EFQM AND IT GOVERNANCE

An organisation cannot be excellent if technology is not managed in an excellent way. The IT Governance paradigm could be used as a reference.

There was a time when Information Technology (IT) was only a support and cost reduction tool. Nowadays, IT is a fundamental pillar of management, relationship with customers and operations. It is part of the strategy definition and review, and frequently services cannot be delivered and products cannot be manufactured without technology. Technology allows the creation of new products and services and has become a key element in any organisation that should be managed properly at any level (strategic, tactical and operational). Everybody should be involved in this. All points of view should be present when analysing IT, not only the technological one.

The differences between IT (information technology) and OT (operations technology) should be kept in mind. The Internet of Things (IoT) is empowering OT and a lot of new uses of technology will be possible in the near future. Robotics in car production, medical devices in health treatments and geolocation in transport are clear examples of OT. Depending on the industry, OT could be even more relevant than IT. Mobility allows the digital transformation of most activities like e-learning, financial services, tourism and leisure, etc.

Information and Technology (IT) Governance is a subset discipline of Corporate Governance. It is also known as Corporate Governance of Information Technology. The main frameworks are ISO/IEC 38500 and COBIT. The first one is based on the AS8015 Australian Standard for Corporate Governance of Information and Communication Technology. Control Objectives for Information and related Technology (COBIT) is regarded as the world's leading framework. The first version was released in 1996 by the Information Systems Audit and Control Association (ISACA). The current version (COBIT 5) has quite a wider scope and is more focused on business requirements than technical issues.

TCOBIT includes the objectives of IT governance and good practices, the detailed description of the 37 processes that propose to manage IT, recommendations for establishing the accountability of each process to the different roles in the organisation, and key performance and goal indicators (KPI & KGI) for the processes according to the Balanced Scorecard structure. COBIT also provides a useful tool to cascade enterprise-level goals into IT-related goals and the IT processes which are more relevant to these IT goals. For example, an organisation where online sales are critical requires sound processes related to the continuity of services. The Capability Maturity Model (CMM) which was originally focused on software engineering provides a useful approach to analyse the strengths and weaknesses of these processes.

IT Governance is composed of four main domains: strategic alignment, value creation, risk management and resources optimisation. The goals of technology should be aligned with the strategic goals of the organisation. The aim of technology is to contribute to the organisation's mission and vision attending to the values of the organisation. There are other objectives with which technology should be aligned, like a Human Resources plan, partnerships, customer relationships, products and services based on technology, online presence and geographical presence, etc. The above-mentioned COBIT cascading tool could be useful.

IT projects and investments on technology must create or add value to the organisation and they should be evaluated on a business basis. Using technology is not an objective. It is a tool to achieve the goals of the organisation. Any investment on technology and project should be analysed according to the ROI expected. Projects require a mature project management methodology like the Project Management Institute (PMI) standards. This analysis can be difficult because of intangible issues like reputation and customer behaviour predictions.

Technology is a great source of opportunities but also plenty of risks, that should be managed accurately. Traditionally, IT risks were analysed with specifics methods like ISO 27000 and NIST series 800 oriented to Information Security Management Systems, but nowadays approaches like ISO 31000 Risk Management proposes a unique method to manage all kinds of risks within the organisation. A risk can be defined as the product of likelihood by impact and impact should be expressed in monetary terms. It is not easy to quantify the impact of the reputation of an adverse incident especially when organisations are using social media as a marketing tool and a communication channel with customers and society in general. Some organisations operate in critical infrastructure scenarios where loss of human life is a possible impact. Transport, energy production and distribution, defence and health are some examples of these critical services. Cybersecurity should be managed at the top level and awareness and education are key elements.

Resource optimisation is a key point in any technological strategy. Cloud services are an alternative to consider instead of classical on-premise IT infrastructures that suppose a change from investments on IT infrastructure to a pay per use approach. The best technology managed by employees without the required capabilities would provide a poor outcome. People are essential in any technology strategy. Third-parties are usually present in IT in any organisation. It is recommended to maintain the appropriate level of technological knowledge inside an organisation, to have the necessary criteria to be able to take decisions and to be conscious that the legal accountability cannot be externalised. Availability of service requirements implies a sound strategy of Business Continuity Plan (BCP) and ISO 22301 Societal Security is a good reference to use.

On the 25th of May 2018, it will be compulsory to comply with the EU's General Data Protection Regulation established to protect privacy and it will be recommended to deploy the role of Data Protection Officer (DPO) within organisations. It is necessary to have a deep reflexion to balance the privacy with paradigms like big data and e-health services based on IoTs. Organisations should develop a compliance and forensic readiness strategy because legislation in IT is growing, it is different in each country and litigation represents a real risk. Organisations need to establish policies to regulate the information security, the use of social media, cloud services, BYOD (bring your own device), mobile devices, data leak prevention, etc. These polices must be observed by employees, third-party personnel, providers and other users of the information systems. All these regulations should be aligned with the values of the organisation.

Technology is a key element in the eight fundamental concepts of EFQM. Excellence through Agility was the title of EFQM Forum which took place in Madrid at the end of October. The word technology does not appear but it is difficult to achieve agility without technology.

Technology is pervasive and this point of view should be present when analysing the EFQM Model. It is present in all the criterion and not only in the 4d (Technology is managed to support the delivery of the strategy). Because technology is so critical, all leaders should be involved. Both, IT and OT should be managed using a holistic vision that comprises business, technology, risk, legal aspects, human resources, audit, etc. A common language about technological issues is necessary. Leaders who will have to take decisions based on technology need to fully understand the concepts and trends of technology. OT is newer than IT and is usually managed in different departments of the organisation like production and research. An excellent organisation should try to avoid any sort of silo approach in technology management.

The weight of technology and the associated risks are more present than ever in the strategy. Specialists in these areas should participate in the definition, measurement and review of the strategy. The quickly changing environment requires agility. Digital competences are compulsory for everyone that contributes to the organisation and these capabilities are evolving rapidly. It is a real challenge to take profit from the technological opportunities and achieve innovating products and services using technology. Mature technological approaches should be a tool to attract and retain talent in an organisation which is necessary to carry out innovation.

It is not possible to manage technology without a sound partnership strategy. However, it is required to have internal technological knowledge to select good partners and to be up-to-date with technological trends. Pioneering involves risks but doing nothing is an even bigger risk. The technological reputation of an organisation could attract partners to collaborate on developing new services and that requires leaders to be involved in this vision and to have trained employees. Cloud services are a key element to change financial approaches from CAPEX to OPEX. The IoT paradigm will change our environment spreading sensors everywhere and facilities' management would be easier and cheaper.

Technology allows the continuous improvement of products and services and permits disruptive changes. Nowadays, it is more difficult to compete in the era of globalisation with all the organisations and customers around the world increasing their preference for online services and communication rather than face-to-face ones.

According to the increasing importance of IT and OT, indicators relating to technology should be more present in leaders' decisions and results monitoring. These indicators would be linked to the IT goals which are linked to the enterprise's objectives. Technology should contribute more to the excellence of organisations and the EFQM principles would be used to improve the management and value of technology. In summary, technology should be deeply analysed in any EFQM implementation and assessment.

Xavier Rubiralta Costa, an expert from the Excellence network and Project Manager in the security of information at the Autonomous University of Barcelona, shares his knowledge of Cybersecurity seems through the prism of EFQM.

Este documento ha sido descargado de la web del Club Excelencia en Gestión: www.clubexcelencia.org