ERNST & YOUNG

Till Stockholms Stadshus AB

Revisorsrapport över faktiska iakttagelser

Utvärdering av intern kontroll i utvalda processer inom Volvo Information Technology AB:s leverans till Stockholms Stadshus AB

Rapport över faktiska iakttagelser

Bakgrund

Stockholms Stadshus AB har beslutat att genomföra en granskning av Volvo Information Technology ABs (Volvo IT) utformning och implementering för ett av Volvo IT definierat kontrollramverk. Ernst & Young har fått i uppdrag av ledningen för Stockholms Stadshus att utföra granskning av kontroller för vissa kontrollmål vilka finns specificerade nedan.

Denna rapport är enbart avsedd för att kunna användas av Stockholms Stadshus AB, bolag inom Stockholms Stadshus-koncernen och dess revisorer, och ska inte användas för något annat syfte.

Genomförd granskning

Vi har genomfört överenskomna granskningsåtgärder av intern kontroll kopplat till etablerade kontrollmål för generella IT-kontroller. Vårt uppdrag har utförts enligt svensk revisionsstandard för näraliggande tjänster vilken är tillämplig för uppdrag som avser granskning enligt särskild överenskommelse (Standard för näraliggande tjänster, SNT 4400).

De överenskomna granskningsåtgärderna för verksamhetsåret 2012 har i huvudsak genomförts i december 2012 samt januari 2013 och har varit följande:

1. Genomgång av Volvo IT:s upprättade process- och kontrollbeskrivningar.
2. Genomgång och bedömning av kontrollernas utformning.
3. Test av efterlevnad genom stickprovsanalys.

Samtliga iakttagelser i denna rapport har stämts av skriftligen med berörda parter.

Granskningens omfattning

Granskningen avser Volvo IT:s identifierade kontrollramverk för generella IT-kontroller för Windows-miljön i tjänstekatalog B inom leveransen till Stockholms Stadshus. Test av efterlevnad har genomförts för perioden 1:a januari – 18:e december 2012. Kontrollmoment som åligger Stockholms stad har inte ingått i granskningen.

Vår granskning har omfattat design och implementering av identifierade kontrollaktiviteter enligt Bilaga 1. Resultatet av genomförda granskningsaktiviteter framgår av kolumnen "Bedömning av kontroll" där följande bedömningskriterier har tillämpats:

- Ja - Ernst & Young har, baserat på genomförda granskningsaktiviteter, kunnat iaktta att kontrollen har utförts i enlighet med tillhandahållen kontrollbeskrivning.
- Nej - Ernst & Young har, baserat på genomförda granskningsaktiviteter, inte kunnat iaktta att kontrollen har utförs i enlighet med tillhandahållen kontrollbeskrivning. Detta beror på att underlag från kontrollutförandet inte finns att tillgå. Ernst & Young har dock genom kompletterande granskningsåtgärder kunnat iaktta att kontrollmoment har genomförts som i allt väsentligt motsvarar angiven kontroll.
- Nej - Ernst & Young har, baserat på genomförda granskningsaktiviteter, inte kunnat iaktta att kontrollen har utförts i enlighet med tillhandahållen kontrollbeskrivning. Kompletterande granskning har inte kunnat fastställa kontrollutförande.

Avvikelser samt eventuella övriga kommentarer till vår granskning framgår av kolumnen "Iakttagelser".

I tabellen nedan presenteras Volvo IT:s kontroller för respektive kontrollmål.

Volvo IT:s processer	Volvo IT:s kontroller
Systemförändringsprocessen	
Ge en rimlig säkerhet att samtliga systemförändringar är korrekt beställda, godkända för utveckling, testade och godkända för produktionssättning innan de flyttas in i produktionsmiljön	15C3 - Approval before implementing changes 15C12 - Emergency changes are documented and approved 15C4 - Separation of duties for IT
Behörighetsprocessen	
Ge en rimlig säkerhet att endast behöriga personer och applikationer har åtkomst till data, transaktioner och master data, och då endast för att kunna utföra specifikt tillåtna uppgifter	19C1 - Verify Security Configuration 18C6 - Verify Approvals of User Access 18C2 - Access Rights Revoke 18C1 - Access Rights Review 15C4 - Separation of duties for IT
Driftprocessen	
Ge en rimlig säkerhet att säkerhetskopior skapas och återläsningstester genomförs, schemalagda jobb körs och övervakas, avvikelser rapporteras, samt att problem- och incidentrapporteringen genomförs	21C2 - Verify Integrity of Restored data 22C1 - Monitoring Batch Jobs 22C3 - Monitoring Production Environment

Eftersom de granskningsåtgärder som vidtagits enligt ovan varken är en revision enligt International Standards on Auditing, ISA, eller en översiktlig granskning enligt Standard för översiktlig granskning, SÖG, bestyrker vi inget om kontrollerna ovan.

Om vi hade genomfört ytterligare granskningsåtgärder eller om vi hade utfört en revision enligt ISA eller en översiktlig granskning enligt SÖG skulle andra förhållanden kanske ha kunnat komma till vår kännedom och ha rapporterats till Er.

Vår rapport är enbart avsedd för det syfte som angivits i det första stycket i denna rapport och för Er information, och ska inte användas för något annat syfte eller spridas till andra parter. Rapporten gäller endast de kontroller som angivits ovan och gäller inte någon av Volvo ITs finansiella rapporter i sin helhet.

Stockholm den 13 februari 2013

Björn Rydberg
Auktoriserad Revisor

Bilagor:

1. Resultat av genomförda granskningsåtgärder

Bilaga 1

Generella IT kontroller

Kompletterande information kring bedömning av systemförändringsprocessen:
Granskningen har fokuserat på Volvo IT:s systemförändringsprocess inom Windowsmiljön i tjänstekatalog B i leveransen till Stockholms Stadshus. Ändringar inom processen är indelade i fyra kategorier beroende på omfattning, komplexitet och tidsaspekt. Tidskritiska ändringar delas in i kategorin akuta ändringar, vilka utgör under en procent av det totala antalet ändringar.

	Volvo IT				Ernst & Young	
#	Kontrollmål	Kontroll	Kontrolltyp specifikation	Kontrollfrekvens	Bedömning av kontroll	Iakttagelser
	Systemförändringsprocessen					
1	Att ge en rimlig säkerhet att samtliga systemförändringar är korrekt beställda, godkända för utveckling, testade och godkända för produktionssättning innan de flyttas in i produktionsmiljön	15C3 Approval before implementing changes Systemförändring är beställd för genomförande av behörig person	Kontrolltyp Manuellt IT-beroende Kontrollutförare Volvo IT:s globala WinSec grupp, vilken ansvarar för säkerheten i samtliga Windows-installationer	Händelsestyrt		Inga väsentliga avvikelser noterade.
		15C3 Approval before implementing changes Systemförändringen är testad enligt beslutad testomfattning	Kontrolltyp Manuell Kontrollutförare Volvo IT:s globala WinSec grupp, vilken ansvarar för säkerheten i samtliga Windows-installationer	Händelsestyrt		Inga väsentliga avvikelser noterade.
		15C3 Approval before implementing changes Systemförändringar är korrekt godkända för produktionssättning	Kontrolltyp Manuellt IT-beroende Kontrollutförare Service runtime manager	Händelsestyrt		Inga väsentliga avvikelser noterade.
		15C12 Emergency changes are documented and approved Akuta systemförändringar verifieras i efterhand	Kontrolltyp Manuellt IT-beroende Kontrollutförare Service runtime manager	Händelsestyrt		Vi har noterat att kontrollen inte appliceras i leveransen till Stockholms Stadshus och att akuta ärenden inte kräver godkännande i efterhand. Akuta ändringar utgör en liten del av det totala antalet ändringar.

	Volvo IT				Ernst & Young	
#	Kontrollmål	Kontroll	Kontrolltyp specifikation	Kontrollfrekvens	Bedömning av kontroll	Iakttagelser
		15C3 Approval before implementing changes Översyn av systemförändringsprocess och policy	Kontrolltyp Manuell Kontrollutförare Intern och extern IT-revisor	Årligen		Inga väsentliga avvikelser. Vi har noterat att Volvo IT årligen genomför testning av sitt kontrollramverk för generella IT-kontroller, testningen innefattar dock inte leveransen mot Stockholms stad. Då samma kontroller i stor utsträckning används för leveransen till Stockholms stad bedöms eventuella problem i kontrolluppsättningen trots detta identifieras via Volvo IT:s testning.
		15C4 - Separation of duties for IT Ändamålsenlig ansvarsfördelning existerar inom system-förändringsprocessen	Kontrolltyp Manuell IT-beroende Kontrollutförare Service runtime manager	Händelsestyrt		Inga väsentliga avvikelser har noterats relaterat till normala ändringar. Vi har dock noterat att akuta ärenden i vissa fall hanteras utan ändamålsenlig ansvarsfördelning. Akuta ändringar utgör en liten del av det totala antalet ändringar.

Kompletterande information kring bedömning av behörighetsprocessen:
Granskningen har fokuserat på Volvo IT:s behörighetsprocess inom tjänstekatalog B i leveransen till Stockholms Stadshus och avgränsats till Windows och MS SQL. För att hantera leveransen har Volvo IT ett antal dedikerade lokala team och ett antal globala team. Samtliga användare från Volvo IT har privilegierade rättigheter för att utföra sina arbetsuppgifter. Utöver användare från Volvo IT finns även ett mindre antal privilegierade användare från Stockholms stad. Dessa användare har inte ingått i granskningen.

	Volvo IT				Ernst & Young	
#	Kontrollmål	Kontroll	Kontrolltyp specifikation	Kontrollfrekvens	Bedömning av kontroll	Iakttagelser
	Behörighetsprocessen					
2	Att ge en rimlig säkerhet att endast behöriga personer och applikationer har åtkomst till data, transaktioner och master data, och då endast för att kunna utföra specifikt tillåtna uppgifter	19C1 - Verify Security Configuration Generella systemsäkerhetsinställningar är korrekta baserat på gällande krav	Kontrolltyp IT-beroende Kontrollutförare Volvo IT:s globala WinSec grupp, vilken ansvarar för säkerheten i samtliga Windows-installationer	Händelsestyrt		*Windows och Active Directory* Vi har noterat att Volvo IT inte använder den inbyggda loggfunktionen i Windows utan istället förlitar sig på en annan lösning med samma syfte. Rutin för att granska loggar relaterat till användarkonton i leveransen till Stockholms stad har inte identifierats. Loggdata finns tillgänglig och kan granskas i efterhand i det fall en incident inträffar, detta hanteras enligt Volvo IT:s process för incidenthantering. Vidare har vi noterat att automatisk uteläsning först sker efter 10 misslyckade inloggningsförsök. *MS SQL* Vi har noterat att Volvo IT inte använder den inbyggda loggfunktionen i MS SQL utan istället förlitar sig på en annan lösning med samma syfte.
		19C1 - Verify Security Configuration Lösenordsinställningar är korrekta baserat på gällande krav	Kontrolltyp IT-beroende Kontrollutförare Volvo IT:s globala WinSec grupp, vilken ansvarar för säkerheten i samtliga Windows-installationer	Händelsestyrt		*Windows och Active Directory* Inga väsentliga avvikelser noterade. *MS SQL* Inga väsentliga avvikelser noterade relaterat till användare från Volvo IT. Vi har dock noterat ett flertal användarkonton från Stockholms stad vilka inte följer lösenordspolicyn som satts centralt via Active Directory.
		18C6 - Verify Approvals of User Access Privilegierade rättigheter är begränsade till lämpliga individer	Kontrolltyp Manuell IT-beroende Kontrollutförare Volvo IT:s globala WinSec grupp, vilken ansvarar för säkerheten i samtliga Windows-installationer	Händelsestyrt		Inga väsentliga avvikelser noterade.

	Volvo IT				Ernst & Young	
#	Kontrollmål	Kontroll	Kontrolltyp specifikation	Kontrollfrekvens	Bedömning av kontroll	Iakttagelser
		18C6 - Verify Approvals of User Access Behörighet till stödjande resurser och program för de applikationer som anses prioriterade är begränsad till lämpliga individer	Kontrolltyp Manuellt IT-beroende Kontrollutförare -	-	Ej tillämplig	Kontrollen bedöms inte tillämplig då granskningen är avgränsad till Windows-miljön inom vilken alla användare från Volvo IT har privilegierade rättigheter.
		18C6 - Verify Approvals of User Access Nya behörigheter är beställda av behörig person och tilldelad behörighet är lämplig	Kontrolltyp Manuellt IT-beroende Kontrollutförare Respektive chef	Händelsestyrt		Inga väsentliga avvikelser noterade.
		18C6 - Verify Approvals of User Access Tilldelade behörigheter gås igenom och verifieras periodvis	Kontrolltyp Manuellt IT-beroende Kontrollutförare -	-		Vi har noterat att Volvo IT har en kontroll för periodisk genomgång av behörigheter, denna kontroll täcker dock inte in Volvo IT:s tilldelade behörigheter inom leveransen till Stockholms stad. Vi har genom kompenserande granskningsaktiviteter granskat ett hundratal användare från Volvo IT med privilegierade rättigheter inom leveransen till Stockholms stad och endast funnit två personer vilka inte behövde rättigheterna för sina arbetsuppgifter eftersom de bytt tjänst inom Volvo IT. Avbeställning av deras rättigheter har initierats.
		18C6 - Verify Approvals of User Access Fysisk tillgång till serverhallar är begränsad	Kontrolltyp Manuellt IT-beroende Kontrollutförare Respektive chef	Händelsestyrt		Inga väsentliga avvikelser noterade.
		18C1 - Access Rights Review, 18C2 - Access Rights Revoke Översyn av behörighetsprocess och policy	Kontrolltyp Manuell Kontrollutförare Intern och extern IT-revisor	Årligen		Inga väsentliga avvikelser. Vi har noterat att Volvo IT årligen genomför testning av sitt kontrollramverk för generella IT-kontroller, testningen innefattar dock inte leveransen mot Stockholms stad. Då samma kontroller i stor utsträckning används för leveransen till Stockholms stad bedöms eventuella problem i kontrolluppsättningen trots detta identifieras via Volvo IT:s testning.
		15C4 - Separation of duties for IT Ändamålsenlig ansvarsfördelning existerar inom behörighetsprocessen	Kontrolltyp Manuellt IT-beroende Kontrollutförare Respektive chef	Händelsestyrt		Inga väsentliga avvikelser noterade.

Kompletterande information kring utvärdering av driftprocessen:
Granskningen har fokuserat på Volvo IT:s driftprocess inom Windowsmiljön i tjänstekatalog B i leveransen till Stockholms Stadshus. För att hantera leveransen har Volvo IT ett antal dedikerade lokala team och ett antal globala team.

	Volvo IT				Ernst & Young	
#	Kontrollmål	Kontroll	Kontrolltyp specifikation	Kontrollfrekvens	Bedömning av kontroll	Iakttagelser
	Driftprocessen					
3	Att ge en rimlig säkerhet att säkerhetskopior skapas och återläsningstester genomförs, schemalagda jobb körs och övervakas, avvikelser rapporteras, samt att problem- och incidentrapporteringen genomförs	21C2 - Verify Integrity of Restored data Data säkerhetskopieras och säkerhetskopior går att återläsa	Kontrolltyp IT-beroende Kontrollutförare Service Monitoring	Händelsestyrt		Inga väsentliga avvikelser noterade. Återläsningstester ingår i leveransen men måste beställas separat av Stockholms stad. Under den granskade perioden har ett återläsningstest beställts och genomförts med lyckat resultat.
		22C1 - Monitoring Batch Jobs Avvikelser från schemalagda körningar identifieras och åtgärdas inom rimlig tid	Kontrolltyp Manuellt IT-beroende Kontrollutförare -	-	Ej tillämplig	Kontrollen bedöms inte vara tillämplig då övervakning av schemalagda körningar, förutom säkerhetskopiering, ej ingår i Volvo IT:s åtaganden inom tjänstekatalog B.
		22C3 - Monitoring Production Environment IT relaterade problem och incidenter identifieras, åtgärdas, granskas och analyseras inom rimlig tid	Kontrolltyp Manuellt IT-beroende Kontrollutförare Service Desk	Händelsestyrt		Inga väsentliga avvikelser noterade. Incidenter som rapporteras kategoriseras av Volvo IT, dessa kategorier är dock inte definierade mot bakgrund av Stockholms stads verksamhet. Vi har ej noterat några felbedömningar, riktlinjerna inom kategoriseringen är dock ett förbättringsområde.