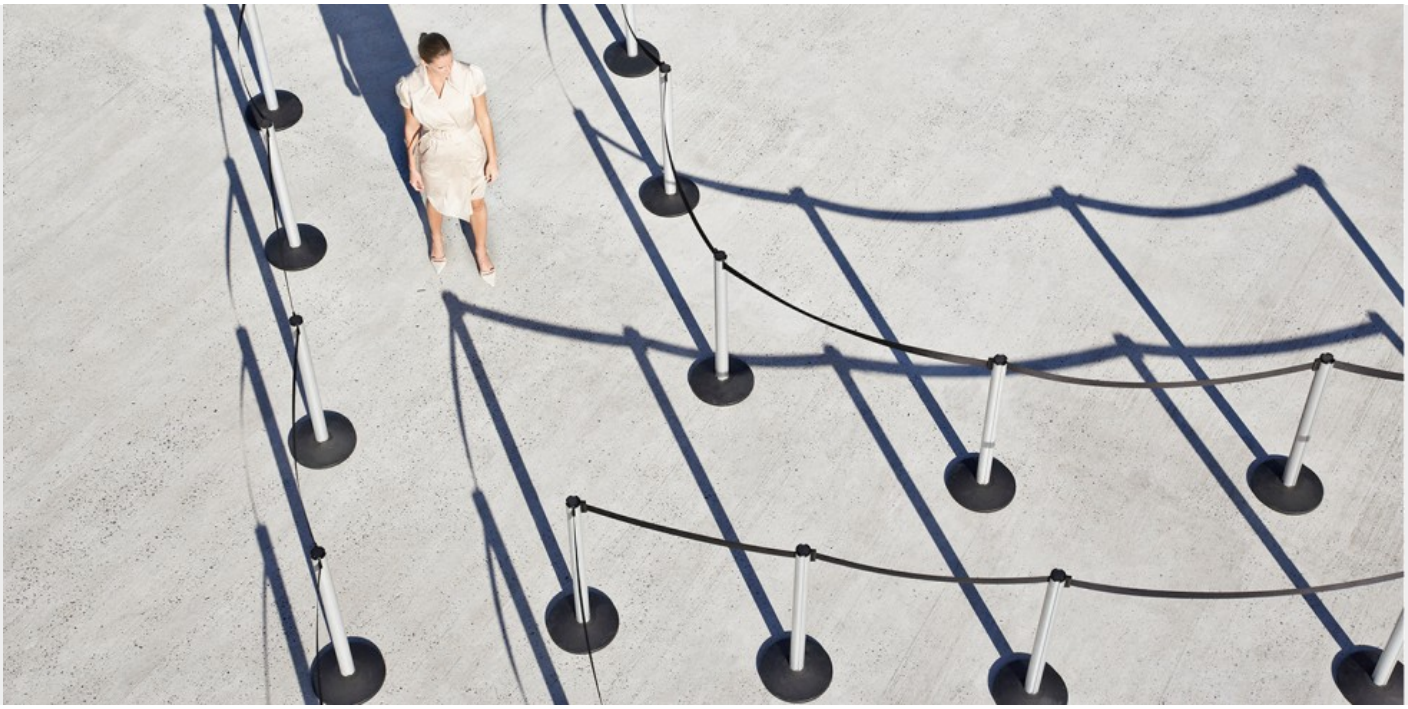
IT GOVERNANCE: AN INTRODUCTION



Nearly all organizations are significantly dependent on technology. Even the smallest of enterprises will probably require a computer or mobile phone for communication, tracking of transactions, research, or accessing government services.

For most corporate entities, their strategies are heavily linked to exploiting emerging technologies through digital transformation. According to IBM's research, executives rank technology as the top external force in 2022 that will impact their businesses in the near term, when compared with regulatory concerns and market factors. The top technologies they expect to deliver business results are:

- IoT
- Cloud computing
- AI

The importance and dependence on technology means that organizations need to carefully ponder their investment in it as well as the risks that result from its use, including underutilization or misuse. Decisions regarding IT spend are no longer relegated to IT practitioners, but nowadays involve the highest levels of leadership.

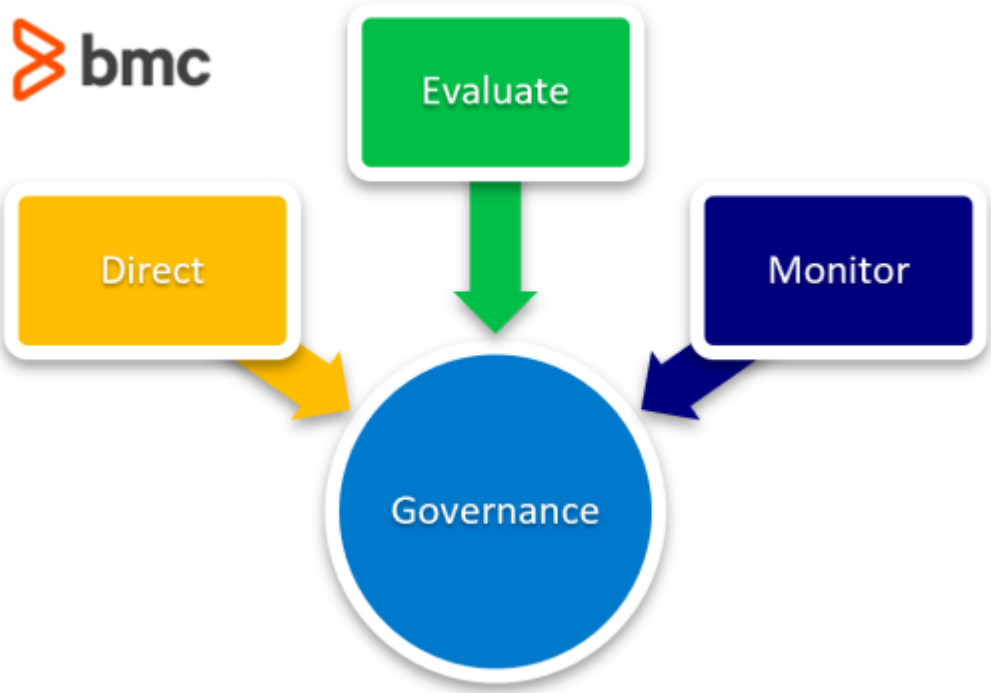
That is where governance comes in—especially for entities which are heavily dependent on technology to achieve business objectives and are wary of the negative effects that could result from IT failures or misuse, such as loss of business and customers, negative reputation, and/or regulatory penalties.

Let's take a deep dive into what IT governance is and how organizations can leverage governance to make a return on their investments in technology as well as limit its harmful impacts.

What is IT Governance?

The ISO/IEC 38500:2015 standard for the governance of IT for the organization defines IT governance as *the system by which the current and future use of IT is directed and controlled*.

Governance facilitates effective and prudent management of IT resources that facilitates long-term business success. IT governance is usually a subset of overall corporate governance, and as a result there is usually significant alignment between the two. The work of IT governance can be grouped into three activities according to COBIT:



- **Evaluating** stakeholder needs, conditions and options to determine balanced, agreed-on enterprise objectives. This would include review of past business performance, future imperatives, as well as current and future operating model and environment. Assessments such as SWOT analysis, PESTEL analysis and risk assessments are important inputs of evaluation.
- **Directing** the organization through prioritization and decision making. This is usually in the form of strategies and policies, as well as establishment of controls.
- **Monitoring** performance and compliance against agreed-on direction, regulations and objectives. This is usually carried out through compliance audits and performance reports.

In most organizations, corporate governance is the responsibility of the board of directors, but specific governance responsibilities may be delegated to specific structures at an appropriate level, especially for large complex entities. An IT governance body might be a subset of the board with some depth of IT knowledge, or a group of senior executives (drawn from both business and IT) directly overseeing funding, management, and usage of IT.

The ITIL 4 Direct Plan and Improve guidance provides examples of key governance roles and their responsibilities:

Governance structure	Role in governance

Board of directors	Responsible for their organization's governance. Specific responsibilities include: • Setting strategic objectives • Providing the leadership to implement strategy • Supervising management • Reporting to shareholders
Shareholders	Responsible for appointing directors and auditors to ensure effective governance
Audit committee	Responsible for supporting the board of directors by providing an independent assessment of management performance and conformance

Good vs bad governance

Governance is a function of human behavior. So, when it comes to good vs bad governance, the outcome is tied to two things:

- Whether the governance body does its job responsibly and effectively.
- Whether the stakeholders (i.e., management, employees, contractors or partners) are committed to upholding the governance framework.

Where the governance body is not knowledgeable or fully committed, there is a possibility that management ends up steering IT in a direction that may later harm the organization. Case in point is the abuse of user personal information or introduction of bias in machine learning by some organizations, which have resulted in severe regulatory penalties and reputational damage, translating into financial loss.

Bad IT governance can be characterized by the following signs:

- The IT function makes all the decisions on the direction of technology without oversight or input from the rest of the business.
- IT budget spend frequently spirals out of controls with unending or stalled projects that do not provide the expected benefits to the organization.
- The governance body is reactive in nature, only called into action when things go wrong such as major IT system failures, negative audit findings, or regulatory issues.
- IT objectives are not aligned with the organization's strategic objectives.

Good IT governance takes a holistic approach, ensuring that all stakeholders are involved and committed to putting in place all the necessary elements required to build and sustain an effective governance framework. COBIT gives a list of such components including: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.

Best practices in governance

The ISO/IEC 38500:2015 standard defines six principles that are necessary for effective governance of IT in the organization:

1. **Responsibility.** Everyone within the organization understands and accepts their responsibilities both in terms of demand and supply of IT and have the authority to meet them.

2. **Strategy.** Business strategy take into account current and future IT capabilities, and the plans for use of IT support current and on-going business strategy.
3. **Acquisition.** All IT investments are made with valid reasons, on the basis of relevant analysis and transparent decision making, with and appropriate balance between benefits, costs, and risks to the organization.
4. **Performance.** IT is fit for purpose, providing services that meet the business requirements in terms of quality and service levels.
5. **Conformance.** The use of IT systems complies with all applicable legislation and regulations, as well organizational policies and practices which should be well defined, implemented and enforced.
6. **Human behavior.** Respect for human behavior is demonstrated in IT policies, practices, and decisions, even as needs evolve among all stakeholders.

Additional principles as defined by COBIT are that the IT governance system should:

- **Satisfy stakeholder needs and generate value** from the use of information and technology.
- **Be built from a number of components** that can be of different types and that work together in a holistic way.
- **Be dynamic,** always considering the effect of changes to any of its design factors.
- **Clearly distinguish** between governance and management activities and structures.
- **Be tailored to the enterprise's needs**, using a set of design factors as parameters to customize and prioritize its components.
- **Cover the enterprise end to end**, focusing on all technology and information processing the enterprise puts in place to achieve its goals, including outsourced processing.

Related reading

- BMC Business of IT Blog
- What Is GRC? Governance, Risk, and Compliance Explained
- COBIT vs ITIL®: Comparing IT Governance Frameworks
- Cloud Governance Best Practices
- Top Governance Books To Read
- Data Management vs Data Governance: Main differences