Göteborgs Stad
Försäkrings AB Göta Lejon

FÖRSÄKRINGS AB GÖTA LEJON	Riktlinje för användarstyrda IT-applikationer		Rättslig grund
			EIOPA-BoS-14/253 Riktlinje 48, 53
Dokumentnamn	**Antagen datum**	**Löpnummer**	**Version**
Riktlinje för användarstyrda IT-applikationer			
Dokumenttyp	**Publiceras**	**Dokumentansvarig**	**Operativt ansvarig**
Riktlinjer	Intranätet	VD	Ekonomichef

Om dokumentet

Bakgrund och syfte

Användarstyrda IT applikationer som exempelvis Excel ark är ofta viktiga komponenter i ekonomisk rapportering och analys likväl som i affärsprocesserna. Karakteristiskt för dessa applikationer är att de inte omfattas av sedvanliga rutiner för utveckling, drift och underhåll av IT-applikationer och att rutinerna utförs av *lokala* funktioner inom bolaget

Användarstyrda IT applikationer är utvecklade och används av slutanvändare utanför de vanliga rutinerna för utveckling och användning av IT-system där formaliserad testning, behörighetsadministration, lagring och ändringsförfarande ofta inte existerar. Det innebär att det finns en risk att fel kan uppkomma i applikationerna, exempelvis på grund av otillräcklig ändringshantering, testförfarande eller handhavandefel.

Syftet med denna riktlinje är att fastställa obligatoriska minimikrav för riskhantering och riskstyrning av användarstyrda IT -applikationer inom bolaget.

Omfattning och avgränsningar

Denna riktlinje omfattar endast applikationer som betraktas som både materiella och komplexa och som:

- stödjer ekonomisk analys och/eller beslutsfattande (t.ex. bedöma rimligheten i finansiella belopp, stöd för prissättning, offerter eller ekonomiska utvärderingar)

- fastställer/beräknar finansiella belopp som direkt skapar poster i ekonomisk redovisning och den finansiella rapporteringen.

Det finns applikationer som kan anses innebära låg risk, s.k. enkla applikationer och dessa omfattas inte av denna riktlinje. Det är applikationer som används för att *stödja* arbetsflöde i operativa processer som till exempel att lista öppna fordringar, obetalda fakturor eller annan information som traditionellt skulle ha hanterats i pappersform.

Dokumentets beslutsordning

Denna riktlinje fastställs av vd och träder i kraft dagen för beslut. Riktlinjen ska fastställas och godkännas minst en gång per år även om inga ändringar beslutas. Ekonomichef ansvarar för att riktlinjen uppdateras.

Efterlevnad

Ekonomichefen ansvarar för att informera om innehållet i detta dokument. Berörda medarbetare ansvarar för att denna riktlinje följs. Chefer i organisationen följer upp att riktlinjen efterlevs och att kunskap om innehållet finns inom gruppen/enheten/avdelningen. Ansvarig för att granska verksamhetens efterlevnad är Compliance.

Definitioner och terminologi

Makro – En åtgärd eller uppsättning med åtgärder som används när uppgifter ska automatiseras i excel ark.

Olika kategorier av användarstyrda IT applikationer

Det finns olika kategorier av användarstyrda IT applikationer:

- **Enkla** - När applikationen endast sammanställer information från olika källor som arbetsstöd i processerna
- **Komplexa** är sådana applikationer som t.ex. innehåller formler, macros och länkar
- **Materiella -** Applikationer som producerar belopp som är större än materialitetsbeloppet (enskild risk) för operativa risker

Krav på materiella/Komplexa användarstyrda applikationer

Alla användarstyrda applikationer som är materiella och komplexa ska uppfylla nedanstående krav. De applikationer som uppfyller dessa krav kallas **säkrade.**

Datakvalitet

Inputkontroller: Det ska finnas robusta kontroller och rutiner för att säkerställa att de data som används som input i materiella applikationer är lämpliga, korrekta och kompletta.

Outputkontroller: Det ska säkerställas att beräkningar/databasfrågor och rapporter är lämpliga, korrekta, kompletta och i linje med de förväntade resultaten.

Oberoende granskning och testning

När en ny applikation utvecklas ska validering/test utföras av en oberoende person (annan än användaren eller utvecklaren) och formellt dokumenteras för att säkerställa korrektheten i applikationen (d.v.s. formler och beräkningar i kalkylblad och/eller data frågor/rapporter från databaser).

Säkerhet/behörighetskontroll

Applikationen ska skyddas mot obehörig åtkomst. Praktiskt innebär detta att begränsa tillgången till applikationen genom att lagra applikationen på en central server och tilldela lämpliga behörigheter. Användarstyrda IT-applikationer ska i lämplig omfattning vara skyddade med lösenord för att begränsa behörighet och undvika oönskade ändringar i applikationens funktionalitet.

Ändringar i applikationen

Ändringskontroller: Ändringar i applikationen ska hanteras på ett kontrollerat sätt vilket inbegriper att det ska finnas ett lämpligt skäl för ändring, god säkerhet vid ändringen och en

tydlig ansvarsuppdelning i förhållande till risken förändringen medför. På samma sätt som vid nyutveckling ska en validering utföras av en oberoende person (annan än användaren eller utvecklaren) och formellt dokumenteras för att säkerställa korrektheten i ändringen.

Versionshantering: Det ska finnas fungerande rutiner för att säkerställa att endast aktuella och godkända versioner av applikationen används i verksamheten.

Säker lagring av applikationen

Materiella/komplexa applikationer ska vara lagrade på nätverksservrar och inte lokalt på hårddisk. Det behöver även finnas en kopia av applikationen.

Dokumentation

Applikationen ska ha en tillhörande dokumentation.

Versionshantering och arkivering

Versionshantering och arkivering av tidigare godkända versioner av applikationen ska säkerställas.

Materiella/Komplexa applikationer som är undantagna kraven

Materiella/Komplexa applikationer – användning vid ett eller få tillfällen

Det kan finnas applikationer som utvecklas för användning vid ett eller mycket få tillfällen. För dessa kan användas ett förenklat förfarande:

- En annan person än den som utvecklat applikationen ska kontrollera och dokumentera att den är korrekt, antingen genom testning eller genom annan kontrollmetod. Ju mer komplex applikation, desto mer omfattande tester krävs.
- De testfall eller andra metoder för kontroll som använts ska dokumenteras.

Befogenheter och ansvar

.

Förteckning över materiella, säkrade applikationer

Ansvarig för funktion ska upprätthålla en förteckning över de materiella säkrade applikationer som används inom hans/hennes funktion. Han/hon är ansvarig för att förteckningen är komplett och aktuell.

Användning av säkrade applikationer

Användaren av en säkrad applikation är ansvarig för att han/hon använder den senast godkända versionen av applikationen.