IT Governance, Risk and Compliance (part one)

by Alan Simmonds

PreterLex (Cambridge) UK

Introduction

PRISM, Accumulo, NSA, surveillance, privacy and intrusion – recent events make these difficult to ignore. Should we be concerned about the types of events brought about by Ellsberg, Woodward, Manning, Snowden and countless others in an article aimed at risk professionals? – only in as much as we recognise that risk is everywhere. The often-quoted 'eternal vigilance is the price of freedom' (Wendell Phillips, 1852 and attributed to many others thereafter) provides a good segue into the basic theme of this set of articles – governance, risk and compliance (GRC) – by way of recognising that freedom for organisations to meet their objectives must be balanced by the appropriate accountabilities, responsibilities and actions.

While we might be tempted into a discussion on ethics, morality, liberty, public interest and whistleblowing – these remind us what the difference between management and governance is. Whether this is at country level or within a small department the distinction is the same – management is typically about 'running the business' while governance is about 'ensuring that the right things are done'.

This is where we leave PRISM behind.

Moving ahead …

This series of articles will look at governance, risk and compliance considering information technology and will build an approach that will help identify core aspects of GRC and will culminate in a proposed operating model that integrates best practice and industry standards. This journey requires that we set the scene with a few general definitions and hints as to the subject matter that will come under scrutiny during this series.

Technology, specifically information and communications technology (ICT), is one of the+ core mechanisms that organisations utilise to meet and sustain their strategic objectives. The assets that comprise the organisation's ICT universe include *hardware, software, architecture, intellectual property, skills, vendor and service provider management (including cloud[(1)]), market awareness, customer management, culture* to name but a few. Just having these available on the balance sheet, as processes or as 'ways of working' is not sufficient – they must be made to work in harmony to provide measurable benefit[(2)] to the organisation.

Assets

The assets outlined above must be fully and effectively utilised by organisations in order to deliver their strategies – in order to do these we recognise 3 core GRC capabilities:

- Protection of assets
- Compliance
- Consistent service provision

Protection of assets is a broad term that includes all assets (see list above) – we recognise that each of these assets has associated use, ownership/stewardship, operation, involvement, influence, and adoption across the organisation all leading to a complex web of

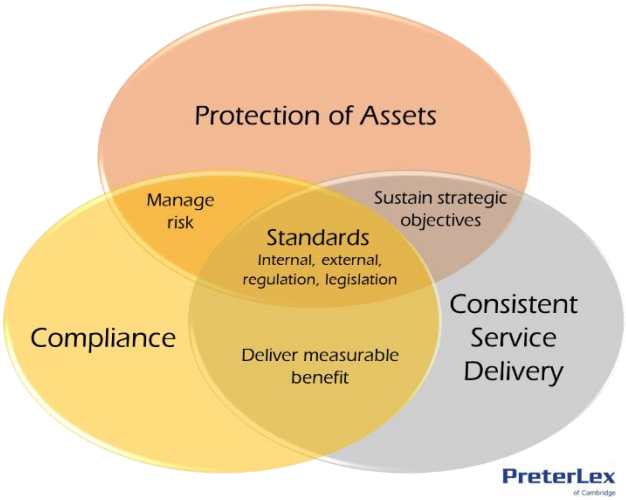
interactions and requirements for governance. One particular challenge we have on the ICT asset front is that the pace of change is accelerated and any down/up-side impact can therefore occur with increasing uncertain frequency and magnitude.

Compliance includes the adherence to rules, designs, regulations and standards as well as includes the acknowledgement of both static (decision rights, structures and authority remit) and dynamic (proper and timely execution of decisions, policies, standards, performance measurement and BRR) sides of governance.

Consistent service provision is the concept of delivery that includes timing, channels, metrics, audience, improvement and recognising that …

These 3 capabilities are linked through a backbone of *standards* which is also an umbrella terms that includes regulation, legislation, internal organisational standards, policies, principles, guidelines and standard operating procedures.

Central to GRC is the requirement to mitigate risk, deliver strategic objectives and provide benefit - over this series of articles we will be exploring how these can be made to work together to drive the correct organisational behaviours and sustain the organisation's strategy. The *'GRC Overview'* diagram provides the overall structure that we'll be following to show this approach.



GRC Overview

IT Governance

Information technology governance is both a necessary and formal partner in this journey and we'll be exploring how frameworks such as COBIT® can be used to provide the support necessary to integrate many of the concepts and constructs mentioned in this article.

Risk Management

The 3 capabilities outlined above will all contribute to risk management – as we'll see the use of frameworks is necessary – indeed the ISO31000 will provide us many opportunities to exercise the direction, control and necessary discipline to help embed effective GRC in the organisation.

Often however the benefits of risk management are 'sold' using threats rather than focussing on risk itself - this leads to a reactive and tactical approach – which is the exact problem we're trying to avoid through proper, informed and established GRC.

To close this first article on GRC we'll highlight some risk challenges both within the ICT and business sides of organisations that must be addressed to support our approach:

- Risk-aware culture must be established in the organisation – all stakeholders must understand the IT risks that affect them
- Measurement and reporting of the effectiveness and efficiency of IT risk management must become business-as-usual

- Risk strategies and architectures must extend beyond near-term regulatory situations
- Well-defined IT risk management processes have been implemented

Next time

We'll be looking at each of the 3 GRC capabilities, exploring risk architecture and how to start aligning the various management frameworks in organisations to deliver effective, risk-aware GRC.

Footnotes:

(1) Cloud computing - an umbrella term for everything from web-based email to business software that is run remotely via the internet instead of only on-site to reduce costs and add flexibility to IT divisions
(2) Measurable benefit is the preferred metric rather than profit as not all organisations are driven by profit – e.g. NGOs, cooperatives etc.