Intern styrning och kontroll

Verksamhetsåret 2009

ISK-projektet:

En oberoende övergripande utvärdering av intern styrning och kontroll (ISK) på Riksbanken, utfördes av Ernst & Young i maj 2009.

Utgångspunkt var COSO-modellens fem områden; kontrollmiljö, riskhantering, kontrollaktiviteter, information och kommunikation samt uppföljning och utvärdering.

Beskrivningar togs fram avseende olika nivåer på ISK inom respektive delområde. Riksbankens målnivå sattes till minst nivå "etablerad", vilket motsvarar nivå 3 av 5 nivåer.

Ernst & Youngs utvärdering baserades på granskning av styrdokument och annan relevant dokumentation, samt intervjuer med olika befattningshavare på Riksbanken. I vissa fall bedömde de att Riksbanken hade uppnått nivå 4 ("avancerad"), men detta redovisas med samma färg som nivå 3 i matrisen. "Grundläggande" nivå, d v s nivå 2, redovisas som gul.

I juni 2009 genomfördes även en enkät bland Riksbankens enhets- och avdelningschefer för att få deras bedömning avseende ISK.

Utifrån utvärderingen och målnivån togs en handlingsplan fram med åtgärder att prioritera under 2009 för att Riksbanken vid årets slut skulle kunna uppnå en tillfredsställande nivå avseende ISK. Den redovisades för direktionen i juni 2009.

I maj påbörjades arbetet med att genomföra aktiviteter i enlighet med handlingsplanen.

I november 2009 gjorde Ernst & Young en ny utvärdering för att bedöma inom vilka områden nivån på ISK höjts, jämfört den första utvärderingen.

ISK Strukturutvärdering

Utvärdering (E&Y) maj 2009

Kontrollmiljö	Riskhantering	Kontrollaktiviteter	Information & Kommunikation	Uppföljning & Utvärdering
Vision, Värderingar, Strategier och Mål	Roller och ansvar för riskhantering (ansvarslinjer)	Kontrollaktiviteter - Effektivitet & Hushållning	Styrande dokument för intern/extern kommunikation	Operationell och ekonomisk verksamhets-uppföljning
Organisation, roller & ansvar	Modell för riskhantering	Kontrollaktiviteter - Lagefterlevnad	Informations- och kommunikationskanaler	Uppföljning av intern styrning och kontroll
Styrmodell och VP-process	Process för riskhantering	Kontrollaktiviteter - Finansiell Rapportering	System för incident- och avvikelsehantering	Internrevision
Styrande dokument för väsentliga verksamhets-områden		Generella IT- kontroller		
Utbildning och kompetensutveckling		Krisberedskap och kontinuitetsplanering		

ISK Strukturutvärdering

Översiktlig bedömning (E&Y) nov 2009

Kontrollmiljö	Riskhantering	Kontrollaktiviteter	Information & Kommunikation	Uppföljning & Utvärdering
Vision, Värderingar, Strategier och Mål	Roller och ansvar för riskhantering (ansvarslinjer)	Kontrollaktiviteter - Effektivitet & Hushållning	Styrande dokument för intern/extern kommunikation	Operationell och ekonomisk verksamhets-uppföljning
Organisation, roller & ansvar	Modell för riskhantering	Kontrollaktiviteter - Lagefterlevnad	Informations- och kommunikationskanaler	Uppföljning av intern styrning och kontroll
Styrmodell och VP-process	Process för riskhantering	Kontrollaktiviteter - Finansiell Rapportering	System för incident- och avvikelsehantering	Internrevision
Styrande dokument för väsentliga verksamhets-områden		Generella IT- kontroller		
Utbildning och kompetensutveckling		Krisberedskap och kontinuitetsplanering		

Handlingsplan 2010

Från "gult till grönt":

- Delegering av ansvar/befogenheter
  - Ta fram formell struktur för delegering av ansvar till nivå under avdelning
- Dokumentera kontrollmoment i processer
  - Genomför processgenomgångar och dokumentera kontroller som möter riskerna (ta fram generell metod/modell).
- Incident- och avvikelsehantering
  - Översyn, samordna det som finns idag, komplettera där "luckor" finns, samordna rapportering, tydliggör rutiner för eskalering

Handlingsplan 2010

Generell nivåhöjning:

- Riskrelaterade processer
  - Vidareutveckla
  - Samordna
- Ansvar och roller i ISK relaterade aktiviteter
  - Inom enheten
  - Inom Riksbanken

Appendix

I bilderna på följande sidor redovisas underlag till bilderna två till sex:

- Utgångsläge (juni 2009), nuläge (slutet av november) och målnivå (vid utgången av 2009) för varje delområde. Inom varje delområde redovisas de beskrivningar som togs fram i det inledande arbetet tillsammans med Ernst & Young, avseende nivåerna på intern styrning och kontroll
- Ernst & Youngs utvärdering från maj 2009 kompletterat med deras översiktliga bedömning i november. 2009 och rekommenderade aktiviteter för 2010.

Kontrollmiljö

Utgångsläge	Nuläge	Mål 2009
Vision, värderingar, strategier och mål är etablerade, dokumenterade, kommunicerade samt finns tillgängliga för medarbetarna		
Organisationsschema finns som omfattar hela verksamheten Roller och ansvar för nyckelfunktioner är definierade		Roller och ansvar följer formella strukturer som tydligt delegerar ansvar och befogenheter. Dessa är dokumenterade, kommunicerade och finns tillgängliga för medarbetarna
Styrmodellen täcker hela verksamheten, är formaliserad och kommunicerad till alla medarbetare. VP-dokumenten är aktuella, anpassade till verksamheten och förstådd av medarbetarna		
Policys och regler finns för väsentliga verksamhetsområden, är tillgängliga för medarbetarna och implementerade i organisationen		
Det finns etablerade handlingsplaner för utbildning och kompetensutveckling och en strukturerad modell för rekrytering och lönesättning		

Riskhantering

Utgångsläge	Nuläge	Mål 2009
Roller och ansvar för de mest väsentliga riskområdena är tydligt definierat		Risk- och kontrollansvaret är tydligt kopplat till affärs- och verksamhetsansvaret Tydlig andra ansvarslinje finns
Vissa modeller för riskhantering finns Fragmentarisk, silo-orienterad riskhantering		Modell som täcker väsentliga riskområden Omfattar centrala enheter/avdelningar
Riskhanteringsprocessen utförs som en separat aktivitet i delar av organisationen		Gemensam riskhanteringsprocess som täcker alla verksamhetsområden Åtgärdsplaner finns, kopplade till oönskad riskexponering

Kontrollaktiviteter

Utgångsläge	Nuläge	Mål 2009
Etablerad process där avvikelser/överträdelser avseende effektivitet och hushållning rapporteras reaktivt till styrelse och ledningsfunktioner		Regelbundna riskanalyser genomförs, utifrån strategier, mål, policys och regler, för att identifiera förbättringsområden. Övergripande nyckeltal eller andra mätetal finns kopplat till effektivitet och hushållning
Regelbundna riskanalyser genomförs kopplat till efterlevnad av lagar och externa regler Strukturerad process etablerad för att kontrollera efterlevnaden av lagar och regler		
Väsentliga kontroller kopplat till finansiell rapportering är definierade Det finns en process där brister i kontrollstruktur rapporteras reaktivt till avdelningschefer		Strukturerade riskanalyser genomförs kopplat till finansiell rapp. Väsentliga kontrollaktiviteter är dokumenterade. Övervaknings-process finns avseende intern kontroll i finansiell rapportering.
Behörighetsadministration, utvecklings- och ändringsprocess, samt driftsprocess är inte formaliserade och uppföljning saknas. Säkerhetskopiering görs och återläsningstester sker ad-hoc.		Systemägare godkänner nya behörigheter och processen utvärderas ad-hoc. Dokumenterade processer finns för systemutveckling- och driftsättning samt drift. Återläsningstester görs regelbundet
Kontinuitetsplanering genomförs enbart inom kritiska verksamheter. Kravställning gentemot interna parter förekommer. Tester av kontinuitetslösningar förekommer.		Dokumenterade kontinuitetsplaner finns. Kravställning gentemot kritiska interna och externa parter sker. Övningar och systemtester integreras.

Information och kommunikation

Utgångsläge	Nuläge	Mål 2009
Policys och regler finns för väsentliga områden, är tillgängliga för medarbetarna och implementerade i organisationen Ansvar och roller för intern och extern kommunikation är tydliga		
Interna och externa informations och kommunikationskanaler är anpassade efter verksamhetens behov. Tekniska hjälpmedel/IT-system används i stor utsträckning för den interna kommunikationen		
Process för incident- och avvikelsehantering finns för kritiska delar av verksamheten		Process och system för incident- och avvikelsehantering finns för alla delar av verksamheten Rapportering och hantering av incidenter och avvikelser sker strukturerat

Uppföljning och utvärdering

Utgångsläge	Nuläge	Mål 2009
Nyckeltal direkt kopplade till målen i verksamhetsplanen		
Ledningen initierar separata utvärderingar av befintlig intern styrning och kontroll Fokus på enskilda delar av den interna styrningen och kontrollen		Brister i intern styrning och kontroll rapporteras kontinuerligt. IS&K-processen följs upp och förbättras kontinuerligt och återkoppling sker till organisationen
IR genomför självständig riskbedömning som grund för internrevisionsplanen Granskar risker och kontroller i operativa processer		

ISK Strukturutvärdering och handlingsplan

Utvärdering maj 2009 och översiktlig bedömning nov 2009

ISK komponent	Delkomponent	Q2 2009	Nov 09	Kommentarer på bedömning nov 09	Rekommenderade aktiviteter
Kontrollmiljö	Vision, Värderingar, Strategier och Mål				• *Uppdatering och utveckling av policys (Medarbetarpolicy, Policy rörande rehabilitering, alkohol och droger samt arbetsmiljö).*
	Organisation, roller & ansvar			*Delegering av ansvar och befogenheter till nivå under Avdelning har inte initierats.*	• *Upprätta formell struktur som tydligt delegerar ansvar och befogenheter till alla nyckelmedarbetare, samt gör den tillgänglig för medarbetarna.*
	Styrmodell och VP-process				
	Styrande dok. för väsentliga verksamhets-områden				
	Utbildning och kompetensutveckling				

Bedömningen (E&Y) i november 2009 har endast skett för de områden som i utvärderingen i maj bedömdes som ej etablerade (gula)

ISK Strukturutvärdering och handlingsplan

Utvärdering maj 2009 och översiktlig bedömning nov 2009

ISK komponent	Delkomponent	Q2 2009	Nov 09	Kommentarer på bedömning nov 09	Rekommenderade aktiviteter
Riskhantering	Roller och ansvar för riskhantering (ansvarslinjer)			*Ansvarsförhållanden har konkretiserats och en tydlig beskrivning av andra ansvarslinjen har upprättats. Ny organisationsmodell har beslutats och arbetet kring implementering av denna har påbörjats.*	• *Redesigna riskrelaterade processer samt konkretisera ansvarsfördelningen ytterligare.*
	Modell för risk-hantering			*En policy för finansiell risk och en policy för operationell risk finns upprättad. Enligt uppgift skall alla riskområden vara inkluderade i dessa policies.*	• *Säkerställ att policies är implementerade fullt ut.*
	Process för risk-hantering			*Riskanalyser avseende operativa risker har under hösten genomförts på avdelningsnivå och konsoliderats på banknivå.* *Riskhantering (åtgärdsplaner) utifrån riskanalyser är kopplat till verksamhetsplanen, men visst dokumentationsarbete återstår för att tydliggöra kopplingen ner till enhetsnivå.* *Initierade aktiviteter troligen tillräckligt för att ligga i linje med andra myndigheter, men oklart om de är tillräckliga enligt formuleringarna i FISK:en.*	• *Koppling mål -> risk -> kontroll/åtgärder kan förtydligas ytterligare.*

Bedömningen (E&Y) i november 2009 har endast skett för de områden som i utvärderingen i maj bedömdes som ej etablerade (gula)

ISK Strukturutvärdering och handlingsplan

Utvärdering maj 2009 och översiktlig bedömning nov 2009

ISK komponent	Delkomponent	Q2 2009	Nov 09	Kommentarer på bedömning nov 09	Rekommenderade aktiviteter
Kontrollaktiviteter	Kontrollaktiviteter - Effektivitet & Hushållning			*I operativa riskanalyser har inte kopplingen tydliggjorts kring vilka kontroller som finns för de olika riskerna.* *Dokumentation av kontroller finns implementerat för vissa avdelningar dock är inte struktur enhetlig samt tillräcklig för att mitigera bankens risker.*	• *Koppling mål/krav -> risk -> kontroll/åtgärder kan förtydligas ytterligare.* • *Ta fram format för att dokumentera kontroller.*
	Kontrollaktiviteter - Lagefterlevnad				
	Kontrollaktiviteter - Finansiell Rapportering			*Kontrollaktiviteter / checklista för upprättande av månadsbokslut finns dokumenterat.*	• *Genomför strukturerade riskanalyser kopplat till den finansiella rapporteringen.*
	Generella IT-kontroller			*Kritikalitetsbedömningar har genomförts (enligt ESCB-modellen) för Colin, Dimension, Agresso och den externa webben. Därutöver har en säkerhetsanalys genomförts för Caesar.* *Projektet "börja och sluta" initieras den 1 december för att sedan införas för hela banken i jan-feb 2010.*	
	Krisberedskap och kontinuitetsplanering			*Dokumenterade kontinuitetsplaner finns för alla bankens kritiska verksamhetsprocesser . Ansvarsfördelning och roller inom kontinuitetsarbetet är tydligt.*	

Bedömningen (E&Y) i november 2009 har endast skett för de områden som i utvärderingen i maj bedömdes som ej etablerade (gula)

ISK Strukturutvärdering och handlingsplan

Utvärdering maj 2009 och översiktlig bedömning nov 2009

ISK komponent	Delkomponent	Q2 2009	Nov 09	Kommentarer på bedömning nov 09	Rekommenderade aktiviteter
Information & Kommunikation	Styrande dokument för intern/extern kommunikation				
	Informations- och kommunikations-kanaler				
	System för incident- och avvikelse-hantering			*Incidentrapporteringsprocesser och system finns etablerat dock har dessa inte harmoniserats.* *Rapportering verkar inte ske tillräkligt strukturerat för att säkerställa fullständighet .*	• *Tydliggöra rutiner för eskalering av incidenter vad gäller när, var, hur och till vem operativa incidenter skall rapporteras.* • *Säkerställa ändamålsenlig hantering av rapporterade incidenter.* • *Implementera strukturerad avrapportering till LG.*
Uppföljning & Utvärdering	Operationell och ekonomisk verksamhets-uppföljning				
	Uppföljning av intern styrning och kontroll			*Ett antal aktiviteter har genomförts under året för att etablera en systematisk uppföljning avseende den interna styrningen och kontrollen, inklusive återkoppling till organisationen.*	• *Fastställa ambitionsnivå på längre sikt.* • *Ta fram ny uppdaterad åtgärdsplan baserat på genomförd utvärdering och fastställd ambitionsnivå.*
	Internrevision				

Bedömningen i november 2009 har endast skett för de områden som i utvärderingen i maj bedömdes som ej etablerade (gula)

Redovisning i ÅR?

Enligt FISKen ska myndigheters ledning i sin årsredovisning avge en bedömning av den "interna styrningen och kontrollen" (hushållning, rapportering, lagenlighet, effektivitet)

Ska RB avge en deklaration i år? Nej…

- Riksbanken bör invänta lagstiftningen
- ISK-arbetet "nytt" på banken – en del kvar att göra för att uppnå en etablerad ISK-nivå med god hållbarhet och med en formaliserad process.

Nästa år → ny enhet och en hel "cykels" arbete