

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА
TRIBUNAL DE CUENTAS EUROPEO
EVROPSKÝ ÚČETNÍ DVŮR
DEN EUROPÆISKE REVISIONSRET
EUROPÄISCHER RECHNUNGSHOF
EUROOPA KONTROLLIKODA
ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ
EUROPEAN COURT OF AUDITORS
COUR DES COMPTES EUROPÉENNE
CÚIRT INIÚCHÓIRÍ NA HEORPA



CORTE DEI CONTI EUROPEA
EIROPAS REVĪZIJAS PALĀTA
EUROPOS AUDITO RŪMAI

EURÓPAI SZÁMVEVŐSZÉK
IL-QORTI EWROPEA TAL-AWDITURI
EUROPESE REKENKAMER
EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
TRIBUNAL DE CONTAS EUROPEU
CURTEA DE CONTURI EUROPEANĂ
EURÓPSKY DVOR AUDÍTOROV
EVROPSKO RAČUNSKO SODIŠČE
EUROOPAN TILINTARKASTUSTUOMIOISTUIN
EUROPEISKA REVISIONSRÄTTEN

Rapport om
granskningen av riskhantering vid
Europeiska centralbanken för budgetåret 2010

med Europeiska centralbankens svar

INNEHÅLL

	Punkt
Inledning	1–4
Granskningens inriktning och omfattning samt granskningsmetod	5–6
Granskningsresultat	7–91
Har ECB fastställt en lämplig och heltäckande styrningsram för riskhantering?	7–18
Övergripande ram för riskhantering	8–14
Upplysningar om ECB:s riskhanteringsram till externa parter	15–18
Är ECB:s hantering av operativa risker ändamålsenlig?	19–66
Hantering av operativa risker	20–39
ECB:s kontinuitetshantering	40–66
Är ECB:s hantering av finansiella risker ändamålsenlig?	67–91
Ram för hantering av finansiella risker avseende investeringar och penningpolitiska transaktioner	69–74
Metod för hantering av finansiella risker	75–83
Tillämpning av metoden för hantering av finansiella risker	84–88
Är rapporteringen av finansiella risker adekvat?	89–91
Slutsatser och rekommendationer	92–100
Har ECB fastställt en lämplig och heltäckande styrningsram för riskhantering?	92–93
Är ECB:s hantering av operativa risker ändamålsenlig?	94–98
Är ECB:s hantering av finansiella risker ändamålsenlig?	99–100

FÖRKORTNINGAR

BIS	Internationella regleringsbanken
D-CO	Kommunikation (direktorat)
ECB	Europeiska centralbanken.
ECBS	Europeiska centralbankssystemet
GD-A	Administration (generaldirektorat)
GD-H	HR, budget och organisation (generaldirektorat)
GD-IS	Informationssystem (generaldirektorat)
GD-M	Marknadsoperationer (generaldirektorat)
GD-P	Betalningssystem och marknadsinfrastruktur (generaldirektorat)
GD-S	Statistik (generaldirektorat)
GIPS	<i>Global Investment Performance Standards</i> , se fotnot 59
IAS	<i>International Accounting Standards</i> , internationell redovisningsstandard
IFRS	<i>International Financial Reporting Standards</i> , internationell standard för finansiell rapportering
RMA	avdelningen för riskhantering (vid GD-H)
VaR	<i>Value at Risk</i> , se fotnot 17

INLEDNING

1. Europeiska centralbanken (ECB) och de nationella centralbankerna i alla Europeiska unionens medlemsstater bildar tillsammans Europeiska centralbankssystemet (ECBS). Det viktigaste målet för ECBS är att upprätthålla prisstabilitet. ECBS stöder också den allmänna ekonomiska politiken inom unionen i syfte att bidra till att förverkliga unionens mål¹. För detta ändamål utför ECB de uppgifter som anges i dess stadga² och ansvarar för förvaltningen av sin verksamhet och sina finanser.
2. Europeiska revisionsrättens granskning av effektiviteten i ECB:s förvaltning baseras på artikel 27.2 i protokollet om stadgan för ECBS och ECB³. Granskningen av budgetåret 2010 gäller de förfaranden och system för riskhantering som ECB har infört och hur de tillämpas.
3. ECB:s beslutsfattande organ är ECB-rådet och direktionen⁴. Direktionen ska genomföra den monetära politiken enligt ECB-rådets riktlinjer och beslut⁵ och har det övergripande ansvaret för förvaltningen av den dagliga verksamheten vid ECB och av dess tillgångar. Direktionen har även det slutliga ansvaret för riskhantering vid ECB.

¹ Artikel 127.1 i fördraget om Europeiska unionens funktionssätt.

² Stadgan för ECBS och ECB är ett protokoll som fogats till fördraget.

³ Artikel 27.2 i protokollet om stadgan för ECBS och ECB: "Artikel 287 i fördraget om Europeiska unionens funktionssätt ska endast tillämpas vid granskning av effektiviteten i ECB:s förvaltning."

⁴ Artikel 9.3 i protokollet om stadgan för ECBS och ECB. ECB-rådet består av de sex ledamöterna i direktionen plus cheferna för de nationella centralbankerna i länderna i euroområdet. Direktionen består av ordföranden, vice ordföranden och fyra andra ledamöter.

⁵ Artikel 12.1 i protokollet om stadgan för ECBS och ECB.

4. Risker hanteras genom två separata ramar vid ECB. Enheten för hantering av operativa risker⁶ hanterar alla operativa risker (se fotnot 22), inbegripet kontinuitet. Riskhanteringsavdelningen hanterar finansiella risker (se punkt 70), inbegripet ECB:s investeringsverksamhet och kredittransaktioner.

GRANSKNINGENS INRIKTNING OCH OMFATTNING SAMT

GRANSKNINGSMETOD

5. Målet för revisionsrättens granskning av budgetåret 2010 var att bedöma lämpligheten i ECB:s ram för hantering av operativa och finansiella risker⁷.

Riskhanteringen vid ECB bedömdes med hjälp av följande centrala revisionsfrågor:

- Har ECB fastställt en lämplig och heltäckande styrningsram för riskhantering?
- Är ECB:s hantering av operativa risker ändamålsenlig?
- Är ECB:s hantering av finansiella risker ändamålsenlig?

6. I granskningen av ECB:s riskhantering⁸ ingick följande delar:

- a) En genomgång av den övergripande ramen för riskhantering vid ECB och av bästa praxis på riskhanteringsområdet vid andra liknande internationella organisationer⁹.

⁶ Enheten för hantering av operativa risker handlägger risker som gäller ECB:s verksamhet och också de risker som gäller processer och projekt inom ECBS/eurosystemet.

⁷ De kriterier som revisionsrätten använde för att bedöma ECB:s ram för hantering av operativa och finansiella risker har kursiverats i rapporten. Om ingen annan hänvisning anges är kriterierna revisionsrättens.

⁸ Riskhanteringen inom Europeiska centralbankssystemet (ECBS) ingick inte i granskningen.

⁹ Informationsbesök gjordes vid USA:s centralbank (*Federal Reserve Bank*) i New York och Kanadas centralbank (*Bank of Canada*) och frågeformulär sändes till USA:s centralbank i New York, Kanadas centralbank och Schweiz centralbank (*Swiss National Bank*).

- b) En genomgång av ramen för hantering av operativa risker och stickprov från sex utvalda affärsområden (generaldirektorat) för att bedöma tillämpningen av riskhanteringsramen. Urvalet gjordes så att i) viktiga operativa risker garanterat ingick, ii) både kärnverksamhet och icke-kärnverksamhet vid ECB ingick och iii) verksamhet som kräver övergripande riskhantering ingick. Följande generaldirektorat valdes ut: Marknadsoperationer (GD-M), Betalningssystem och marknadsinfrastruktur (GD-P), Statistik (GD-S), Administration (GD-A), Informationssystem (GD-IS) och direktoratet för kommunikation (D-CO).
- c) En genomgång av ramen för hantering av finansiella risker och detaljgranskning av riskhanteringsavdelningen vid GD HR, budget och organisation (GD-H) och av avdelningarna för marknadsoperationssystem, finansiella transaktionstjänster och investeringar vid GD-M. Bedömningen av ECB:s riskhanteringsmetod och hur den tillämpas gjordes med tekniskt stöd från experter på finansiell risk från Ernst och Young, Luxemburg.

GRANSKNINGSRESULTAT

Har ECB fastställt en lämplig och heltäckande styrningsram för riskhantering?

7. ECB:s ambition är att tillämpa bästa praxis vid sin riskhantering. José Manuel Gonzáles-Páramo, ledamot av ECB:s direktion, skrev 2009 att Europeiska centralbanken redan från första början lade särskilt vikt vid riskhantering och att ECB som ny medlem i centralbanksgemenskapen hade ambitionen att uppfylla de högsta styrningsnormerna när man organiserade riskhanteringsfunktionen inom institutionerna, och att man ville tillämpa de allra bästa verktygen¹⁰.

¹⁰ Manuel Gonzáles-Páramo, Ulrich Bindseil och Evangelos Tabakis, *Risk Management for Central Banks and Other Public Investors* (riskhantering för centralbanker och andra offentliga investerare), Cambridge University Press 2009.

Övergripande ram för riskhantering

8. *En stark riskkultur som genomsyrar hela institutionen är ett av nyckelelementen för en ändamålsenlig riskhantering. En av förutsättningarna för att en sådan riskkultur ska kunna skapas är att det inrättas en heltäckande (innefattande alla risktyper, verksamhetsområden och relevanta risker) och oberoende riskhanteringsfunktion som är direkt underställd riskchefen, eller den högsta ledningen om ingen riskchef har utsetts, i enlighet med proportionalitetsprincipen¹¹.*

9. Vid ECB ansvarar varje organisatorisk enhet¹² för hanteringen av sina egna risker och kontroller. Två funktioner/avdelningar stöder de organisatoriska enheterna i riskhanteringsprocessen:

- Funktionen för hantering av operativa risker/kontinuitetshantering¹³ ansvarar för metodunderhåll, samordnar all verksamhet som gäller operativ risk och ger förebyggande rådgivning till affärsområdena¹⁴.
- Riskhanteringsavdelningen har hand om finansiella risker¹⁵. Den ansvarar för att lägga fram förslag på strategier och förfaranden och för att ge organisatoriskt stöd för riskhantering för alla finansmarknadstransaktioner som utförs av ECB eller av eurosyste­met för ECB:s räkning. Avdelningen är uppdelad i två enheter: sektionerna för riskanalys respektive riskstrategi.

¹¹ *High level principles for risk management* (högnivåprinciper för riskhantering), Europeiska banktillsynskommittén (*Committee of European Banking Supervisors*, CEBS), februari 2010. (Kursivering av Europeiska revisionsrätten, fetstil och normalt typsnitt i originalet).

¹² Sektion, avdelning, direktorat eller generaldirektorat.

¹³ Ingår i GD-H.

¹⁴ Funktionen för hantering av operativa risker/kontinuitetshantering är även sekretariat för kommittén för operativ risk.

¹⁵ Riskhanteringsavdelningen är administrativt en del av GD-H men rapporterar direkt till den direktionsledamot som ansvarar för hanteringen av finansiella risker.

10. Som stöd till direktionens beslutsfattande har det inrättats flera kommittéer som behandlar olika aspekter av riskhantering, såsom kommittén för operativa risker, investeringskommittén, kommittén för tillgångar och skulder samt kreditkommittén.

11. Det finns en heltäckande organisatorisk struktur med tydligt fördelade roller och ansvarsområden. Det finns dock en tydlig avgränsning mellan hanteringen av finansiella och operativa risker vid ECB, vilket ökar risken för att överblicken över bankens totala exponering kanske inte är heltäckande.

12. Det har inte inrättats något särskilt och oberoende organ, såsom en riskchef eller en övergripande riskhanteringskommitté, mellan direktionen och de två riskfunktionerna/riskenheterna - hantering av operativa risker/kontinuitetshantering och riskhanteringsavdelningen. När granskningen gjordes hade direktionsledamoten med ansvar för riskhantering också ett antal andra ansvarsområden medan en riskchef enbart skulle koncentrera sig på riskförvaltning.

13. Att det saknas en hierarkiskt oberoende riskhanteringsfunktion ökar också risken för att riskhanteringsfrågorna inte får tillräcklig uppmärksamhet, till exempel vilka personalresurser som anslås till riskhanteringsuppgifter, eftersom dessa frågor avgörs av GD-H.

14. En genomgång av bästa praxis vid andra liknande internationella organisationer visar att Kanadas centralbank har antagit en integrerad ram för riskhantering som inbegriper en riskchef och en arbetsgrupp för riskhantering. Båda arbetar med att fastställa en heltäckande riskprofil för banken där affärsmässiga, operativa och finansiella risker ingår, se **ruta 1**. Bankens ram för riskhantering är integrerad i processerna för den strategiska planeringen, budgetarbetet och resultatutvärderingen vid årets slut.

Ruta 1 - Ett exempel på integrerad riskhantering - Kanadas centralbank

Riskchefen har ansvar för följande områden:

- Leder arbetet med att ta fram och förbättra en ram för den integrerade riskhanteringsstrategin som ska godkännas av ledningen.

- Ger anvisningar och råd om riskhantering till övriga medlemmar i den högsta ledningen och är ordförande i arbetsgruppen för riskhantering.
- Är tillsammans med finansdepartementet ordförande i fondförvaltningskommitténs riskkommitté.

Arbetsgruppen för riskförvaltning har följande arbetsuppgifter:

- Är behjälplig vid den fullständiga uppdateringen av bankens självbedömning avseende risk och vid utarbetandet av halvårs- och årsrapporterna om riskhantering.
- Sammanträder tre till fyra gånger per år för att se över bankens riskprofil och diskutera riskhanteringsinitiativ med företrädare för funktioner/avdelningar.

Upplysningar om ECB:s riskhanteringsram till externa parter

15. *Det bör offentliggöras tillräckliga upplysningar för att externa parter ska kunna bedöma ECB:s metod för riskhantering.*

16. ECB offentliggör en årsrapport med årsredovisningen och tillhörande upplysningar¹⁶. Informationen om riskhantering i årsredovisningen är relativt begränsad, och informationen om de principer och siffror som gäller för ECB:s riskhantering är inte offentlig (utom när det gäller det konsoliderade beloppet för *Value at Risk*¹⁷ (VaR)). ECB:s årsrapport innehåller kortfattad information om vissa riskhanteringsfrågor men ger ingen översikt över hur riskhanteringsprocessen inom organisationen ser ut, vilka risker organisationen utsätts för eller hur ledningen hanterar dessa risker.

¹⁶ ECB tillämpar sin egen ram för redovisningsrapportering som fastställts genom beslut ECB/2006/17 om Europeiska centralbankens årsbokslut, i ändrad lydelse.

¹⁷ *Value at Risk* (VaR) är ett ofta använt riskmått på risken för förlust avseende en specifik portfölj med finansiella tillgångar. För en given portfölj, sannolikhet och tidshorisont definieras VaR som ett tröskelvärde där sannolikheten för att en omvärdering av portföljen till aktuellt marknadsvärde över den givna tidshorisonten ger en förlust som överskrider detta värde, med normala marknader och utan handel i portföljen, är den givna sannolikhetsnivån (se *Value at Risk: The New Benchmark for Managing Financial Risk* (det nya riktmärket för hantering av finansiell risk (3:e upplagan), Philippe Jorion, McGraw-Hill Professional, 2006).

17. Användning av de internationella redovisningsstandarderna IFRS (*International Financial Reporting Standards*)¹⁸ är bästa praxis för framläggandet av en enhets räkenskaper. IFRS 7 "Finansiella instrument: Upplysningar" som handlar om hur en organisation presenterar de risker den utsätts för i sin redovisning, har dock inte tillämpats av ECB.

18. Andra internationella eller nationella centralbanksorganisationer såsom Internationella regleringsbanken (BIS) och Kanadas centralbank ger i sina årsredovisningar information om riskhantering även om en av dem inte tillämpar IFRS (se [ruta 2](#)).

Ruta 2 - Illustration av tillämpningen av upplysningar om riskhantering		
Organisation	Upplysningar om riskhantering i årsredovisningen	Ram för finansiell rapportering
Internationella regleringsbanken (BIS)	I årsredovisningen ges upplysningar om de risker banken utsätts för och om metod för och organisation av riskhantering samt en detaljerad översikt över kreditrisk, marknadsrisk, likviditetsrisk och operativ risk.	En särskild ram för finansiell rapportering föreskrivs i bankens stadgar.
Kanadas centralbank	I årsredovisningen ges en översikt över riskhanteringsprocessen, riskstyrningsstrukturen, rollen för chefen för finansiell risk, de finansiella risker banken utsätts för och en detaljerad översikt över kreditrisk, marknadsrisk och likviditetsrisk.	IFRS ¹⁹

¹⁸ IFRS är de principbaserade standarder och tolkningar och den ram som antagits av *International Accounting Standards Board* (IASB), även kända under sitt gamla namn *International Accounting Standards* (IAS, internationella redovisningsstandarder). I februari 2001 lade kommissionen fram ett förslag till en förordning med krav på att alla EU-företag som är noterade på en reglerad marknad, inbegripet banker och försäkringsbolag, utarbetar konsoliderade räkenskaper i enlighet med IAS senast från och med 2005. EU:s medlemsstater gavs möjlighet att utvidga detta krav till räkenskaperna för olistade företag och enskilda företag. Det upprättades en godkännandemekanism för EU, på både politisk och teknisk nivå, för att övervaka införandet av IAS i EU.

¹⁹ Kanadas centralbank rapporterade till och med den 31 december 2010 i enlighet med god redovisningssed i Kanada (*Canadian Generally accepted accounting principles*). Informationen om riskhantering kunde dock jämföras med IFRS. Från och med den 1 januari 2011 rapporterar Kanadas centralbank i enlighet med IFRS.

Är ECB:s hantering av operativa risker ändamålsenlig?

19. Kontinuitetshantering kompletterar ECB:s ram för hantering av operativa risker, och de är båda en viktig del av bolagsstyrningen²⁰.

Hantering av operativa risker

20. I en ändamålsenlig ram för hantering av operativa risker ingår tydliga strategier och tillsyn från styrelse och högsta ledning, en stark kultur avseende operativa risker och intern kontroll (med tydlig ansvarsfördelning och åtskillnad av funktioner) och en ändamålsenlig internrapportering.

21. För att bedöma ECB:s hantering av operativa risker undersökte revisionsrätten följande:

- De strategier för hantering av operativa risker som fastställts vid ECB.
- Organisationsstruktur och ansvarsområden för hanteringen av operativa risker.
- Kopplingen till den strategiska och finansiella planeringen (den årliga budgetcykeln).
- Riskidentifiering, riskbedömning och riskrespons, rapportering, övervakning och uppföljning inom affärsområdena liksom på central nivå.

Strategier för operativa risker

22. *Strategierna för hantering av operativa risker bör ge en tydlig definition av operativ risk som gäller för hela banken och ange strategierna för bankens metod för att identifiera, bedöma, övervaka och kontrollera/minska riskerna.*

23. ECB:s ram för hantering av operativa risker antogs av direktionen i oktober 2007²¹ och beskrivs i handboken om affärspraxis (*Business Practice*

²⁰ *Business Practices Handbook* (handbok om affärspraxis), kapitel 26.

Handbook) som finns på intranätet och är tillgänglig för hela personalen. Där anges huvuddragen i ECB:s definition av hantering av operativa risker²², dess risktoleranspolicy, roller och ansvarsområden samt strategier för bedömning, respons, rapportering och övervakning.

24. De fastställda strategierna för hantering av operativa risker ger en tydlig definition av operativ risk som gäller för hela banken och fastställer strategierna för bankens metod för att bedöma, övervaka och kontrollera/minska risker. Handboken om affärspraxis ger dock inga detaljer om bankens metod för att identifiera risker.

Organisationsstruktur och ansvarsområden

25. *Affärsområdenas ledning bör ha ansvaret för tillämpningen av strategier, processer och förfaranden för den hantering av operativa risker som rör bankens alla väsentliga verksamheter, processer och system. Banken bör även ha ett system för hantering av operativa risker med tydliga ansvarsområden som tilldelas en riskhanteringsfunktion.*

26. Direktionen har det slutliga ansvaret för hanteringen av operativa risker vid ECB. Kommittén för operativa risker har hand om strategiska frågor och frågor på medellång sikt liksom relevanta kortsiktiga frågor och särskilda frågor²³. Kommittén består av en direktionsledamot (ordförande) och sju ledande befattningshavare i banken²⁴. Den har befogenhet att fatta beslut som gäller

²¹ Direktionen beslutade 2008 att anpassa ECB:s ram för hantering av operativa risker till den ram som har antagits på ECBS-nivå.

²² Operativ risk definieras som risken för negativa finansiella, affärsmässiga och/eller anseendemässiga konsekvenser av att interna styrnings- och affärsprocesser, eller människor, system eller externa händelser, är olämpliga eller inte fungerar.

²³ Kommittén har fått i uppdrag att uppmuntra och övervaka framtagningen, genomförandet och underhållet av den operativa riskhanteringen vid ECB.

²⁴ Ledamöter är ledande befattningshavare från Marknadsoperationer, Informationssystem, Administration, HR, budget och organisation och två av affärsområdena med kärnverksamhet som byts ut varje år enligt ett roterande schema samt rådgivaren till generaldirektören för HR, budget och organisation.

riskacceptans på medelnivå medan högnivårisker alltid måste accepteras av direktionen. Sammanträden hålls varannan månad eller oftare vid behov.

27. I handboken om affärspraxis anges tydligt att det är affärsområdena som ansvarar för hanteringen av sina operativa risker²⁵. Varje affärsområde bör därför utse (minst) en risksamordnare som hjälper affärsområdescheferna med hanteringen av operativa risker och som fungerar som kontaktperson för allt som gäller hantering av operativa risker inom affärsområdet.

Affärsområdescheferna ansvarar också för att se till att personalen förvärvar och upprätthåller den kompetens som krävs för att kunna ansvara och vara redovisningsskyldig för hanteringen av operativa risker. Funktionen för hantering av operativa risker/kontinuitetshantering ska utarbeta och underhålla ramen för hantering av operativa risker och samordna affärsområdenas metoder för hantering av operativa risker.

28. Av de åtta anställda inom funktionen för hantering av operativa risker/kontinuitetshantering var endast fyra fast anställda då revisionen gjordes. De övriga var utsända från nationella centralbanker eller hade tidsbestämda kontrakt på mellan tre månader och två år. Detta innebär att personalomsättningen är hög, vilket leder till bristande kontinuitet vid en viktig funktion och ökar risken för att ramen för hantering av operativa risker inte tillämpas på ett adekvat sätt vid ECB.

29. Personalens kännedom om ramen för hantering av operativa risker behandlades i personalenkäter 2009 och 2010. Av enkäten 2009 framkom att omkring 40 % av de svarande sa sig inte få tillräcklig information om hantering av operativa risker; 56 % visste inte vem som var risksamordnare för deras affärsområde och 45 % visste inte var informationen om hantering av operativa risker fanns på intranätet. I enkäten 2010 visste 40 % fortfarande inte var man hittade information om hantering av operativa risker.

²⁵ Det affärsområde (riskägaren) som ansvarar för den övergripande risken (det vill säga en risk som påverkar flera affärsområden) bör rekommendera och/eller genomföra lämpliga riskbehandlingsåtgärder som ska tillämpas inom hela ECB.

Kopplingen till den strategiska och finansiella planeringen (den årliga budgetcykeln)

30. *Riskhanteringen bör vara inbyggd i styrningen av ECB som en integrerad del av bankens strategiska, affärsmässiga och finansiella planering.*

31. En viktig del vid fastställandet av ECB:s riskprofil är den årliga bedömning av operativa risker som görs av affärsområdena och funktionen för hantering av operativa risker/kontinuitetshantering. Bedömningarna för 2009 gjordes av affärsområdena mellan juni och augusti 2009, och därefter hölls ett samordningsmöte med risksamordnarna. *Top-down*-rapporten var klar i januari 2010.

32. Riskprofilen bör vara en av ingredienserna i den strategiska planeringsprocessen som i sin tur leder fram till den finansiella planen. Av granskningen framkom dock att den årliga bedömningen av operativa risker inte integreras i ECB:s strategiska och finansiella planeringscykel. Risken är därför att hanteringen av operativa risker blir en isolerad övning och att den finansiella planen inte styr resurserna på lämpligaste sätt för att de strategiska målen ska uppnås²⁶.

33. Ett exempel på god praxis är Kanadas centralbank där bankens riskprofil är en integrerad del av bankens övergripande strategiska och finansiella planeringscykel²⁷.

²⁶ Baserat på slutsatserna i artikeln *ERM at the Federal Reserve Bank of Richmond* (företagsövergripande riskhantering vid *Federal Reserve Bank of Richmond*), 2007, Jack Dorminey och Richard Mohn.

²⁷ *Källa:* Webbplatsen för Kanadas centralbank *Medium-term plan 2010-12* (plan på medellång sikt 2010–2012) (www.bankofcanada.ca per den 13 juli 2011).

Processen för hantering av operativa risker: Riskidentifiering, riskbedömning och riskrespons, rapportering, övervakning och uppföljning

Riskidentifiering, riskbedömning och riskrespons

34. Alla operativa risker som är inbyggda i verksamheter, processer och system bör identifieras och bedömas. Risker bör utvärderas i förhållande till den befintliga strategin och toleransnivån så att en lämplig respons baserad på tillräckliga kostnadsberäkningar kan fastställas. Relevant information bör regelbundet rapporteras till ledningen och direktionen för att stödja en förebyggande hantering av operativa risker.

35. Ramen för hantering av operativa risker har i första hand genomförts genom *top-down*-bedömningar. Enligt ECB:s riskstrategi ska affärsområdena också kontinuerligt göra *bottom-up*-bedömningar av affärsområdets processer, och de risker som identifieras ska godkännas²⁸.

36. ECB gjorde *top-down*-bedömningar 2008 och 2009. Från funktionen för hantering av operativa risker/kontinuitetshantering fick affärsområdena några på förhand fastställda högnivårisker som var utgångspunkt för deras riskbedömningar. I slutrapporten fanns en handlingsplan för varje affärsområde.

Enligt handboken om affärspraxis ska affärsområdena analysera och definiera strategier för riskrespons och göra en kostnadsnyttoanalys av tänkbara lösningar.

37. Alla affärsområden hade identifierat risker och respons vid *top-down*-bedömningen 2009. Rapporten om *top-down*-bedömningen 2009 innehöll uppföljningsåtgärder för varje affärsområde. Det finns dock ingen

²⁸ För projekt såsom IT finns det särskilda förfaranden som anges i dokumentet om projektorganisation och kontrollförfaranden. Projektrisker rapporteras separat via projektstyrningskommittén eller projektstyrningskommittén för nya lokaler. Riskhanteringen av specifika projekt har inte tagits med i denna granskning.

dokumentation av kostnadsnyttoanalyser för de affärsområden som ingick i urvalet.

38. För några risker tog det godkännandeförfarande som tillämpas av kommittén för operativa risker och direktionen mycket lång tid efter det att affärsområdet hade identifierat risken. Exempelvis hade två risker som identifierades i juli-augusti 2009 ännu inte godkänts i december 2010. Av den lista över punkter som ännu inte har åtgärdats som går igenom vid kommitténs sammanträden framgår också att några punkter hade funnits med i över ett år och andra upp till två år.

39. Endast för tre av de sex affärsområdena i urvalet var det möjligt att identifiera de särskilda medel som hade avsatts för operativa riskhanteringsåtgärder i deras arbetsprogram, men beskrivningen av åtgärderna var vag och det var inte möjligt att spåra åtgärdsförslagen från *top-down*-bedömningen 2009 i affärsområdenas arbetsprogram.

ECB:s kontinuitetshantering

40. Kontinuitetshantering är en viktig del av hanteringen av operativa risker. Det måste finnas beredskapsplaner och rekonstruktionsplaner för olika krissituationer för att garantera att centrala verksamheter och processer kan fortsätta om en kris skulle inträffa.

41. Revisionsrätten undersökte om

- (i) den övergripande ramen för kontinuitetshantering är adekvat och följer bästa praxis,
- (ii) de centrala processerna har identifierats på ett adekvat sätt,
- (iii) de enskilda kontinuitetsplanerna för de utvalda affärsområdena behandlar risker på ett lämpligt sätt som garanterar att centrala operationer fortsätter att fungera korrekt,
- (iv) kontinuitetsarrangemangen har testats på lämpligt sätt,

- (v) personalen känner till och har utbildats om kontinuitetsarrangemangen.

Ramen för kontinuitetshantering

42. *Kontinuitetshantering är en heltäckande metod för verksamheten med strategier, standarder och förfaranden som ska garantera att specificerade operationer kan fortgå eller snabbt återskapas vid ett avbrott. Syftet är att minimera de operativa, finansiella, rättsliga, anseendemässiga och andra väsentliga konsekvenser som kan uppkomma till följd av ett avbrott*²⁹.

43. Kontinuitetshanteringen ska garantera att arrangemangen och lösningarna för kontinuitet överensstämmer med ECB:s mål, förpliktelser och skyldigheter enligt fördragen och med ECB:s risktoleranspolicy³⁰.

44. Vid granskningen gjordes en genomgång av de nyckeldokument som bildar ramen för kontinuitetshanteringen:

- Kapitel 26 i handboken om affärspraxis anger den allmänna ramen, definierar vilka processer och vilken output som ska fortsätta att produceras och roller och ansvarsområden.
- ECB:s strategi för test av och utbildning om kontinuitet.
- Programmet för test av kontinuitet.
- Handboken om krishantering.

45. ECB har tagit fram en handbok om krishantering med definitioner av roller, ansvarsområden och processer vid en krissituation och krishanteringsteamets kontaktuppgifter. Varje affärsområde har det fulla ansvaret för att utarbeta sin kontinuitetsplan. Emellertid krävs det inte enligt mallen för kontinuitetsplaner en övergripande kontinuitetsplan för ECB, och någon sådan har inte utarbetats.

²⁹ *High-level principles for business continuity* (högnivåprinciper för driftskontinuitet), Baselkommittén för banktillsyn, augusti 2006, punkt 9.

³⁰ *Business Practice Handbook* (handbok om affärspraxis), femte utgåvan, ECB, 24 september 2010.

46. ECB har upprättat en stabil ram med vägledning i strategier, processer och ansvarsområden för organisationens kontinuitetshantering. Om det inte sker en strikt samordning leder emellertid det decentraliserade tillvägagångssättet även till en risk för att kontinuitetshanteringen inte tillämpas enhetligt inom hela organisationen.

Identifiering av centrala processer

47. Verksamhetsanalys är en dynamisk process för identifiering av centrala operationer och tjänster, viktiga interna och externa samband och lämpliga motståndskraftsnivåer. Det är en bedömning av risker och potentiella konsekvenser för en organisations operationer och anseende vid olika avbrottsscenarier³¹.

48. Den senaste fullständiga verksamhetsanalysen gjordes 2006³² för att identifiera de produkter och tjänster från ECB som är centrala för att bankens viktigaste operationer ska kunna fortgå. Verksamhetsanalysen var inriktad på följande nyckelområden:

- Identifiering av de processer som är centrala för verksamheten.
- Kategorisering av centrala behov.
- Vägledning i hanteringen av icke återkommande eller sällan förekommande processer.
- Identifiering av ytterligare stödbehov.

49. När det 2007 gjordes en omfattande uppföljning av verksamhetsanalysen identifierades luckor som gällde kontinuiteten och de arrangemang som då gällde. En uppföljningsstrategi utarbetades med alternativen att antingen täppa

³¹ *High-level principles for business continuity* (högnivåprinciper för driftskontinuitet), Baselkommittén för banktillsyn, augusti 2006, punkt 10.

³² *ECB Business Impact Analyses* (verksamhetsanalyser avseende ECB), genomgång 2006, generaldirektoratet för HR, budget och organisation, 16 januari 2007.

till de identifierade luckorna eller acceptera riskerna och kostnaderna. I dokumentet angavs kostnaderna för IT-lösningar eller lösningar i form av logistisk infrastruktur, men kostnaderna hade inte brutits ner så att det framgick hur de påverkades vid olika risknivåer.

50. Den senaste uppdateringen av verksamhetsanalysen för att täppa till de luckor som identifierades 2007 slutfördes under 2010. Det har inte gjorts någon fullständig verksamhetsanalys efter finanskrisen.

Kontinuitetsplaner

Centrala operationer

51. Kontinuitetsplanerna ska vara utformade så att centrala operationer identifieras för att garantera att ECB kan fullgöra sina skyldigheter enligt fördragen såsom de anges i protokollet om ECB:s stadga³³.

Kontinuitetsplanerna ska utarbetas för ett värsta krisscenario och så att responsen kan justeras ner för att anpassas till den faktiska krisen³⁴.

52. ECB har satt upp primära riktvärden för att rangordna ett antal risker utifrån hur centrala de är och utifrån bankens skyldigheter enligt fördragen (se **ruta 3**).

Ruta 3 - Primära riktvärden för att rangordna risker efter hur centrala de är

Fullgöra skyldigheter enligt fördraget, inbegripet att

- utforma och genomföra euroområdet monetära politik,
- genomföra valutatransaktioner,
- inneha och förvalta euroländernas officiella valutareserver,
- främja väl fungerande betalningssystem.

³³ I artikel 3 i protokoll (nr 4) om stadgan för Europeiska centralbankssystemet och Europeiska centralbanken anges de uppgifter som ECB ska utföra enligt fördragen.

³⁴ *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery* (riktlinje om driftskontinuitet: praktisk vägledning i beredskap vid nödlägen, krishantering och återhämtning efter katastrofer), *ASIS international*, 2005, punkt 11.3.

Konsekvenserna av avbrott för en identifierad process när det gäller

- instabilitet på marknaden,
- förlust av trovärdighet/image/anseende,
- ekonomisk förlust för ECB,
- ekonomisk förlust för andra institutioner,
- eventuella rättsliga problem,
- andra konsekvenser som inte nämns ovan.

Källa: ECB, översyn av verksamhetsanalysen 2006.

53. Enligt revisionsrättens genomgång av dessa primära riktvärden och en preliminär bedömning av i vilken utsträckning operationer fortsätter att fungera vid de angivna scenarierna³⁵, var de planer som tagits fram utformade för att garantera att skyldigheterna enligt fördragen uppfylls. Vid revisionsrättens genomgång av kontinuitetsplanerna konstaterades dock att det saknades planer för att hantera en stor förlust av personal³⁶ vid en katastrof. De processansvariga affärsområdena hade definierat vilken personal som behövdes för fortsatt drift och identifierat deras ersättare, men inget affärsområde hade en reservplan för en situation där stora delar av personalen inte var disponibel.

Överensstämmelse med den allmänna mallen för kontinuitetsplaner

54. Enligt den allmänna mallen för kontinuitetsplaner som fastställs på hög nivå ska kontinuitetsplanerna för enskilda affärsområden innefatta

- organisatoriska aspekter³⁷,
- centrala processer³⁸,

³⁵ Med utgångspunkt från sex katastrofscenarier övervägs i verksamhetsanalysen konsekvenserna för varje affärsområdes operativa kapacitet.

³⁶ Sådana planer ska finnas enligt högnivåprinciperna för driftskontinuitet, Baselkommittén för banktillsyn, augusti 2006, punkt 23.

³⁷ Det vill säga de organ som fattar beslut vid en kris, kontinuitetsteamets sammansättning, relationer med andra team och kontinuitetsteamens lokalisering.

³⁸ Det vill säga de som har identifierats och godkänts vid verksamhetsanalysen och en uppgiftsförteckning över de specifika aktiviteter som krävs för att garantera att de ovan nämnda centrala processerna kan fortgå.

- *behov*³⁹,
- *en förteckning över berörda parter.*

*En organisation ska väga sin direkta nytta av åtgärder för att förbättra sin motståndskraft mot operativa avbrott mot kostnaderna för dessa åtgärder*⁴⁰.

55. ECB:s övergripande mall för kontinuitetsplaner anger den obligatoriska strukturen på och det obligatoriska innehållet i de enskilda affärsområdenas kontinuitetsplaner. Mallen innehåller endast strukturen på de dokument om kontinuitetsplaner som affärsområdena ska lägga fram.

56. Kontinuitetsplaner utarbetas för affärsområden, avdelningar eller sektioner. Mallen för kontinuitetsplaner följs i allmänhet när det gäller det obligatoriska innehållet men skillnaderna är stora i hur detaljerade planerna är. Funktionen för hantering av operativa risker/kontinuitetshantering spelar en central roll som samordnare, men kvaliteten på de enskilda kontinuitetsplanerna är beroende av den som är ansvarig på affärsområdesnivå. Det fanns inga bevis för att de enskilda kontinuitetsplanerna blir tillräckligt granskade av funktionen för hantering av operativa risker/kontinuitetshantering.

57. Av de fem affärsområden⁴¹ som valdes ut för närmare kontroll hade fyra en kontinuitetsplan som överensstämde med kraven, och av dessa behandlade tre fullt ut de centrala processer som hade identifierats i verksamhetsanalysen.

58. För de flesta fallen saknades dokumentation om kostnads–nyttoanalyser av kontinuitetsalternativen för affärsområdena i urvalet, inbegripet en bedömning av olika risknivåer.

³⁹ Det vill säga IT-utrustning och kontorsutrustning samt handböcker.

⁴⁰ *High-level principles for business continuity* (högnivåprinciper för driftskontinuitet), Baselkommittén för banktillsyn, augusti 2006, punkt 13.

⁴¹ GD-IS har en separat kontinuitetsprocess. En extern revisor kontrollerar att den överensstämmer med ISO 20000 och den har därför uteslutits från revisionsrättens granskning 2010.

Testning

59. *Organisationer ska testa sina kontinuitetsplaner, utvärdera deras ändamålsenlighet och uppdatera sin kontinuitetshantering efter behov⁴². Enligt BS 25999⁴³ ska organisationen se till att dess arrangemang för kontinuitetshantering valideras genom övning och översyn och hålls uppdaterade.*

60. Följande dokument granskades:

- Strategin för testning av kontinuitet⁴⁴.
- Testningsprogram och tidsplaner för perioden 2008-2010.
- Testningsrapporter.

61. Testningsstrategin är inriktad på de kontinuitetsplaner och de planer för återskapande av informationssystem som man har tagit fram för att se över de processer som enligt verksamhetsanalysen är centrala. I testningsramen anges en tydlig ansvarsfördelning, testningens omfattning, rapporteringskrav, testningsfrekvens och relevanta testningsprogram på medellång sikt. Granskningen visade att det har fastställts en adekvat testningsram i enlighet med kraven i BS 25999.

62. De gjorda testerna visade att testövningarna, även om de innefattade nyckelpersonal och genomfördes regelbundet, inte alltid återskapade de omständigheter som ECB skulle ställas inför vid ett större verksamhetsavbrott. De tester som planerades för 2009 och 2010 täckte inte in alla de scenarier

⁴² *High-level principles for business continuity* (högnivåprinciper för driftskontinuitet), Baselkommittén för banktillsyn, augusti 2006, punkt 6.

⁴³ *British Standard's Code of Practice for BCM* (Storbritanniens norm för kontinuitetshantering).

⁴⁴ *ECB Business Continuity Testing and Training Strategy* (strategin för testning av och utbildning om kontinuitet), kommittén för operativa risker, 4 mars 2008.

som ECB hade satt upp, och alla de tester som ursprungligen var planerade genomfördes inte.

Utbildning och kännedom

63. *Krishanteringsteamerna och responsteamerna bör utbildas om sina ansvarsområden och skyldigheter. Teamerna bör vidareutbildas minst varje år och nya medlemmar bör utbildas när de börjar i teamet. All personal bör utbildas i att utföra sina respektive plikter vid en krissituation. De bör också känna till de viktigaste delarna av kontinuitetsplanen*⁴⁵.

64. I den utbildningsstrategi som ECB har antagit föreskrivs att all personal ska få ta del av ett program för ökad kännedom om kontinuitetshantering⁴⁶. När det gäller testning sägs i utbildningsstrategin att det ska upprättas ett utbildningsprogram med närmare uppgifter om genomförandet.

65. Under 2010 hölls fem halvdagsutbildningar om krishantering med en genomgång av den handbok om krishantering som ECB har antagit. Allmänt sett gav kursdeltagarna positiva omdömen både om införandet av handboken och om utbildningen, men det noterades också att simuleringsövningar skulle vara mycket uppskattade.

66. Vid granskningen framkom tydliga bevis för att den personal som är relevant för kontinuiteten utbildas, nämligen genom testningen av kontinuitetsplanen, men det fanns inga bevis för att man aktivt försökte förbättra den övriga personalens kännedom om ramen och processerna för kontinuitet. I flera interna referensdokument⁴⁷ konstateras att även om testning

⁴⁵ *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery* (riktlinje om driftskontinuitet: praktisk vägledning i beredskap vid nödlägen, krishantering och återhämtning efter katastrofer), ASIS international, 2005, punkt 12.11.

⁴⁶ *ECB Business Continuity Testing and Training Strategy* (strategin för testning av och utbildning om kontinuitet), kommittén för operativa risker, 4 mars 2008.

⁴⁷ Se s.15 i *ECB Business Continuity Testing and Training Strategy* (strategi för testning av och utbildning om kontinuitet), 26.1 i *Business Practice Handbook* (handbok om affärspraxis), *Business Continuity Framework* (kontinuitetsram)

spelar en nyckelroll vid utbildningen av personalen finns det behov av att nå hela personalen genom ett program för att öka kännedomen. Något sådant program har ännu inte utarbetats eftersom den centrala funktionen för hantering av operativa risker/kontinuitetshantering anser att personalens kännedom om arrangemangen för kontinuitet är tillfredsställande. Av en intern enkät⁴⁸ framgår det dock att över 12 % (20 % 2009) av de svarande inte känner till kontinuitetsarrangemangen för sitt affärsområde och inte vet var man hittar information om hur man ska reagera i en krissituation.

Är ECB:s hantering av finansiella risker ändamålsenlig?

67. Hanteringen av finansiella risker är en process för att handskas med osäkerhet på finansmarknaderna. Den innefattar bedömning av de finansiella risker som en organisation ställs inför och framtagning av hanteringsstrategier i enlighet med interna prioriteringar och intern policy.

68. Revisionsrätten undersökte om

- den övergripande ramen för hantering av finansiella risker avseende investeringar och penningpolitiska transaktioner är lämplig och överensstämmer med bästa praxis,
- den metod för finansiella risker som ECB använder är lämplig för hantering av finansiella risker,
- ECB tillämpar metoden för finansiella risker på ett ändamålsenligt sätt,
- rapporteringen om hantering av finansiella risker är regelbunden och tillförlitlig.

(ECB:s intranät) och *Business Continuity Management Policy document* (policydokument om kontinuitetshantering).

⁴⁸ Rapporterna om ECB:s interna kundenkät 2010 och 2009.

Ram för hantering av finansiella risker avseende investeringar och penningpolitiska transaktioner

69. *Ramen bör definiera den finansiella risken för hela banken och ange principerna för hur finansiella risker ska identifieras, bedömas, övervakas och kontrolleras/minskas⁴⁹. Banken ska ha ett system för hantering av finansiella risker med tydligt fördelade ansvarsområden.*

70. ECB:s ram för hantering av finansiella risker har utformats så att den ska täcka risker i samband med två typer av ECB-transaktioner: i) investeringar och ii) kredit. Investeringstransaktionerna gäller de två investeringsportföljerna, valutareserver⁵⁰ (60 600 miljoner euro per den 31 december 2010) och egna medel⁵¹ (13 300 miljoner euro per den 31 december 2010).

Kredittransaktionerna gäller penningpolitiska transaktioner⁵². I ECB:s investeringsverksamhet ingår förvaltningen av ECB:s valutareserver⁵³, ECB:s portfölj med egna medel, förvaltningen av pensionsfonden och verksamhet med anknytning till de två portföljer som används för penningpolitiska syften⁵⁴.

⁴⁹ Basel, *ERM COSO (Enterprise Risk Management Committee of Sponsoring Organizations, COSO-modellen för företagsövergripande riskhantering)*.

⁵⁰ Europeiska centralbankens riktlinje av den 20 juni 2008 om de nationella centralbankernas förvaltning av Europeiska centralbankens reservtillgångar och den rättsliga dokumentationen för transaktioner som gäller sådana tillgångar (omarbetning) (ECB/2008/5) (2008/596/EG).

⁵¹ Riktlinje om förvaltning av egna medel, juli 2010, *The ECB's Own Funds Investment Guidelines* (ECB:s riktlinjer om investering av egna medel), september 2010.

⁵² Europeiska centralbankens riktlinje av den 26 september 2002 om minimistandarder för Europeiska centralbanken och de nationella centralbankerna vid genomförandet av penningpolitiska transaktioner, valutatransaktioner med ECB:s valutareserver och vid förvaltningen av ECB:s reservtillgångar (ECB/2002/6).

⁵³ Inbegripet guldreserven.

⁵⁴ Programmet för inköp av säkerställda obligationer (CBPP) och programmet för värdepapper (SMP).

71. Riskhanteringsavdelningen har ansvaret för underhållet av den allmänna riskhanteringsramen för investeringstransaktioner och övervakningen, bedömningen och kontrollen av risker i samband med dessa transaktioner. Den övervakar att överenskomna strategier och processer för hanteringen av risker avseende marknaden och krediter efterlevs. Fall av bristande efterlevnad rapporteras i enlighet med överenskomna eskaleringsförfaranden.

72. GD-M är det affärsområde som utför investeringstransaktioner vid ECB. Det ansvarar även för underhåll och vidareutveckling av eurosystemets program för portföljhantering⁵⁵. Investeringsavdelningen inom GD-M har ansvar för att utarbeta investeringskommitténs förslag till taktiskt riktmärke för portföljerna med reservtillgångar och för den direkta förvaltningen av ECB:s portfölj med egna medel.

73. I handboken om hantering av finansiella risker⁵⁶, nyckeldokumentet om hantering av finansiella risker i samband med investeringsverksamhet, görs en heltäckande genomgång av alla relevanta strategier, processer och förfaranden med hänvisningar i första hand till de dokument som har antagits av ECB:s beslutsfattande organ.

74. Den övergripande ramen och den hantering av finansiella risker som ECB har infört för förvaltningen av investeringar och penningpolitiska transaktioner definierar finansiell risk för hela banken och anger principerna för hur finansiella risker ska identifieras, bedömas, övervakas och kontrolleras/minskas.

Metod för hantering av finansiella risker

75. *Man bör ta fram lämpliga investeringsriktlinjer för att tillräckligt fastställa riskbenägenhet och ge heltäckande anvisningar för investeringstransaktioner.*

⁵⁵ Program som används för förvaltningen av ECB:s valutareserver och egna medel och för att ta fram resultatsiffror.

⁵⁶ *Handbook of Financial Risk Management, Policies and procedures* (handbok om hantering, strategier och förfaranden när det gäller finansiella risker), mars 2008.

76. I ECB:s handbok om hantering av finansiella risker definieras följande delar:

- (i) ECB:s risktolerans.
- (ii) Godkända instrument och transaktioner.
- (iii) Godkända motparter och utgivare och fastställandet av gränser.
- (iv) Strategisk tillgångsallokering.
- (v) Övervakningsrapportering och bedömningar.
- (vi) Översyn av ramen⁵⁷.

77. Processen för investering av reservtillgångar styrs genom en struktur med tre nivåer bestående av det strategiska riktmärket, det taktiska riktmärket och de faktiska portföljerna. Det strategiska riktmärket återspeglar de långsiktiga risk- och avkastningspreferenserna och fastställs av ECB-rådet.

78. Processen för investeringar av egna medel bygger på en struktur i två nivåer - det strategiska riktvärdet och den faktiska portföljen. Det strategiska riktmärket fastställs av direktionen.

79. Avkastning maximeras med hänsyn till kravet att det inte får uppstå förlust och det krav som gäller tillgångsallokering och fördelas enligt en specifik tillgångsallokeringsstrategi⁵⁸.

80. Förteckningarna över godkända länder, utgivare och motparter upprätthålls av riskhanteringsavdelningen. Gränser för motparterna fastställs av riskhanteringsavdelningen enligt den metod som har godkänts av direktionen. För förvaltningen av reservtillgångar sätts gränserna för nationella centralbanker enligt den metod som har godkänts av ECB-rådet. Alla gränser

⁵⁷ Direktionen eller ECB-rådet ska regelbundet eller minst en gång om året se över punkterna (i)–(v).

⁵⁸ Beslutas av ECB-rådet när det gäller reservtillgångar och av direktionen när det gäller egna medel baserat på förslag från riskhanteringsavdelningen.

uppdateras systematiskt en gång om året. Dessutom får ändringar av kreditvärdigheten omedelbart konsekvenser för godkännande och gränser.

81. För den strategiska tillgångsallokeringen tas det hänsyn till följande strategiska högnivåkrav:

- (i) Mål för innehav av reservtillgångar.
- (ii) Risk- och avkastningspreferenser.
- (iii) Filosofi för utarbetandet av modeller.
- (iv) Investeringshorisont och ändringsfrekvens.
- (v) Ansvarsuppdelning mellan det strategiska riktvärdet och taktiska nivåer i investeringskedjan.
- (vi) Innehåll i den information som ligger till grund för investeringsbeslut.
- (vii) Godkända investeringar.
- (viii) Föreskrivna begränsningar för investeringar.

Investerings- och riskhorisonterna har angetts till ett år för reservtillgångar och fem år för egna medel.

82. Revisionsrätten granskade följande:

- Att definitionerna av riskbenägenhet och riskstrategi är fullständiga och lämpliga.
- Riktlinjerna för investeringar.
- Beslutsprocessen för att fastställa begränsningar för investeringar.
- Riskåtgärderna och hur konsekventa de är: marknadsrisk, kreditrisk, motpartsrisk, likviditetsrisk och operativ risk vid investeringsverksamhet.

83. Genomgången av ramen för hantering av finansiell risk visar att metoden för hantering av finansiell risk tillräckligt fastställer riskbenägenhet och ger heltäckande riktlinjer för investeringstransaktionerna vid ECB.

Tillämpning av metoden för hantering av finansiella risker

84. Den metod för hantering av finansiella risker som beskrivs i det föregående avsnittet bör tillämpas på ett ändamålsenligt sätt i praktiken.

85. Revisionsrätten utförde följande granskningsåtgärder:

- (i) Genomgång av om riktmärkena är lämpliga i förhållande till portföljens riskprofil, inbegripet felåtgärder, kvaliteten på uppgifter, hanteringen av uppgifter och säkerheten avseende uppgifter för strategiska och taktiska riktmärken.
- (ii) Genomgång av de verktyg och system som stödjer beräkningen och uppdateringen av portföljer och riktvärden.
- (iii) Genomgång av förvaltningen av ändring av riktmärken.

86. När det gäller ramen för *Value at Risk* övervägdes följande aspekter:

- (i) Analys av uppgifternas kvalitet och förvaltningen av uppgifter samt genomgång av uppgifterna om säkerhet och kontroll.
- (ii) Analys av tekniken för utarbetande av modeller, modellantaganden och av nyckelkomponenter för utarbetandet av modeller.
- (iii) Rimlighetstester, genomgång av resultat av utfallstester och analys av rapportering.

87. Granskningen visade att metoden tillämpades på ett lämpligt sätt. Den så kallade fyra-ögon-principen hade dock inte dokumenterats. Vidare visade genomgången av de modeller som används för att beräkna de strategiska och taktiska riktmärkena och för VaR-beräkningarna, inbegripet valideringen av modellen, att för några modeller

- a) hade det inte på senare tid gjorts regelbunda, dokumenterade utfallstester av modellerna,
- b) hade det inte gjorts en oberoende validering av de modeller som användes, och modellerna hade inte uppdaterats nyligen,
- c) var inte alltid modellantagandena tillräckligt dokumenterade.

88. En genomgång av bästa praxis vid andra liknande internationella organisationer visade att efter finanskrisen i USA, och som en del av förbättringen av kapaciteten att förvalta finansiella risker, inrättade USA:s centralbank i New York ett team som skulle validera modeller. Teamets nyckeluppgifter beskrivs i **ruta 4**.

Ruta 4 - Modellvalideringsteamet vid USA:s centralbank i New York

Teamets nyckeluppgifter är att:

- inventera alla modeller som används vid hantering av finansiella risker,
- gå igenom och validera dokumentationen om modellerna,
- ta fram detaljerad dokumentation när dokumentationen bedöms vara otillräcklig,
- testa modeller.

Är rapporteringen av finansiella risker adekvat?

89. *Det bör finnas en process för regelbunden övervakning av riskprofiler och väsentlig förlustexponering. Det bör införas ett tillförlitligt system för övervakning och rapportering.*

90. Riskhanteringsavdelningen övervakar att överenskomna strategier för riskhantering och riskprocesser avseende marknads- och kreditrisker efterlevs,

och den har också ansvaret för att rapportera bristande efterlevnad i enlighet med överenskomna eskaleringsförfaranden. Riskhanteringsavdelningen vid ECB rapporterar regelbundet om risk/avkastning och resultat för ECB:s portföljer för både valutareserver och egna medel liksom om de tillhörande strategiska och taktiska riktmärkena. Rapporteringen sker varje dag, vecka, månad, kvartal och år.

91. Den granskning och de intervjuer som revisorerna gjorde bekräftade att resultaten rapporteras regelbundet och omgående överlämnas till ledningen. Dock noterade revisorerna att GIPS-standarderna⁵⁹, som anses vara bästa praxis, inte efterlevs fullt ut när det gäller ECB:s interna rapportering av resultat.

SLUTSATSER OCH REKOMMENDATIONER

Har ECB fastställt en lämplig och heltäckande styrningsram för riskhantering?

92. ECB har fastställt en heltäckande struktur för organisationen, och roller och ansvarsområden är tydligt fördelade. Det finns dock en tydlig avgränsning mellan hanteringen av finansiella och operativa risker vid banken, och detta ökar risken för att överblicken över bankens totala exponeringar kanske inte är heltäckande. Det har inte inrättats något särskilt och oberoende organ, såsom en riskansvarig eller en riskhanteringskommitté, mellan direktionen och de två riskfunktionerna/riskenheterna - hantering av operativa risker/kontinuitetshantering och riskhanteringsavdelningen.

93. ECB:s årsredovisning innehåller endast kortfattad information om vissa riskhanteringsfrågor och ger ingen översikt över hur riskhanteringsprocessen i

⁵⁹ GIPS (*Global Investment Performance Standards*) är en uppsättning branschtäckande etiska principer som formuleras och förvaltas av CFA-institutet (*Chartered Financial Analyst*, auktoriserad finansanalytiker) och som ger anvisningar om hur investeringsresultat ska beräknas och rapporteras. De är frivilliga och bygger på de grundläggande principerna om full insyn i och rättvisande framställning av avkastningen på investeringar.

organisationen ser ut, vilka risker den utsätts för eller ledningens strategi för dessa risker.

Rekommendationer

1. ECB bör överväga att inrätta en hierarkiskt oberoende, särskild riskhanteringsfunktion, såsom en riskchef eller riskkommitté, som enbart skulle ägna sig åt riskhantering och garantera en heltäckande överblick över bankens exponeringar.
2. ECB bör ytterligare förbättra de upplysningar den offentliggör om riskhanteringspraxis till externa parter i årsredovisningen genom att tillämpa bästa praxis, såsom IFRS 7.

Är ECB:s hantering av operativa risker ändamålsenlig?

94. ECB har en tydlig organisatorisk struktur och etablerade adekvata strategier för hanteringen av operativa risker där bankens metoder för att bedöma, övervaka och kontrollera/minska risker anges.

95. Det gjordes *top-down*-bedömningar 2008 och 2009, och det togs fram handlingsprogram för varje affärsområde, men inga kostnadsnyttoanalyser fanns dokumenterade.

96. Det har införts ett system för rapportering, övervakning och uppföljning, och man har kommit överens om en tidtabell för uppföljningen av åtgärderna för att minska risken när det gäller medelhöga och höga risker. För några risker tog dock det godkännandeförfarande som tillämpas av kommittén för operativa risker och av direktionen mycket lång tid. Cyklerna för planering och hantering av operativa risker är inte integrerade. Vidare presenterades inte den operativa riskhanteringsverksamheten tydligt i några av de granskade affärsområdenas arbetsprogram.

97. ECB har tagit fram en utförlig handbok om krishantering där roller, ansvarsområden och processer vid en krissituation definieras och kontaktuppgifter till krishanteringsteamet anges. Varje affärsområde har det fulla ansvaret för att utarbeta sin kontinuitetsplan.

98. ECB har infört en stabil ram med riktlinjer om strategier, processer och ansvarsområden för kontinuitetshantering i organisationen. Dock konstaterades följande:

- a) Det gjordes en omfattande uppdatering av verksamhetsanalysen 2007 som slutfördes 2010, men det har inte gjorts någon fullständig verksamhetsanalys sedan finanskrisen började.
- b) Det konstaterades att det saknas planer för att hantera en stor förlust av personal.
- c) De planerade testerna täckte inte in alla de katastrofscenarier som ECB hade planerat.
- d) Några av de tester som var planerade för 2009 och 2010 hade inte utförts.

Rekommendationer

- 3. Den årliga bedömningen av operativa risker bör införas i ECB:s cykel för strategisk och finansiell planering och i de enskilda affärsområdenas årliga arbetsprogram.
- 4. Det bör snarast antas åtgärder för att hantera medelhöga till höga operativa risker.
- 5. ECB bör fortsätta att förbättra sina kontinuitetsplaner och sitt testningsprogram och sträva efter att se till att alla planerade tester genomförs.

Är ECB:s hantering av finansiella risker ändamålsenlig?

99. Den övergripande ram och den hantering av finansiella risker som ECB har infört för att hantera investeringar och penningpolitiska transaktioner är adekvat. Genomgången av ramen för hantering av finansiella risker visade att den metod för hantering av finansiella risker som har utformats är stabil och adekvat för hanteringen av investeringar och penningpolitiska transaktioner vid ECB. Den praktiska tillämpningen av metoden behöver dock förbättras, till exempel när det gäller de modeller som används för att beräkna strategiska och taktiska riktvärden liksom vid beräkningar av VaR.

100. De interna rapporterna om riskhantering ger ECB:s högsta ledning och direktion korrekt, adekvat och uttömmande information om hanteringen av finansiella risker. Resultat rapporteras regelbundet och i tid, men rapporteringen uppdateras inte regelbundet så att den återspeglar ändringar av GIPS-standarderna.

Rekommendationer

6. ECB bör fortsätta att förbättra översynen och valideringen av de modeller som används för att beräkna strategiska och taktiska riktvärden liksom vid beräkningen av VaR och också ta fram detaljerad dokumentation där den bedöms vara bristfällig, testa modellerna och regelbundet se över modellantagandena.
7. Ändringar av GIPS-standarderna bör ses över varje år, och man bör överväga att tillämpa dem fullt ut för ECB:s interna resultatrapportering.

Denna rapport har antagits av revisionsrättens avdelning IV, med ledamoten Louis GALEA som ordförande, vid dess sammanträde i Luxemburg den 27 mars 2012.

För revisionsrätten

Vítor Manuel da SILVA CALDEIRA
Ordförande

EUROPEISKA CENTRALBANKENS SVAR

svar på revisionsrättens rapport om effektiviteten i Europeiska centralbankens förvaltning för budgetåret 2010

Europeiska centralbanken (ECB) välkomnar revisionsrättens rapport för budgetåret 2010 och uttrycker sin uppskattning över revisionsrättens iakttagelser och rekommendationer för förbättringar. ECB noterar att revisionsrätten bekräftar att i) ECB har en klar organisationsstruktur och har etablerat en lämplig policy för hantering av operationella risker och att ii) det övergripande ramverket för finansiell riskhantering som upprättats av ECB för hantering av policytransaktioner och investeringar är tillfredställande.

ECB noterar rättens observationer och rekommendationer för förbättringar. ECB:s kommentarer vad gäller särskilda punkter och de sju rekommendationerna redovisas nedan.

Punkt 9 till 13 och 92

Vad gäller Revisionsrättens beskrivning av ECB:s övergripande system för riskhantering skulle vi vilja notera följande:

Ramverket för hantering av operativa risker, inklusive mätning och hantering av operativa risker vid ECB sorterar under Operativ riskhantering & Driftskontinuitet inom generaldirektoratet (ORM/BCM) för HR, budget och organisation. Ramverket för finansiell riskhantering avseende marknadsoperationer, samt mätning och hantering av operativa risker vid sådana operationer sorterar under Kontoret för riskhantering. Denna typ av organisering är vanlig bland centralbanker och likartade organisationer. Att det finns både en specialiserad funktion och ett kontor ska inte tolkas som en gränsdragning mellan hanteringen av finansiella och av operativa risker utan snarare som ett organisatoriskt val för att säkerställa en effektiv uppgiftsallokering för ECB:s övergripande riskhantering under direktionens gemensamma ansvar.

Avseende den senaste utvecklingen efter Revisionsrättens granskning, önskar ECB meddela att

- vad gäller operativa risker leds Kommittén för operativa risker (ORC) nu av ECB:s vice ordförande. Kommittén har ansvar för att främja och övervaka utveckling, tillämpning och underhåll av Operativ riskhantering (ORM).
- vad gäller finansiella risker, omorganiserade ECB i juli 2011 den tidigare avdelningen för riskhantering (RMA) till ett fristående kontor för riskhantering (RMO), vilket rapporterar direkt till direktionen via en annan direktionsledamot än den ledamot som har ansvaret för Generaldirektoratet för marknadsoperationer. Denna ändring berodde på: i) den allt viktigare roll som riskhantering spelar i centralbanker i allmänhet och ECB i synnerhet samt ii) den vägledning som ECB ger till alla centralbankerna i Eurosystemet avseende uppdelningen av rapporteringsvägar till de direktionsledamöter som har ansvaret för marknadsoperationer och riskhanteringen.

Se även svaret till rekommendation 1.

Punkt 16, 17 och 93

Information om riskhantering behandlas i flera kapitel i ECB:s årsrapport samt i ECB:s årsredovisning, som upprättats i enlighet med redovisningsprinciper som ECB-rådet anser vara lämpliga för en centralbanks verksamhet. Dessa redovisningsprinciper tillämpas för eurosystemstransaktioner av samtliga centralbanker i Eurosystemet och betraktas internationellt som lämpliga finansiella rapporteringsstandarder för centralbanker.

ECB:s rättsliga ram för redovisning och finansiell rapportering har lagts fast i beslutet om Europeiska centralbankens årsbokslut (ECB/2010/21). ECB följer värderingsprinciper som överensstämmer med IFRS redovisningsstandarder (International Financial Reporting Standards), vilka antagits av Europeiska unionen, om en viss bokföringsåtgärd inte behandlas i beslut ECB/2010/21 och förutsatt att ECB-rådet inte fattat något beslut om motsatsen. I enlighet med ovannämnda beslut utarbetar ECB sin årsredovisning baserat på ECB-rådets bedömning av lämplig grad av information och är inte bunden av den informationsskyldighet som fastlagts i IFRS 7.

Se även svaret till rekommendation 2.

Punkt 24

ECB önskar påpeka att ORM:s kommunikation på intranätet förser risksamordnare och chefer med all relevant information, inklusive information om klassificering av händelser och skälen till dessa. Mer vägledning till affärsområden om hur risker ska identifieras tillhandahålls vid varje uppdatering av den bankövergripande riskklassificeringsbedömningen.

Punkt 28

Antalet fast anställda i ORM/BCM ökades nyligen till fem. ECB är av uppfattningen att den nuvarande personalsammansättningen i det här området gör det möjligt att dra nytta av den externa arbetserfarenhet som kollegor från andra centralbanker bidrar med och att det inte ökar risken för en otillräcklig implementering av ORM-ramverket.

Punkt 29 och 66

För att ytterligare förbättra kännedomen om ORM:s ramverk och driftskontinuitet kommer ECB att ge mer relevant information på intranätet om ORM och BCM och uppmuntra chefer för riskgrupper att regelbundet göra presentationer för de som arbetar inom dessa affärsområden.

Punkt 37, 58 och 95

Policyn för ORM förordar att en kostnads–nyttoanalys görs när möjliga reaktioner på olika risker har definierats. Denna riskåtgärdsprocess ska säkerställa att strategierna är kostnadseffektiva. En sådan analys blir dock viktig först när ett beslut fattas om en konkret åtgärd för att bemöta risker. När ett projekt lanseras vid ECB erfordras t.ex. alltid en kostnads–nyttoanalys.

Punkt 50 och 98(a)

ECB har som praxis att uppdatera sin verksamhetsanalys vid behov snarare än på regelbunden basis för att säkerställa att ytterligare krav på driftskontinuitet, som t.ex. vid organisatoriska förändringar eller systemförändringar, nya processer eller tillämpningsprogram, beaktas i god tid. Sedan resultatet av en fullständig verksamhetsanalys presenterades för direktionen 2007 har ytterligare krav på driftskontinuitet integrerats i BCM-ramverket vid flera tillfällen.

Punkt 53 och 98(b)

ECB anser att dess omfattande planering för åtgärder i händelse av en pandemi är tillräcklig för att täcka för ett större bortfall i personalresurserna. I den osannolika situationen av ett totalt bortfall av personal har ECB upprättat reservsystem för att säkerställa att de viktigaste processerna kan fortsätta.

Punkt 62 och 98(c) och (d)

Den aktuella finanskrisen, som tvingat ECB:s nyckelfunktioner att vara tillgängliga i princip varje helg, har oundvikligen begränsat möjligheterna till och omfattningen av resurser för övergripande testning av driftskontinuiteten. Även om krishanteringsgrupper regelbundet utför konkreta scenariobaserade tester har en mer försiktig linje antagits vad gäller tester av ECB:s planer för den totala driftskontinuiteten och återställande av IT-funktioner för att begränsa risken för störningar av verksamheten.

Se även svaret till rekommendation 5.

Punkt 91 och 100

ECB har ännu inte fullt ut antagit ramverket för Global Investment Performance Standards (GIPS) av anledningen att det inte är helt tillämpligt på den verksamhet som bedrivs av en centralbank.

Se även svaret till rekommendation 7.

Rekommendation 1

ECB överväger och uppskattar alltid rekommendationer för att ytterligare förbättra riskhanteringen och tillämpa de allra senaste teknikerna för centralbankspraxis. Den aktuella organisationsstrukturen för riskhantering vid ECB ger en effektiv ram för uppgiftsallokering i ECB:s övergripande riskhantering under direktionens gemensamma ansvar.

Rekommendation 2

ECB uppfyller redan de relevanta rättsliga kraven för finansiell rapportering i enlighet med beslut ECB/2010/21. ECB har bevakat och kommer att fortsätta bevaka utvecklingen inom IFRS, särskilt sådan utveckling som är lämplig för ECB:s finansiella rapportering.

Rekommendation 3

ECB accepterar denna rekommendation. Även om enskilda verksamhetsområden inom ECB redan har införlivat åtgärder och kostnader för implementering av riskreducerande åtgärder i sina årliga arbetsprogram och budgetförslag, har ECB nyligen modifierat tidsplanen för de relevanta processerna för hela ECB i syfte att fullt ut samordna den årliga uppdateringen av den operativa riskhanteringsutvärderingen med de strategiska och finansiella planeringscyklerna.

Rekommendation 4

ECB accepterar denna rekommendation.

Rekommendation 5

ECB accepterar rekommendationen. ECB har ett starkt engagemang för att fortsätta att stärka sina beredskaps- och kontinuitetsplaner och kommer att sträva efter att testprogrammen för alla relevanta processer och resultat genomförs enligt tidsplan. Samtidigt kommer banken att väga hur brådskande det är att genomföra planerade tester mot kravet att minimera riskerna i verksamheten, särskilt nu med tanke på hur viktigt det är att komma över den aktuella finanskrisen.

Rekommendation 6

ECB accepterar denna rekommendation och har ett starkt engagemang att fortsätta övervaka, testa och dokumentera sin tillgångsallokering och sina riskmodeller i syfte att uppnå högsta möjliga standarder.

Rekommendation 7

ECB har bevakat och kommer att fortsätta att bevaka utvecklingen inom GIPS, särskilt sådan utveckling som är tillämplig för ECB:s interna rapportering av placeringsresultat.