Necessary Frameworks for IT Governance

Clarifying the Tangled Web

February 28, 2007
Table of Contents

1. **Introduction** .............................................................................................................................................. 3
   1.1. IT Governance – The Need ............................................................................................................. 3
   1.2. IT Governance – The Definition ..................................................................................................... 4
   1.3. IT Governance – The Alphabet Soup (A Quagmire?) ..................................................................... 4
   1.4. IT Governance – Differing Viewpoints ............................................................................................ 4
       1.4.1. Areas of Significance for the Interest Groups ........................................................................... 5
   1.5. IT Governance – The Crucial Need for a Framework Support Infrastructure .......................... 5
   1.6. IT Governance – The Need for Managed Process Environment ............................................... 5
   1.7. Governance – a White Elephant? .................................................................................................... 6

2. **Elements of Governance** ....................................................................................................................... 7
   2.1. Standards Framework ....................................................................................................................... 7
   2.2. Best-Practice Framework ................................................................................................................. 7
       2.2.1. For Infrastructure Support ........................................................................................................ 7
       2.2.2. For Development ....................................................................................................................... 8
   2.3. Compliance Framework .................................................................................................................... 9
   2.4. Continuous Improvement Framework ............................................................................................ 9

3. **How Frameworks Interact** ..................................................................................................................... 11
   3.1. ITIL and ISO ..................................................................................................................................... 11
   3.2. ITIL and COBIT ............................................................................................................................... 11
   3.3. ITIL and CMMI ............................................................................................................................... 12
   3.4. ITIL and Six Sigma .......................................................................................................................... 13
   3.5. Integration of Frameworks – An Example ...................................................................................... 13

4. **Overall Governance Model is underpinned by Best Practice** ....................................................... 15
   4.1. Metrics – Crucial to Manage Frameworks ..................................................................................... 15
   4.2. Apply Parts of Each Framework Incrementally and As Needed ............................................... 16
1. Introduction

“Governance” is a lofty term. What does it mean? Why is it important? How does an organization establish effective governance? This white paper will attempt to answer these questions.

1.1. IT Governance – The Need

*Absence of effective Governance will invariably lead to a decline in the business readiness of any organizational function. IT is no different.* Even with initial optimized readiness, the decline can occur due to a variety of reasons, such as:

- Management changes and restructuring
- Lack of focus leading to complacency
- Merger and acquisition
- IT function perceived as overhead
- IT culture

Even though IT is an enabling function for business processes, it is often taken for granted. This, coupled with IT taking pride in *firefighting*, compounds the problem. As depicted in Fig. 1, ineffective Governance will also cause the decline to remain undetected and insidious; this situation could ultimately result in a catastrophic failure!

![Fig. 1: Decline of Business Readiness](image)

This is not a conjecture. For example:

When the largest Asian Stock Exchange suffered a widely publicized “worst-ever” systems crash in November, 2005, trading was suspended for half a day due to an incorrect software patch installation in the market's trading system – this happened because of a lack of Governance.

The payroll deposits of millions of customers of a major bank were affected in June, 2004 when many transactions went unrecorded for two days due to problems during an update to their computer systems – another example of lack of effective Governance.

An erroneous change made to an airline ticketing system resulted in hundreds of international travel tickets being sold for less than $100!

*Effective Governance allows an organization to minimize such catastrophes. If one does occur, the organization can react far more rapidly to rectify it. The needed effort is also less. The overall business impact will be reduced substantially as a direct result of effective Governance.*
1.2. IT Governance – The Definition

*IT Governance* directs and controls how an IT organization administers necessary IT services to its clients. IT Governance specifies the rights and responsibilities of the parties involved, such as customers, regulators and stakeholders. It defines **the policies and procedures under which an IT organization functions, as well as the mechanism to ensure compliance with those rules and regulations.** IT Governance also provides the structure through which the IT Organization’s objectives are set, and the means of attaining those objectives and monitoring its performance.

(The above definition closely follows the corporate governance definition outlined by OECD (Organization for Economic Co-operation and Development). Located in Paris, it groups thirty member countries which share a commitment to democratic government and market economy.)

1.3. IT Governance – The Alphabet Soup (A Quagmire?)

Organizations use standards/frameworks to achieve Governance for business excellence and regulatory Compliance. Framework implementations are expensive and require care to maximize a benefits-to-efforts ratio. Such implementations also require careful planning since a variety of frameworks exist. They apparently address similar issues, thereby causing confusion. A host of frameworks can impact IT Governance. Among them are: **ISO, CMMI, ITIL, COBIT and Six Sigma** (these terms are defined later).

In addition to these major frameworks, others such as **ISO 20000** for IT Quality Standard and **ISO 17799** for IT Security Management also relate to IT Governance.

With so many frameworks and standards to choose from, organizations will need to decide which of them apply. They need to ask:

- Will there be adequate coverage?
- Will there be duplication of effort?
- Are there complementary benefits?
- Once a new governance environment is established, how do we know that it is being sustained?
- How can the frameworks help us to stay competitive – i.e. by improving efficiency and effectiveness – in view of external (and internal) pressures?
- Is a certification (where applicable) necessary for our organization?
- Will implementations also lead to tangible results in regulatory Compliance?

1.4. IT Governance – Differing Viewpoints

Governance drives the functions of an organization according to a set of policies and rules applicable to the organization. The policies and rules are formulated by its managers. Basically there are three groups who have an interest in how Governance is practiced in an IT organization:

- **Regulators** – typically from some level of government
- **Customers** – recipients of the services provided by an IT organization
- **Stakeholders** – managers and employees of an IT organization

Each of the three groups has a different perception and varying expectation of IT Governance.

**Regulators** are specifically interested in Compliance with certain acts – such as the Sarbanes-Oxley Act (SOXA) in the U.S.A. or Bill 198 in Ontario, Canada. Regardless of how effectively or efficiently an IT organization is run, the Regulators are satisfied as long as the requirements of the acts are met.

**Customers** are the recipients of IT services and are primarily interested in the Effectiveness of IT Service Delivery. Their main concerns are with the price and the quality (including timeliness) of needed services. Customers are somewhat interested in knowing if their IT organization is meeting regulatory Compliance, but it is not their primary concern.

**Stakeholders** are concerned with all aspects of IT governance; namely efficiency, effectiveness and Compliance. They want to ensure that IT services provided not only meet customer price and quality requirements and regulatory Compliance, but also address operational efficiency.
### 1.4.1. Areas of Significance for the Interest Groups

**Compliance** with regulatory issues had been a relatively low-profile item among most organizations. The financial fiascos in companies such as Enron, WorldCom and Tyco have brought regulatory Compliance to the forefront. Lack of Compliance due to fraudulent actions can result in heavy fines and/or imprisonment and government agencies are zealously enforcing the regulations. Also, disclosure of “Material Weaknesses” in financial Controls can adversely affect investor confidence. Material weaknesses are those that mean there is a likelihood that a critical misstatement of the annual or interim financial reports will not be prevented or detected.

**Effectiveness** is how well customer expectations are met. Customers require delivery of products and/or services that will meet their expectations in terms of their specifications.

**Efficiency** has now become the byword for productivity improvement in view of intense business competition. Efficiency seeks to maximize the output for a given input.

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Compliance</th>
<th>Effectiveness</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulators</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Stakeholders</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1 summarizes the interests of the three groups in IT Governance.

*The Governance issues remain the same regardless of whether the IT organization is internal and dedicated, or external and outsourced.*

### 1.5. IT Governance – The Crucial Need for a Framework Support Infrastructure

It is not necessary to implement each framework to its fullest extent - the extent to which a framework is deployed should be based on the business needs of the organization. However, certain principles need to be addressed for a successful deployment even if the deployment is partial. Successful deployments require that the processes be:

- **Aligned** – by ensuring that the process objectives address business needs
- **Streamlined** – through adoption of best practice
- **Mapped** – through detailed mapping of tasks for workflows and role assignments
- **Verified** – by various organizational functions to meet their business requirements
- **Owned** – by assigning formal roles for accountability
- **Documented** – for consistency of implementation throughout the organization
- **Measured** – to ensure that the process is effective and efficient while meeting Compliance

A framework must not be deployed without a framework support infrastructure. A support infrastructure essentially includes a number of well-defined roles (and how they interact), such as the champions, process owners, process managers and others depending on the nature of the framework and the organization. While the roles are not necessarily dedicated, they have to be formal. **Such an infrastructure is created only when there is a no-nonsense commitment from top management.**

### 1.6. IT Governance – The Need for Managed Process Environment

IT business processes operating under a number of frameworks ultimately underpin IT Governance. The “Managed Process Environment” for IT processes, a concept cultivated by Consulting-Portal and shown in Fig. 2 is essential for good Governance for **ITSM** (IT Service Management).
The Managed Process Environment promotes Governance and has a structure that includes a support infrastructure – needed for any framework (Section 1.5) and requires the following characteristics:

- Presence of Executive sponsorship and Steering Committee
- Processes having recognized owners
- Roles & responsibilities clearly defined and communicated
- Processes built on Best Practice in a standard manner
- Monitoring and Controls in place
- Measurements taken and acted upon
- Processes being continuously improved

**Governance is much more than process management – even though such processes underpin Governance.** Subsequent sections in this article explain this further.

### 1.7. Governance – a White Elephant?

Governance – particularly regarding Compliance – is often described as being overbearing. The feelings are that this is another example of government interference with no tangible benefits and or any real benefit to the bottom line.

However, Compliance requirements are here to stay – perhaps becoming even more stringent in the future. Thought leaders in business are using Compliance regulations to take an opportunistic view. They see these regulations as the means to facilitate business process optimization and achieve performance excellence. For example, if Compliance requires certain Controls for the Change Management process (one of the IT processes), this will also create a more robust process. As mentioned above, lack of robustness has led to serious outages resulting in significant financial damages.

Lack of effective IT Governance can lead to material weaknesses in financial disclosure. Public companies have to disclose weaknesses in publicly stated financial statements. Such stated weaknesses in financial disclosure are also NOT conducive to investor confidence. CEO’s and Finance Directors can also be fined up to $20 Million and serve up to 10 years in prison for fraudulent practices.

**Superior governance is hardly a white elephant.**
2. Elements of Governance

An overall Governance framework has several elements which address the interests of the three groups mentioned earlier. They are:

- **Standards** against which Governance efficacy can be evaluated
- **Set of Practices** for the processes of an organization
- **Compliance** to ensure Governance meets government regulations
- **Continuous Improvement** of Governance maturity level achieved by measures which ensure that Governance addresses environmental changes and functions effectively and efficiently

2.1. Standards Framework

**Governance is compared against standards to determine its degree of maturity.** In the context of this white paper, quality and government regulations are the two types of standards. Adherence to quality standards is an initiative to which many organizations have subscribed and which allows them to be competitive. The most common body of standards is the internationally accepted ISO. ISO standards require organizational commitment to documenting business processes and certification by external auditors.

**ISO**, an acronym for the International Standardization Organization, was set up in 1947 and is headquartered in Geneva. Its primary purpose is to facilitate and support international trade by developing universally acceptable standards. ISO first published its ISO 9001 quality standards in 1987. ISO 9001 applies to all types of organizations – both product manufacturers and service providers. ISO standards do not specifically address the quality of a product or service since “quality” is dependent on customer specifications. It allows a customer to evaluate prospective vendors based on their ISO certifications.

**SOXA** (Sarbanes-Oxley Act) is perhaps the most commonly known government regulation enacted in the U.S.A. in response to a number of financial fiascos in the 90s within large companies such as Enron, WorldCom and Tyco. Most public companies have to comply with SOXA requirements for financial disclosure. Financial disclosures are intimately tied to information technology. This will be discussed more fully in the Compliance framework section.

**Compliance with acts such as SOXA does not have a certification process.** However, external auditors do audit and in essence “certify” an organization, once they can verify that an organization has identified all major financial risks, has put in place measures to control such risks and can exhibit evidence of Control. The penalties for material weaknesses in financial disclosure due to fraud can be severe – ranging from fines of millions of dollars to years in jail, or both. Even without fraud, reporting material weakness in the financial assertions of a public company can lead to lack of investor confidence and potential loss of share value.

**Adopting ISO as a quality standard is an option – but for most public companies, adopting a Compliance standard such as SOXA is mandatory.**

2.2. Best-Practice Framework

Essentially best practice applies in two areas of an IT organization. The two areas relate to **Infrastructure Support** and **Development**. Development may be mission-critical in certain industries such as finance; but infrastructure support will apply to any IT organization, regardless of the emphasis on development.

2.2.1. For Infrastructure Support

IT departments provide services to enable a technology platform for other departments and business functions through infrastructure support. These services allow other departments and functions in an organization to interact internally as well as externally.

In order to provide such a platform, an IT department has to execute a variety of business processes within itself and with other departments. These business processes are generic and have been “standardized” as best practices to ensure the realization of the full benefits of various IT processes. There are several advantages in adopting a best practice framework:

- Adoption of well-defined and proven practices without the need to develop them
• Ability to implement easily by following guidelines  
• Improved chances of success by reducing risks and errors  
• Improved quality of IT services  
• Reduced costs through standardization  
• Ability to benchmark with other organizations adopting similar best practices to determine areas for improvement (as part of Continuous Improvement described later),  
• Improved acceptance by stakeholders, customers and regulators  
• Improved ability to manage the processes  
• Ability to improve IT service maturity level  

**ITIL** (IT Infrastructure Library) is a set of practices created by the Office of Government Commerce (OGC) of the British Government. ITIL has become the de facto standard of IT infrastructure support in the world. From their web site ([www.itil.co.uk](http://www.itil.co.uk)):  

"**ITIL® provides a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualifications scheme, accredited training organisations, and implementation and assessment tools. The best practice processes promoted in ITIL® support and are supported by, the British Standards Institution's standard for IT service Management (BS15000).**"  

**ITIL does not lay down specific workflows for processes to depict “who-does-what-and-why”.** It certainly does not provide *procedures* – which are the details of a process – to show the "how". Specific process workflows and procedures depend on a particular deployment and reflect the business requirements of an organization. **Consulting-Portal, Inc.** ([www.cportalinc.com](http://www.cportalinc.com)) provides services to tailor ITIL implementations in various organizations.

**IT infrastructure Support is more mission-critical for certain industries than others.** For example, if the IT infrastructure of a stock exchange falters, the event can impact countless customers extensively and immediately. If the same event in a metal smelting company were to affect its plant maintenance system, the company could still perform the maintenance tasks with manual procedures, at least for a short period of time. However, if the infrastructure for a process control system of a major oil refinery is inoperative, there can be a serious impact on workplace safety and the company’s bottom line.

The underpinning of IT Governance issues by IT best practice is described later.

### 2.2.2. For Development

**SEI** (Software Engineering Institute) is a US government funded research and development center established in 1984 at Carnegie Mellon University, Pittsburgh. In view of the importance of software in systems increasing dramatically, the mandate was to develop a strong process framework for software development. The focus was to be on processes as well as on products (software applications). Consequently, SEI developed a *maturity model*, which is a structured collection of various elements to describe a process. According to SEI ([www.sei.cmu.edu/](http://www.sei.cmu.edu/)):

**CMM describes an evolutionary improvement path from an ad hoc, immature process to a mature, disciplined process.** Due to its well-defined structure, the model can also be used to benchmark the capability maturity of an organization for software development. It covers practices for planning, engineering, and managing software development and maintenance. Following these key practices will improve the ability of organizations to meet the goals for cost, schedule, functionality, and product quality.

CMM itself has undergone enhancement with the creation of **CMMI** (Capability Maturity Model® Integration), which now supports the entire engineering life cycle - not just the development life cycle. CMMI can be used to guide process improvement across a project, a division, or an entire organization.

An organization can be assessed to determine which level it is at. It can then adopt the best practice laid out by SEI to achieve progressively higher levels.
SEI has come up with a five-level model for CMMI (a concept also used by Consulting-Portal for IT Service Management assessments using ITOptimizer SM):

1. Initial (ad-hoc processes)
2. Repeatable (focus on individual processes)
3. Defined (institutionalized processes)
4. Managed (measured processes)
5. Optimized (continuous improvement of processes)

The Project Management principles that are part of CMMI, are also applicable for support - all projects should follow project management principles. They also provide an interface to connect infrastructure support and development environments.

CMMI may appear to be unimportant in organizations where little development is performed – such as when “off-the-shelf” software is used. Even so, there may be situations where such software may require custom integrations/interfaces which could very well be mission-critical. Development and subsequent maintenance of such integrations/interfaces can certainly fall under the CMMI umbrella. Operating them falls under the ITIL umbrella.

2.3. Compliance Framework

Compliance standards such as SOXA also require a framework solution. SOXA is primarily about financial assertions by public companies and in simple terms requires identification of financial processes, associated risks ("what can go wrong"), financial Controls to mitigate such risks and Control evidence to ensure that the Controls are effective. Since a financial process is almost always underpinned by information technology, application of an IT Control framework is therefore a necessity to mitigate risks associated with information processing.

The Compliance standards for IT processes emanate from financial Compliance standards such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) which is a voluntary organization in the private sector. SEC (Securities and Exchange Commission (www.sec.gov/rules/final)) has suggested the use of the COSO framework:

“The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements. However, the final rules do not mandate use of a particular framework, such as the COSO Framework, in recognition of the fact that other evaluation standards exist outside of the United States, and that frameworks other than COSO may be developed within the United States in the future, that satisfy the intent of the statute without diminishing the benefits to investors.”

Since virtually all accounting processes needed for financial Control use IT in one form or another, verification of financial Controls will definitely require verification of data produced by IT. IT Controls in essence underpin financial Controls.

COBIT (Control Objectives for Information and Related Technology) provides IT Controls following the COSO framework. COBIT is a framework developed by IT Governance Institute, an arm of ISACA (Information Systems Audit and Control Association (www.isaca.org)).

Even though the COBIT framework has not been formally recommended by PCAOB (Public Company Accounting Oversight Board) – the SOXA enforcing arm of SEC – it is the de facto standard for IT Controls meant to address financial assertions.

2.4. Continuous Improvement Framework

For Governance to be effective, it needs to be sustained and, where possible, improved. Business requirements change and this forces the re-evaluation of the Governance framework from time to time. Moreover, organizations need to be not only effective, but efficient as well. The concept of efficiency is addressed by methodologies such as Continuous Improvement and Six Sigma that have been practiced in
Continuous Improvement concept was first introduced by Walter A. Shewhart, a statistician at the Hawthorne plant of Western Electric. W. Edwards Deming furthered the concepts developed by Shewhart. Shewhart also developed an approach for process improvement called the Shewhart Cycle (known in Japan as the Deming cycle): **Plan-Do-Check-Act.** This approach emphasizes the continuing, never-ending nature of process improvement. The **PDCA Cycle** is really a simple feedback loop system:

**Fig. 3: The PDCA Cycle**

- **Plan** – a plan is developed to improve a process
- **Do** – the plan is tested in a small field test
- **Check** – the results of the test are assessed
- **Act** – if successful, the plan is implemented

The improvement process then begins again and the cycle is repeated.

The Software Engineering Institute liberally adopted TQM and ISO principles for CMM (initially) and CMMI (subsequently) frameworks.

**Six Sigma further advances the Continuous Improvement concept.** Six Sigma packages tools and techniques (borrowed from various disciplines) in a structured manner, provides a roadmap and more importantly, prescribes an infrastructure to support the Six Sigma initiatives.

The Six Sigma methodology arguably captures the essence of most of the best concepts of TQM (Total Quality Management), SPC (Statistical Process Control), Lean Manufacturing, TOC (Theory of Constraints), BPR (Business Process Reengineering) and ISO. It forces organizations to adopt data-driven decision making by following a structured roadmap. The financial benefits derived from a Six Sigma project have to be “hard” and quantifiable. They go directly to a company’s bottom line and most often with no capital investment. Six Sigma had its origin in Motorola in the 1980s.

In a Six Sigma program, trained Black Belts (BBs) are assigned to projects to improve specific processes, while working under the technical guidance of Master Black Belts (MBBs). BBs and MBBs typically report to Six Sigma Champions. Another key role is that of the Process Owner who is responsible for ensuring that the process continues to perform at a level determined at the completion of the Six Sigma project.

A Six Sigma project for a business process goes through five sequential phases:

1. **Define** the process for scope
2. **Measure** by collecting the right data
3. **Analyze** the process data
4. **Improve** the process through analyses (also identify the benefits)
5. **Control** the process by monitoring to sustain the benefits

Therefore a Six Sigma process improvement exercise is often called a **DMAIC** exercise. A major benefit of using Six Sigma is that it helps to minimize bias and helps to focus on customer requirements. Proper application of a Six Sigma program also allows for sustaining the benefits gained and avoids the “flash-in-the-pan” syndrome.

**In Six Sigma, one typically starts with a clean slate and therefore defines the process from scratch. One advantage of combining Six Sigma principles with ITIL processes is that one starts with well-defined and best-practice-based processes and, subject to the specific requirements of the organization, the metrics may already be defined by ITIL.**
3. How Frameworks Interact
The frameworks should not work in isolation. As described below, there are many areas in which they complement each other. If deployed appropriately, such complementary traits will maximize deployment benefits. However, it may not be necessary for an organization to have all of the above frameworks. For example, a privately held organization does not have to comply with SOXA.

Also, even when an organization chooses a set of frameworks, it does not necessarily have to deploy them fully. Full deployments of frameworks will allow an organization to extract maximum benefits – but partial implementation of certain elements will enable an organization to gain a variety of benefits. Examples are discussed later.

3.1. ITIL and ISO
ISO 9001:20000 Quality Management System is made up of at least 21 processes and provides Requirements and Guidelines. An organization has to meet formal Requirements in order to be certified. On the other hand, Guidelines are voluntary and can be applied in a flexible manner, based on an organization’s business requirements.

ISO does not provide best practice. An organization needs to develop or adopt practices (such as those described by ITIL) that have to meet the ISO Requirements and follow its Guidelines.

ISO has many derivatives for industry/function specific processes. ISO 20000 was developed to provide a quality standard for IT processes. It originated from BS 15000, a British standard that was derived from ITIL to provide quality certification on IT processes. ISO 20000 is the international version of BS 15000.

The diagram in Fig. 4 depicts how an organization may achieve certification. Every IT organization has its own in-house procedures for its deployed solutions. They need to align such solutions with ITIL best practice as the first step. If for business needs the organization desires to achieve ISO 20000 certification also, the organization has to then adopt the code of practice (i.e. guidelines) and lastly meet the specifications that are required for certification.

Another area where ISO aligns with ITIL is the area of IT security articulated by ISO 17799. Such an alignment is also necessary for Compliance in which COBIT related Controls will be addressed by employing ISO 17799 security aspects for ITIL processes.

3.2. ITIL and COBIT
While ITIL is about best practice processes, COBIT is about Control points. COBIT provides check points, security points, etc. so that execution of procedures will require appropriate authority and/or proof that
will meet specific and formal criteria. **Procedures are mapped by following ITIL best-practice.** If ITIL is being implemented to support a corporate initiative for best practice deployment, COBIT can be implemented simultaneously to establish the corresponding Control points.

Since COBIT follows the COSO model, it requires the following for regulatory Compliance:

- Display the **Process**
- Define **Control Objectives**
- Identify **Risks** (or “what-can-go-wrong”) in the process
- Define specific **Controls** that are in place to mitigate the above Risks
- Produce **Evidence** to prove that the above Controls are effective

The auditors (internal as well as external) will check that the above have been followed.

Since ITIL processes are based on best practice, they will be less prone to risks and what risks there are will be defined through metrics. The documentation required for ITIL deployment will also provide the necessary documents for Compliance.

**Software tools are almost always employed to administer ITIL processes.** Each of the ITIL processes is usually a module in these tools. One can incrementally deploy ITIL processes and will need to implement the corresponding tool modules simultaneously.

Such tools are invaluable in providing **Audit Logs**, used as **Control Evidence** to demonstrate that imposed Controls are indeed effective. Audit Logs are a sub-set of the Journal/Activity Logs that the tools also provide. For example, in Change Management the life-cycle of a change request can be tracked to provide a chronology of events in the life of the change.

The tools however, have to capture all necessary information needed for comprehensive audit logs. An audit log has to show separation of duties by proving that approval, implementation, testing, verification/acceptance, etc. of a change is indeed performed by different individuals with the appropriate authority. Information related to who is making the actual alteration – for example – in a software module, may not be easily traceable. It is an even greater challenge for older software.

An example of how the analysis of a problem in the ITIL Problem Management process can address Compliance is discussed later (Section 3.5). It shows the interaction of four frameworks: ITIL, Six Sigma, CMMI and COBIT.

### 3.3. ITIL and CMMI

Perhaps the two most complementary frameworks in IT Governance are ITIL and CMMI. As Fig. 5 illustrates, ITIL takes over where CMMI leaves off and vice versa. In effect it is a continuous cycle and analogous to the PDCA cycle for Continuous Improvement (Section 2.4).

**Application development cannot be an island.** Applications are developed based on business requirements. Then they need to be serviced through the use of an infrastructure – an **IT Service Management** infrastructure – for release, delivery, support and optimization. For example, an ITIL process such as Problem Management will capture application design related “Known Errors” that can be handed over to Development for fixes. These fixes can then be implemented through the ITIL Change Management process. Fig. 5 illustrates the relationship between these two frameworks.

![Fig. 5: Application Management](source: ITIL: Application Management (2002, p.7))
Table 2 (shown below) also describes how ITIL and CMMI specifically interact in a sample of ITIL processes.

Table 2 – Examples of CMMI and ITIL Interfaces

<table>
<thead>
<tr>
<th>ITIL Process</th>
<th>Output to Development</th>
<th>Input from Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Management</td>
<td>Incident data</td>
<td>Application support documents,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard Operating Procedures (SOPs)</td>
</tr>
<tr>
<td>Problem Management</td>
<td>Problem and Known Error data</td>
<td>Permanent Fixes, Work-around Solutions</td>
</tr>
<tr>
<td>Change Management</td>
<td>Request for Change data for:</td>
<td>Completed Changes, Changes initiated by Development</td>
</tr>
<tr>
<td></td>
<td>• Functional Changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Proactive Changes to mitigate failure risks</td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td>IT infrastructure data on impacted CIs*</td>
<td>New CI data to update CMDB**</td>
</tr>
<tr>
<td></td>
<td>(relationships, versions, status, etc.), CI Naming Conventions</td>
<td></td>
</tr>
<tr>
<td>Service Level Management</td>
<td>Functional Specifications, Constraints</td>
<td>Functions, Constraints</td>
</tr>
<tr>
<td>Capacity Management</td>
<td>Specifications related to performance (transaction timing, size of users), infrastructure (hardware, storage, processing speed, operating system, network, etc.), testing, etc.</td>
<td>Application capability data that corresponds to the same set on the left.</td>
</tr>
<tr>
<td>Availability Management</td>
<td>Availability specifications (agreed service times, response times, etc.),</td>
<td>Application capability regarding reliability, serviceability, resilience</td>
</tr>
</tbody>
</table>

*Configuration Items  ** Configuration Management Database

3.4. ITIL and Six Sigma

Customer specifications define quality (of a product or a service) in Six Sigma analysis. Any deviation from the specifications will be a “defect” in Six Sigma terms and one strives to attain no more than 3.47 defects per million opportunities.

Six Sigma defines **CTQ** (Critical to Quality) metrics for a process – metrics that will signify the health of a process (typically tied to customer specification). A CTQ is an “effect”, for which there are underlying “causes”. Effect (“y”) is a function of causes (“x”). Both have to be identified and measured (where possible, since not all causes can be measured quantitatively).

ITIL defines **KPI** (Key Performance Indicator) metrics as indicators of the health of the process in question. ITIL does not get into “causes” as defined in Six Sigma and some of the KPIs may very well be causes (“x’s). Most of the ITIL KPIs however are “y’s or CTQ’s (measures of process health).

**ITIL processes are best practices that have been developed for rapid adoption** – unlike the development of a Six Sigma process that typically starts with a blank slate from which an efficient process has to be developed. Also, ITIL suggests KPIs that are metrics for such processes. Even though an organization may decide to adopt other metrics, ITIL at least provides a starting point. Where these metrics are CTQs and based on customer specifications (as described in Service Level Agreements), the corresponding defects can also be determined.

3.5. Integration of Frameworks – An Example

Problem Management in ITIL requires investigation of current and past incident data and subsequent diagnosis. Tools used in Six Sigma, such as Cause and Effect (also known as Ishikawa or Fishbone)
diagrams and **FMEA** (Failure Modes and Effects Analysis) can be used for Problem analyses to determine “Root Causes”.

Ishikawa diagrams and FMEA have long been used in manufacturing and engineering settings to determine root causes. After a Problem ticket has been created in the ITIL process, a Fishbone diagram can be developed to identify a list of root causes which can then be applied to FMEA for prioritizing.

Once the root causes are added to the Knowledge Base, Service Desk personnel can resolve incidents rapidly – thereby increasing the First Call Resolution percentage, a well-known metric that reflects the efficiency of the Incident Management process (an ITIL process).

Also, once the causes are determined through a “Fishbone” analysis, the uncovered “causes” are the same as the risks (“what-can-go-wrong”) that have to be identified for regulatory Compliance documentation discussed under COBIT (**Section 3.2**). FMEA also utilizes a “control” factor (to determine prioritization of “causes”), which is the same item that must be identified for Compliance purposes.

If the Problem Management activities uncover a root cause that is related to application design, the output can then be handed over to the development as described in **Table 2**. Development process comes under CMMI best-practice framework.

In this example, in effect four separate frameworks – ITIL, CMMI, COBIT and Six Sigma – interact in an underpinning process to achieve superior IT governance.
4. Overall Governance Model is underpinned by Best Practice

Fig. 6 describes the overall IT Governance model and the high-level relationships among its various framework elements.

Fig. 6: Elements in IT Governance

The key message here is that Fig. 6 shows how formal deployment of best-practice infrastructure support processes is essential for overall Governance or even any of its specific elements. To be more precise:

- ITIL helps to provide Controls for COBIT by supplying the necessary documentation and information on Control evidence for identified Controls to mitigate related risks
- ITIL processes will also underpin support and maintenance of applications developed under CMMI
- ITIL processes provide the direct lineage from which ISO 20000 (previously known as BSI 15000) was developed. ITIL best practice has to be implemented if an organization wants ISO 20000 certification
- Continuous improvement utilizing a methodology such as Six Sigma can only occur when streamlined processes are in place through deployment of best practice (ITIL)

The ITIL best practice implementation therefore underpins each of the components of the overall Governance framework and thus the overall Governance framework itself.

4.1. Metrics – Crucial to Manage Frameworks

IT Governance elements need appropriate metrics that are collected and monitored to ensure that Governance is indeed effective and performing according to predefined expectations. Metrics need to be defined for each of the frameworks (the Governance elements) as well as for the framework processes themselves. A framework metric can be its maturity level (such as for ITIL and CMMI). There are well-accepted assessment procedures to determine these. Consulting-Portal’s ITOptimizer™ is a well-proven in-depth methodology used to assess the ITIL maturity of an IT organization as well as to subsequently implement ITIL best practice.

Since processes underpin frameworks (and by extension the overall IT Governance itself), process metrics are crucial. The 3M principle (Measure-to-Monitor-to-Manage) applies here. A process that is not monitored cannot be managed, and one has to measure to monitor process health.

Continuous improvement is NOT possible without appropriate metrics.
Metrics are also well defined in best practice for frameworks. For example, ITIL identifies specific metrics for each of the ten processes and can be enhanced based on business requirements to make them organization specific. Moreover, metrics can be defined for “effects” or for associated “causes” (Section 3.5) by applying Six Sigma principles.

Metrics are often presented in the form of charts and tables as part of reports for process health. Traditional charts are usually based on point values which typically are “average” numbers. Point values mask variations and may hide troublesome issues. Instead, one can apply statistical concepts by following Six Sigma principles and such exercises reveal far more information than charts using simple point values only. Those who view such statistical charts will, however, require rudimentary training on statistics to fully appreciate such charts.

Finally, the maturity level of overall IT Governance can also be determined through an assessment.

4.2. Apply Parts of Each Framework Incrementally and As Needed

For organizations desiring to achieve superior Governance, it is not necessary to implement each of the elements of the Governance framework. Most organizations are resource limited and framework implementations require a lot of effort. Parts of most of the elements can be adopted gradually and to the extent required by the organization.

The business goals of the organization will decide which frameworks are deployed first. Most major public companies have to address regulatory issues (such as SOXA) regardless. Starting with a Compliance framework utilizing elements of COBIT is not a choice for them. Since Governance is underpinned by processes, implementation of best practice in an ITIL framework is the next logical initiative. If ITIL best practice is in place, it is much easier to meet regulation Compliance. If an organization is heavily dependent on internal development, CMMI will also be another framework to adopt. Finally, once the organization has reached a comfort level with the above frameworks, they will want to deploy Six Sigma or at least elements thereof to extract maximum benefits from a continuous improvement environment.

Not only is the creation of overall IT Governance very complex, implementation of even one specific framework within its umbrella is also difficult. Organizational dynamics critically impact the establishment of superior Governance. Strong and committed leadership is not just crucial, it is absolutely mandatory to achieve superior Governance.

A framework such as ITIL implementation typically occurs incrementally – often starting with Incident Management followed by Problem Management and Change Management. Other processes such as Release Management, Configuration Management, Availability Management, etc. then follow.

While the choice of a standard such as SOXA is not optional since the requirements of regulatory Compliance are mandatory, implementation of ISO and Six Sigma certainly are optional. Even so, progressive organizations know that such implementations have business benefits and allow them to stay ahead of the competition. As Fig. 6 shows, an organization can be compliant with SOXA without adopting ITIL, since Compliance does not require effectiveness or efficiency. However, today’s business climate also demands both effectiveness and efficiency – hence the need to combine them and underpin them with best practice as prescribed by ITIL.

Certain products and company names mentioned in this white paper may be trademarks of their respective owners.