COMPLIANCE RISKS AND CONTROLS

UNIVERSITA' degli STUDI di ROMA
TOR VERGATA

COURSE OF BUSINESS AUDITING
UNIVERSITY OF ROME TOR VERGATA

NOVEMBER 2022

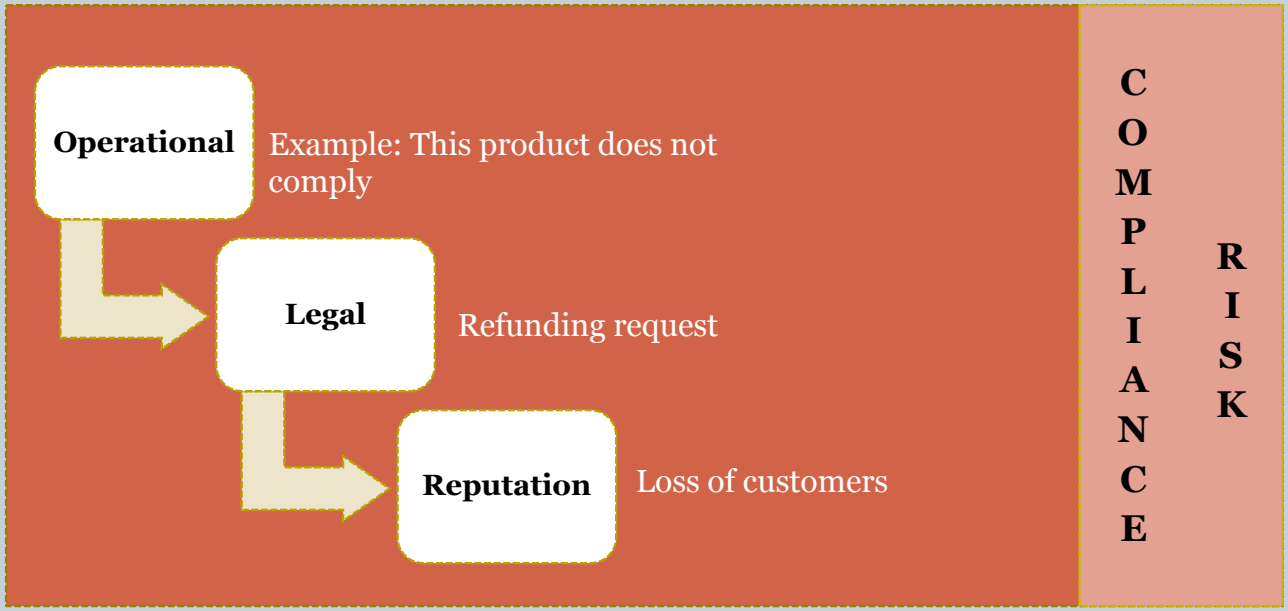
-PROF FABIO ACCARDI

Compliance Risk in Enterprise Risk Management: Definition

1) What is Compliance risk?

Compliance risk is exposure to legal penalties, financial forfeiture and material loss an organization faces when it fails to act in accordance with industry laws and regulations, internal policies or prescribed best practices.

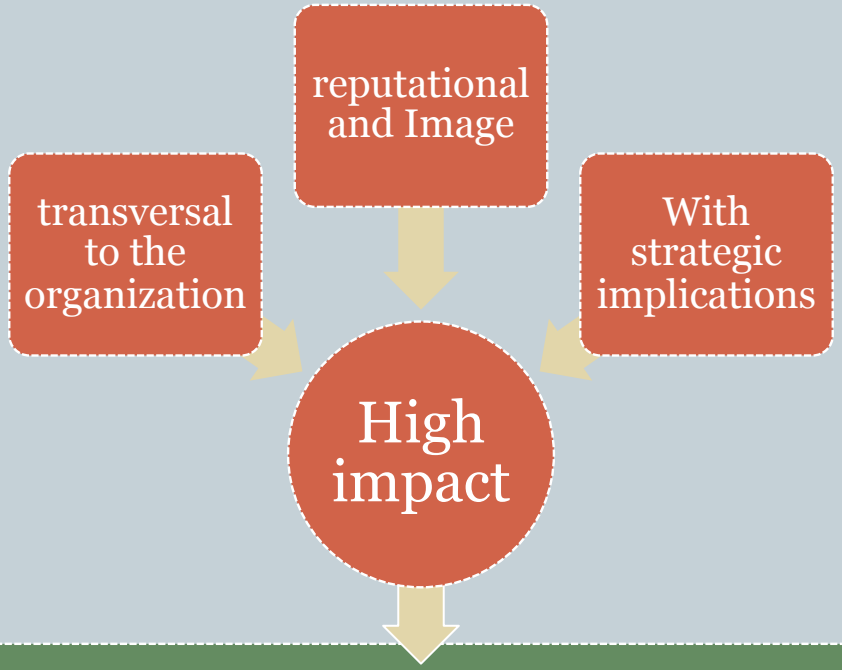
This risk is closely interconnected with the operational risk, legal and reputation, so that from one follows the other.



Compliance Risk in Enterprise Risk Management: Characteristics

2) What are the main characteristics of Compliance Risk?

Failure to comply with laws, regulations and procedures is a risk :



Consequently it must be managed through an ex ante compliance program
(identification, evaluation, monitoring, reporting)
that will reduce the probability of occurrence

COSO Report I: Focus on the Compliance

According to the COSO Report I, internal control is a **process**, done by **people** (from the board of directors, managers and other workers of the company structure), which aims to provide **reasonable assurance** on the achievement of business objectives.

Among the business objectives over the **effectiveness** and **efficiency** of operations and the Reliability of budget Information the COSO Report I identifies as the general category the

COMPLIANCE: intended as compliance with laws and regulations

The Internal Control System consists of five interrelated components:

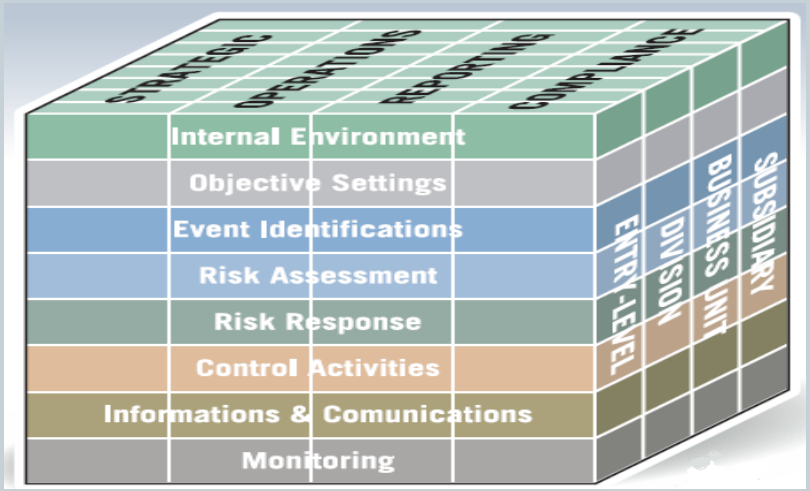
1. Control environment
2. Risk assessment
3. Control Activities
4. Information & Communication
5. monitoring

Each of the components must exist and operate in an integrated way in the different levels of the organization because the objectives, including compliance, are achieved

ERM: Focus on the Compliance

Enterprise Risk Management is a **process** set up by the Board of Directors, the Management and other operators of the corporate structure used for the formulation of **strategies** across the organization, designed to identify potential events that may affect the company **to manage the risk within the limits of acceptable risk and to provide reasonable assurance regarding the achievement of corporate objectives.** They have identified four major categories of objectives:

✓ **strategic**	These are general aims in line with the corporate mission.They are declined and contextualized in the other three categories of objectives;
✓ **operational**	Effective and efficient use of resources
✓ **reporting**	Reliability of information both internally and externally
✓ **COMPLIANCE**	Compliance with laws and regulations



The eight components which compose the ERM apply to each category of objective and the company both as a whole and in the various levels / processes / functions.

The following slides are designed to analyze the size of Compliance in COSO I and ERM, applying the components of the Framework to the Compliance Risk.

Application of the components of the COSO / ERM to management of Compliance Risk

ERM COMPONENTS	COMPLIANCE PROGRAM
1 – Internal Environment	
The control environment forms the essential identity of an organization and determines the ways in which the risk is considered to be tackled. Is the foundation of the other components of the Enterprise Risk Management; it is affected / influenced by factors such as the philosophy of risk management, the level of acceptable risk, the supervision of the Board, the integrity, ethical values, competence, the modalities of the delegation of powers and responsibilities, training staff	Management of Risk Compliance requires the definition of: • **Codes of Conduct and Ethical Principles;** • **Policy Management;** • **Management Procedures;** • **Bonus plans (which include compliance objectives);** • **Penalty System**
2 – Objective Settings	
The definition of objectives is a prerequisite for an effective event identification, risk assessment and risk response. The strategic objectives are the foundation for defining the operational objectives, reporting and compliance. For choosing targets, it must make sure to align themselves to acceptable risk, fixed by the company, which are determined by the levels of risk tolerance	The main objective of a Compliance Program is to **ensure the compliance of business operations** by defining tools and methodologies for the identification and assessment of compliance risk **in support of the internal decision processes**
3 – Event Identifications	
Management must identify events which may affect the company. If they compromise the achievement of the objectives they represent risks that require evaluation and determination of response measures. If they can have a positive impact, they represent opportunities to pursue redefining strategies. The events are influenced by internal and external factors and their identification involves the application of structured techniques	They have identified three categories of events for Compliance risks: 1. **Violation of external regulations (mandatory)** 2. **Violation of internal rules (soft law / internal procedures)** 3. **Non-compliance / update of internal regulations than sorting external / legislative development**

Application of the components of the COSO / ERM to management of Compliance Risk

ERM COMPONENTS	COMPLIANCE PROGRAM
4 – Risk Assessment	
Risk assessment measures the impact of a potential event on the achievement of objectives in terms of likelihood and impact, through qualitative and / or quantitative techniques. The evaluation regards both the individual event categories of potential events interconnected in the various levels of the company. Risks can be assessed in terms of inherent risk (that is independent from the existing control system) and in terms of residual risk, which considers the effects on the probability and / or impact of the risk responses activated	In a risk assessment of compliance must consider many factors affecting impact and probability, such as: **1. P / L**: impact on the budget; **2. Customer**: compromised of customer relationships; **3. Market**: perceived value by stakeholders; **4. Business**: impact on business interruption, interdiction and reduced productivity; **5. Penalties**: administrative charges and penalties; **6. Bureaucracy**: the total cost of compliance
5 – Risk Response	
Based on the risk assessment, management must select the most appropriate responses to the risk (avoiding the risk, reducing it, share it, to accept it). The choice depends on several factors: cost / benefit analysis; desired effects on the probability / impact; capacity to reduce risk within the limits of tolerance. The risk mitigation strategy should allow to bring the overall level of residual risk within the limits of acceptability set by top management.	**In determining the best strategy to respond to the compliance risk must perform a cost - benefit analysis that takes into account the hidden costs mainly of non - compliance**
6 – Control Activities	
Control activities are the application of policies and procedures to ensure to the management that directives to address the risks that may affect the achievement of the objectives are implemented. Control activities are implemented at all levels of the organization, and may consist of approvals, authorizations, verifications, reconciliations, review of operational performance, protection of company assets, separation of duties.	**The prevailing treatment is mitigating risk through appropriate controls (first, second and third level), staff training, the formalization of procedures, the provision of specific funds (legal risks)**

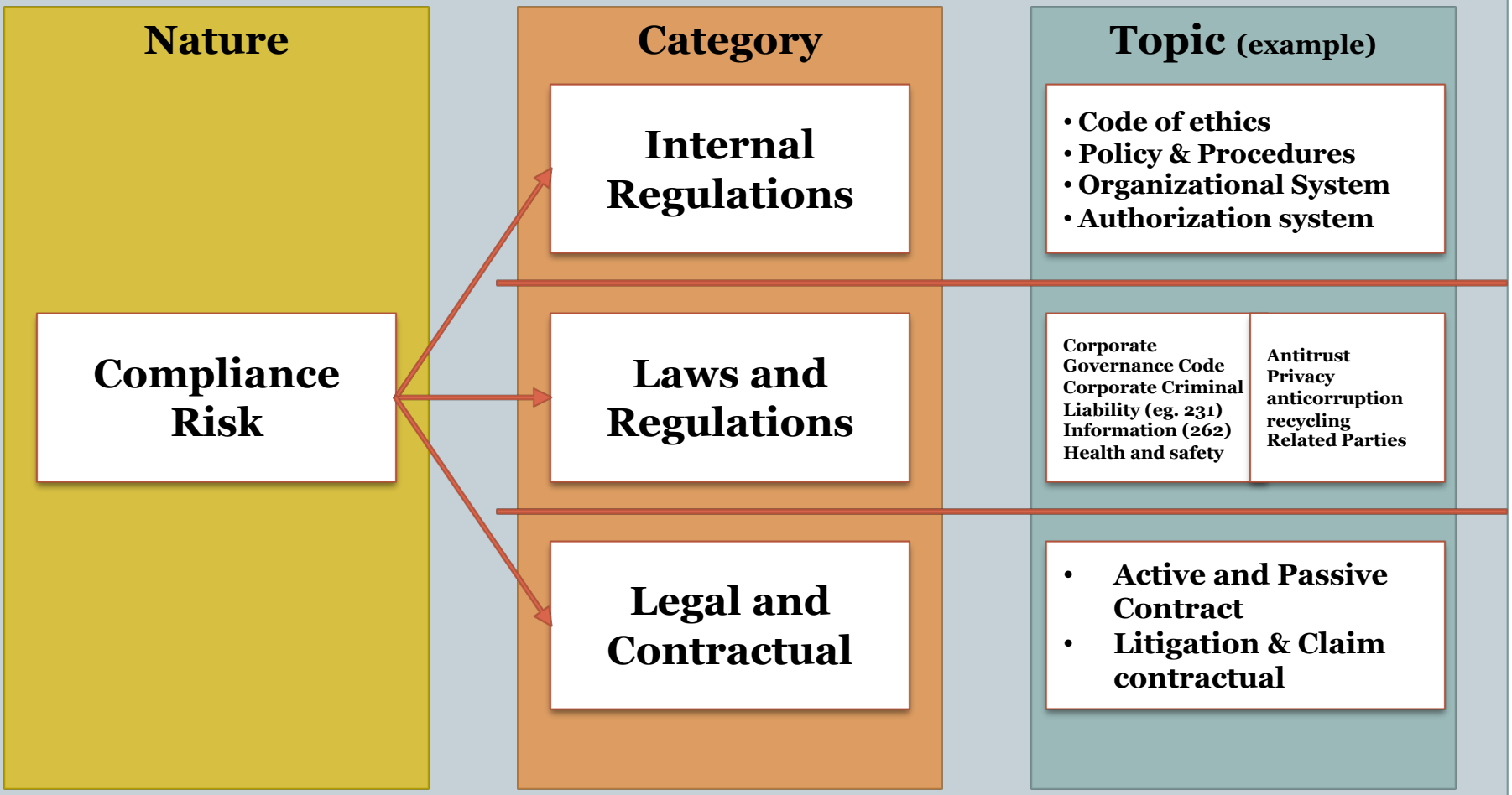
Application of the components of the COSO / ERM to management of Compliance Risk

ERM COMPONENTS	COMPLIANCE PROGRAM
7 – Informations and Comunications	
The company should identify, collect and disseminate relevant information to enable everyone to fulfill their responsibilities. They must be implemented information systems that deal with both internal and external information for the risk management and decision making. There must be effective communications to flow through the entire organization: top-down (eg. Communication objectives); bottom-up (reports significant); transversal (ie. management processes); to third parties.	There should be an internal information system that allows to promptly **intercept non-compliant behavior and report them to the parties have the power to put an early correction**
8 – Monitoring	
Monitoring has the function of assessing the presence and operation in time of the components of the control and risk management system. Is carried out through continuous supervision, by the operating management, or through specific testing and evaluation, the scope and frequency depends on the risk assessment and effectiveness of continuous oversight.	The monitoring is mainly competence: i. **Compliance Officer** who is responsible for overseeing the Compliance Risk proactively, through the 'identification, assessment, monitoring and reporting on compliance; Internal audit must include the compliance risk in their plans and submit to an independent review the Compliance

Do not exist in Italy obligations "mandatory“ of implementation of the Models COSO / ERM. However, the implementation of a process COSO / ERM allows you to manage in a structured and organic way a series of regulatory requirements with which companies, especially if listed, you have to compare (eg. Codes of Conduct, Legislative Decree no. 231/2001 , Legislative Decree no. 261/2005, privacy, Standard ISO, etc.)

Decomposition of Compliance Risk

4) What are the different types it can be decomposed compliance risk?



Decomposition of Compliance Risk (continued)
Internal Regulations

Code of ethics

Explains the values and ethical principles which the Company's employees must base their conduct to pursue objectives of legitimacy, fairness, transparency and verifiability

- Corporate Values
- Rules of Conduct
- Methods of implementation

Policy and Procedures

Constitute the corporate provisions likely to provide the framework for the regulation of activities and define the operational modalities of reference

- Policies & Guidelines
- Procedures
- IT System

Organizational System

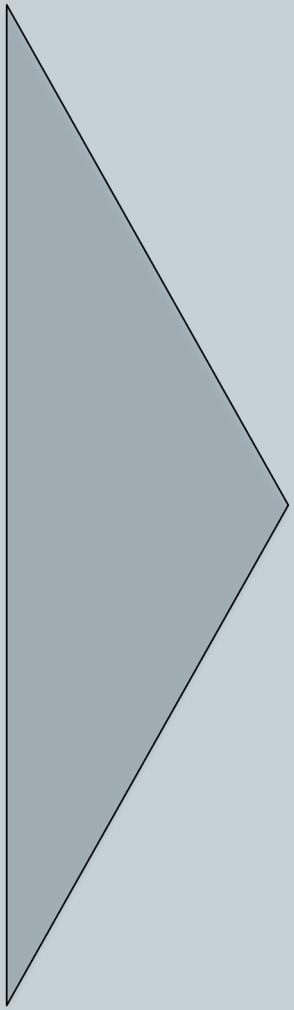
It defines the hierarchy of the company positions and responsibilities for the conduct of activities, ensuring balance of power between who execute, checks and authorizes and absence of conflict of interest

- Org Chart
- Carry lines
- Job description

Authorization system

He attributes powers of internal authorization and signature / representation towards the outside in accordance with the organizational system

- Delegations and power of attorney
- Spending Limits
- Profiling Data



- Behavioral principles
- Policies and Procedures
- Segregation of Duties
- power of attorney