

Internal control: towards governance and risk control

Internal control has traditionally been seen as a curb to business development. With the 2007 release of the guidelines to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and COSO 2 in 2008, internal control came into play in a big way: yes, you have to identify, to assess, to control, to insure/transfer/reinsure! And not only to appease regulators or risk-adverse pen pushers...but to manage your business efficiently.

ERM as a key point

Enterprise Risk Management (ERM) became a must, converging with principles from Basel II's Pillar 2.

Unfortunately, time was too short... and the financial crisis hit most companies before they were able to reinvent and incorporate internal control practices into their day-to-day operations.

Following shock after adverse shock, the financial crisis has left business people in recovery mode. They now understand why a discrete and comprehensive system is needed to control and manage risks. Internal control is finally winning over its last detractors.

First, it's important to note that the process of internal control must be integrated into every relevant aspect of a business, not merely to serve as a "ticking the boxes" exercise. This process is ideally brought into play by all management levels in order to obtain "reasonable" assurance in achieving the three following objectives:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting,
- Compliance with applicable laws and regulations.

Internal control aims to function as a virtuous circle, in which a business process cartography clarifies how a business operates and its overarching mission: charting a structure for business processes helps to identify and assess risk. Controls can then be identified and set up. Process improvements and management (risk mitigation) complete the circle.

Internal control process

Indeed, such a structuring process requires a very highly developed information system (data warehousing, business processes and risks cartographies, procedures, databases, incident databases, control plans, etc.). But crucially, the eight blocks laid out in COSO (and listed below) help to establish an intelligent internal control system:

- **Internal environment** (organizational units' identification with entity level, notably by developing risk management philosophy, culture and organizational structure),
- **Objective setting** (strategic, operations, reporting and compliance objective setting, for each division, business unit and subsidiary). These objectives should fit the entity-wide risk appetite and must be clear and strategic,
- **Event identification** (identifying events that could influence organizational performance, either positively or negatively),
- **Risk assessment** (assessing the identified risks in terms of probability of occurrence and potential impact on the organization),
- **Risk response** (defining risk management strategy: acceptance, avoidance, sharing and reduction),
- **Control activities** (selecting controls to manage identified risks),
- **Information and communication** (collecting information and reporting on risk actions; communication on ERM),
- **Monitoring** (monitoring the effectiveness of implementation plans) Control levels,
- **Information and communication** (collecting information and reporting on risk actions; communication on ERM),
- **Monitoring** (monitoring the effectiveness of implementation plans) Control levels.

Control levels

Internal control is based on permanent and periodic controls. The three control levels are strictly divided to ensure accuracy and impartiality. The first two levels report to executive management; the third reports to the deliberating apparatus (e.g., the board of directors or supervisory board).

- **First level:** daily, exhaustive, supervised and auditable (shrinkable) controls,
- **Second level:** the "permanent" control. This is conducted by a permanent control department or any actor who did not participate in the first control level. The goal is to ensure efficiency at the first level, by auto-evaluations (control by operations) or testing (controlling the control). Besides the dissuasive effect against laxity or embezzlement by operational actors, this second level is a means to assess the risk control process, in order to detect its weak points,
- **Third level:** periodic controls, made by audit or general inspection. Internal audit is an independent activity that focuses on specific objectives (as outlined in the eight blocks above). The third level is responsible for control planning, diagnostics and for improving advice.

Sarbanes-Oxley regulations have been the source of significant control audits; the organization of internal control process and reporting to regulators is, quite often, still underway.

...for an efficient risk management

In 2007, any bank would have dismissed a major financial crisis and cataclysmic changes within the economic landscape as impossible, especially because controls were considered to be reliable. And then came 2008.

Backed by the strong commitment of all involved financial actors to consistent and proactive internal control, the COSO 2 release provides an excellent opportunity for setting up efficient risk management. Such a system not only controls abnormal operations, it also prevents them from occurring in the first place, therefore injecting an entire company's culture with an aversion to unwarranted risk.