

The Basics on Risk & Control Governance



UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

COURSE OF BUSINESS AUDITING
UNIVERSITY OF ROME TOR VERGATA

NOVEMBER 2021

PROF FABIO ACCARDI

RISK CULTURE



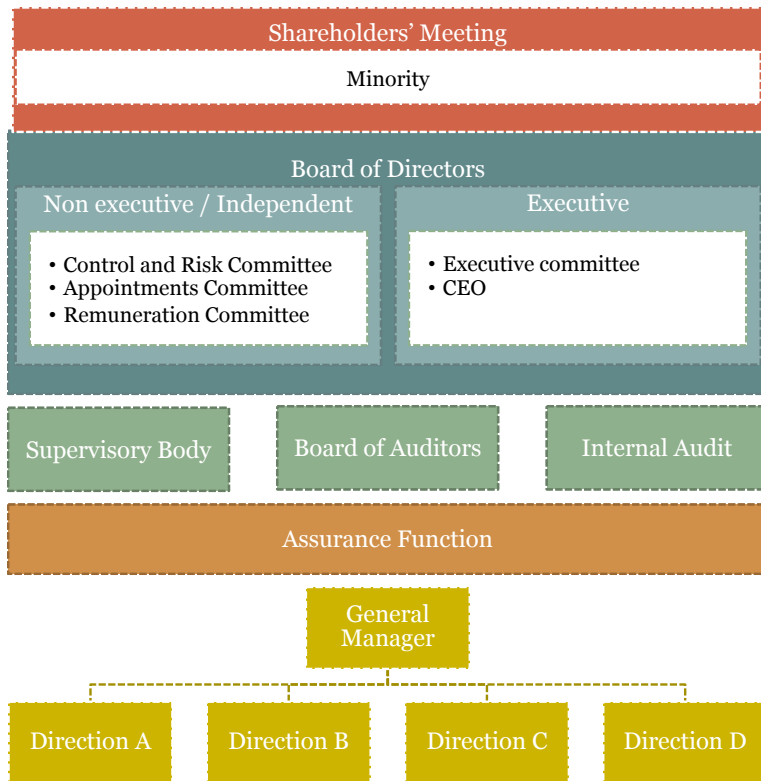
«For all the rethoric about its importance and the money invested in it, risk management is too often treated as a compliance issue»

«A firm's ability to weather storms depends on how seriously executives take risk management when the sun is shining and no clouds are on the horizon»

Corporate Governance System in a listed Italian Company



Internal Control



Direction,
Coordination and
Supervisory

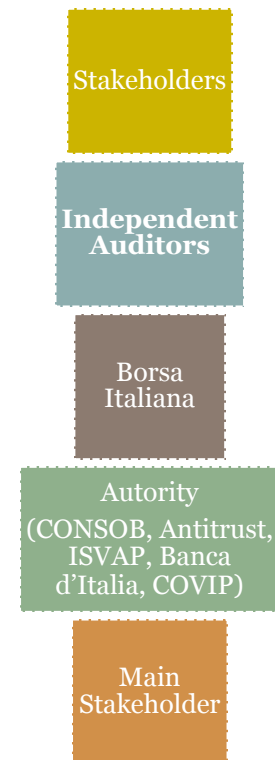
Supervisory,
Monitoring and
Third Level

Controls
Second Level
Controls

Line Controls

Adaptation by Internal Auditing (Dittmeier)

External Control



Corporate Governance System: the example of a listed company



Shareholders' Meeting

It approves the Financial Statements, appoints the Board of Directors, Board of auditors and Independent Auditors and also resolves upon amendments to the Company By-Laws

Board of Directors

It defines strategic policies and is responsible for managing the company

Board of Statutory Auditors

It supervises compliance with legislation and the Company's By-Laws and is responsible for controlling management

Independent Auditors

They are responsible for auditing company accounts

Control and Risk Committee

It helps the BoD to assess the suitability of the internal auditing system. It also assesses the correct use of accounting standards.

Remuneration Committee

It is responsible for proposing the fees for directors with specific offices as well as incentive and salary schemes for top managers, supervising application of BoD decisions

Related Parties Committee

It voices opinions on the Company's interest regarding the performance of transactions with related parties, as per advantages and substantial correctness of the relative conditions

Appointments Committee

It expresses opinions on BoD size, composition and professional skills of the directors within the Board; Propose Directors in case of co-optation should there be necessary to substitute independent Directors

Supervisory Body

It checks that the Model231 functions correctly and is responsible for relative updates

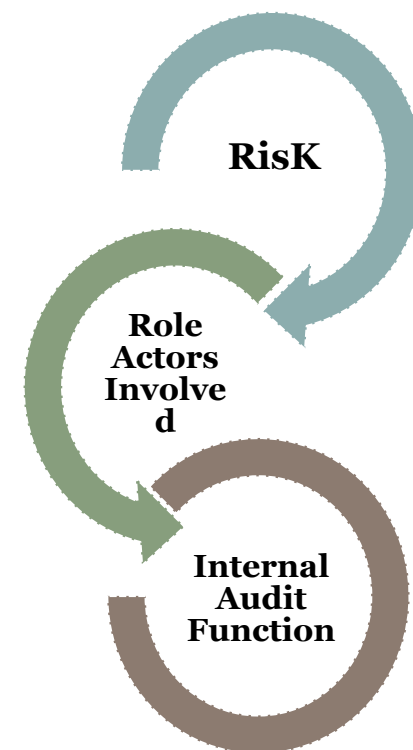
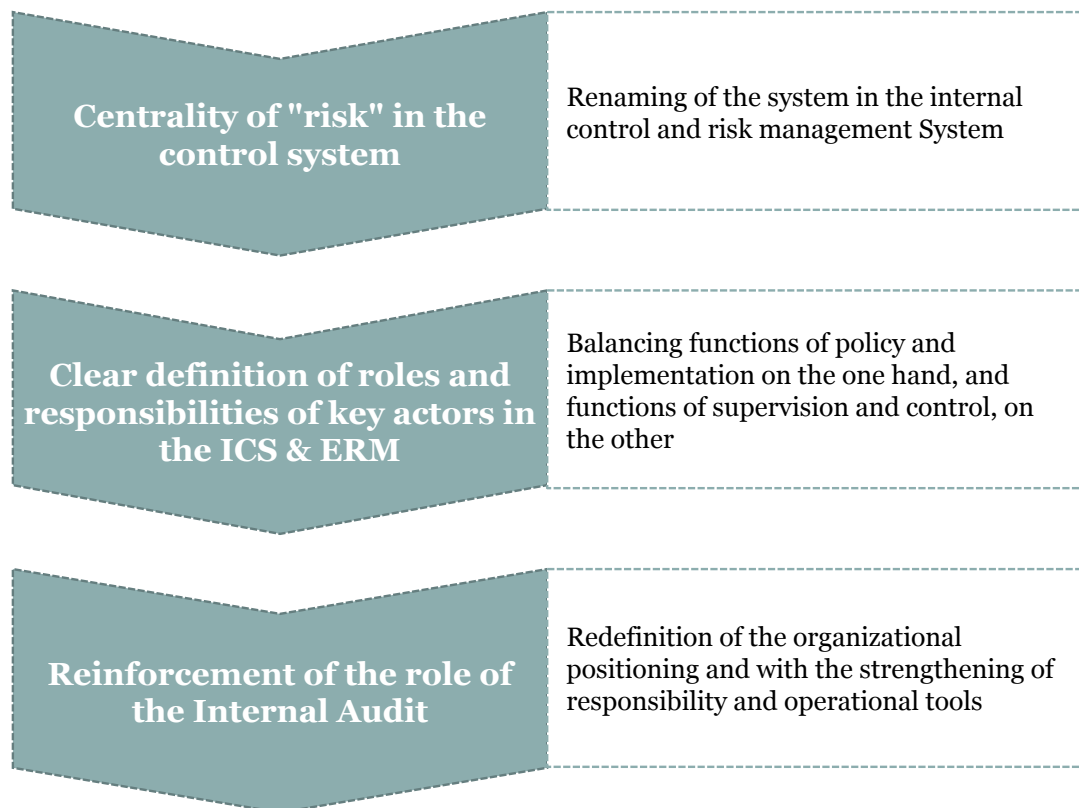
Executive Appointed to draft Corporate Accountants

It is responsible for checking the actual application and suitability of accounting and administrative procedures

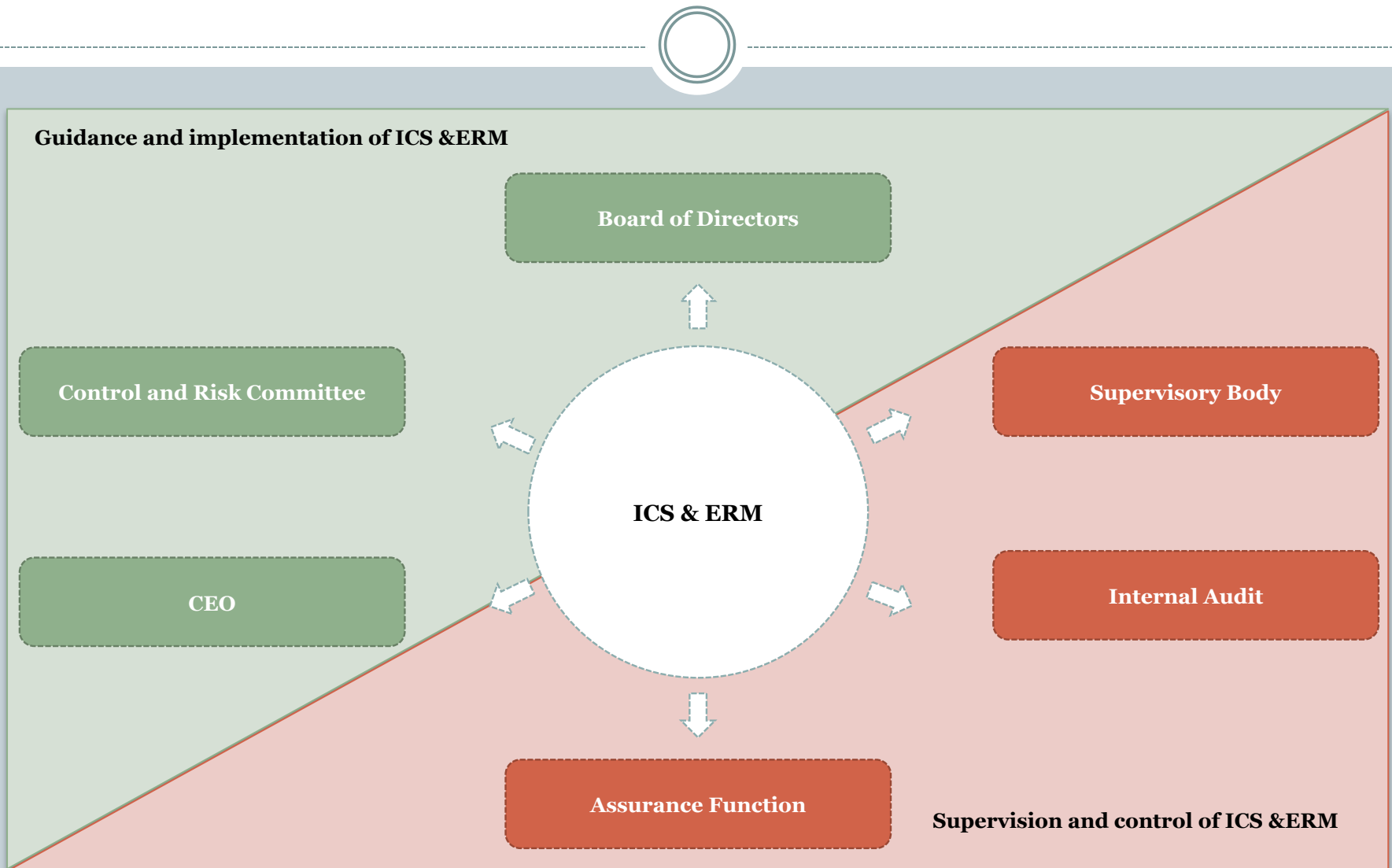
“Corporate Gov. Code : focus on Internal Control and Risk Management System



Recommendations on the Internal Control and Risk Management System are based on the following principles:



Internal Control and Risk Management System: balancing roles and reporting lines



FOCUS ON Internal control and risk management system: the role by the main players according to the “ Italian Corporate Governance Code ”



Board of Directors

Role

- shall provide strategic guidance and evaluation on the overall adequacy of the system, considering the risk profile of the company and the risk appetite defined by the same Board of Directors

Main duties

- defines the guidelines of the internal control and risk management system, so that the main risks concerning the issuer and its subsidiaries are correctly identified and adequately measured, managed and monitored, determining, moreover, the level of compatibility of such risks with the management of the company in a manner consistent with its strategic objectives
- evaluates, at least on an annual basis, the adequacy of the internal control and risk management system taking into account the characteristics of the company and its risk profile, as well as its effectiveness;
- approves, at least on an annual basis, the plan drafted by the person in charge of internal audit, after hearing the Board of statutory auditors and the director in charge of the internal control system;
- describes, in the Corporate Governance Report, the main features of the internal control and risk management system and how the different subjects involved therein are coordinated, expressing the evaluation on its adequacy;
- after hearing the Board of statutory auditors, it assesses the findings reported by the external auditor in the suggestions letter, if any, and in the report on the main issues resulting from the auditing;
- appoints and revoke the person in charge of the internal audit function and ensure that such a person is provided with the adequate resources for the fulfilment of his/her responsibilities and define the relevant remuneration consistently with company's policies

FOCUS ON Internal control and risk management system

The role of main palyers according to Corporate Governance Code



Control and Risk Committee

Role

- proposing and consultative functions towards the BoD, regarding to the activities of supervisory the overall performance of the Company and shall meet at least once a three months

Composition

- corporate body established as internal structure of the Board of Directors, is made up of independent directors of non executive directors, the majority of which being independent ones;

Operations

- to perform its functions it makes use of Internal Audit Director, which ensures the flow of information by the other assurance functions

Main duties

- supports the BoD in the evaluation of the adequacy of the internal control and risk management system as well as its effectiveness;
- evaluates together with the person responsible for the preparation of the corporate financial documents, after hearing the external auditors and the Board of statutory auditors, the correct application of the accounting principles, as well as their consistency for the purpose of the preparation of the consolidated financial statements, in any;
- expresses opinions on specific aspects relating to the identification of the main risks for the company;
- reviews the periodic reports of the internal audit function concerning the assessment of the internal control and risk management system, as well as the other reports of the internal audit function that are particularly significant;
- monitors the independence, adequacy, efficiency and effectiveness of the internal audit function;
- requests the internal audit function to carry out reviews of specific operational areas, giving simultaneous notice to the chairman of the Board of statutory auditors;
- reports to the Board of Directors, at least every six months, on the occasion of the approval of the annual and half-year financial report, on the activity carried out, as well as on the adequacy of the internal control and risk management system;

Source: Corporate Governance code



Director in charge of the internal control and risk management system

Role

- establishing and maintaining an internal control and risk management system, adopting the strategic guidance of the Board

Main Duties

- identify the main business risks, taking into account the characteristics of the activities carried out by the issuer and its subsidiaries, and submit them periodically to the review of the Board of Directors;
- implement the guidelines defined by the Board of Directors, taking care of the planning, realization and management of the internal control and risk system, constantly monitoring its adequacy and effectiveness;
- request to internal audit function to carry out reviews of specific operational areas and on the compliance of business operation with rules and internal procedures, giving simultaneous notice to the chairman of the Board of Directors, the chairman of control and risk committee and the chairman of the Board of statutory auditors;
- promptly report to the control and risk committee(or to the Board of Directors) issues and problems that resulted from his/her activity or of which he/she became aware in order for the committee (or the Board) to take the appropriate actions.

FOCUS ON Internal control and risk management system: The role of main palyers according to Corporate Governance Code



Board of Statutory Auditors

Role

- Within internal control and risk management systems, supervises the adequacy of internal control system;
- In accordance with the directions of CONSOB and Corporate Governance Code of Borsa Italiana S.p.A. supervises:
 - compliance with the law and bylaws
 - respect of the principles of correct administration
 - the adequacy of the Company's organizational, administrative and accounting structure

Composition

- The Shareholders' Ordinary Meeting appoints the members of the Board of Auditors. The Board of Auditors is formed of three Standing Auditors and three Alternate Auditors, who hold office for a period of three fiscal years. Minority shareholders are entitled to appoint one Standing Auditor, who shall operate as Chairman of the Board of Auditors, and one Alternate Auditor.

Main Duties

- Participates to the meetings of the BoD and Shareholders' Ordinary meetings;
- Convoques The Shareholders' Ordinary Meeting in the case of omission or unjustified delay on the part by the directors;
- Monitoring the adequacy of instructions given to subsidiaries and the adequacy of the internal control and Administrative Accounting System
- Assessing the findings reported by the external auditor in the suggestions letter, if any, and in the report on the main issues resulting from the auditing.
- Monitoring the independence of the external auditors and the effectiveness of the audit process

Source: Various

FOCUS ON Internal control and risk management system: The role of main palyers according to Corporate Governance Code



Supervisory Body

Role

- Is the body which, according to the law, is entrusted with supervising the effectivevess and efficiency of and the compliance with the Model, for the purpose of preventing offences from being committed.
- it operates in a steady and continuous way watching over the adequacy, the updating of and the compliance with the Model.

Composition

- The Supervisory Body may be constituted of one sole member or by a plurality of members, which must meet the following requirements: autonomy and independence, professionalism and reputation, continuity of action;

Main Duties

- Supervising the effectiveness and efficiency of the Model: adequacy in terms of suitability to prevent predicate offences from being committed;
- Supervising the compliance with the Model: actual application;
- The Supervisory Body is responsible for giving the Company's top management notice of the occurrence of conditions (originating both within or out of the Company) requiring to amend and/or supplement the Model;
- verifications on the compliance of management, operative, and accounting-administrative procedures with the principles of D.Lgs. 231.



CHIEF AUDIT OFFICER (CAE)

Role

- Check the functioning and adequacy of the overall internal control and risk management system through third-level controls that include the review of activities of other assurance functions

Main Duties

- verify, both on a continuous basis and in relation to special needs, in conformity with international professional standards, the adequacy and effective functioning of the internal control and risk management system, through an audit plan, to be approved by the Board of Directors. Such a plan shall be based on a structured analysis and ranking of the main risks;
- draft periodic reports containing adequate information on its own activity, and on the company's risk management process, as well as about the compliance with the management plans defined for risk mitigation. Such periodic reports contain an evaluation on the adequacy of the internal control and risk management system;
- verify, according to the audit plan, the reliability of information systems, including the accounting one.

Focus 231

- Verifies the proper implementation of the organizational model, based on the guidelines issued by the SB;
- Accesses, on behalf of the Body, in any business document;
- Manages the flow of information (structured and unstructured) to the Supervisory Board;
- Receives reports of suspected violations of the Ethic Code and/or Model and transmits all this information to SB;
- Coordinates training of staff in the administrative liability of legal persons;
- Supports the SB in the update of the Organizational Model

Source: Corporate Governance code

The Internal Audit function & CAE



Positioning

Reporting directly to the Board of Directors

The Board appoints and dismisses the CAE endows the resources of the internal audit function, establishes the remuneration of the CAE and approves the audit plan.

Main requirement

Independence

The CAE is not responsible for any operational area and reports to the Board of Directors

Duties

Verify operation and suitability of
➤ **internal control systems**
➤ **risk management systems**

The Internal Audit Department performs control activities of third level in compliance with international standards (The IIA): coordinates the flow of information from other assurance functions and reviews the work

Instrument s

Audit Plan based on the prioritization of risks

The audit plan, approved by the board of directors, must be based on a structured analysis and ranking of the main risks and should include checks on the reliability of information systems including accounting systems

Centrality of risk in internal auditing



The objective of the internal audit activity is provide management an independent and objective assurance that

The main risks are managed properly

The level of residual risk is contained within the limits of acceptability in accordance with the risk appetite defined by management

There is reasonable assurance of the achievement of objectives

Risk Management and Internal Audit Systems operate effectively

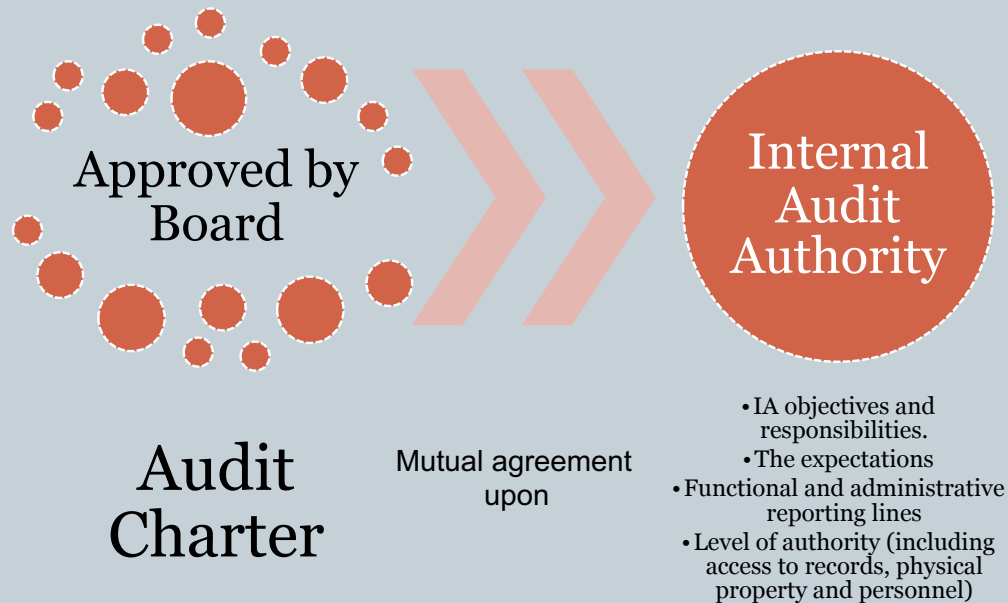
Risk management and internal control system effectively implemented within the analyzed process are in line with the framework of reference adopted by the company (eg. ERM, COSO Report, Model 231)

Attribute Standards

1000 – Purpose, Authority, and Responsibility



The **purpose, authority, and responsibility** of the internal audit activity must be formally defined in an **internal audit charter**, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.



Attribute Standards

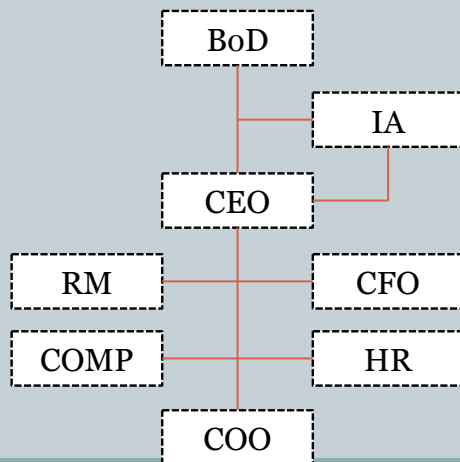
1100 – Independence and Objectivity



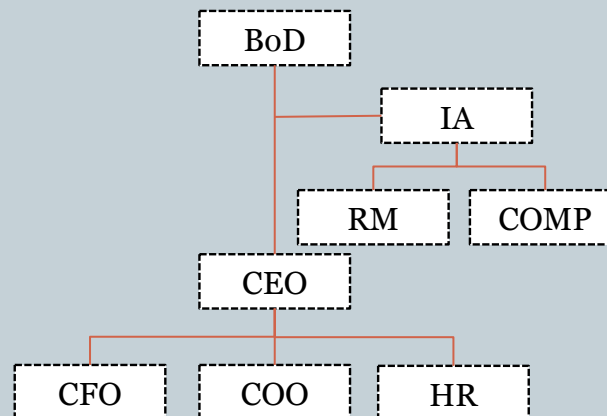
The internal audit activity must be **independent**, and internal auditors must be **objective** in performing their work.

**Which is the best organizational position for IA Activity?
Select one and explain why**

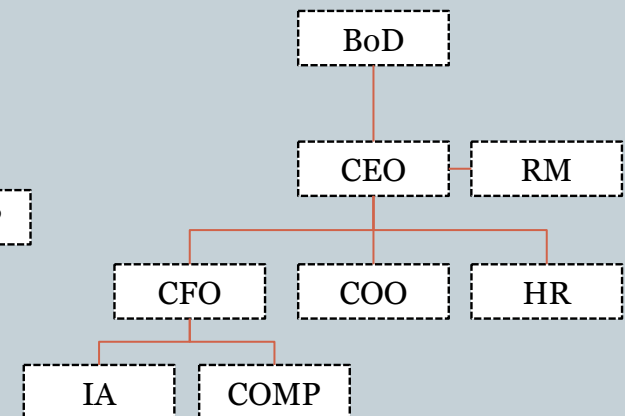
A



B



C



Attribute Standards

1100 – Independence and Objectivity



*The internal audit activity must be **independent**, and internal auditors must be **objective** in performing their work.*

