IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

COURT OF AUDITORS

REPORT

on the audit of risk management of the European Central Bank for the financial year 2010, together with the ECB's replies

(2012/C 173/01)

TABLE OF CONTENTS

	Paragraph	*Page*
INTRODUCTION	1-4	3
AUDIT SCOPE AND APPROACH	5-6	3
AUDIT FINDINGS	7-91	3
Did the ECB establish an appropriate and comprehensive governance framework for risk management?	7-18	3
Overall risk management framework	8-14	3
Disclosure of ECB's risk management framework to external parties	15-18	4
Did the ECB manage its operational risks in an effective manner?	19-66	5
Operational risk management	20-39	5
ECB business continuity management	40-66	7
Did the ECB manage its financial risks in an effective manner?	67-91	10
Financial risk management framework for investments and policy operations	69-74	10
Financial risk management methodology	75-83	11
Application of the financial risk management methodology	84-88	12
Adequacy of reporting financial risks	89-91	12
CONCLUSIONS AND RECOMMENDATIONS	92-100	13
Did the ECB establish an appropriate and comprehensive governance framework for risk management?	92-93	13
Did the ECB manage its operational risks in an effective manner?	94-98	13
Did the ECB manage its financial risks in an effective manner?	99-100	13
Replies of the European Central Bank		15

ABBREVIATIONS

BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analyses
BIS	Bank for International Settlements
BPH	Business Practice Handbook
CBPP	Covered Bonds Purchase Programme
CRO	Chief Risk Officer
D-CO	Directorate Communication
DG-A	Directorate-General Administration
DG-H	Directorate-General Human Resources, Budget and Organisation
DG-IS	Directorate-General Information System
DG-M	Directorate-General Market Operations
DG-P	Directorate-General Payment Systems
DG-S	Directorate-General Statistics
EB	Executive Board
ECB	European Central Bank
ESCB	European System of Central Banks
FOS	Financial Operation Services
GIPS	Global Investment Performance Standards
IAS	International Accounting Standards
IASB	International Accounting Standards Board
IFRS	International Financial Reporting Standards
INV	Investment division
MOS	Market Operations Systems
NCBs	National Central Banks
OFM	Own Funds Management
ORC	Operational Risk Committee
ORM	Operational Risk Management
RMA	Risk Management Division (of DG-H)
SMP	Securities Markets Programme
VaR	Value at Risk

INTRODUCTION

1. The European Central Bank (ECB) and the national central banks of all European Union (EU) Member States together constitute the European System of Central Banks (ESCB). The primary objective of the ESCB is to maintain price stability. The ESCB also supports the general economic policies of the EU with a view to contributing to the achievement of the EU's objectives ([1]). For this purpose, the ECB carries out the tasks specified in its Statute ([2]) and is responsible for managing its activities and finances.

2. The European Court of Auditor's (the Court) audit of the operational efficiency of the ECB is based on Article 27(2) of the Protocol on the Statute of the ESCB and of the ECB ([3]). The 2010 audit covers the risk management procedures and systems established by the ECB and their application.

3. The decision-making bodies of the ECB are the Governing Council and the Executive Board ([4]). The Executive Board implements monetary policy in accordance with the guidelines and decisions laid down by the Governing Council ([5]) and has overall responsibility for the management of the day-to-day business of the ECB and its resources. The Executive Board is also ultimately responsible for risk management at the ECB.

4. Risks are managed through two separate frameworks at the ECB. The operational risk management unit (ORM ([6])/BCM) covers all operational risks (see footnote 22) including business continuity. The Risk management division (RMA) deals with the financial risk management (see paragraph 70), including the ECB's investment activities and credit operations.

AUDIT SCOPE AND APPROACH

5. The objective of the Court's 2010 financial year audit was to assess the adequacy of the ECB's operational and financial risk management framework ([7]). The risk management at the ECB was assessed in terms of the following key audit questions:

— Did the ECB establish an appropriate and comprehensive governance framework for risk management?

— Did the ECB manage its operational risks in an effective manner?

— Did the ECB manage its financial risks in an effective manner?

6. The audit of the risk management of the ECB ([8]) included the following elements:

(a) Review of the overall risk management framework at the ECB including review of the best practices in other similar international organisations in the area of risk management ([9]);

(b) Review of the operational risk management framework and testing of six selected business areas (Directorates-General) to assess the implementation of the risk management framework. The selection was based on: (i) ensuring coverage of significant operational risks; (ii) covering both core and non-core ECB activities; and (iii) covering activities requiring horizontal risk management. The selected Directorates-General (DG) were: Market Operations (DG-M), Payment Systems (DG-P), Statistics (DG-S), Administration (DG-A), Information Systems (DG-IS) and Directorate Communications (D-CO).

(c) Review of the financial risk management framework and detailed testing covering Risk management division (RMA) of DG Human Resources Budget and Organisation (DG-H) and market operations systems (MOS), financial operations services (FOS) and Investment (INV) divisions of the DG-M. The assessment of the ECB risk management methodology and its application was performed using the technical assistance of a team of financial risk experts from Ernst and Young, Luxembourg.

AUDIT FINDINGS

Did the ECB establish an appropriate and comprehensive governance framework for risk management?

7. The ECB's stated ambition is to apply best practice in its risk management: 'The European Central Bank placed, from the very beginning, particular attention to risk management. As a new member of the central bank community, it had the ambition of fulfilling the highest governance standards in organising its risk management function within the institution and applying state-of-the-art tools' ([10]).

Overall risk management framework

8. *'A strong institution-wide risk culture is one of the key elements for effective risk management. One of the prerequisites for creating this*

([1]) Article 127(1) of the Treaty on the Functioning of the European Union.

([2]) The Statute of the ESCB and of the ECB is a protocol attached to the Treaty.

([3]) Article 27(2) of the Protocol on the Statute of the ESCB and of the ECB stipulates: 'The provisions of Article 287 of the Treaty on the Functioning of the European Union shall only apply to an examination of the operational efficiency of the management of the ECB'.

([4]) Article 9(3) of the Protocol on the Statute of the ESCB and of the ECB. The Governing Council consists of the six Members of the Executive Board, plus the Governors of the national central banks of the Member States whose currency is the euro. The Executive Board consists of the President, the Vice-President and four other Members.

([5]) Article 12(1) of the Protocol on the Statute of the ESCB and of the ECB.

([6]) The scope of ORM covers risks related to activities of the ECB, including those related to ESCB/Eurosystem processes and projects.

([7]) The criteria against which the Court assessed the operational and financial risk management framework of the ECB are shown in this document in italics. Unless otherwise referenced, the criteria are the Court's.

([8]) The audit scope excluded the risk management at the level of European System of the Central Banks (ESCB).

([9]) Information visits were held with Federal Reserve Bank of New York and the Bank of Canada, questionnaires were sent to the Federal Reserve Bank of New York, the Bank of Canada and the Swiss National Bank.

([10]) José Manuel González-Páramo, Member of the Executive Board of the ECB, Ulrich Bindseil and Evangelos Tabakis, *Risk Management for Central Banks and Other Public Investors*, Cambridge University Press 2009.

risk culture is the establishment of a comprehensive (covering all risk types, business lines and relevant risks) and independent risk management function under the direct responsibility of the Chief Risk Officer (CRO), or the senior management if a CRO is not appointed, following the principle of proportionality' ([11]).

9. At the ECB each organisational unit ([12]) is responsible for managing its own risks and controls. Two functions/divisions support organisational units in the risk management process:

— the ORM/BCM function ([13]) is responsible for methodological maintenance, coordination of all operational risk related activities, as well as proactive advice to business areas ([14]),

— the Risk management division (RMA) deals with financial risks ([15]). The Risk management division is responsible for proposing policies and procedures and organisational support on risk management for all financial market operations conducted by the ECB or by the Eurosystem on behalf of the ECB. The division is organised in two units: risk analysis and risk strategy sections.

10. As a support to the Executive Board's (EB) decision-making, several committees have been set up which deal with various aspects of risk management, including the Operational Risk Committee, Investment Committee, Assets and Liabilities Committee and Credit Committee.

11. There is a comprehensive organisational structure with clearly assigned roles and responsibilities. However, there is a strong demarcation between the management of financial and operational risks in the ECB which increases the risk that the view of the Bank wide exposures might not be comprehensive.

12. No independent, single, body, such as a Chief Risk Officer or overall risk management committee, has been set up between the EB and the two risk function/units, ORM/BCM and RMA. At the time of the audit the EB member charged with risk management also had a number of other areas of responsibility, whereas a CRO would solely concentrate on risk management.

13. Furthermore, the lack of a hierarchically independent risk management function increases the risk that insufficient priority is given to risk management issues, e.g. allocation of staff resources to risk management tasks, as such matters are subject to DG-H decisions.

14. A review of best practices in other similar international organisations has shown that the Bank of Canada has adopted an integrated risk management framework, including a Chief Risk Officer and a risk management working group. Both deal with establishing a comprehensive risk profile for the Bank that includes business, operational and financial risks as described in *Box 1*. The Bank's risk management framework is fully embedded within its strategic planning, budgeting and year-end performance evaluation processes.

Box 1

An example of integrated risk management — Bank of Canada

The *Chief Risk Officer* has the following responsibilities:

— leads the development and improvement of the integrated risk management policy framework, and obtains management approval,

— provides risk management guidance and advice to other members of senior management, and chairs the Risk Management Working Group,

— co-chairs the Risk Committee of the Funds Management Committee with the Department of Finance.

The *Risk Management Working Group* has the following tasks:

— facilitates the full update of the Bank's risk self-assessment and the development of the annual and mid-year risk management report,

— meets three to four times a year to review the Bank's risk profile and to share risk management initiatives with the representatives' functions/departments.

Disclosure of ECB's risk management framework to external parties

15. *There should be sufficient public disclosure to allow external parties to assess the ECB's approach to risk management.*

16. The ECB publishes an annual report, including the annual accounts and the accompanying disclosure notes ([16]). The information about risk management in the annual accounts is rather limited and the information about the ECB's risk management principles and figures is not publicly

([11]) 'High level principles for risk management', Committee of European Banking Supervisors (CEBS), February 2010 (italics European Court of Auditors, original text in bold shown in normal typeface).
([12]) Section, division, directorate or directorate-general.
([13]) Which is part of DG-H.
([14]) The ORM/BCM function is also secretariat for the Operational Risk Committee (ORC).
([15]) The RMA is administratively part of DG-H but reports directly to the Executive Board member responsible for management of financial risks.
([16]) The ECB applies its own accounting reporting framework established by Decision ECB/2006/17 on ECB annual accounts as amended.

available (except for the consolidated value at risk [17] (VaR) figure). The annual report of the ECB contains brief information about certain risk management issues but does not disclose an overview of the risk management process in the organisation, the risks faced as well as the management's approach to those risks.

17. The use of International Financial Reporting Standards (IFRS) [18] is best practice in presenting an entity's accounts. The IFRS 7 'Financial instruments disclosure', deals with the presentation of the risks faced by an organisation in its accounts, however, it has not been applied by the ECB.

18. Other international or national central bank organisations such as the Bank for International Settlement (BIS) and the Bank of Canada disclose, in their annual financial statements, risk management information even though one of them does not apply IFRS (see *Box 2* below).

Box 2

Illustration of application of risk management disclosures

Organisation	Risk management disclosure in the annual accounts	Financial reporting framework
Bank for International Settlements (BIS)	The annual accounts disclose the risks faced by the bank, risk management approach and organisation, detailed overview of credit risk, market risk, liquidity risk and operational risk.	Specific financial reporting framework stipulated by the statutes of the bank
Bank of Canada	The annual accounts disclose an overview of the risk management process, risk-governance structure, the role of the Financial Risk Officer, financial risk faced by the bank, detailed overview of the credit risk, market risk and liquidity risk.	IFRS [19]

Did the ECB manage its operational risks in an effective manner?

19. Business continuity management complements the ECB's operational risk management (ORM) framework, and both form an important element of corporate governance [20].

Operational risk management

20. An effective operational risk management framework includes clear strategies and oversight by the board of directors and senior management, a strong operational risk culture and internal control culture (including clear lines of responsibility and segregation of duties) and effective internal reporting.

21. To assess the management of operational risks at the ECB the Court examined:

— the ORM policies established at the ECB,

— the organisational structure and responsibilities of operational risk management,

— its link to the strategic and financial planning (the annual budget cycle), and

— the risk identification, assessment and response, reporting, monitoring and follow-up in the business areas as well as at central level.

Operational risk policies

22. *The ORM policies should provide a clear bank-wide definition of operational risk and lay down the policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk.*

[17] Value at risk (VaR) is a widely used risk measure of the risk of loss on a specific portfolio of financial assets. For a given portfolio, probability and time horizon, VaR is defined as a threshold value such that the probability that the mark-to-market loss on the portfolio over the given time horizon exceeds this value, assuming normal markets and no trading in the portfolio, is the given probability level (According to: *Value at Risk: The New Benchmark for Managing Financial Risk (3rd edition)*, Philippe Jorion, McGraw-Hill Professional, 2006).

[18] International Financial Reporting Standards are principles-based Standards, Interpretations and the Framework adopted by the International Accounting Standards Board (IASB), also known by their old name of International Accounting Standards (IAS). In February 2001, the European Commission proposed a Regulation that required all EU companies listed on a regulated market, including banks and insurance companies to prepare consolidated accounts in accordance with IAS by 2005, at the latest. EU Member States were given the option to extend this requirement to unlisted companies and to individual company accounts. An EU endorsement mechanism, both on a political and technical level, was established to oversee the integration of IAS in the EU.

[19] Until 31 December 2010 the Bank of Canada had reported under Canadian Generally Accepted Accounting Principles, nevertheless, disclosing risk management information comparable to IFRS. From 1 January 2011 the Bank of Canada reports under IFRS.

[20] 'Business Practices Handbook', Chapter 26.

23. The operational risk management framework of the ECB was approved by the Executive Board in October 2007 [21] and is described in the Business Practice Handbook (BPH) published on the intranet and available to all staff. It outlines the ECB's ORM definition [22], risk tolerance policy, roles and responsibilities as well as outlining the policies for assessment, response and reporting and monitoring.

24. The ORM policies established provide a clear bank-wide definition of operational risk and lay down the policies outlining the Bank's approach to assessing, monitoring and controlling/mitigating the risk. However, the BPH does not provide details of the Bank's approach to identifying risks.

Organisational structure and responsibilities

25. *Business area management should have responsibility for implementing the policies, processes and procedures for managing operational risk in all of the bank's material activities, processes and systems. The bank should also have an operational risk management system with clear responsibilities assigned to a risk management function.*

26. The EB is ultimately responsible for operational risk management at the ECB. The Operational Risk Committee (ORC) deals with strategic and medium-term topics, as well as relevant short-term and ad-hoc topics [23]. The committee consists of EB member (Chairman) and seven senior managers of the Bank [24]. It has decision-making powers for risk acceptance at medium level whereas high-level risks must always be accepted by the EB. Meetings are held every two months or more frequently if needed.

27. The BPH clearly outlines the business areas as responsible for managing their operational risks [25]. Accordingly, each business area should nominate (at least) one risk coordinator who supports business area managers in ORM and acts as the first point of contact in ORM matters within the business area. Business area managers are also responsible for ensuring that staff gain and maintain the necessary competences to assume responsibility and accountability as regards ORM. The ORM/BCM function should develop and maintain the ORM framework and coordinates the business areas approach to ORM.

28. Of eight staff in the ORM-BCM function only four were permanent employees at the time of the audit. The others were on secondment from national central banks or on fixed-term contracts of three months to two years. This means that there is a high staff turnover which leads to a loss of continuity in an important function and increases the risk of the ORM framework not being adequately implemented in the ECB.

29. The awareness of staff of the ORM framework was included in staff surveys in 2009 and 2010. The 2009 survey showed that approximately 40 % of the respondents said they did not receive enough information about ORM; 56 % did not know who was appointed risk coordinator of their business area and 45 % did not know where to find information about ORM on the intranet. In the 2010 survey 40 % still did not know where to find information about ORM.

Link to the strategic and financial planning (the annual budget cycle)

30. *Risk management should be embedded in the ECB's governance as an integral part of the strategic, business and financial planning of the bank.*

31. An important part of establishing the ECB's risk profile is the annual assessment of operational risks conducted by the business areas and the ORM/BCM function. The assessments for 2009 were carried out by the business areas in June to August 2009 and a calibration meeting took place afterwards with the risk coordinators. The top-down report was finalised in January 2010.

32. The risk profile should be one of the inputs to the strategic planning process, which in turn drives the financial plan. The audit showed, however, that there is no integration of the annual assessment of operational risks and the strategic and financial planning cycle of the ECB. Therefore, ORM runs the risk of becoming an isolated exercise, and the financial plan may not be directing resources appropriately to achieve strategic goals [26].

[21] In 2008 the Executive Board decided to align the ORM framework of the ECB to the framework adopted at ESCB level.

[22] Operational risk is defined as 'the risk of a negative financial, business and/or reputational impact resulting from inadequate or failure of internal governance and business processes or from people, systems or external events'.

[23] It is mandated to stimulate and oversee the development, implementation and maintenance of operational risk management at the ECB.

[24] Members are senior managers from Market Operations, Information Systems, Administration, HR, Budget & Organisation, two core business areas on a one-year rotating basis and the Adviser to the Director General HR, Budget & Organisation.

[25] Business area (the risk owner) responsible for the horizontal risk (a risk that has impact on several business areas) should recommend and/or implement appropriate risk treatment measures that are applicable across the ECB.

[26] Based on the conclusion from the article 'ERM at the Federal Reserve Bank of Richmond', 2007, Jack Dorminey and Richard Mohn.

33. An example of good practice is the Bank of Canada where the risk profile of the bank is an integrated part of the overall strategic and financial planning cycle of the bank [27].

The ORM process: Risk identification, assessment and response, reporting, monitoring and follow-up

Risk identification, assessment and response

34. *All operational risk inherent in activities, processes and systems should be identified and assessed. Risks should be evaluated against the existing policy and tolerance level to determine an adequate response based on sufficient cost-calculations. There should be regular reporting of pertinent information to senior management and the Executive Board that supports the proactive management of operational risk.*

35. The ORM framework has been implemented mainly by top-down assessments. According to the risk policy of the ECB the business areas should also continuously perform bottom-up assessments of business area processes and the risks identified should be approved [28].

36. The ECB has conducted top-down risk assessments in 2008 and 2009. The ORM/BCM function provided the business areas with some pre-defined high-level risks which was the basis for their risk assessments. In the final report an action plan for each of the business areas was included. The BPH requires that the business areas should analyse and define risk response strategies and conduct a cost-benefit analysis of possible solutions.

37. All business areas had identified risks and responses in relation to the 2009 top-down exercise. The 2009 top-down assessment report contained follow-up action points for each business area. However, no cost-benefit analyses were documented in the sampled business areas.

38. For some risks the acceptance procedure by the ORC/EB was very slow after the risk was identified by the business area. For example, two risks identified in July-August 2009 were still not approved as of December 2010. The list of open action points reviewed at the ORC meetings also shows that some remained open for more than one year and some for up to two years.

39. For only three out of six sampled business areas was it possible to identify specific resources allocated to the ORM-activities in their work programme, but the description of ORM activities was vague and it was not possible to trace the action points from the 2009 ORM top-down exercise to the business area work programmes.

ECB business continuity management

40. Business continuity management (BCM) is a significant component of operational risk management. It requires contingency and recovery plans for the worst case scenarios to ensure continuity of critical activities and processes should a crisis occur.

41. The Court examined whether:

(i) the overall BCM framework is adequate and in line with best practice;

(ii) the critical processes are adequately identified;

(iii) the individual business continuity plans (BCPs) of selected business areas adequately address the risks to ensure proper continuity of critical operations;

(iv) the business continuity arrangements were adequately tested; and whether

(v) the staff was aware and trained in respect of business continuity arrangements.

BCM framework

42. *Business continuity management is an overall business approach that includes policies, standards and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption* [29].

43. The purpose of BCM is to ensure that the business continuity arrangements and solutions comply with the ECB's objectives, obligations, statutory duties and the ECB's risk tolerance policy [30].

44. The audit included a review of the key documents constituting the BCM framework:

— chapter 26 in the Business Practice Handbook sets the broad framework, defines the further processes and outputs to be produced, and defines roles and responsibilities,

(27) *Source:* The Bank of Canada website 'Medium-term plan 2010-12' (www.bankofcanada.ca as at 13 July 2011).

(28) For projects, such as IT, specific procedures exist as outlined in the Project Organisation and Control Procedures. Project risks are reported separately via the Project Steering Committee/New Premises Project Steering Committee. Risk management related to specific projects has been excluded from the scope of this audit.

(29) 'High-level principles for business continuity', Basel Committee on Banking Supervision, August 2006, paragraph 9.

(30) 'Business Practice Handbook' (BPH), 5th release, ECB, 24 September 2010.

— ECB business continuity testing and training strategy,

— business continuity testing programme, and

— crisis management manual.

45. The ECB has developed a crisis manual that defines roles, responsibilities and processes in the event of a crisis as well as contact details of the crisis management team. Each business area has full responsibility for developing its BCP. However, the high-level BCP template does not require an overall BCP at ECB level and one has not been prepared.

46. The ECB has set up a sound framework providing guidance on the BCM policies, processes and responsibilities in the organisation. However, its decentralised approach also creates a risk that, in the absence of strict coordination, BCM might not be consistently implemented across the organisation.

Identification of critical processes

47. *Business impact analyses (BIA) is a dynamic process for identifying critical operations and services, key internal and external dependencies and appropriate resilience levels. It assesses the risks and potential impact of various disruption scenarios on an organisation's operations and reputation* ([31]).

48. The most recent full business impact analysis (BIA) was performed in 2006 ([32]) to identify the ECB's deliverables and services critical to the continuity of the Bank's main operations. The key areas of focus for the BIA performed included:

— identification of the critical business processes,

— categorisation of the critical requirements,

— guidance on how to address non-recurring or infrequent processes,

— identification of additional support requirements.

49. A comprehensive BIA update performed in 2007 identified gaps in terms of business continuity and the arrangements valid at that time. A follow-up strategy was established. It included options to close the identified gaps or accept the risks and costs. However, whilst this document presented the costs in terms of IT and logistical infrastructure solutions, this was not broken-down to show the impact of the different risk-levels on costs.

([31]) 'High-level principles for business continuity', Basel Committee on Banking Supervision, August 2006, paragraph 10.

([32]) 'ECB Business Impact Analyses', Review 2006, Directorate-General Human Resources, Budget and Organisation, 16 January 2007.

50. The most recent BIA update to close the gaps identified in 2007 was completed in 2010. No full business impact analysis has been made since the financial crisis.

Business continuity plans

Critical operations

51. *The BCPs should be designed so that the critical operations are identified to ensure that the ECB should be able to fulfil its statutory obligations as defined in the relevant protocol on the statute of the ECB* ([33]). *BCPs should be developed around a 'worst case scenario' with the understanding that the response can be scaled down appropriately to match the actual crisis* ([34]).

52. The ECB has set primary benchmarks for the determination of criticality relative to a number of risks and based on its statutory obligations (see *Box 3*).

Box 3

Primary benchmarks for the determination of criticality

Meeting the statutory obligations, including:

— the definition and implementation of monetary policy for the euro area,

— the conduct of foreign exchange operations,

— the holding and management of official foreign reserves of the euro area countries, and

— the promotion of the smooth operation of payment systems.

The impact of interruption to an identified process with respect to:

— instability of market,

— loss of credibility/image/reputation,

— financial loss for the ECB,

— financial loss for other institutions,

— potential legal problems,

— other impacts not included above.

Source: ECB BIA review 2006.

([33]) Article 3 of the Protocol (No 4) on the statute of the European System of Central Banks and of the European Central Bank defines the statutory tasks to be performed by the ECB.

([34]) *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery*, ASIS international, 2005, paragraph 11.3.

53. Based on the Court's review of these primary benchmarks and a preliminary assessment of the potential level of operations continued under scenarios established ([35]), the plans developed were designed to ensure that the statutory obligations would be met. However, the Court's review of the BCPs identified a lack of plans to address a serious loss of human resources ([36]) in case of disaster. Although the business areas in charge of the processes defined the business continuity staff and identified their replacements, none had a back-up plan in case of wide-scale unavailability of staff.

Compliance with the high level BCP template

54. *According to the high-level BCP template, the individual BCPs of the business areas should cover:*

— *organisational aspects* ([37]),

— *critical processes* ([38]),

— *requirements* ([39]), *and*

— *stakeholders listing.*

An organisation shall weigh its direct benefit from measures to improve its resilience to operational disruptions against the cost of those measures ([40]).

55. The overall ECB high-level BCP template provides the mandatory structure and contents of individual business area BCPs. As such, this template only includes the structure of the BCP documents to be provided by the areas.

56. BCPs are prepared at the level of business area, department or division. The high-level BCP template is generally respected in terms of mandatory content, but there are large differences in the degree of the detail. Although the ORM/BCM function plays a central coordination role, the quality of the individual BCPs depends on the person responsible at the business area level. There was no evidence that the individual BCPs are sufficiently reviewed by the ORM/BCM function.

57. Out of the five business areas ([41]) selected for detailed testing, four delivered a BCP in line with the requirements, three of which fully addressed the critical processes identified in the BIA.

58. In most of the cases, no cost-benefit analysis was documented in the sampled business areas regarding the business continuity options, including assessment of various risk levels.

Testing

59. *Organisations should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate* ([42]). *BS25999* ([43]) *requires the organisation to ensure that its BCM arrangements are validated by exercise and review and are kept up to date.*

60. The following documents were reviewed:

— the business continuity testing strategy ([44]),

— the testing programmes and schedules for the period 2008-2010, and

— test reports.

61. The testing strategy focuses on the BCPs and information systems recovery plans developed to review critical processes according to the BIA. The testing framework includes a clear allocation of responsibilities, setting the scope of testing, reporting requirements, test frequency as well as relevant medium-term testing programme. The review indicated that an adequate testing framework has been established in line with the requirements of BS 25999.

62. The tests held identified that the testing exercises, although covering key personnel and carried out on a regular basis, do not always simulate the circumstances the ECB would face in case of major business disruption. Tests planned in 2009 and 2010 did not cover all scenarios set up by the ECB and not all tests originally planned were carried out.

([35]) Based on six disaster scenarios, the BIA considers the impact on the operational capability of each business area.

([36]) As required by 'High-level principles for business continuity', Basel Committee on Banking Supervision, August 2006, paragraph 23.

([37]) I.e. decision-making bodies in the event of a crisis, business continuity team composition, relations with other teams, business continuity team locations.

([38]) I.e. those that were identified and approved as part of the BIA, task list detailing the specific activities needed so as to ensure continuity of the abovementioned critical processes.

([39]) I.e. IT and office equipment, manuals.

([40]) 'High-level principles for business continuity', Basel Committee on Banking Supervision, August 2006, paragraph 13.

([41]) DG-IS has a separate business continuity process. It is subject to external audit for compliance with the ISO 20000 and for this reason the BCP of the DG-IS has been excluded from the scope of the Court's 2010 audit.

([42]) 'High-level principles for business continuity', Basel Committee on Banking Supervision, August 2006, principle 6.

([43]) British Standard's Code of Practice for BCM.

([44]) 'ECB Business Continuity Testing and Training Strategy', Operational Risk Committee, 4 March 2008.

Training and awareness

63. *The crisis management and response teams should be educated about their responsibilities and duties. Teams should be trained at least annually and new members should be trained when they join. All personnel should be trained to perform their individual responsibilities in case of a crisis. They should also be briefed on the key components of the business continuity plan* ([45]).

64. The training strategy adopted by the ECB specifies that all staff should benefit from a BCM awareness enhancement programme ([46]). As for testing, the training strategy foresees the establishment of a training programme that shall provide implementation details.

65. In 2010 five half day crisis management training programmes were held to provide a 'walk through' of the Crisis Manual adopted by the ECB. Overall, both the introduction of the manual as well as the training session received positive assessments from the course participants, but it was also noted that simulation testing would be highly appreciated.

66. Whilst the audit found clear evidence that the training of relevant business continuity personnel takes place, namely through the BCPs testing, it did not find evidence that other staff's awareness of the business continuity framework and processes was actively addressed. Several internal reference documents ([47]) recognise that although testing plays a key role in staff training, there is a need to address all staff by means of a staff awareness programme. Such a programme has not been developed so far, as the central ORM/BCM function considers that the awareness among staff of the business continuity arrangements is satisfactory. Nevertheless, an internal survey ([48]) points out that more than 12 % (20 % in 2009) of respondents are not aware of the business continuity arrangements for their business area and would not know where to find information on how to respond in the case of a crisis.

Did the ECB manage its financial risks in an effective manner?

67. Financial risk management is a process to deal with the uncertainties resulting from financial markets. It involves assessing the financial risks facing an organisation and developing management strategies consistent with internal priorities and policies.

68. The Court examined whether:

— the overall financial risk management framework for investments and policy operations is adequate and in line with best practice,

— the financial risk methodology used by the ECB is adequate for managing the financial risks,

— the financial risk methodology is applied effectively by the ECB, and

— the reporting on the financial risk management is regular and reliable.

Financial risk management framework for investments and policy operations

69. *The framework should provide a firm-wide definition of financial risk and lay down the principles of how financial risk is to be identified, assessed, monitored, and controlled/mitigated* ([49]). *The bank must have a financial risk management system with clear responsibilities assigned.*

70. The ECB's financial risk management framework is designed to cover risks arising from two ECB's operations: (i) investment; and (ii) credit. The investment operations relate to the two investment portfolios, foreign reserves ([50]) (60 600 million euro as at 31 December 2010) and own funds ([51]) (13 300 million euro as at 31 December 2010). The credit operations relate to monetary policy operations ([52]). The ECB's investment activities include the management of the foreign reserves of the ECB ([53]), the ECB's own funds portfolio, the management of the pension fund and activities related to the two portfolios held for monetary policy purposes ([54]).

([45]) *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery*; ASIS international; 2005; paragraph 12.1.1.

([46]) 'ECB Business Continuity Testing and Training Strategy', Operational Risk Committee, 4 March 2008.

([47]) 'Business continuity testing and training strategy', p. 15; 'Business Practice Handbook', 26.1; 'Business Continuity Framework' (ECB intranet); 'Business Continuity Management Policy document'.

([48]) Report of the 2010 and 2009 ECB Internal Customer Satisfaction Survey.

([49]) Basel, ERM COSO (Enterprise Risk Management Committee of Sponsoring Organisations).

([50]) Guideline of the European Central Bank of 20 June 2008 on the management of the foreign reserve assets of the European Central Bank by the national central banks and the legal documentation for operations involving such assets (recast) (ECB/2008/5) (2008/596/EC).

([51]) 'OFM Guideline', July 2010, 'The ECB's Own Funds Investment Guidelines', September 2010.

([52]) Guideline of the European Central Bank of 26 September 2002 on minimum standards for the European Central Bank and national central banks when conducting monetary policy operations, foreign exchange operations with the ECB's foreign reserves and managing the ECB's foreign reserve assets (ECB/2002/6).

([53]) Including the gold reserves.

([54]) Covered bonds purchase programme portfolio (CBPP) and the Securities markets programme (SMP) portfolio.

71. The RMA division is responsible for maintaining the general risk management framework for investment operations and monitoring, assessment and controls of the risks resulting from these operations. It monitors compliance with agreed market and credit risk management policies and processes. Cases of non-compliance are reported according to agreed escalation procedures.

72. DG-M is the business area conducting investment operations at the ECB. It is also responsible for the maintenance and further development of the Eurosystem's portfolio management application ([55]). The Investment Division of DG-M is responsible for the preparation of Investment Committee proposals for the tactical benchmark for the foreign reserves portfolios and the direct management of the ECB's own funds portfolio.

73. The Handbook of Financial Risk Management ([56]), the key document for financial risk management of investment activities, provides a comprehensive overview of all the relevant policies, processes and procedures in particular by referring to the documents endorsed by the ECB's decision-making body.

74. The overall framework and the financial risk management set up by the ECB for the management of investment and policy operations provides a bank-wide definition of financial risk and lays down the principles of how financial risk is to be identified, assessed, monitored, and controlled/mitigated.

Financial risk management methodology

75. *Adequate investment guidelines should be established to sufficiently determine the risk appetite and provide comprehensive guidance for the investment operations.*

76. The ECB Handbook of Financial Risk Management defines the following elements:

(i) the ECB's risk tolerance;

(ii) the approved instruments and operations;

(iii) eligible counterparties and issuers, limit setting;

(iv) strategic asset allocation;

(v) monitoring reporting and assessment; and

(vi) framework review ([57]).

([55]) Application used for the management of the ECB's foreign reserves and own funds, and to produce the performance figures.

([56]) 'Handbook of Financial Risk Management, Policies and procedures', March 2008.

([57]) Review of points (i) to (v) regularly or at least once a year by the Executive Board or the Governing Council.

77. The foreign reserves investment process is steered by a three-layer structure encompassing the strategic benchmark, the tactical benchmark and the actual portfolios. The strategic benchmark reflects the long term risk-return preferences and is decided by the Governing Council.

78. The own funds investment process is based on a two-layer structure, the strategic benchmark and the actual portfolio. The strategic benchmark is decided by the Executive Board.

79. Returns are maximised subject to the no-loss and asset allocation constraints and are implemented through a specific strategic asset allocation ([58]).

80. Lists of eligible countries, issuers and counterparties are maintained by the RMA. Limits for the counterparties are set by RMA based on the methodology approved by the Executive Board. For foreign reserves management, the limits are allocated to NCBs based on the methodology approved by the Governing Council. Once a year, a systematic update of all limits is undertaken. In addition, implications of rating changes on eligibility and limits are taken into account immediately.

81. The strategic asset allocation takes into account the following high level policy requirements:

(i) objectives for holding the reserves;

(ii) risk/return preferences;

(iii) the modelling philosophy;

(iv) the investment horizon and revision frequency;

(v) the division of responsibilities between the strategic benchmark and tactical layers in the investment chain;

(vi) the information content that feeds into investment decisions;

(vii) eligible investments; and

(viii) the imposed investment constraints.

The investment and risk horizons are set at one year for the foreign reserves and at five years for the own funds.

82. The Court's audit included a review of:

— the completeness and adequacy of risk appetite and risk strategy definition,

([58]) Decided by the Governing Council for the Foreign Reserves and Executive Board for the own funds based on the proposals from RMA.

— the investment guidelines,

— the decision process establishing investment limits,

— risk measures and their consistency: market risk, credit risk, counterparty risk, liquidity risk and operational risk of investment activities.

83. The review of the financial risk management framework indicates that the financial risk management methodology sufficiently determines the risk appetite and provides comprehensive guidance for the investment operations at the ECB.

Application of the financial risk management methodology

84. *The financial risk management methodology as described in the previous section should be effectively applied in practice.*

85. The Court's audit included:

(i) review of the adequacy of benchmarks against the portfolio risk profile, including error measures, data quality, data management and data security of strategic and tactical benchmarks;

(ii) review of the tools and system supporting the computation and update of portfolios and benchmarks; and

(iii) review of the benchmark change management.

86. For the value at risk framework review the following aspects were considered:

(i) analyses of data quality and data management, review of the security and control data;

(ii) analyses of modelling technique, model assumptions, key modelling components; and

(iii) reasonability tests, review of back-test results, analyses of reporting.

87. The testing showed that the methodology was adequately implemented. However, the 'four eyes principle' had not been documented. In addition, the review of the models used for the calculation of the strategic and tactical benchmarks as well as VaR calculations, including the model validation showed that for some of the models:

(a) recently, no regular back testing of the models was carried out and documented;

(b) no independent validation or recent update had been done for the models applied;

(c) the model assumptions were not always sufficiently documented.

88. A review of best practices in other similar international organisations has shown that following the financial crisis in the US and as part of strengthening its financial risk management capabilities, the Federal Reserve Bank of New York set up a model validation team. The key tasks of this team are described in *Box 4*.

Box 4

Model validation team at Federal Reserve Bank of New York

The key tasks of the team are outlined below:

— inventory of all models used in respect of financial risk management,

— review and validation of the model documentation,

— establishing detailed documentation in cases where the documentation is assessed as insufficient,

— testing of models.

Adequacy of reporting financial risks

89. *There should be a process to regularly monitor risk profiles and material exposures to losses. A reliable monitoring and reporting system should be put in place.*

90. Compliance with agreed market and credit risk management policies and processes is monitored by RMA, which is also responsible for reporting non-compliance according to agreed escalation procedures. The ECB RMA reports regularly on risk return and performance of both the ECB foreign reserves and own funds portfolios as well as on the associated strategic and tactical benchmarks. Reporting takes place at daily, weekly, monthly, quarterly and annual frequency.

91. The tests and interviews performed by the auditors confirmed that reporting of performance is done regularly and is distributed to the executive management on a timely manner. However, it was noted that GIPS ([59]) standards, considered to be best practice, is not fully complied with for the purpose of ECB internal reporting of performance.

([59]) The GIPS (Global Investment Performance Standards) are a set of standardised, industry-wide ethical principles, created and administered by CFA (Chartered Financial Analyst) Institute, that provide guidance on how to calculate and report investment results. They are voluntary and are based on the fundamental principles of full disclosure and fair representation of investment performance results.

CONCLUSIONS AND RECOMMENDATIONS

Did the ECB establish an appropriate and comprehensive governance framework for risk management?

92. The ECB has established a comprehensive organisational structure, the roles and responsibilities are clearly assigned. However, there is a strong demarcation between the management of financial and operational risks in the Bank, this increases the risk that the view of the Bank's exposures might not be comprehensive. No independent, single, body, such as a risk officer or committee, has been set up between the Executive Board and the two risk function/units, ORM/BCM and RMA.

93. The annual accounts of the ECB contain only brief information about certain risk management issues rather than disclosing an overview of the risk management process in the organisation, the risks faced as well as the management's approach to those risks.

Recommendations
1. The ECB should consider setting-up a hierarchically independent, single, risk management function, such as a chief risk officer or committee that would concentrate solely on risk management and ensure a comprehensive view of the Bank's exposures.
2. The ECB should further improve its public disclosure of risk management practices to external parties in the annual accounts by applying best practices, such as IFRS 7.

Did the ECB manage its operational risks in an effective manner?

94. The ECB has a clear organisational structure and established adequate operational risk management policies outlining the Bank's approach to assessing, monitoring and controlling/mitigating risks.

95. Although top-down assessments were conducted in 2008 and 2009, and action plans for each business area were identified, no cost-benefit analyses were documented.

96. A system of reporting, monitoring and follow-up has been established and a timetable agreed for the follow-up of the risk mitigation measures for medium and high risks. However, for some risks, the acceptance procedure by the ORC/EB took a very long time. There is no integration of planning and ORM cycles. Also, the ORM activities were not clearly shown in the work programmes of some business areas tested.

97. The ECB has developed a comprehensive crisis manual that defines roles, responsibilities and processes in the event of a crisis as well as contact details of the crisis management team. Each business area has full responsibility for developing its BCP.

98. The ECB has set up a sound framework providing guidance on the BCM policies, processes and responsibilities in the organisation. However:

(a) although a comprehensive business impact analysis update was performed in 2007 and completed in 2010, no full business impact analysis has been made since the start of the financial crisis;

(b) a lack of plans to address a serious loss of human resources was identified;

(c) tests planned did not fully cover all the disaster scenarios planned by the ECB; and

(d) some tests planned for 2009 and 2010 were not carried out.

Recommendations
3. The annual assessment of the operational risks should be included in the strategic and financial planning cycle of the ECB and in the annual work programmes of the individual business areas.
4. The measures for addressing medium to high operational risks should be resolved quickly.
5. The ECB should continue to enhance its business continuity plans and their testing programme, and strive to ensure that all the tests planned are carried out.

Did the ECB manage its financial risks in an effective manner?

99. The overall framework and the financial risk management set up by the ECB for the management of investment and policy operations is adequate. The review of the financial risk management framework indicated that the financial risk management methodology designed is sound and adequate for the management of investment and policy operations at the ECB. However, improvements are required in the practical application of the methodology, e.g. in the area of models used for the calculations of strategic and tactical benchmarks as well as VaR calculations.

100. The internal risk management reports provide accurate, adequate and comprehensive financial risk management information to the senior management and to the Board of the ECB. Reporting of performance is regular and timely, but it is not regularly updated to reflect changes in GIPS standards.

Recommendations
6. The ECB should continue to improve the review and validation of the models used for calculations of the strategic and tactical benchmarks as well as VaR calculations, including establishing detailed documentation in cases where documentation is assessed as insufficient, testing of the models and regular review of the model assumptions. 7. Changes in the GIPS standards should be reviewed on an annual basis and full application considered to the ECB internal reporting of performance.

This Report was adopted by Chamber IV, headed by Mr Louis GALEA, Member of the Court of Auditors, in Luxembourg at its meeting of 27 March 2012.

For the Court of Auditors

Vítor Manuel da SILVA CALDEIRA

President

REPLIES OF THE EUROPEAN CENTRAL BANK

The European Central Bank (ECB) welcomes the report of the European Court of Auditors for the financial year 2010 and expresses its appreciation for the Court's observations and recommendations for improvement. The ECB also notes the Court's acknowledgement that: (i) the ECB has a clear organisational structure and has established adequate operational risk management policies; and (ii) the overall framework for financial risk management as set up by the ECB for the management of investment and policy operations is adequate.

The ECB takes note of the Court's observations and recommendations for improvement. Comments by the ECB with regard to specific paragraphs and the seven recommendations can be found below.

Paragraphs 9 to 13 and 92

With reference to the Court's description of the ECB's overall risk management framework, we would like to note that:

The operational risk management framework, including the measurement and monitoring of operational risks at the ECB, fall under the competence of the Operational Risk Management & Business Continuity Management Function (ORM/BCM) within the Directorate-General Human Resources, Budget and Organisation. The financial risk management framework for market operations, as well as the measurement and monitoring of risk exposures from such operations, fall under the responsibility of the Risk Management Office (RMO). This type of organisational set-up is common in central banks and related organisations. Accordingly, the existence of a specialised function and office should not be interpreted as a demarcation between the management of financial and operational risks, but rather as an organisational choice aiming to ensure the efficient allocation of tasks under the Executive Board's collegial responsibility for the overall risk management at the ECB.

With regard to recent developments since the time of the Court's audit, the ECB would like to communicate that:

— in the area of operational risks, the Operational Risk Committee (ORC), which is responsible for fostering and overseeing the development, implementation and maintenance of ORM, is now chaired by the Vice-President of the ECB,

— in the area of financial risks, in July 2011 the ECB reorganised its former Risk Management Division (RMA) into a stand-alone Risk Management Office (RMO), which reports to the Executive Board via a different board member than the one responsible for its Directorate-General Market Operations. This change was the result of: (i) the more significant role played by financial risk management in central banks in general and the ECB in particular; and (ii) the guidance provided by the Governing Council to all Eurosystem central banks with regard to separating reporting lines to the board members responsible for the market operations function and the financial risk management function.

See also the response to Recommendation 1.

Paragraphs 16, 17 and 93

Information relating to risk management appears in several chapters of the ECB's Annual Report including the ECB's Annual Accounts, which are prepared in accordance with the accounting policies that the Governing Council of the ECB considers appropriate for central banking activities. These policies are applied consistently by all Eurosystem central banks for Eurosystem operations, and are regarded internationally as appropriate financial reporting standards for central banks.

The ECB's legal requirements vis-à-vis financial reporting are laid down in the Decision on the ECB's Annual Accounts (Decision ECB/2010/21). The ECB follows valuation principles in accordance with International Financial Reporting Standards (IFRSs), as adopted by the European Union, when a specific accounting treatment is not laid down in Decision ECB/2010/21 and in the absence of a decision to the contrary by the Governing Council of the ECB. Moreover, pursuant to the abovementioned Decision, the ECB prepares its Annual Accounts based on the Governing Council's appreciation of the appropriate level of accompanying disclosures, and is not required to comply with the disclosure requirements set out in IFRS 7.

See also the response to Recommendation 2.

Paragraph 24

The ECB would like to point out that its ORM intranet communication provides risk coordinators and managers with all relevant information, including information on the classification of events and root causes. Additional guidance to business areas on how to identify risks is provided at the launch of each annual update of the bank-wide operational risk assessment.

Paragraph 28

The number of permanent staff members in the ORM/BCM function was recently increased to five. In the ECB's opinion, the current composition of staff in this area allows benefits to be derived from the secondment of central banking staff and does not increase the risk of an inadequate implementation of the ORM framework.

Paragraphs 29 and 66

To further improve awareness of the ORM framework and business continuity arrangements, the ECB will enhance the presentation of the relevant information on its ORM and BCM intranet communications and invite risk team leaders to make regular presentations to staff in their business areas.

Paragraphs 37, 58 and 95

While the ORM policy advocates carrying out a cost-benefit analysis when initially defining possible risk response strategies in order to ensure that these strategies are cost-effective, such an analysis becomes essential when a decision on a concrete risk response measure is taken. For example, a cost-benefit analysis is always required when a project is initiated at the ECB.

Paragraphs 50 and 98(a)

The ECB's practice is to update its business impact analysis when necessary rather than at regular intervals to ensure that additional business continuity requirements, such as organisational or system changes, new processes or applications, are addressed in a timely manner. Indeed, since the outcome of a full business impact analysis was provided to the Executive Board in 2007, additional business continuity requirements have been integrated into the BCM framework on several occasions.

Paragraphs 53 and 98(b)

The ECB considers its fully-fledged pandemic planning to be sufficient to address a serious loss of human resources. Moreover, in the extremely unlikely event of total staff unavailability, the ECB has made fallback arrangements to ensure that its most critical processes continue to be carried out.

Paragraphs 62 and 98(c) and (d)

The current financial crisis, which has required key ECB functions to be available almost every weekend, has inevitably limited the scope for and frequency of its overall business continuity testing. As such, while very concrete scenario-based tests are conducted on a regular basis by the crisis management team, a more prudent approach has been adopted in respect of testing overall ECB business continuity plans and IT recovery facilities, in order to limit the risk of disruption to its ongoing tasks.

See also the response to Recommendation 5.

Paragraphs 91 and 100

The ECB has not adopted the full Global Investment Performance Standards (GIPS) framework on the grounds that it is not fully applicable to its activities as a central bank.

See also the response to Recommendation 7.

Recommendation 1

The ECB always considers and appreciates recommendations for further improving its risk management and applying state-of-the-art central bank practices. The current organisational structure for risk management at the ECB provides for an efficient framework for the allocation of tasks under the Executive Board's collegiate responsibility for the Bank's overall risk management.

Recommendation 2

The ECB already complies with the relevant legal requirements for its financial reporting as laid down in Decision ECB/2010/21. The ECB has kept and will continue to keep developments in the IFRS under review with particular regard to their appropriateness for the ECB's financial reporting.

Recommendation 3

The ECB accepts this recommendation. While individual ECB business areas have always incorporated actions and costs relating to the implementation of risk mitigation measures in their annual work programmes and budget submissions, the ECB has recently modified the timing of the relevant ECB-wide processes in order to fully align the annual update of the operational risk assessment with the strategic and financial planning cycles.

Recommendation 4

The ECB accepts this recommendation.

Recommendation 5

The ECB accepts the recommendation. The ECB is fully committed to continuing to enhance its business continuity plans, and will strive to ensure that testing programmes for all its relevant processes and deliverables are carried out in a timely manner. At the same time, however, it will weigh the urgency to carry out planned tests against the requirement to minimise risks in the execution of its tasks, particularly at this crucial moment in terms of overcoming the current financial crisis.

Recommendation 6

The ECB accepts this recommendation and remains committed to continuing to review, test and fully document its asset allocation and risk models with a view to attaining the highest possible standards.

Recommendation 7

The ECB has kept and will continue to keep developments in the GIPS under review with particular regard to their appropriateness for the ECB's internal reporting of investment performance.