IT Governance, Risk and Compliance (part two)

by Alan Simmonds

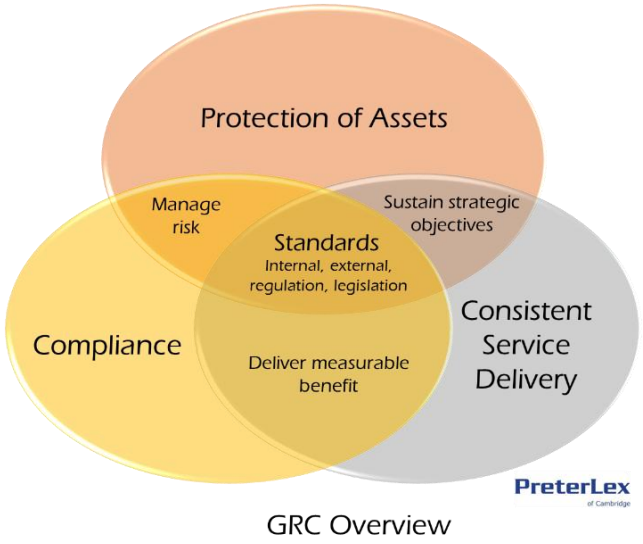
PreterLex (Cambridge) UK

Introduction

In the first article of this series we introduced GRC (governance, risk and compliance) as an organisational competence to help achieve and also sustain strategic objectives. Specifically we proposed 3 core GRC capabilities:

- Protection of assets
- Compliance
- Consistent service provision

The focus of this article[1] is on the *Protection of Assets,* being critical for all functions and all asset types across the organisation.



GRC Overview

Previously we proposed a universe of assets in the IT space that require management and recognising that each of these assets has associated use, ownership/stewardship, operation, involvement, influence, and adoption across the organisation. Within the IT space we recognise further challenges such as accelerated pace of change and the consequential impact that can occur with increasing uncertain frequency and magnitude.

In this series we differentiate between capabilities, competencies and frameworks:

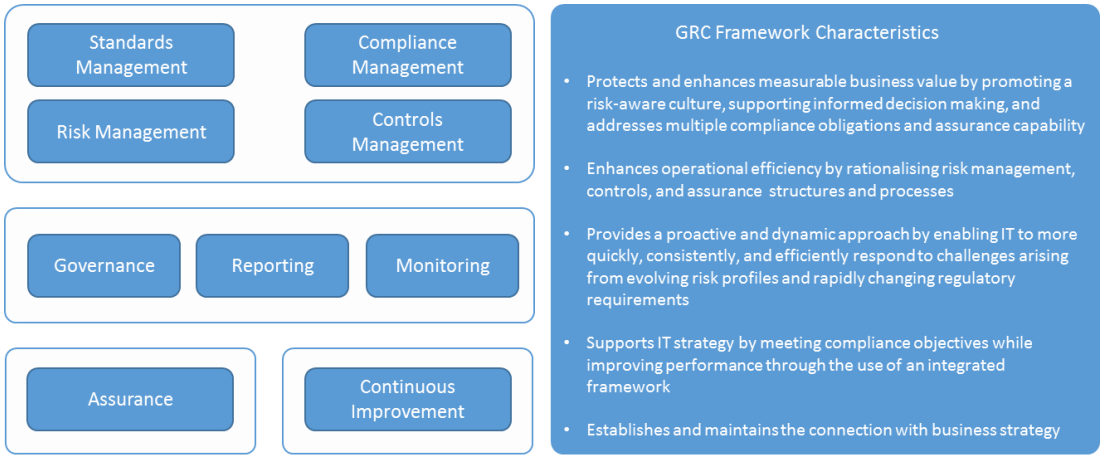
- *Capabilities* are defined as the set of organisational, personal or system abilities that typically require a combination of organisation, people, processes and technology to achieve. Capabilities are directly related to the operations and functioning of the organisation and are necessary to deliver and sustain the organisation's strategy
- *Competencies* arise from collective learning across the organization, especially the capacity to coordinate differing skills to integrate these across the technology and operational landscape of the organisation – they are particular strengths relative to other organisations in the same industry which provide added measurable benefit
- *Frameworks* should contain a detailed method, supporting tools, common standards, an organisationally-relevant vocabulary, monitoring and reporting, identified metrics and KxIs (x = Goal, Performance, Risk, Assessment etc.)

Protection of Assets

While this capability refers to the digital and physical assets of the organisation our focus is on IT and in particular digital assets. Most organisations are not clear about how much data they own or have access to – in operational and archival systems – and consequently this leads to the proposition that they are often unaware of the amount of information that can be created from that data. This can lead to unintended consequences such as information leakage, reduced focus on asset security and limited capability to respond when assets are compromised. Typically we expect asset protection to consider the characteristics of assets such as availability, confidentiality, integrity, volatility and access. ISO 27000 provides a firm start in that it identifies current best practice recommendations on information security management and controls within the context of an information security management system.

Assets such as credit rating, market position, reputation etc. must be considered within the remit of asset protection – each of these, and others, must be protected against value dilution through theft or compromise.

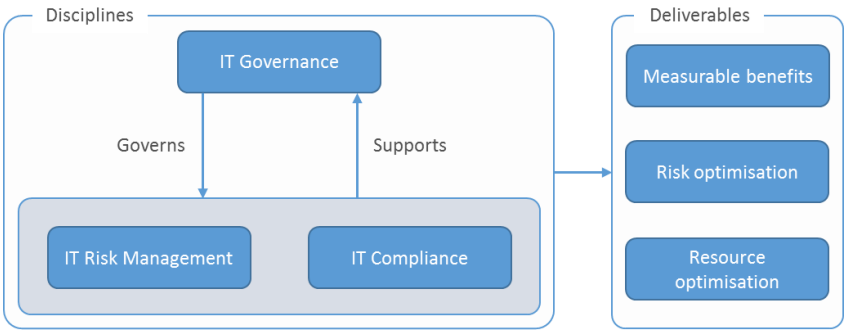
Taking the above into account it is now possible to propose the basis of a GRC framework that will be developed during this set of articles and culminate in a target operating model to assist in the establishment of an enterprise-wide ERM capability.



GRC Framework

With the spread of the web, extended company structures, cloud and BYOD etc. it is necessary to consider a formal risk management[2] approach within an enterprise-wide GRC initiative.

The protection of assets requires investment in technologies, staff awareness and corporate behaviour. The balance between organisational expenditure and risk should be managed through IT governance (*see adjacent figure*).



Disciplines and Deliverables

Even when this investment has been made we are reminded [1] of a series of unintended consequences:

- Increase in procedural controls and individual compliance requirements (less convenience)
- Users relinquish control and self-reflective IT use in exchange for organisational protection
- Limited functionality and reduced set of available applications create an illusion of security
- Trend toward prescriptive rule setting rather than principles-based security governance
- Shift toward user/employee liability in the context of strict rules for IT usage, little tolerance for human error

All of which themselves subtly, but significantly, play upon the perception of the prioritization of the individual risk metrics within the overall risk-space, itself an unintended consequence.

The practice of asset protection is wide-ranging and must include the establishment of policies and procedures for inventorying, tracking assets, and reporting on information technology and digital related assets.

Assets are by definition what provide measurable value and capability to organisations and as such the approach must include exploring opportunities for maximizing or exploiting unused or partially used IT assets to achieve full efficiency and delivery positive ROI. In this set of activities we must include the supporting planning, monitoring, maintaining and recording of all xLAs (x = enterprise, service and operational) – particularly for those assets that are provided (and potentially managed):

Externally

- Develop, establish, implement, and enforce supplier and outsource service provider strategies, guidelines and obligations
- Establish and manage vendor and outsource service provider audits when required
- Manage contracts and relationships to maximise measurable benefit and reduce costs for licensing, maintenance, and service offerings.
- Compare warranties, maintenance agreements, and vendor (hardware, software, cloud and other service) contracts to assist with asset maintenance, upgrades, repair and replacement
- Manage contracts so that they support monitoring the performance and contract compliance of all suppliers

Internally

- Conduct and report asset reconciliation and audit activities on a timely basis, including financial, licensing, warranty, and maintenance/support contract information
- Communicate asset (management and) protection strategies
- Research industry best practices and compare against the organisation's practices in order to establish benchmarks for protecting IT assets
- Be aware of and factor in the subtleties of large transactions such as M&A, JVs, divestments on the full process of asset protection on the current and future state of the asset base
- Continuously monitor, assess and improve the asset protection capability, including the adoption and sharing of best practice
- Ensure service is provided in accordance with the organisation's procedures/processes and controls
- Create and publish regular scorecards for asset performance and risk profiling of each asset and asset class

As a general capability asset protection should also include monitoring and analysing trends in investment and return in order to make recommendations and to identify areas for asset optimization and protection that were previously not recognised.

When assets are compromised

As organisational assets may be compromised through many different means we should be aware that the GRC framework must consider how to protect and manage the impact across a wide range of areas. Specifically the framework must recognise the following [1]:

- Operational impact
- Reputational impact
- Immediate financial damage
- Indirect financial damage

- Contingent financial damage
- Legal and legislative impact

A complete plan for asset protection must also include crisis management for when our organisational assets (digital and others) are compromised so it is necessary to consider:

- Speed, precision and effectiveness of communication within the organisation and also to those outside the organisation who are directly or indirectly affected
- Consistency of message – being 'on message' is critical during this stage as future communication will build on the initial information burst
- Access to the right information for those who need it for recovery and communications
- Decisive and orchestrated remedial action by all major stakeholders (internal and external)
- Clear and articulated recovery strategy

This part of asset protection must be proactive and is dependent on good planning, appropriate training, and effective early detection systems.

Takeaway messages …

GRC, when fully implemented, will assist in improving risk management and compliance efforts by:

- Reducing inconsistent risk identification and assessment approaches
- Improving the coordination among the risk management and compliance functions
- Optimizing costs associated with risk management and compliance across the organization
- Focussing on standards, and the correct organisational responses and behaviours
- Enhancing the measurable benefit and coverage of existing risk assessment and review processes

Next time

We'll be looking at Compliance as the second of our 3 core GRC capabilities and start to introduce the concept of a target operating model to support our approach.

Note: Previously we mentioned that the 3 core GRC capabilities are linked through a backbone of *standards* (including regulation, legislation, internal organisational standards, policies, principles, guidelines and standard operating procedures) – this will be addressed as a separate article).

Footnotes

(1) As this series is written with IT in mind, we retain the focus on this discipline while recognising that IT risk is always inherent in all organisations whether or not they recognise or detect it. It should also be recognised that the approach taken throughout this series is also generally applicable to areas outside IT

(2) Risk management refers to the architecture (principles, framework and process) for managing risks effectively, while 'managing risk' refers to applying that architecture to particular risks [ISO31000]

References

[1] *Transforming Cybersecurity: Using COBIT 5*, ISACA, Information Systems Audit and Control Association, 2013.