10 Legal & Regulatory Aspects of IT Governance

In recent years there has been a general increase in the number of regulations affecting the use of IT and also the number of situations where legal measures need to be considered. This is due to the need to guard against a wide range of new IT related risks and from a general increase in corporate regulations.

- The impact of not taking sufficient care over legal or regulatory requirements can be considerable including:
  - *Loss of reputation*
  - *Inability to trade*
  - *Financial penalties and losses*
  - *Loss of competitive advantage*
  - *Loss of opportunity*
- On the other hand the benefit of complying with regulatory requirements and using legal measures to protect commercial interests can be considerable, including:
  - *General improvement in overall control of IT related activities*
  - *Reduced losses and administrative costs*
  - *More efficient and effective negotiation of commercial transactions*
  - *A greater ability and confidence to take risks – because senior management feel more in control*

There are a wide range of laws and regulations, some specific to industry sectors that can have an impact on IT. Every organisation must identify the specific regulations affecting them and respond accordingly, and ensure that the roles and responsibilities for understanding legal and regulatory matters are properly defined for each group of stakeholder so that each group can apply its specific expertise effectively. External advice must be sought whenever the issues are sufficiently risky or complex.

Every organisation relies on a growing number of third parties for support of IT services. From a legal and regulatory perspective this means that there is potentially a complex hierarchy of responsibilities that combine to meet the legal and regulatory needs of the customer. Ultimately it is the customer's responsibility to ensure that all the right controls are in place with any third party that is relied upon for legal and regulatory compliance.

10.1 Legal and regulatory factors affecting IT Governance

- The recent increase in the number of regulations affecting the use of IT is due to a number of factors, including:

- *A greater interest by regulators in the operations of all organisations caused by major corporate financial failures and scandals, which is resulting in regulations like the US Sarbanes-Oxley Act forcing Boards of Directors to express opinions about their systems of control.*
- *Concerns about security and privacy fueled by the overall increase in use of computers and networks and the impact of the Internet.*
- *Laws to protect personal information and its potential misuse in electronic form.*
- *A growth in the use of computer systems and networks for criminal activity and terrorism, including viruses, hacking, money laundering and pornography etc.*
- *A growth in complex contractual relationships for IT services and products (outsourcing, managed services, product licenses etc.).*
- *The growth in all forms of electronic media and the potential for misuse of valuable information assets, resulting in copyright and intellectual property issues of concern to both vendors and users.*

What might appear to be an initial regulatory burden can become an opportunity to transform to better managed practices if the rules are used positively and applied productively. Corporate regulations like the Sarbanes-Oxley Act can be just a minimalist compliance procedure with no potential benefit to the business or be used as an opportunity to invest in better IT controls. Compliance with IT-related legal and regulatory requirements and the effective use of legal contracts are clearly part of the effective control and oversight of IT activities by senior management and therefore key aspects of IT Governance.

There are a wide range of laws and regulations, some specific to industry sectors, that can have an impact on IT. Every organisation must identify the specific regulations affecting them and respond accordingly.

▼ The IMPACT SIG has identified the following areas that ought to be considered:

- *Personal data and privacy*
- *Corporate Governance, financial reporting, stock market requirements*
- *Money laundering, and other criminal acts*
- *Intellectual Property, Trademarks and Copyright*
- *Electronic communication, signatures etc.*
- *Electronic commerce*
- *Email monitoring, appropriate use and confidentiality*
- *Email defamation*
- *Document and record retention*
- *IT products and services contracts*
- *Sector specific regulations e.g. financial, health, pharmaceutical etc.*

10.2 Roles and Responsibilities

Dealing with legal and regulatory requirements and knowing how best to use legal contracts can be challenging for IT experts who are not knowledgeable about legal matters, and for business managers who may not appreciate all the legal risks and issues associated with the use of advanced technology.

Organisations should therefore ensure that the roles and responsibilities for understanding legal and regulatory matters are properly defined for each group of stakeholder so that each group can apply its specific expertise effectively. External advice must be sought whenever the issues are sufficiently risky or complex.

Who needs to be involved?		
Investors	**Providers**	**Controllers**
• The Board • IT Council/Management Team • Senior business unit managers e.g. key customers of IT services • Business Partners • External investors/shareholders – as part of corporate governance	• Project and change managers (IT and Business) • Project and change managers (IT and Business) • Programme managers • Business managers and users • Technical delivery and support teams • Key players e.g. Business sponsors, Project champions • Relationship managers and internal communications teams • Suppliers (especially outsourced service providers) • Contract and procurement management • Peripheral players/influencers/Policy owners e.g. HR, Facilities Management, Legal	• Internal audit and external audit (due diligence) • External regulators • Corporate governance coordinator • Risk managers • Compliance – regulatory and internal • Finance/Project Managers/IT and business managers – reviewers of benefits/ROI • Post investment appraisal/Post project review teams
Legal and Regulatory Responsibilities		
• Understand requirements (what regulations are to be complied with) • Set the mandate • Set priorities and expectations • Establish and ensure the expected degree of compliance • Based on advice concerning risk and cost: • Assess impact on business • Provide resource and funding to ensure issues are addressed • Define who is accountable • Obtain internal or external assurance as required that issues have been addressed and controls established • Monitor and evaluate compliance programmes and significant commercial contracts • Sign off specific compliance programmes • Provide approvals when required for significant legal or regulatory decisions	• Advise on IT related technical and commercial risks that could impact legal and regulatory requirements • Provide proposals and business cases for legal and regulatory programmes, projects or action plans • Formulate solutions for compliance or commercial contracts • Identify best practices for ongoing good control of legal and regulatory requirements • Exploit technology and tools where appropriate for ensuring compliance (e.g. asset registers) • Execution of compliance and contractual processes, and operation of elated controls • Provide compliance framework to ensure a sustainable “business as usual” approach to compliance • Provide evidence of compliance • Provide information relating to the cost of compliance and also cost of any incidents • Evaluate impact on business environment together with business units • Ensure vendors, service providers, and subcontractors are involved properly and integrated within the overall compliance approach	• Maintain awareness of current and emerging laws, and regulations affecting IT to assess their impact on the organisation’s business • Develop an understanding of their impact on the organisation and advise accordingly on “what is needed” - not necessarily “how” • Monitor adequacy of controls and compliance processes • Monitor the business and IT functions for performance in meeting legal and regulatory requirements and report back to management with advice regarding any shortcomings • Provide independent assurance to management that adequate controls are in place to deal with legal and regulatory requirements

Table 10.2

10.3 Best approach to compliance

Ideally organisations should deal with legal and regulatory requirements on a “business as usual” basis instead of reacting on a case-by-case basis.

In practice, it is recommended that a framework for dealing with legal and regulatory issues be established. Because IT is fast changing and new regulations are also emerging, any such framework must be flexible and responsive to new requirements.

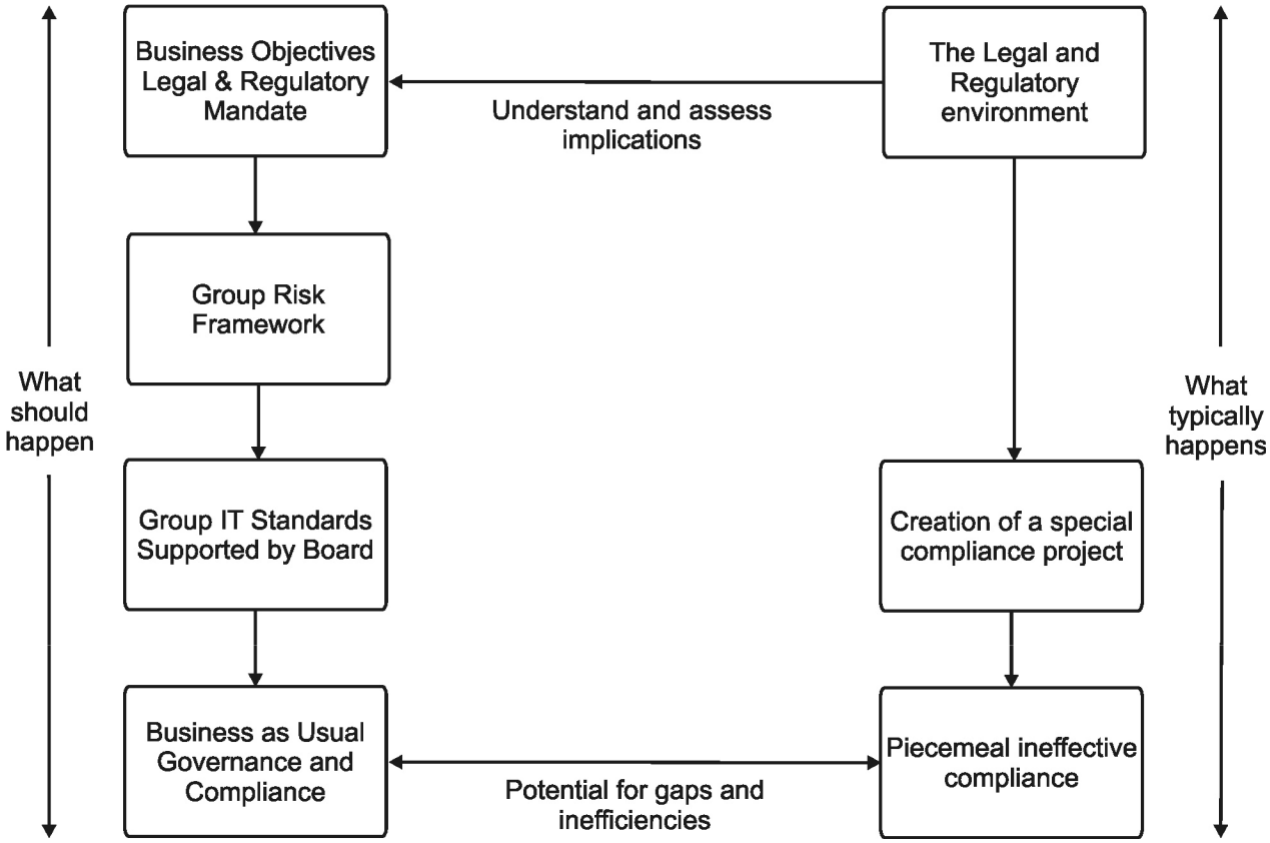

Figure 10.3

Figure 10.3 illustrates a common problem when new regulatory requirements are imposed. To be effectively handled the decisions concerning the regulation should be taken at the level at which business objectives are set and within the group or business risk framework. This is the necessary level at which priorities can be determined and the standards framework can be applied.

However, as illustrated, a special programme is frequently set up outside the remit of existing standards and governance in the hope that the new regulatory environment can be incorporated. This is usually unsuccessful or inefficient because outside of existing governance it is very difficult to allocate and establish responsibilities for monitoring and testing. Similarly, there can be no clear prioritisation or co-ordination among different regulatory requirements. Conversely, when the left-hand route is followed and a new regulation comes into force, it is possible to identify where there are already procedures in place that enable the new requirements to be met.

- For complex IT environments, the importance of the framework is emphasised by the need to understand which standards affect which systems. Then it becomes possible to address all the relevant systems when standards have to change:
  - *Consider regulatory issues together*
  - *Do not set up separate projects which may conflict with the standard approach Decision making must*
  - *rest with the business in terms of the extent and nature of compliance*

10.4 What IT has to do

Historically, most IT people did not think about compliance- except in terms of good practice, because regulations rarely impacted the technical environment. Gradually this has changed, first with IT specific legislation like the Data Protection act, and most recently by the realisation that corporate level regulations like Sarbanes-Oxley must be inextricably linked to the IT systems because corporate information and financial reporting has become so automated.

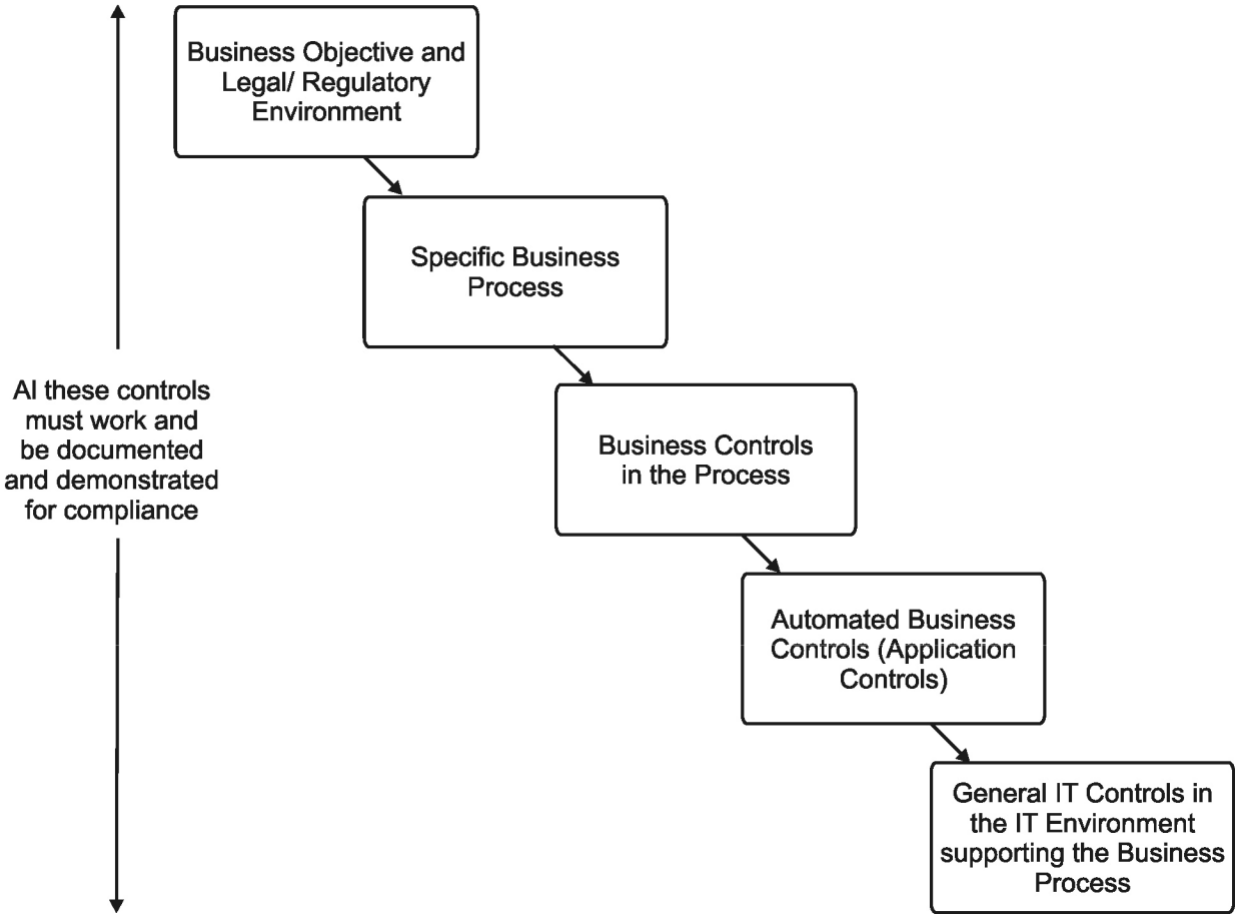

Figure 10.4

In addition, due to the very significant cost of IT investments, and the complexity of customer and supplier relationships, legal contracts for IT services are being given much more careful attention. These contracts in turn demand greater controls be demonstrated by the parties to the contract, over many issues such as security, intellectual property, service availability, ownership of deliverables, support of products etc.

As a consequence, IT service providers, vendors, and internal IT functions are all realising that they must be better organised from a control and compliance perspective. It is only a relatively recent realisation that IT related controls should be documented and monitored by IT functions, increasingly driven by regulatory pressure.

Business objectives and processes should drive the system of internal control and therefore the documentation process. The flow should be:

For an efficient and effective compliance process, the documentation should be in a language that auditors would use, and therefore it is best to work with the audit community and adopt a common language and approach such as CobiT.

- IT functions increasingly need to be more involved in legal and regulatory requirements and should:
  - *Work with the business users and risk management groups to identify critical systems and compliance priorities.*
  - *Document architectures so that the overall environment is understood on a continuous basis.*
  - *Define processes in IT in a logical well ordered fashion, meaningful to auditors and management (e.g. based on CobiT).*
  - *Appoint process owners so there is accountability and responsibility.*
  - *Understand control concepts, the need for IT controls, and how they relate to business level controls.*
  - *Document these processes and controls (especially for compliance critical systems), and maintain the documentation as changes occur.*

- *Standardise wherever possible to avoid duplication of effort.*
- *Maintain evidence of controls being exercised to be better able to demonstrate compliance.*
- *Generate business benefits from the control and compliance projects by performing gap analyses to drive improvements and efficiencies as well as building good controls.*
- *Consider the whole infrastructure rather than tackling items on a piecemeal basis. Be responsible for*
- *diligent procurement and proper control and management of third parties.*

▼ To achieve these objectives:

- *IT should seek advice from HR, Legal, and Audit, and if necessary external experts.*
- *Adopt standard approaches and best practices – don't attempt to reinvent the wheel as it wastes time and makes working with partners and auditors much less effective (compare with accounting-standard procedures are essential).*
- *Build in the need for third party testing as required.*

10.5 Dealing with third parties

Every organisation relies on a growing number of third parties for support of IT services. From a legal and regulatory perspective this means that there is potentially a complex hierarchy of responsibilities that combine to meet the legal and regulatory needs of the customer. Ultimately it is the customer's responsibility to ensure that all the right controls are in place with any third party that is relied upon for legal and regulatory compliance.

▼ Conversely, service providers have their own corporate governance agenda, combined with the pressures of their business models – usually to provide a better service at a lower cost than the customer had previously experienced:

- *They have to work with differing governance models of business partners and clients.*
- *In theory they might use a standard model across all but in practice this is unlikely.*
  - *Large clients, in particular, are unwilling to change their own model.*
  - *Clients cannot be obliged to do business in a way specified by the provider.*

▼ The outsourcer or provider may not ensure full coverage of legal and regulatory requirements:

- *The customer may go to the provider and specify what is required or provide a questionnaire, but the provider may still not have taken action himself or know what is required.*
- *People who negotiate outsourcing contracts are usually at a commercial business level, not driven by controls and compliance issues.*

In order for both sides to be clear on responsibilities it is essential that sufficient in-house capability is retained. Most organisations actually get more rigour when they outsource but most contracts are built around existing operations with all their limitations. The onus should be on the provider to spell out the risks – but the provider will not improve controls unless paid to do so, or can see a commercial benefit in making the necessary investment.

Legally there is a standard reasonable expectation of basic service, and ultimately it is a question of negligence if controls were not operated properly.

The provider is unlikely to provide a higher level of control in specific situations (such as security) than the client had originally operated himself – but must have nevertheless an adequate set of controls. Special requirements such as vulnerability testing will not normally be seen as part of a contract unless formally requested and paid for.

10.6 Critical success factors

- The IMPACT SIG identified the following success factors to enable effective ongoing legal and regulatory compliance and proper control of legal contracts:

  - *Establish the right culture to encourage diligence and good controls Communication throughout the*
  - *organisation based on a Board level mandate is essential to make sure everyone takes the issues seriously and uniformly Involve the right people as advisors but do not abdicate responsibility*
  -
  - *Retaining responsibility for control and compliance when using service providers Standardisation and*
  - *a common approach is the most effective and efficient way to meet compliance requirements*
  - *Use frameworks and accepted compliance models especially those accepted by auditors*
  - *Integrate compliance objectives into the IT strategy*
  - *Ensure management are actively involved – not just performing a sign-off at the end*
    - *Set the tone at the top*
  - *Institutionalise compliance behaviour*
    - *Engage the governance and risk management groups (those who own the framework) as soon as possible*
    - *Provide a positive spin – good controls can be very beneficial*
    - *Make compliance normal business practice rather than a project*
  - *Make compliance meaningful and relevant*
    - *Translate into normal language*
    - *Explain business context*
    - *Carry out awareness training*
  - *Establish mechanisms for evidence and documentation*
  - *Establish metrics for monitoring performance*
  - *Create incentives and/or penalties as part of personal objectives*
  - *Do regular compliance checking and tests*
  - *Do regular review of risks (include 3rd parties)*
  - *Have good incident management procedures to learn from legal and regulatory incidents*