ASSURANCE IS A VALUE ADDED TOOL

John Mitchell – Chairman, Information and Risk Management Assurance (IRMA) Specialist Group

Computerised systems add great value to an organisation when they operate correctly, but can have significantly adverse operational and reputational consequences when they go wrong. The immediacy of the impact leaves little time for the organisation to rectify the problem before it enters the public domain. The increasing use of social media means that the problem is quickly widely advertised and the organisation is often perceived as being unresponsive and uncaring in its response. Technology is not static and in the last forty years we have moved from mainframe computers running single batch programs to cloud computing. Our risks have changed and so have our control paradigms. They will continue to change as the technology changes and so will our assurance processes. Regardless of the technology, the IT function basically provides two main business services: the acquisition and implementation of new business solutions (development) and the delivery and support of those services to the customer (operations). In order for the business to have assurance that it is effectively receiving these services a 'wrapper' is usually applied which provides for the management of the IT function and measurement of its performance. This wrapper is often defined as IT Governance. The Information Risk Management and Assurance Group (IRMA) is one of the oldest and most lively groups within the BCS. Although at first sight the group's title may imply that its membership are primarily auditors, the reality is quite different, as risk management and the associated assurance requirement are now at the forefront of IT governance. Stakeholders of many different persuasions increasingly demand confirmation that IT risks are being identified and managed. Historically, the IT function has been viewed as a business cost, but today, more enlightened stakeholders perceive the value added to the business by IT as being the actual value of the business itself. This is because without IT the business would not function. It therefore stands to reason that assurance that IT is being well managed also has great value. The regulatory authorities take a poor view of organisations that do not deliver an appropriate level of service, or which breach statutory requirements. The resulting poor publicity is often a driver in changing the occupants of the top posts. Far better to identify potential problems before they enter the public domain. This requires good governance and management structures and a wide understanding of both the scope and impact of IT on the efficiency and effectiveness of business operations. This is where the IRMA specialist group comes in. Its two-thousand members are experts in analysing the effectiveness of IT governance structures and processes in delivering value for money within an increasingly dynamic business and regulatory framework. Most members will have appropriate academic and professional certifications[i]. They also have an immense tool-set available to them in the form of relevant ISO standards, supported by the IT Infrastructure Library (ITIL), the Capability Maturity Model (CMM)

and Control Objectives for IT (COBIT). Because they speak the language of both business and IT and because they report to very senior management they are ideal ambassadors and interpreters between the various business functions. They understand not just the risks, but also the controls to manage those risks. Because most of IT is invisible (only the hardware and people can be seen) they have developed tools which enable the extraction of data for subsequent analysis and the re-performance of software logic to confirm that the IT systems are performing as intended. They may identify actual, or potential errors, which unless rectified may cause subsequent problems. One financial services company was found not to be controlling its critical spreadsheets. It accepted the fact, but was slow in rectifying the issue. As a result it is was fined £1.6 million by the regulators. Although this may seem insignificant when compared with fines levied against Microsoft and Google it hurt the business both in its pocket and its reputation. This is not an isolated case. Newspapers report daily on poor levels of IT service, data protection breaches, denial of service attacks, fraud and hacking. The simple defacing of a web site may well cause customers to question the security of their personal data. The Financial Services Authority, which was replaced in April 2013 by the Financial Conduct Authority, levied £292 million ($458 million) in fines during 2012 against firms that had inadequate risk management and controls. The role of the IRMA member is to help the organisation by identifying such problems before they hurt, but it is management's job to fix the issue. This identification and fix before it hurts process requires co-operation between the IT service deliverers and the assurance providers and is an essential requirement if the business is to obtain maximum value from both its IT and assurance investments. Co-operation is not the same as acquiescence and the relationship can certainly be tense at times, as can be expected when two professionals go head-to-head over an issue. Confidentiality, integrity, availability and compliance are the top management business concerns, but in the IT context they can be technically complex. Reporting that 'port 80 is insecure' is unhelpful to management even if factually accurate. Converting this into business terms is a skill in its own right. Ultimately, it is managements responsibility to run the business and to take the risks, but it should do so with full information of the implications. It is the job of the assurance provider to supply this information in a business context.

---

[i] CITP – Chartered Information Technology Professional
CISA – Certified Information Systems Auditor
CISM - Certified Information Security Manager
CRISC – Certified in Risk and Information Systems Control
CGEIT – Certified in the Governance of Enterprise IT