Draft guide on governance and risk culture

Description: This publication outlines supervisory expectations for Banks within the European Union regarding their governance structures and risk culture. It emphasises the importance of effective management bodies, robust internal control functions, and comprehensive risk appetite frameworks. The guidance aims to enhance the stability and resilience of the financial system by providing a framework for sound decision-making and risk management practices.

Overview: This document provides comprehensive supervisory expectations for the governance and risk culture of Banks within the European Union. The guidance emphasizes the critical role of good governance and robust risk culture in maintaining financial stability. It outlines key components such as the functioning and effectiveness of management bodies, governance of internal control functions, and the design and implementation of risk appetite frameworks. The document also details the ECB's supervisory approach, including on-site inspections and off-site assessments. By setting out these expectations, the ECB aims to ensure Banks are well-prepared to handle various challenges, drawing on lessons from past financial crises to enhance the overall stability and trust in the Banking sector.

Key Topics:

A. Governance and Risk Culture: Importance for Banks

1) Overview of Governance and Risk Culture Components

- Governance Components:
  - **Management Body:** The management body is responsible for the overall direction and control of the bank. This includes setting strategies, ensuring effective oversight, and establishing clear governance frameworks.
  - **Organisational Structure:** A well-defined organisational structure should be in place to ensure clear lines of authority and responsibility.
  - **Accountability and Transparency:** Ensures that decision-making processes are transparent and that there is accountability at all levels of the organisation.
  - **Communication Channels:** Effective communication channels within the Bank are essential for ensuring that information flows freely and that all relevant stakeholders are informed.
- Risk Culture Components:
  - **Tone from the Top:** Senior management and the board of directors must set the right tone regarding risk management and ethical behaviour.
  - **Accountability:** Employees at all levels should understand their roles and responsibilities in managing risks.
  - **Effective Challenge:** Encourages a culture where employees feel comfortable challenging decisions and practices that may pose risks.

- **Incentives:** The Bank should align its incentive structures with its risk management objectives, ensuring that compensation practices do not encourage excessive risk-taking.

2) Governance Assessment of Specific Structures
   - Management Body:
     - **Effectiveness:** Assesses how well the management body performs its oversight function, including its ability to challenge executive decisions and manage conflicts of interest.
     - **Composition:** Evaluates the diversity, skills, and experience of the board members to ensure a balanced and comprehensive oversight capability.
     - **Functioning:** Examines the processes and dynamics within the board, such as meeting frequency, attendance, and the quality of discussions.
   - Committees and Sub-Committees:
     - **Audit Committee:** Reviews the effectiveness of internal controls and financial reporting processes.
     - **Risk Committee:** Oversees the Bank's risk management framework and ensures that all material risks are identified and managed.
     - **Remuneration Committee:** Ensures that the Bank's compensation practices are aligned with its risk appetite and long-term strategy.

3) Importance of Risk Culture for Banks
   - Culture Drivers:
     - **Leadership Commitment:** Senior leaders must demonstrate a commitment to fostering a strong risk culture through their actions and decisions.
     - **Values and Ethics:** The bank's core values and ethical standards should be clearly articulated and consistently reinforced.
     - **Behavioural Norms:** Encourages behaviours that support prudent risk-taking and compliance with regulatory requirements.
   - Risk Awareness and Reporting:
     - **Transparency:** Promotes a culture of openness where risk issues are openly discussed and reported.
     - **Training Programs:** Regular training and development programs should be conducted to enhance risk awareness and understanding across the organisation.
     - **Incident Reporting:** Establishes mechanisms for reporting and analysing risk incidents to learn from past mistakes and improve risk management practices.

B. Functioning and Effectiveness of Management Bodies

1) Roles and Responsibilities
   - Supervisory Function:
     - **Oversight:** Ensures that the supervisory function provides effective oversight of the management function, challenging decisions when necessary.

- **Separation of Roles:** Clearly defines the roles and responsibilities of the supervisory and management functions to avoid conflicts of interest.
- **Evaluation:** Regular assessments of the effectiveness of the supervisory function in fulfilling its oversight responsibilities.

- Decision-Making Process:
  - **Documentation:** Decision-making processes should be thoroughly documented to provide a clear audit trail.
  - **Transparency:** Ensures that decision-making is transparent, with all relevant information considered and debated.
  - **Diverse Perspectives:** Encourages the inclusion of diverse perspectives in the decision-making process to enhance the quality of decisions.

2) Composition and Policies

- Composition:
  - **Diversity:** Promotes diversity in terms of gender, skills, experience and background to enhance the effectiveness of the management body.
  - **Suitability:** Evaluates the suitability of individual members and the collective composition of the board to ensure it has the necessary expertise and experience.
- Governance Policies:
  - **Conflicts of Interest:** Establishes policies to manage and mitigate conflicts of interest within the management body.
  - **Succession Planning:** Develops robust succession planning processes to ensure continuity in leadership.
  - **Performance Evaluations:** Conducts regular performance evaluations of board members and the board as a whole to identify areas for improvement.

C. Internal Control Functions

1) Governance of Internal Control Functions

- Three Lines of Defence:
  - **1st line (Operational Management):** Responsible for managing risks and implementing internal controls within their areas of responsibility.
  - **2nd Line (Risk Management and Compliance):** Provides oversight and support to the 1st line, ensuring that risks are properly identified, assessed and managed.
  - **3rd line (Internal Audit):** Provides independent assurance on the effectiveness of the internal controls and risk management processes.
- Independence and Resources:
  - **Independence:** Ensures that internal control functions are independent from the business lines they monitor, with direct access to the management body.
  - **Resources:** Allocates sufficient resources, including skilled personnel and technological tools, to support the effective operation of internal control functions.

2) Specific Internal Control Functions

- Risk Management:
    - **Risk Identification:** Identifies and assesses all material risks facing the Bank, including credit, market, operational, and liquidity risks.
    - **Risk Monitoring:** Continuously monitors risk exposures and ensures that they remain within the Bank's risk appetite.
    - **Reporting:** Provides regular risk reports to the management body and relevant committees, highlighting key risk issues and trends.
- Compliance:
    - **Regulatory Adherence:** Ensures compliance with all applicable laws, regulations, and internal policies.
    - **Policy Implementation:** Develops and implements compliance policies and procedures to mitigate compliance risks.
    - **Monitoring and Reporting:** Monitors compliance with regulatory requirements and reports and breaches to the management body.
- Internal Audit:
    - **Audit Planning:** Develops a risk-based audit plan that covers all significant areas of the Bank's operations.
    - **Audit Execution:** Conducts audits in accordance with the plan, providing independent and objective evaluations of the bank's internal controls and risk management processes.
    - **Reporting:** Reports audit findings to the audit committee and management body, making recommendations for improvement and following up on their implementation.

D. Risk Appetite Framework (RAF)

1) Design and Implementation

- Defining Risk Appetite:
    - **Risk Appetite Statement:** Develops a clear and concise risk appetite statement that articulates the levels and types of risk the Bank is willing to take.
    - **Approval and Communication:** Ensures that the risk appetite statement is approved by the management body and communicated throughout the organisation.
- Components of RAF:
    - **Risk Limits:** Establishes specific risk limits that align with the Bank's risk appetite and strategic objectives.
    - **Monitoring and Reporting:** Implements processes for monitoring and reporting risk exposures against established limits.
    - **Integration:** Integrates the RAF with the Bank's strategic planning, capital planning and risk management frameworks.

2) Aligning with Strategic Objectives

- Integration:

- **Strategic Alignment:** Ensures that the RAF is aligned with the Bank's business strategy and financial goals.
- **Decision-Making:** Incorporates risk appetite considerations into the Bank's decision-making processes at all levels.

- Review and Update:
  - **Periodic Reviews:** Conducts regular reviews and updates of the RAF to ensure it remains relevant and effective.
  - **Stress Testing:** Performs stress testing and scenario analysis to assess the robustness of the RAF under various adverse conditions.

E. Supervisory Approach

1) Supervisory Methods and Tools

- On-Site Inspections:
  - **Evaluation:** Conducts comprehensive evaluations of the bank's governance and risk culture through on-site inspections.
  - **Techniques:** Uses techniques such as interviews, document reviews, and observations of management body meetings to assess effectiveness.
- Off-site Assessments:
  - **Data Analysis**: Analyses reports, public information, and other relevant data to identify potential governance and risk culture issues.
  - **Continuous Monitoring:** Engages in continuous monitoring to detect emerging risks and assess the bank's ongoing compliance with regulatory requirements.

2) Supervisory Dialogue

- Ongoing Interaction:
  - **Regular Meetings:** Holds regular meetings with Bank representatives to discuss governance and risk culture practices and address any concerns.
  - **Communication Channels:** Maintains open and effective communication channels between supervisors and banks to facilitate timely information exchange.
- Feedback Mechanisms:
  - **Supervisory Feedback:** Provides feedback to Banks on their governance and risk culture practices, identifying areas for improvement.
  - **Recommendations:** Issues recommendations for addressing identified issues and monitors the implementation of corrective actions.

F. Annex: Changes versus the Supervisory Statement on Governance and Risk Appetite of 2016

Key Changes and Updates

- Building on the 2016 statement, inclusion of more detailed chapters on a wider range and number of topics. Heightened focus on the topic of risk culture, including the link with remuneration and accountability as well as behavioural aspects.

- Part on risk culture, internal control functions and SSM supervisory tools now included – no dedicated sections on these topics in the supervisory statement of 2016.
- Enhancement of the 2016 statement's substance, with clearer supervisory expectations and a list of observed good practices per topic based on supervisory experience.
- Reflection of more recent ECB publications as well as updated CRD provisions, EBA Guidelines and international standards.

Conclusion

To sum up, this draft document by the ECB establishes comprehensive and updated supervisory expectations aimed at strengthening the governance frameworks and risk cultures of Banks within the European Union. By enhancing the focus on risk culture, detailing governance requirements, expanding internal control functions, refining risk appetite frameworks, and emphasising proportionality, the guidance addresses the evolving regulatory landscape and emerging challenges faced by Banks. It highlights the importance of effective leadership, clear organisational structures, robust internal controls, and continuous supervisory dialogue to ensure bank's resilience and stability. The document underscores the ECB's commitment to fostering a sound banking environment that aligns with international standards and best practices, thereby safeguarding the financial system's integrity and stability.