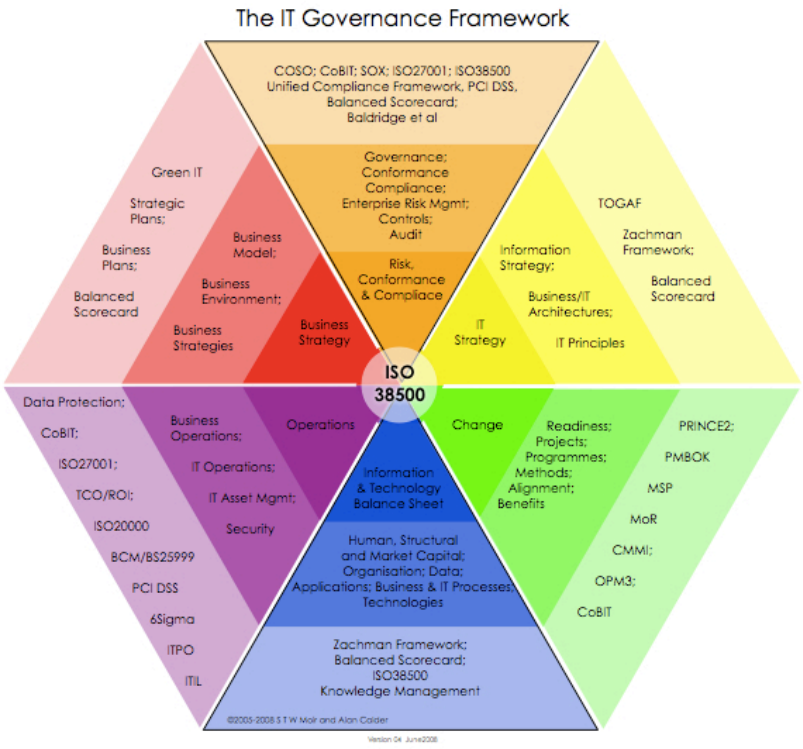
THE CALDER-MOIR IT GOVERNANCE FRAMEWORK

Overview



Version 2
July 2008

THE IT GOVERNANCE & ISO38500 IMPLEMENTATION FRAMEWORK

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

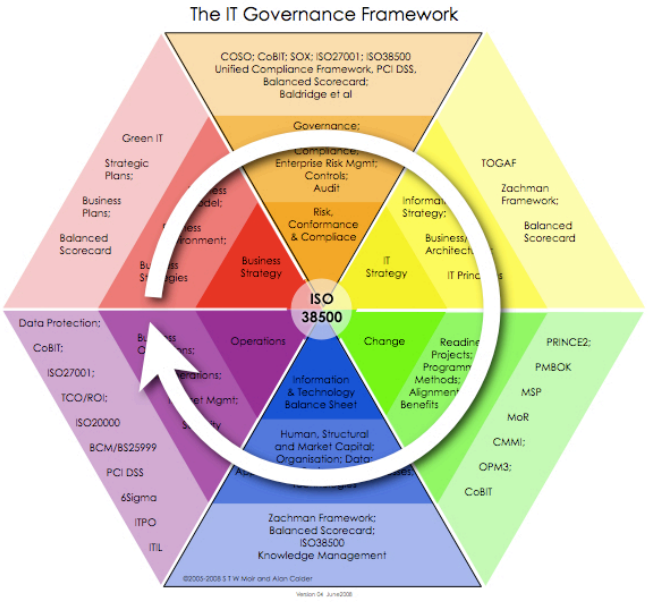
IT governance is a broad subject that involves many disciplines: information technology, risk management, strategy, intellectual property, business design, project management, compliance, and so on. Most of these disciplines offer IT governance solutions and tools, but most of the tools are very detailed, 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 with all compliance requirements; and IT policies and practices should take human behaviour into account.

The IT Calder-Moir 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 innermost 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



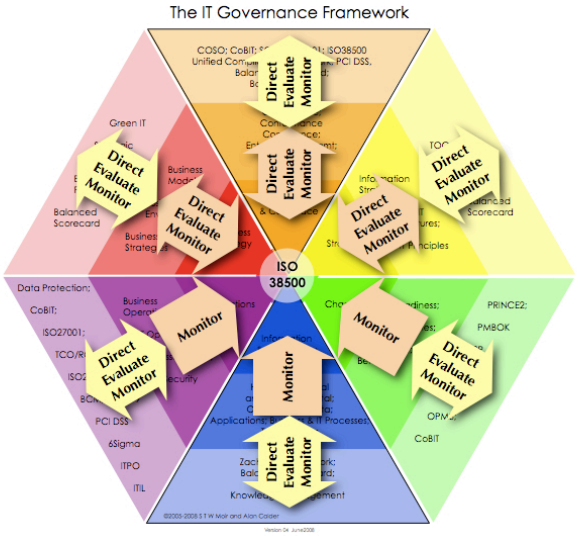
The top half of the framework covers the processes that establish direction, specify constraints, make decisions, and plan. The bottom half covers the processes that develop new capabilities, manage the capabilities, and use IT to deliver business products and services. Start at the "9 o'clock" position (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, 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



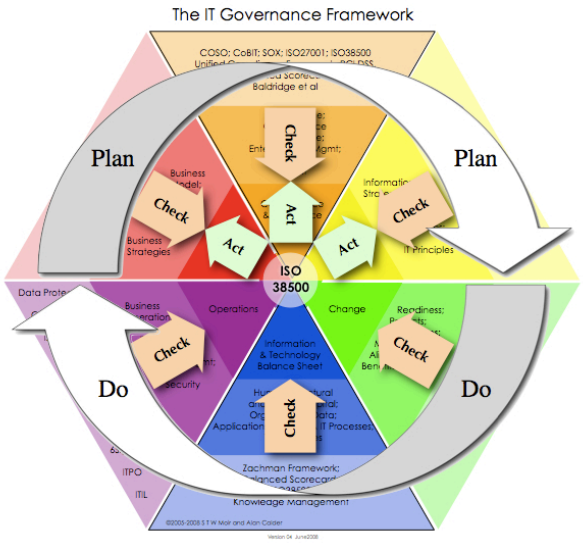
The international standard ISO/IEC 38500-2008 (Corporate Governance of Information and Communication Technology) identifies three main IT governance tasks for directors:

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



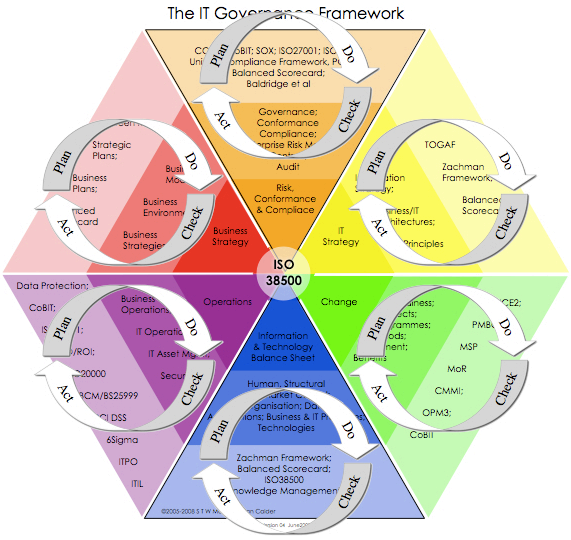
The Framework is also a representation of a PDCA management cycle - Plan, Do, Check Act.

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.
