THE CALDER-MOIR
IT GOVERNANCE FRAMEWORK

February 2013
The IT Governance Framework is a straightforward tool to help organisations implement the ISO/IEC 38500 standard for IT governance in the real world.

IT governance is a broad subject that involves many disciplines: information technology, risk management, strategy, intellectual property, business design, project management, compliance, and so on. Most of these disciplines offer IT governance solutions and tools, but most of the tools are very detailed, and have narrow scopes. No single standard discipline or tool provides a full picture of IT governance, and collectively they can provide a confusing picture that hinders the purpose of IT governance, which is to equip boards with information and levers for directing, evaluating, and monitoring IT support for their core businesses.
ISO/IEC 38500 is the first international standard that provides guidelines for corporate governance of IT. It provides a set of six principles for good corporate governance of IT. The six principles are: ensure that IT responsibilities are clearly established; corporate and IT strategy should be aligned; IT acquisitions and investments should be made properly; IT should deliver required performance; IT should also conform to all compliance requirements; and IT policies and practices should take human behaviour into account.

The Calder-Moir IT Governance Framework - first introduced in Alan Calder’s IT Governance Today: a Practitioner’s Handbook - is not another solution, but a way of organising IT governance issues and tools to support the board, executives, and practitioners. It places IT governance tools in the context of an end-to-end process, and provides a simple reference point for discussing the many aspects of IT direction and performance.

The framework consists of six segments, each of which represents one step in the end-to-end process that starts with business strategy and finishes with IT operational support for delivery of business value against that strategy. Each segment is divided into three layers. The inner-most layer represents the board, which directs, evaluates, and monitors information technology support for business. The middle layer represents executive management, which is responsible for managing the activities that deliver the end-to-end process. The outermost layer represents the IT practitioners and IT governance practitioners, who use proven tools and methodologies to plan, design, assess, control, and deliver the IT support for business.

Navigating the framework

The top half of the framework covers the processes that establish direction, specify constraints, make decisions, and plan. The bottom half covers the processes that develop new capabilities, manage the capabilities, and use IT to deliver business products and services. Start at the "9 o’clock" position (business strategy), and follow the segments clockwise through the end-to-end process.

The board provides direction on the organisation’s direction and business strategies.

These are analysed and designed by the executive managers and their strategy practitioners. The strategies must operate within one or more corporate governance regimes (The Combined Code, Sarbanes Oxley, Basel II/III, and so on). They also operate within a risk environment, so it is critical to undertake a thorough risk assessment to decide which controls will be the most appropriate. The first two segments, then, describe the organisation’s path and desired outcomes, the constraints within which it must operate, and the controls that will be most appropriate in those contexts.

Once the business strategies, governance regimes, risk assessment, and controls have been developed, IT works with the business to develop architectures and plans to deliver on those requirements. The result is a set of proposals and plans that describe what business and IT should look like, the expected performance, the changes required to deliver that performance, and the resource implications. IT Governance processes verify that the proposals meet the business strategy and corporate
governance requirements (including risk management and controls), and help the Board to evaluate the merits of the plans and proposals.

After the Board approves the plans and proposals, they can be implemented through a series of change projects - subject to regular monitoring within the IT Governance regime including controls developed by the risk assessment process. The projects create or update the organisation’s business and IT capabilities, which should then meet the performance and control criteria established during the planning phases. The capabilities are then deployed into business and IT operations for delivery of products and services - again governed by the performance and control criteria.

**Evaluate, Direct, Monitor**

The international standard ISO/IEC 38500-2008 (Corporate Governance of Information and Communication Technology) identifies three main IT governance tasks for directors:

1. evaluate
2. direct
3. monitor

The board evaluates the business conditions, strategies, constraints, and IT proposals. It directs by guiding the way IT should be used (IT principles), the appropriate risk and compliance posture, and the investment in IT proposals. And it monitors all process in the hexagon - business strategy, the business and risk environment (and constraints), IT strategy, change, capabilities, and operations. If any of these processes fail - that is, don’t deliver exactly what is required - then the Board intervenes (directs) through the processes in the top half of the Framework, refining or reinforcing the guidelines for business and IT.

Similarly, Executive managers Direct, Evaluate, and Monitor the processes carried out by practitioners, but are - for obvious reasons - more closely involved than the directors in all activities in both halves of the framework.

**Plan, Do, Check, Act**

The Framework is also a representation of a PDCA management cycle - Plan, Do, Check Act.

PDCA applies at two levels - a high level reflecting the board’s involvement, and a detailed level reflecting execution of the tasks in the end-to-end process.

At a high level the top half of the framework represents the Plan stage, the lower half represents the Do stage, monitoring activities in every task represent the Check stage, and feedback into the top half represents the directors’ Act stage.

At a more detailed level, executive managers and their practitioners are
interested in each of the tasks, the tools that are being used, and the outcomes that are produced at each step in the end-to-end process. The tasks within each segment should be well-defined, with clear measurable objectives, management processes, and performance improvement feedback loops.

Some subtleties

Finally, while it can be easy to read too much into a simplified diagram such as the IT governance framework, it is worth highlighting a small number of interactions between the segments:

- Completion of the end-to-end process - in Operations - is also the beginning of a new cycle, as actual performance is fed back into business strategy;
- Risk and compliance activities, while they initially constrain strategy, operate across all other segments in the end-to-end process;
- IT strategy and architecture activities depend on the capabilities activities and knowledge base to develop gap analyses, priorities, and strategies;
- Change is not only development or acquisition of IT systems - it is also preparing and changing the business, and making sure that the change delivers the intended outcomes in operation.
Further Reading

**ISO38500 (ISO 38500) IT Governance Standard**

ISO 38500 is the IT governance standard, providing guidance for directors of organisations on the effective, efficient, and acceptable use of IT. Available in hardcopy or PDF format.  
[www.itgovernance.co.uk/shop/product/iso38500-iso-38500-it-governance-standard](http://www.itgovernance.co.uk/shop/product/iso38500-iso-38500-it-governance-standard)

**ISO/IEC 38500 Pocket Guide**

This useful pocket guide provides an account of the scope and objectives of the standard. It outlines the standard’s six core principles, sets out the three major tasks that the standard assigns to directors regarding IT, and explains the interrelationship between the two. The guide also offers advice on how to set up and implement the IT governance framework.  
[www.itgovernance.co.uk/shop/product/isoiec-38500-the-it-governance-standard](http://www.itgovernance.co.uk/shop/product/isoiec-38500-the-it-governance-standard)

**IT Governance Framework Toolkit**

This toolkit contains all the tools and guidance that you will need in order to develop and implement an appropriate ISO/IEC 38500 IT governance framework for your organisation.  
[www.itgovernance.co.uk/shop/product/calder-moir-it-governance-framework-toolkit](http://www.itgovernance.co.uk/shop/product/calder-moir-it-governance-framework-toolkit)
IT Governance Solutions

IT Governance source, create and deliver products and services to meet the evolving IT governance needs of today’s organisations, directors, managers and practitioners.

IT Governance is your one-stop-shop for corporate and IT governance information, books, tools, training and consultancy. Our products and services are unique in that all elements are designed to work harmoniously together so you can benefit from them individually and also use different elements to build something bigger and better.

Books

Through our website, www.itgovernance.co.uk, we sell the most sought after publications covering all areas of corporate and IT governance. We also offer all appropriate standards documents.

In addition, our publishing team develops a growing collection of titles written to provide practical advice for staff taking part in IT Governance projects, suitable for all levels of staff knowledge, responsibility and experience.

Toolkits

Our unique documentation toolkits are designed to help small and medium organisations adapt quickly and adopt best management practice using pre-written policies, forms and documents.

Visit www.itgovernance.co.uk/free_trial to view and trial all of our available toolkits.

Training

We offer training courses from staff awareness and foundation courses, through to advanced programmes for IT Practitioners and Certified Lead Implementers and Auditors.

Our training team organises and runs in-house and public training courses all year round, covering a growing number of IT governance topics.

Visit www.itgovernance.co.uk/training for more information.

Through our website, you can also browse and book training courses throughout the UK that are run by a number of different suppliers.

Consultancy

Our company is an acknowledged world leader in our field. We can use our experienced consultants, with multi-sector and multi-standard knowledge and experience to help you accelerate your IT GRC (governance, risk, compliance) projects.

Visit www.itgovernance.co.uk/consulting for more information.

Software

Our industry-leading software tools, developed with your needs and requirements in mind, make information security risk management straightforward and affordable for all, enabling organisations worldwide to be ISO27001-compliant.

Visit www.itgovernance.co.uk/software.aspx for more information.

Contact us:

www.itgovernance.co.uk

servicecentre@itgovernance.co.uk

+ 44 (0) 845 070 1750