagna för hantering av programförändringar för IT-system vid IT-staben på FMV. Riksrevisionen gör bedömningen att denna gemensamma processbeskrivning inte är känd inom hela myndigheten eftersom den inte tillämpas för IT-systemet PLS. Vidare har Riksrevisionen noterat att det inte finns någon specifik testmetodik på IT-staben, men att en behovsanalys av detta ska påbörjas. Som ett resultat av att processbeskrivningen inte är känd har Riksrevisionen noterat att det inte alltid finns ett formaliserat godkännande av beställning av programförändringar liksom formaliserat godkännande av produktionssättning. Vidare har Riksrevisionen noterat att test före driftsättning av utvecklade programförändringar inte alltid har genomförts på grund av tidsbrist.

Avsaknad av kunskap och kännedom om en myndighetsgemensam rutin för programförändringar medför att det kan utformas enskilda rutiner för varje system eller att det saknas rutiner samt att arbetssättet inom myndigheten inte blir enhetligt och att befintliga rutiner inte efterlevs. Vidare medförde det att inte testade och godkända förändringar har förts in i PLS produktionsmiljö.

Rekommendation

Riksrevisionen rekommenderar FMV att informera om vilket stöd inom förändringshantering som finns framtaget centralt vad gäller riktlinjer och processer för att öka kunskapen om detta. Vidare bör FMV påtala vikten av att dessa riktlinjer och processer efterlevs inom myndigheten. En testmetodik bör också utformas och implementeras där det framgår vilka krav på test som finns avseende testplaner, testfall och dokumentation av utförda tester. Slutligen bör en process för att följa upp efterlevnad av interna rutiner och processer utformas och implementeras.

1.2 Åtkomst till utveckling- och testmiljöer är inte separerat från produktionsmiljön

Riksrevisionen har, liksom föregående år, noterat att åtkomst till utvecklings- och testmiljöer inte är separerad från produktionsmiljön, dvs. utvecklare har även åtkomst till produktionsmiljön.

Användare med höga behörigheter i båda miljöerna ökar risken att förändringar produktionssätts utan lämpliga tester eller godkännande, med eller utan avsikt.

Rekommendation

Riksrevisionen rekommenderar FMV att, om det är praktiskt möjligt, tillse att separerade arbetsuppgifter upprätthålls genom att utvecklare inte också har skrivrättigheter till produktionsdatabasen. Om detta är praktiskt svårt att genomföra bör en manuell kontroll upprättas där FMV följer upp vilka aktiviteter som utförs av dessa användarkonton med höga behörigheter genom att kontrollera loggar.

2. Brister i rutiner för programförändringar

2.1 Tilldelning av behörigheter godkänns inte alltid av chef

Enligt beslut (16FMV7590-1:1) ska chef kontrollera och godkänna ansökan om behörighet genom att skicka en blankett via e-post till funktionsbrevlådan för behörigheter i PLS. I vårt urval om 30 stickprov saknades det i 7 fall godkännanden från chef.

Tilldelade ej godkända behörigheter ökar risken för att behörigheter inte tilldelas enligt användarens ansvar och arbetsuppgifter och kan leda till otillbörlig åtkomst i PLS.

Rekommendation

Riksrevisionen rekommenderar att FMV säkerställer att rutinen för tilldelning av behörigheter efterlevs.

2.2 Borttag av behörigheter sker inte alltid i samband med att anställda slutar eller byter arbetsuppgift

Riksrevisionen har under granskningen noterat vid stickprovstestning av 30 personer att 17 som avslutat anställning fortfarande var aktiva i PLS. Orsaken till att behörigheter inte tagits bort för personer som slutat är enligt uppgift att det tidigare har varit automatisk överföring från IDHA (LandaID-systemet) till PLS med avslutade personer. Men sedan något år tillbaka då IDHA bytte plattform fungerar inte längre överföringarna (integrationsproblem) mellan IDHA och PLS, vilket upptäcktes först under vår granskning. Enligt uppgift har en efterföljande översyn genomförts av att behörigheter tagits bort för alla anställda som har slutat. Det konstaterades då att det var många anställda som fortfarande hade status aktiv även om de slutat. Den 28 oktober 2016 lästes en fil in i PLS från lönesystemet Palasso med information om vilka anställda som har slutat. Ett beslut ska tas om det ska ske automatiska överföringarna från Palasso till PLS framöver.

En icke ändamålsenlig rutin för borttag av roller och behörigheter i PLS medför otillbörlig åtkomst och att behörigheter inte är i linje med användarens ansvar och arbetsuppgifter.

Rekommendation

Riksrevisionen rekommenderar att rutinen för borttag ses över och formaliseras samt att ansvarsfrågan för borttag tydliggörs.

2.3 Avsaknad av periodisk genomgång av behörigheter i PLS

Riksrevisionen har noterat att ingen periodisk genomgång av behörigheter sker i PLS. Enligt beslut (16FMV7590-1:1) skulle regelbunden uppföljning av behörigheter i PLS systematiserats under hösten 2016.

Utan periodiska genomgångar av behörigheter samt ej tillförlitlig borttagsrutin ökar risken för otillbörlig åtkomst som kan leda till medvetna/omedvetna ändringar som kan påverka den finansiella redovisningen.

Rekommendation

Riksrevisionen rekommenderar att rutiner för periodisk genomgång av samtliga behörigheter i PLS utformas och implementeras. Genomgången bör även omfatta att användarens behörighet är i linje med arbetsuppgifter och ansvar och bör utföras av

närmaste chef. Genomgången bör dokumenteras och en uppföljning bör ske att den är fullständigt utförd.

2.4 Behörighetsmodellen är inte anpassad till verksamheten

En behörighetsmodell togs fram 2013, dock hade inte hänsyn tagits till stödfunktionernas roller i PLS. Ett initiativ har tagits till att utveckla behörighetsmodellen och enligt plan skulle den ha omarbetats under hösten 2016. Riksrevisionen har dock noterat att detta arbete inte har prioriterats under året och att behörighetsmodellen inte är färdigställd. Riksrevisionen noterade även att en detaljerad beskrivning av rollerna i den befintliga behörighetsmodellen inte tagits fram.

Roller som inte är uppdaterade enligt ny behörighetsmodell ökar risken för att behörigheter tilldelas som inte är i linje med arbetsuppgifter och ansvar och kan leda till otillbörlig åtkomst. Avsaknad av beskrivning av roller ökar risken för att felaktiga roller tilldelas och kan leda till otillbörlig åtkomst.

Rekommendation

Riksrevisionen rekommenderar att arbetet med att utveckla behörighetsmodellen slutförs och att detaljerade beskrivningar av samtliga roller utformas.

2.5 Ingen uppföljning av kritiska loggar sker.

Enligt uppgift loggas alla förändringar i PLS. Dock sker, liksom föregående år, ingen uppföljning av dessa loggar regelbundet, endast om behov uppstår. Det är oklart vem som har åtkomst till loggarna.

Otillräcklig loggуppföljning ökar risken för att inte upptäcka otillåten eller oönskad användning av IT-resurser samt att inte upptäcka och snabbt kunna agera på säkerhetsincidenter eller avvikelser mot interna och externa regelverk.

Rekommendation

Riksrevisionen rekommenderar att krav avseende loggning och uppföljning formaliseras samt att rutin för uppföljning införs.

DNR: 3.1.2-2016-0454
BESLUT: 2017-04-18

Ansvarig revisor Tomas Janhed har beslutat i detta ärende. Uppdragsledare Louise Ros har varit föredragande

Tomas Janhed

Louise Ros

Kopia för kännedom:

Regeringen
Försvarsdepartementet