Information Security Now – 29

IT governance can be defined as ‘a structure of relationships and processes to direct and control the IT function in order to achieve the enterprise’s goals by sustaining and extending the enterprise’s strategies and objectives’. Today, the value of IT to the business is often the value of the business itself because without IT the business could not effectively function. IT Governance is a wrapper which surrounds the two things that all IT departments do, either directly or indirectly. Those two things being: the provision of new business solutions and the delivery and support of those solutions to the customer. The governance wrapper itself comprises two elements: the organisation and provision of IT services and the performance measurement and enhancement of these services. It is in relation to this latter element that the concept of assurance arises.

Assurance is an important component of IT governance. How can the Chief Information Officer (CIO) show that the IT service is meeting its value for money and service objectives? Usually this is through the provision of provision of performance metrics, but how can s(he) prove that these metrics and associated analysis are reliable? I once attended a meeting with a Chief Executive and his six direct reports, two of whom were the CIO and the Chief Internal Auditor (CIA). I asked each head of department in turn who was responsible for internal control in their company? Without hesitation each one pointed to the CIA. When I then asked them how frequently the CIA audited their controls they responded ‘every three years’. When I then asked them who was responsible in-between the three year period, they shuffled their feet, avoided by eyes and remained silent. I then pressed them on risk management. They accepted that this was their responsibility, but when I then pointed out that risk was managed by controls they started to realise that control was their responsibility too. Assurance is primarily achieved by measuring the effectiveness of controls in managing risks. Unfortunately most auditors and very few managers cannot define what a control is and how it operates, so it is not too surprising that our IT assurance processes are somewhat suspect. I would even go further by asserting that our current control paradigm is not fit for purpose.

Our technology has changed beyond recognition in the last forty years. From mainframe computers running single batch programmes to cloud computing. Apart from the hardware and the people, most of IT is invisible to the eye. We cannot see the software, data, or transactions which comprise our IT systems. Even the bits we can see may be operated by a remote third-party. We are attempting to control twenty-first technologies with eighteenth century controls, without even knowing what a control is. So here I lay out my assurance definitions. A control is ‘anything which monitors, or modifies a process so as to (hopefully) ensure the predictability of the process’. How does it work? A control works by comparing something against a known answer. It is simply a test. As an example, let us consider a gender field with a single allowable entry of either ‘M’, or ‘F’. The monitoring mechanism checks for an allowable entry. If it meets the ‘M’ or ‘F’ criteria then it is allowed to pass through to the next process. If it fails the test however, the process is modified so that the transaction is returned to the initiator. So all controls are processes, but not all processes are controls.

Applying this to risk management we now need to consider the movement from inherent (gross) risk to residual (net) risk. The risk equation has two components: reducing the likelihood and reducing the consequence. To do both you need a minimum of two controls and this assumes that each control is one hundred percent effective. I can prove with some pseudo mathematics that this is not the case. By deconstructing a control into its four elements: design, implementation, monitoring and evaluation and then assigning a maximum value to each element. I then assess the actual value of each element for a particular control and mathematically calculate the overall effectiveness of that control. This shows that few, if any controls, actually reduce the inherent risk to an acceptable residual level. In many cases we can only manage one side of the risk equation; either we reduce likelihood, or we reduce the consequence, but we may not be able to do both. So all those risk registers which show a movement from inherent red risk to residual green risk are basically wistful thinking. In most cases the best we can achieve is a movement from red to yellow. Nowhere is this better illustrated than in our change management process which in most entities rely on trust as the control mechanism. Trust the programmer to not add any unauthorised code and trust the tester to find it if s(he) did. Unfortunately, trust is not a control, but rather a reliance on human behaviour. We can only manage humans, not control them, because they have free will, so trust is not a control and we should therefore acknowledge that anything which relies on it is flawed.

So I leave you with a conundrum. If IT governance effectiveness is assured by controls and our control paradigm is flawed, then where does that leave us? My answer is in a quagmire. We are truly up the creek without the preverbal paddle. The only solace that I can offer is that we now have a more ‘scientific’ method of measuring control effectiveness, which at least can provide a more accurate picture of where we really are in our risk management process.. Assurance, or lack of it, truly has business value, because it can show senior management where they really are regarding their residual IT risks. Unfortunately, this is likely to be a most uncomfortable experience.

John Mitchell

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of Council and current chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638