INSTITUT DER WIRTSCHAFTSPRÜFER

New Assurance Engagements For Governance, Risk and Compliance In Germany

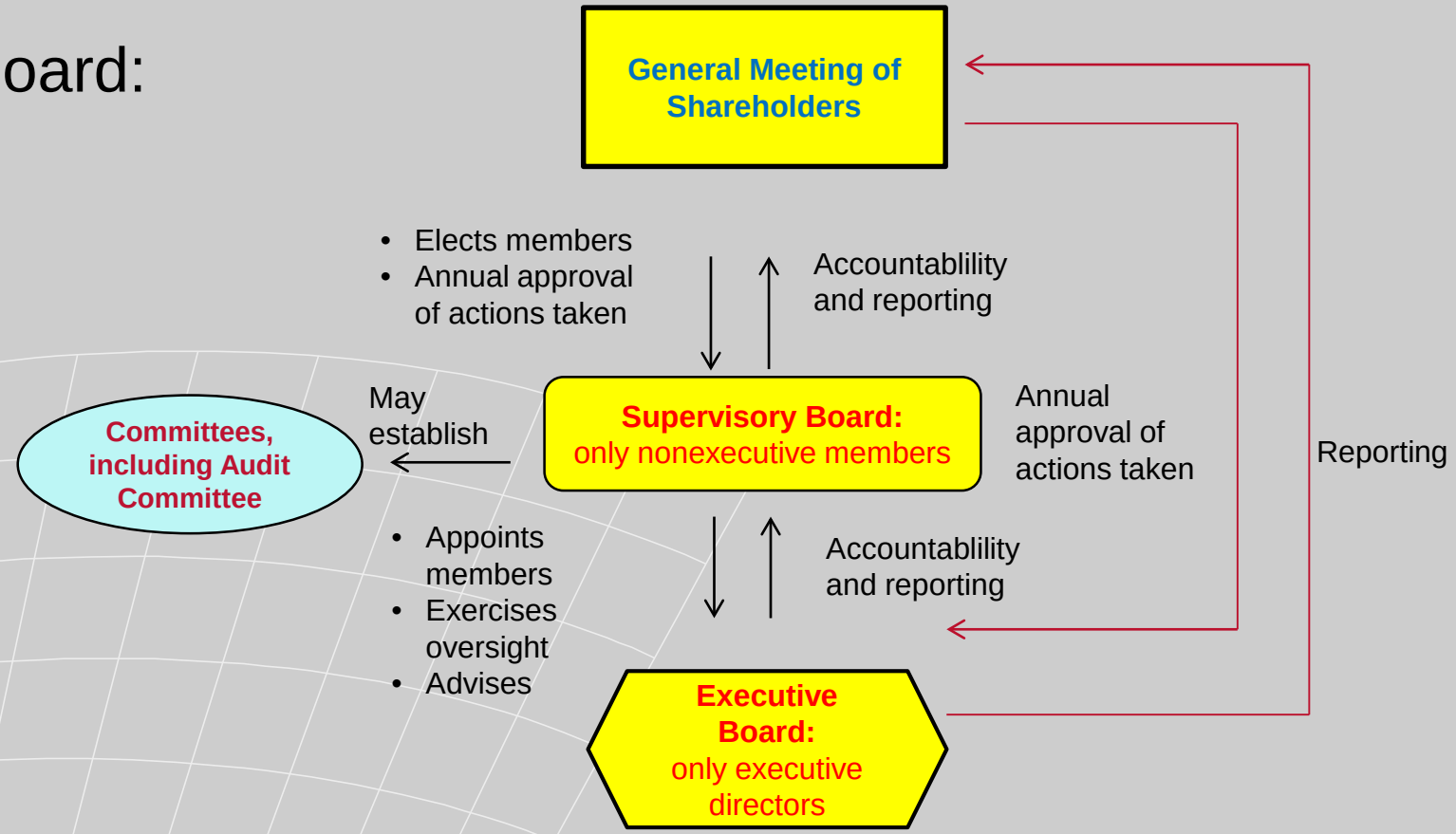
by
Wolf Böhm
Director, Assurance Standards,
IDW, Germany
Technical Advisor, IAASB

Contents of Presentation

- Governance and Legal Context
- Historical Context: Corporate Scandals
- Assurance on Compliance Management System
- Further Governance and Risk Issues
- Response: GRC Project
- Some Key Issues Identified GRC Project
- Questions

Legal and Governance Context (1)

- Two-tier Board:



- Two-tier Board is required for all Aktiengesellschaften [Stock Corporations] by law

Governance and Legal Context (2)

- Some legal responsibilities of supervisory board (1):
  - In particular, overseeing the organisation of management as a whole (§ 111 (1) AktG)
  - Basis for oversight:
    - reporting responsibilities of executive board (§ 90 AktG)
    - right of supervisory board to inspect, verify and engage experts (§ 111 AktG)
    - Federal High Court decision 1997: application of business judgment rule
      - Managers required to be adequately informed and reach reasonable decisions in company‘s best interests
      - Otherwise potential liability for faulty decisions

Governance and Legal Context (3)

- Some legal responsibilities of supervisory board (2):
  - Since 2009 pursuant § 107 (3) AktG: oversight by the supervisory board or the audit committee includes addressing the stock corporation‘s
    - financial reporting process
    - operating effectiveness of its
      - ***internal control system***
      - ***risk management system***
      - ***internal audit function***
    - audit of its financial statements, including auditor independence and non-audit services provided
- German Code of Corporate Governance: supervisory board also responsible for overseeing ***compliance***

Historical Context: Corporate Scandals

- A selection of scandals:
  - Heidelberg Cement et al 2003: Anti-trust violations (Fines on various cement manufacturers of up to € 170 million)
  - Volkswagen 2005: Bribing employee council members (union leaders) with money and „all-inclusive“ luxury vacations outside Europe (led to criminal convictions)
  - Siemens 2006: Bribing potential customers – cost company $ 2.5 billion in fines, legal fees and other costs
  - Deutsche Telekom 2009: Spying on own managers, supervisory board, and on journalists (criminal conviction of manager responsible for corporate security)
  - Daimler 2010: Bribing potential customers – cost € 185 million in fines (legal fees and other costs unclear)

Assurance on Compliance Management System

- Potential legal liability of supervisory & executive board
- **But:** law permits supervisory board to engage experts
  - Assurance on compliance: rear-view mirror – no support on oversight diligence or liability risk if noncompliance discovered through engagement or afterwards
  - Diligence in preventing or detecting noncompliance needs to be more forward-looking or timely, respectively:
    - Reporting on whether effective systems are in place and what can be done to improve them
    - ***Solution: Assurance on Compliance Management System (CMS) [IDW PS 980] issued 2011***
    - Verdict 2015: „It changed the terms of debate on compliance in corporate Germany“.

Further Governance and Risk Issues

- Thyssen-Krupp 2011: Losses of over € 5 billion in steel mills in Brasil and Alabama (due to corruption, poor quality control over building materials, noncompliance with environmental laws, other criminal acts, etc.)
- Subsidiary of Ergo 2011: Scandal over sales force incentive trips to Eastern Europe (large-scale unethical non-monetary incentives – loss of reputation)
- Various supermarket chains, wholesalers und meat producers 2013: Horsemeat scandal
- RWE, E.ON et al. 2013-2014: € Multibillion losses each due to the change in Germany‘s policies moving towards non-nuclear renewable energy sources

GRC Project (1)

- (G)overnance, (R)isk and (C)ompliance Project
- Build on success of assurance on CMS and use experience obtained to develop new standards
- Align with responsibility of supervisory board to address operating effectiveness of entity's
  - internal control system
  - risk management system
  - internal audit function
- Basis: COSO ERM,

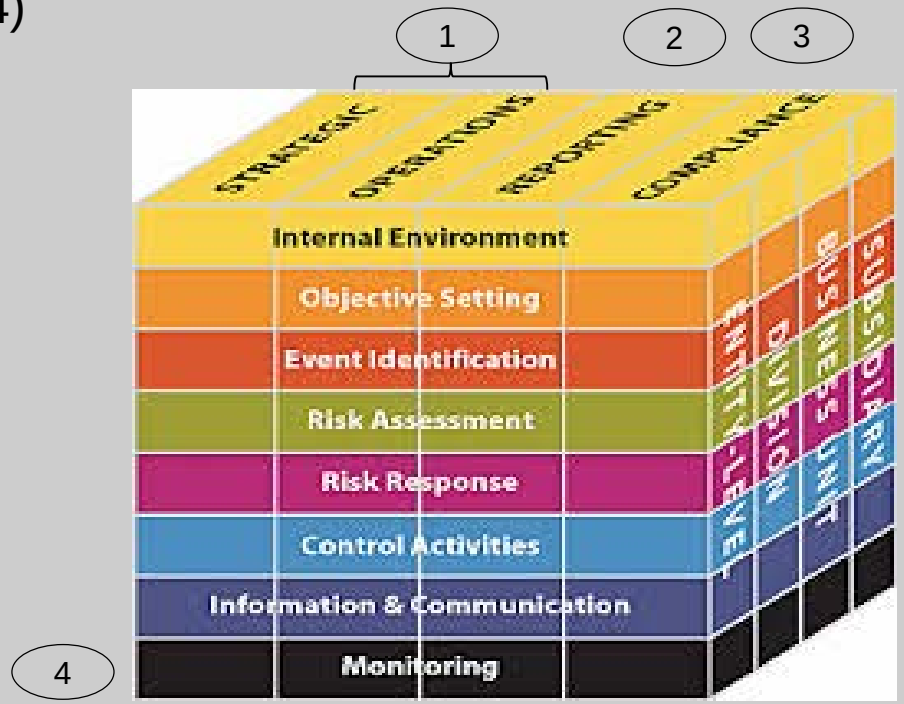
  but other frameworks also

  drawn upon (ISO 31000, NZS 4360:2004,

  COSO IC Framework, IPPF of the IIA)

GRC Project (2)

- The Project includes four sub-projects, for each of which a separate standard is being developed:
  - Assurance on risk management system (RMS) over strategy/operations (1)
  - Assurance on internal control (IC) part of risk management over reporting (2)
  - Assurance on the CMS (revision of IDW PS 980?) (3)
  - Assurance on the internal audit function part of monitoring (4)
- Workshops and other outreach with members of supervisory boards and other stakeholders
  - **Reaction of supervisory board members and other stakeholders: we thought the financial statement audit already includes assurance on all of these!**
  - **Implication: major educational effort is needed to rectify stakeholder expectations of financial statement audits**



GRC Project (2)

- Project objectives:
  - Assist superisory board in meeting its oversight responsibilities
  - Increase engagement harmonization
  - Contribute to the development of improved corporate governance and thereby add value
- **Good corporate governance has become a competitive advantage that adds value to entities**
- Due to business judgment rule, the executive board and other levels of management (e.g., compliance or risk officers) have increasingly become engaging parties for these types of engagements to demonstrate that they have met their management responsibilities

Some Key Issues Identified GRC Project

- Projects contemplate reasonable assurance on appropriate design and implementation or also on effective operation – no limited assurance
- Stakeholders want assurance on entire system, but e.g., assurance on CMS provided only on parts of system
  - Is there a way of limiting the conclusion provided on the whole system to some aspect of whole system?
- Obtaining assurance on parts without looking at the whole
- Management prefers direct engagements; projects con- ceived as attestation engagements (description by management must accompany assurance report)
- Basis for criteria for operating effectiveness

Questions

Thank you for your attention!