
What is 'Important' about IT Governance

G. Johnston. ParryMcGill LLC.

16 February 2009



IT Governance: Definition

Before analysing what is 'important' about IT Governance, we should agree on a common definition.

Wikipedia (www.wikipedia.org) quotes the IT Governance Institute definition of "... *the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.*"

The ISO Standard (ISO 38500 Corporate Governance of Information Technology, International Standards Organisation, Geneva, Switzerland) defines 'Corporate Governance of IT as *'The system by which current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization.'*

I also find this definition from **Forrester** (Craig Symons, IT Governance Framework, Forrester, 2005) very useful, as it puts 'Governance' into more 'Operational' terms that I think we can all more easily understand, *'IT governance is the process by which decisions are made around IT investments. How decisions are made, who makes the decisions, who is held accountable, and how the results of decisions are measured and monitored are all parts of IT governance.'*

So IT Governance is there to make sure that when the business spends money on IT, that it; gets what it wants, that it does not take unnecessary risk, that it also obtains value for money, and that it can show all of the above when required. If only Corporate Governance (especially in the banking industry!) had been so well understood and executed over the last few years, then perhaps the world economy would not be in such a sorry state as it currently is!

Understanding IT Governance is one thing, but how do we implement it?

IT Governance: Frameworks

There are many 'IT Governance Frameworks' available. COBIT, ITIL, ISO 20000 and ISO 27001 could all be labelled as 'examples of IT Governance Frameworks'. However, bear in mind the following where 'frameworks' are concerned.

- They are by their very nature more tactics than strategy focussed
- Since these are 'off the shelf', you should ask yourself, are they really applicable to your own company?

If you have already defined your strategy, clearly, and down to the first level of tactics, and one of the frameworks above 'fits the bill', then it may be that one of the frameworks is entirely suitable to your organisation.

However, it is more likely that while parts of the above frameworks will be applicable to your own situation, other parts may not be and while implementing one of the frameworks is better than not implementing any at all, each has its own inherent advantages and disadvantages.

So the best way to implement IT Governance may be to take what we need from the frameworks available and to tailor them to our own more specific needs (and resources and timescales and scope and budget!).

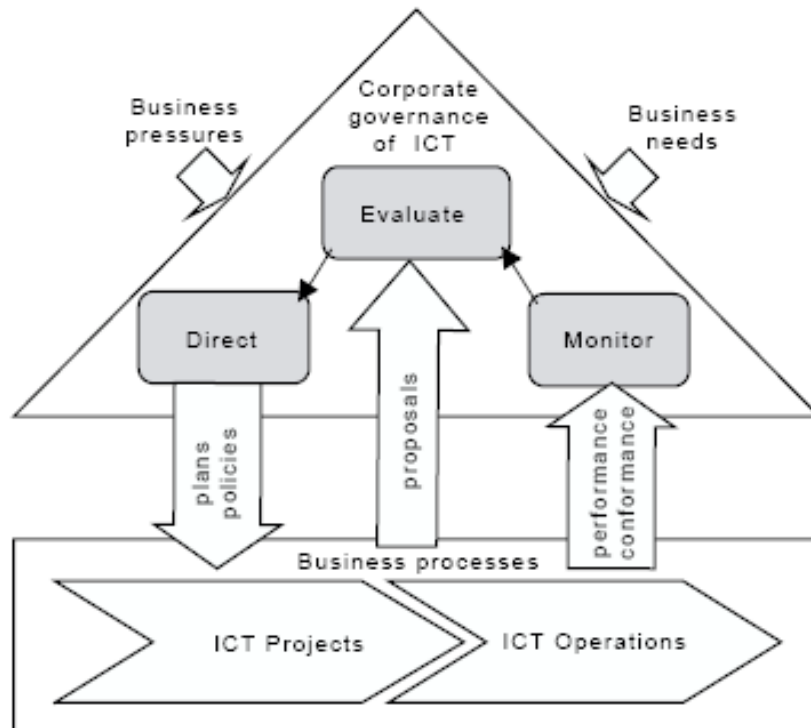
IT Governance: The ISO Standard

Let's look at IT Governance as having two parts:

- The first part makes sure that we do nothing 'wrong', that we manage our risks, deliver what the business requires, and we don't make big mistakes (defensive!).
- The second part ensures that we perform well or 'best in class', and that we continually strive to perform better over time (offensive!)

My own view is that the ISO standard (ISO 38500 Corporate Governance of IT) helps us considerably here. It is not a 'checklist' or a 'list' of processes and policies that we need to implement (that is tactics), but it is more 'strategy' focussed. It tells us what we should be looking at and what our strategy should take into account. Once we understand this, then we can concentrate on tactics (which are more 'framework' based) and *we will then know what parts of each framework we really want to implement in our own situation.*

The diagram below is taken from the ISO 38500 standard, but is freely available on the internet since it predates the standard. It shows three key activities, 'Direct, Evaluate, and Monitor'.



The theory behind the ISO Standard is simple and I will break the whole standard down into just two bullet points:

- There are six principles or 'areas of activity' that we need to encompass, these are summed as: responsibility, strategy, acquisition, performance, conformance, and human behavior
- We need to put processes into place such that we ensure that we direct, evaluate, and monitor each of the principles or 'areas of activity' above.

If we look at the above, then using; guidance from the standard, our knowledge of the frameworks available, and past experience of implementations and results, it is relatively easy to define the framework (and therefore tactics) for the implementation that **we** require, for **our** situation.

Once we have defined our own framework (probably taking a lot from the industry standard frameworks described above) it is then relatively easy to benchmark ourselves and take the improvement actions required.

IT Governance: What is important about IT Governance

It is important when discussing the Governance of IT, that we address the two issues above (defensive and offensive), in a common sense and pragmatic way.

We need to control and/or reduce the risks and we need to work within set boundaries, but we also need to strive to be 'best in class', and all this needs to be 'within reason'.

Referring to the ISO Standard helps us reduce risk in our implementation (ie helps with the 'defensive' points above) since the ISO Standard has a history (ie. has been developed, reviewed, and improved over time) meaning that if we follow it properly, we will not miss any 'important' areas or risks.

Using 'off the shelf' frameworks will help with the 'offensive' part of IT Governance, since these frameworks have been developed by a lot of clever people and improved with the hindsight of multiple levels of experience over time. They are accepted as 'Industry Best Practice', and what is in them is like gold dust... they are the key for us. However, we don't want to implement everything from them (from rote) from the books (in my opinion the biggest single cause of failure, or disappointment with the implementation), since they are designed to be applicable to all companies, everywhere, of every size and in every industry. It cannot all therefore be applicable to our company, right now.

We should implement what we need only.

Therefore I repeat: what is important about IT Governance is that we control the risks, work within set boundaries and we strive to be 'best in class', but all with pragmatism and within reason.

© G. Johnston. ParryMcGill LLC.