DNR: 32-2014-0537

MYNDIGHETEN FÖR YRKESHÖGSKOLAN
722 12 VÄSTERÅS

BESLUT: 2015-05-18

Myndigheten för yrkeshögskolan – Granskning av rutiner och kontroll för behörigheter och systemförändringar avseende applikation ELLA samt några applikationskontroller

Riksrevisionen har som ett led i den årliga revisionen av Myndigheten för yrkeshögskolan (MYh) granskat rutiner och kontroller för behörigheter och systemförändringar inom IT samt några applikationskontroller för applikationen ELLA. Bakgrunden är att dessa rutiner och kontroller relaterade till ELLA bedöms vara viktiga för att säkerställa en fullständig och korrekt årsredovisning.

Applikationen ELLA används för hantering och handläggning av nya och pågående utbildningar.

Granskningen har resulterat i iakttagelser som Riksrevisionen vill fästa Myndigheten för yrkeshögskolans uppmärksamhet på i denna revisionsrapport.

Riksrevisionen önskar information senast 2015-06-18 med anledning av våra iakttagelser i denna rapport.

Sammanfattning

EY har biträtt Riksrevisionen i denna granskning. EY har avrapporterat sin genomförda granskning till Riksrevisionen. Granskningen visar att kontrollerna för *programförändringar* för ELLA och de *identifierade applikationskontrollerna* överlag är ändamålsenligt utformade och i bruk under 2014. De brister som har identifierats bedöms inte medföra någon väsentlig påverkan på den interna kontrollen för finansiell rapportering, varför den samlade bedömningen är att Riksrevisionen kan förlita sig i stort på de generella IT-kontrollerna för programförändringar och identifierade applikationskontroller.

Vidare visar EYs granskning att kontrollerna för *hantering av behörighet* inte är dokumenterade på en sådan nivå att det är möjligt att bedöma huruvida de är ändamålsenligt utformade och i bruk. De ytterligare insatser (tester) som EY genomfört visar dock att risken för fel på grund av dessa brister är lägre och att de generella IT-kontrollerna sammantaget ger nödvändigt stöd för att Riksrevisionen ska kunna förlita sig på att applikationskontroller i ELLA med rimlig säkerhet fungerat på ett enhetligt sätt under 2014.

RIKSREVISIONEN

NYBROGATAN 55
114 90 STOCKHOLM
08-5171 40 00 | WWW.RIKSREVISIONEN.SE

DNR: 32-2014-0537

MYNDIGHETEN FÖR YRKESHÖGSKOLAN
722 12 VÄSTERÅS

BESLUT: 2015-05-18

1. Iakttagelser från utförd granskning

Det finns, som framgår ovan, iakttagelser avseende främst behörighetshanteringen. Dessa bör åtgärdas för att stärka den interna kontrollen ytterligare. De främsta iakttagelserna och rekommendationerna är:

1.1. Konsulter från driftsleverantören får användare med högsta behörighet som standard

I granskningen noterades att konsulter från driftsleverantören som standard tilldelas högsta behörighet till ELLA och till Active Directory. Att slentrianmässigt tilldela högsta behörighet medför att risken för oegentligheter ökar då den höga behörigheten tillåter att befintliga kontroller kan kringgås.

Rekommendation
Riksrevisionen rekommenderar att MYh bör inventera och dokumentera samtliga användare med höga behörigheter, inklusive tredje part. Vidare bör MYh utvärdera och säkerställa att samtliga användare ges en behörighetsprofil som endast medger den åtkomst som krävs för att lösa personens arbetsuppgifter samt ta bort de behörigheter som bedöms som ej nödvändiga.

1.2. Ej individuella testkonton identifierades i produktionsmiljön

Under granskningen identifierades sju test- och gruppkonton som inte kunde kopplas till en unik individ. Dessa testkonton identifierades i produktionsmiljön, dvs i Active Directory. Det saknas information om vem som har tillgång till dessa konton och om de då får tillgång till konton med högre behörigheter än vad användaren själv har. Användning av ej individuella konton eller gruppkonton omöjliggör spårbarhet av ändringar utförda av användaren. Det ökar även risken för oegentligheter på grund av att medarbetare kan inneha behörigheter som medger otillåtet handlande.

Rekommendation
Vi rekommenderar MYh att se över sina centrala riktlinjer och krav när det gäller användarkonton samt att eliminera användningen av ej individuella konton eller gruppkonton genom att omgående radera dessa och ersätta med personliga konton.

1.3. Spårbarhet i process för behörighetshantering saknas

Vid granskningen av myndighetens hantering av nya användare, användare vars behörigheter modifierats och användare vars behörigheter tagits bort noterades att MYh saknar en formaliserad rutin för behörighetshantering. Det saknas information om vem som begärt, godkänt, skapat eller avslutat ett användarkonto. En otillräcklig behörighetsprocess för styrning av åtkomst till MYh:s system samt stödjande IT-infrastruktur kan innebära ökad risk för obehörig åtkomst till program eller information.

DNR: 32-2014-0537

MYNDIGHETEN FÖR YRKESHÖGSKOLAN
722 12 VÄSTERÅS

BESLUT: 2015-05-18

Rekommendation
Riksrevisionen rekommenderar MYh att dokumentera och fastställa rutiner och riktlinjer för styrning av åtkomst till ELLA samt stödjande IT-infrastruktur.

1.4. Administratorkonto i domänen är aktivt
I granskningen noterades att Administratorkontot i domänen är aktivt, dock är det noterat att i fältet beskrivning för kontot att det ej ska användas. Användare med hög behörighet, såsom Administrator, medges obegränsad åtkomst till systemet eller domänen. Risken för att t.ex. förvanska eller radera affärskritisk information i MYh:s system ökar då den höga behörigheten tillåter att befintliga kontroller kan kringgås.

Rekommendation
Riksrevisionen rekommenderar att MYh bör inventera samtliga användare med höga behörigheter i domänen, inklusive tredje part. Vidare bör MYh säkerställa att Administratorkontot inaktiveras, samt att samtliga användare ges en behörighetsprofil som endast medger den åtkomst som krävs för att lösa arbetsuppgifterna.

1.5. Periodisk genomgång av användare saknas
Vid granskningen noterades att MYh inte genomför några periodiska genomgångar av användare där användarens behörighet bekräftas. Obehörig åtkomst ökar risken för oegentligheter på grund av att medarbetare har behörigheter som medger otillåtet handlande. Det finns även risk för att personer som inte längre jobbar kvar eller har fått ändrade arbetsuppgifter har kvar gamla behörigheter i systemet.

Rekommendation
Riksrevisionen rekommenderar MYh att dokumentera och fastställa rutiner och riktlinjer för periodiska genomgångar av användare. I denna rutin rekommenderas att ansvarig chef utvärderar och säkerställer att samtliga användare innehar en behörighetsprofil som endast medger den åtkomst som krävs för att lösa arbetsuppgifterna samt ta bort de behörigheter som bedöms som övertaliga. Detta bör genomföras minst en gång per år.

Ansvarig revisor Agneta Bergman har beslutat i detta ärende. Uppdragsledare Iréne Lindström har varit föredragande

Agneta Bergman Iréne Lindström

Kopia för kännedom:
Regeringen
Utbildningsdepartementet
Finansdepartementet, budgetavdelningen