Haris Hamidovic, CIA, is chief information security officer at Microcredit Foundation EKI Sarajevo, Bosnia and Herzegovina. Prior to his current assignment, Hamidovic served as IT specialist in the North Atlantic Treaty Organization (NATO)-led Stabilization Force (SFOR) in Bosnia and Herzegovina. He is the author of four books and more than 60 articles for business and IT-related publications. Hamidovic is a certified information technology expert appointed by the Federal Ministry of Justice of Bosnia and Herzegovina.

Fundamentals of IT Governance Based on ISO/IEC 38500

The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper function of a market economy.1

Governance is a process by which a board of directors, through management, guides an institution in fulfilling its corporate mission and protects the institution’s assets. Effective governance occurs when a board provides proper guidance to management regarding the strategic direction for the institution and oversees management’s efforts to move in this direction.2

Over the years, IT has become the backbone of businesses to the point where it would be impossible for many to function without it. IT is no longer separate from the enterprise; it is an essential element of it. While, in the past, business executives could delegate, ignore or avoid IT decisions, this is now impossible in most sectors and industries.3

A lack of board oversight for IT activities is dangerous; it puts the enterprise at risk in the same way that failing to audit its books would.4 In fact, the Bank for International Settlements (BIS) has pointed out that board members in financial institutions should address IT as they would any other strategic board agenda item.5

Critical dependency on information technology calls for a specific focus on IT governance to ensure that the investments in IT will generate the required business value and that risks associated with IT are mitigated.6

The main objective of this article is to provide an introduction to the key elements of IT governance, to key industry frameworks used by organizations, and to guiding principles for directors of organizations on the effective, efficient and acceptable use of IT within their organizations based on ISO/IEC 38500:2008.7 It should assist board members in starting to fulfill obligations in respect to their organizations’ use of IT.

WHAT DOES IT GOVERNANCE COVER?
The IT Governance Institute® (ITGI®) states that, fundamentally, the governance of IT is concerned about two things: IT’s delivery of value to the business and the mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement. IT governance is also a continuous life cycle.8

IT governance is distinct from IT management. Governance determines who makes the decisions. Management is the process of making and implementing the decisions.9

IT governance is about who is entitled to make major decisions, who has input and who is accountable for implementing those decisions. It is not synonymous with IT management. IT governance is about decision rights, whereas IT management is about making and implementing specific IT decisions.10

IT GOVERNANCE FRAMEWORKS
A number of experts suggest frameworks that are detailed and intended for implementation by middle managers. These are known as IT governance “frameworks.” Some of the frequently cited frameworks are:11

• COBIT12
• IT Infrastructure Library (ITIL)\textsuperscript{13}
• ISO/IEC 27001\textsuperscript{14}

Although these frameworks are characterized as “IT governance frameworks,” some of them are in fact management frameworks.\textsuperscript{15}

These frameworks are not alternative treatments of the same issues.

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.\textsuperscript{16}

ITIL is essentially a series of documents that are used to aid the implementation of a framework for IT service management. This customizable framework defines how service management is applied within an organization. Although ITIL was originally created by the Central Computer and Telecommunications Agency (CCTA), a UK government agency, it is now being adopted and used across the world as the \textit{de facto} standard for best practice in the provision of IT service. Although ITIL covers a number of areas, its main focus is on IT service management.\textsuperscript{17}

ISO/IEC 27001:2005 is a standard that sets out the requirements for an information security management system. It helps identify, manage and minimize the range of threats to which information is regularly subjected. The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties, including an organization’s customers.\textsuperscript{18}

PRINCIPLES FOR GOOD CORPORATE GOVERNANCE OF IT

An example of the growing importance of IT governance, ISO released in 2008 a new worldwide standard, the objective of which is to provide a framework of principles for directors to use when evaluating, directing and monitoring the use of IT in their organizations. In this standard, ISO puts forward six principles for governance of IT:\textsuperscript{19}

1. Responsibility—Individuals and groups within the organization understand and accept their responsibilities in respect of the supply of and the demand for IT. Those with responsibility for actions also have the authority to perform those actions.

2. Strategy—The organization’s business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization’s business strategy.

3. Acquisition—IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is an appropriate balance between benefits, opportunities, costs and risks, in both the short term and the long term.

4. Performance—IT is fit for purpose in supporting the organization and in providing the services, the levels of service, and the service quality required to meet current and future business requirements.

5. Conformance—IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

6. Human behavior—IT policies, practices and decisions demonstrate respect for human behavior, including the current and evolving needs of all the “people in the process.”

ISO/IEC 38500 recommends that directors should govern IT through three main tasks:

• Evaluate the current and future use of IT.
• Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives.
• Monitor conformance to policies and performance against the plans.

IT GOVERNANCE IMPLEMENTATION

Enterprises implement their governance arrangements through a set of governance mechanisms: structures, processes and communications.\textsuperscript{20} Well-designed, well-understood and transparent governance mechanisms promote desirable IT behaviors. Conversely, if mechanisms are poorly implemented, then governance arrangements will fail to yield desirable results.

Effective governance deploys three different types of mechanisms:

• Decision-making structures—Organizational units and roles responsible for making IT decisions, such as committees, executive teams and business/IT relationship managers...
• **Alignment processes**—Formal processes for ensuring that daily behaviors are consistent with IT policies and provide input back to decisions. These include IT investment proposal and evaluation processes, architecture exception processes, service-level agreements, chargeback, and metrics.

• **Communication approaches**—Announcements, advocates, channels and education efforts that disseminate IT governance principles and policies and outcomes of IT decision-making processes

**WHAT QUESTIONS SHOULD BE ASKED?**

The Australian Computer Society president, Richard Hogg, said:

*Just as [information and communication technologies (ICT)] managers are having to broaden their skills to better understand the business structure and processes they are required to support, so must boards enhance their awareness of the various issues associated with IT. Corporate boards must learn what questions to ask about ICT governance... It is poor corporate governance to push ICT governance down to the IT manager level. ICT is an integral part of their business and ICT governance is an integral part of corporate governance.*

*\(^{21}\)*

Asking tough questions is an effective way to get started in implementing IT governance. Of course, those responsible for governance want good answers to these questions. Then they want action. Then they need follow-up. It is essential to determine not just the action, but also who is responsible to deliver what by when.\(^ {22}\)

The Canadian Institute of Chartered Accountants (CICA) released a brochure called “20 Questions Directors Should Ask About IT” to assist corporate directors in the discharge of their responsibilities. The document is also intended to be helpful to audit and IT steering committees.\(^ {23}\) The questions make it clear that the prime responsibility rests with management to implement the necessary procedures. The board members need to determine that management has done so—that the procedures are in place.

Moreover, if the directors are to perform an effective oversight role with regard to management, they would be remiss to rely simply on the representations of management, no matter how honest and reliable management might be. Therefore, some corroborating evidence would be essential. Directors must determine that procedures are in place, that the procedures are appropriate, and they must obtain corroborating evidence.\(^ {24}\)

**CONCLUSION**

Maturity of the governance of key assets varies significantly in most enterprises today. Financial and physical assets are typically the best governed, and information assets are among the worst governed. However, IT governance should be an integral part of corporate governance. Asking proper questions is an effective way to get started in implementing IT governance. Board members must learn what questions to ask about IT governance. Then, they need good answers to these questions and they must require action. The next step is to implement governance arrangements through a set of governance mechanisms—structures, processes and communications.

**ENDNOTES**

1 Organisation for Economic Co-operation and Development (OECD), *OECD Principles of Corporate Governance*, France, 2004

2 Rock, Rachel; Maria Otero; Sonia Saltzman; *Principles and Practices of Microfinance Governance*, ACCION International, USA, August 1998


6 Op cit, Van Grembergen and DeHaes, 2008


8 ITGI, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003