

CHANGE GOVERNANCE SERIES

Making Sense of regulations and best practices

August 2006

Eddy Pauwels, Serena Software, Inc.



TABLE OF CONTENTS

Abstract.....	3
Introduction	4
Improvement Methodologies and Business Drivers	4
THE PDCA CYCLE	6
THE IDEALSM MODEL	8
SIX SIGMA	9
BUSINESS DRIVERS	11
“MUST” DRIVERS (EXTERNAL)	11
“NEEDED” DRIVERS (INTERNAL/EXTERNAL)	11
“WANTED” DRIVERS (INTERNAL)	11
Industry Best Practices and Guidelines	13
INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)	13
CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)	14
CAPABILITY MATURITY MODEL (CMM/CMMI)	16
ISO STANDARDS	19
SAS 70	21
COSO	22
Regulations and Compliance	23
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)	23
GRAMM-LEACH-BLILEY FINANCIAL SERVICES MODERNIZATION ACT (GLBA)	24
SARBANES-OXLEY ACT	25
BASEL II	27
21 CODE OF FEDERAL REGULATION PART 11	29
Summary	30
References	31

Abstract

IT is an economic investment made by the business and exists to serve the business' needs in a way that maximizes efficiency and profitability. To gauge the return on its investment in IT, an organization needs to have measurements or performance indicators to assess its current situation, as well as to evaluate its progress toward defined objectives. Depending on target audience and objectives, organizations can choose from a variety of best practices and methodologies that have been developed to provide guidelines for and evaluations of progress. In addition to this, organizations in some industries must comply with government regulations, which may entail certain expectations and a set of common practices. The purpose of this white paper is to clarify the difference between a regulation and a best practice, as well as to explain key differences between the best practices.

Introduction

IT is an economic investment made by the business that must continually evolve to serve the business' ongoing need to increase efficiency and value in its operations. Fulfilling that objective requires organizations to plan for IT improvements in a way that takes into account:

- improvement methodologies
- industry best practices and frameworks
- industry regulations

First, in order to increase or improve the effectiveness of IT, an organization must have measurements or performance indicators that enable it to assess the current situation, as well as to understand and evaluate progress made towards meeting the objectives. A variety of best practices and methodologies have been developed to provide guidelines for and evaluations of progress. Section One of this paper deals with three of the most popular improvement methodologies, which are often embedded as elements of today's best practices (such as CMM, ITIL, and others).

This paper also describes the various reasons that lead an organization to implement best practices, which can be a costly undertaking. Building from the readers' better understanding of what motivates enterprises to implement best practices, and what it means to improve a certain aspect of a business, Section Two then describes the major guidelines and practices that are being implemented today, including:

Industry Best Practice	Focus
CMM	Software development
ITIL	IT service (operations) management
COBIT	IT risk (control objectives)
COSO	Enterprise risk management
SAS 70	(IT) controls auditing
ISO 9000	Quality management process
ISO 14000	Environmental management process

Many of the above best practices and frameworks are often (but not exclusively) used in the context of complying with a certain industry regulation. Section Three presents basic background on some of the main industry regulations that impact IT, including:

Regulation	Industry	Regulation Focus
Sarbanes-Oxley	Any US exchange listed public company	Accuracy & reliability of corporate disclosures
BASEL II	Finance	Risk management & market discipline
21 CFR Part 11	Pharmaceutical	Risk & quality management for electronic records & signatures
HIPAA	Healthcare	Security & privacy of data
GLBA	Finance	Security & privacy of data

There are similarities in the types of regulations for different industries, and also between the regulations and the various best practices. The common objective is to minimize cost and to maximize business value, and the common method is the development, usage, and auditing or certification of processes. These processes need to become embedded within the existing business processes through proper *orchestration*, and for compliance assurance their usage also *enforced*. The difference is that an industry regulation focuses on WHAT is expected, and a best practice focuses on HOW to achieve the expectations.

Best practices also provide guidance for ensuring these processes are accepted and enforced within an enterprise. Many people will only interact with a new process if they must in order to do their jobs, so organizations often use new applications to enforce processes and achieve compliance requirements.

Section Four, the final section of this paper, provides an overall summary and describes some of the relationships between regulations and best practices.

Improvement Methodologies and Business Drivers

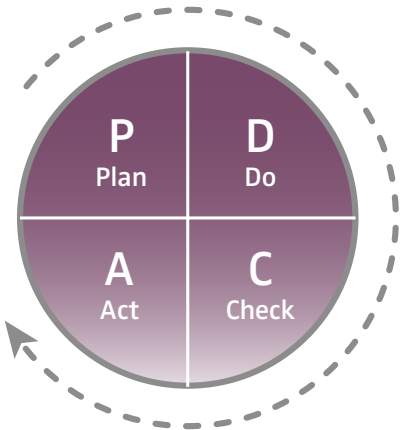
In order to increase or improve an aspect of the business—whether efficiency, cost, or value—an organization must first know its current status and have a way of assessing progress towards its objectives. Many improvement methodologies have emerged to assist organizations. This white paper focuses on three of the most well-known methodologies: the PDCA cycle, the IDEALSM model from the SEI, and Six Sigma.

Regardless of the methodology, an organization will need accurate performance indicators and measurements in order to improve. Capturing these measurements within IT is easier in operations than in IT development: operational data can be automatically obtained from operating systems, network, system, and storage management tools. But in IT development, any process to capture data will impact the people within the organization and will often result in a more complex and lengthy change process.

Take for example the need to align business needs closer to IT spending: to provide this alignment, an organization must be able to capture the business requirements and relate them to all the work (carried out by different resources within the organization) associated in achieving these requirements. In order to do capture and association, every resource involved in the process will have to account for its time and work as well as relate this work to the relevant business requirements. This change in process will require staff to take additional steps, which they may perceive as irrelevant or distracting from their main objectives. To achieve success in this change process, organizations often use external change consultants to coach and guide staff and rely as much as possible on tools that help automate the process in order to minimize disruption.

THE PDCA CYCLE

The PDCA Cycle is a checklist of the four stages that a company must go through to get from 'problem faced' to 'problem solved'. These four stages are Plan-Do-Check-Act (PDCA), and they are carried out in the cycle illustrated below.



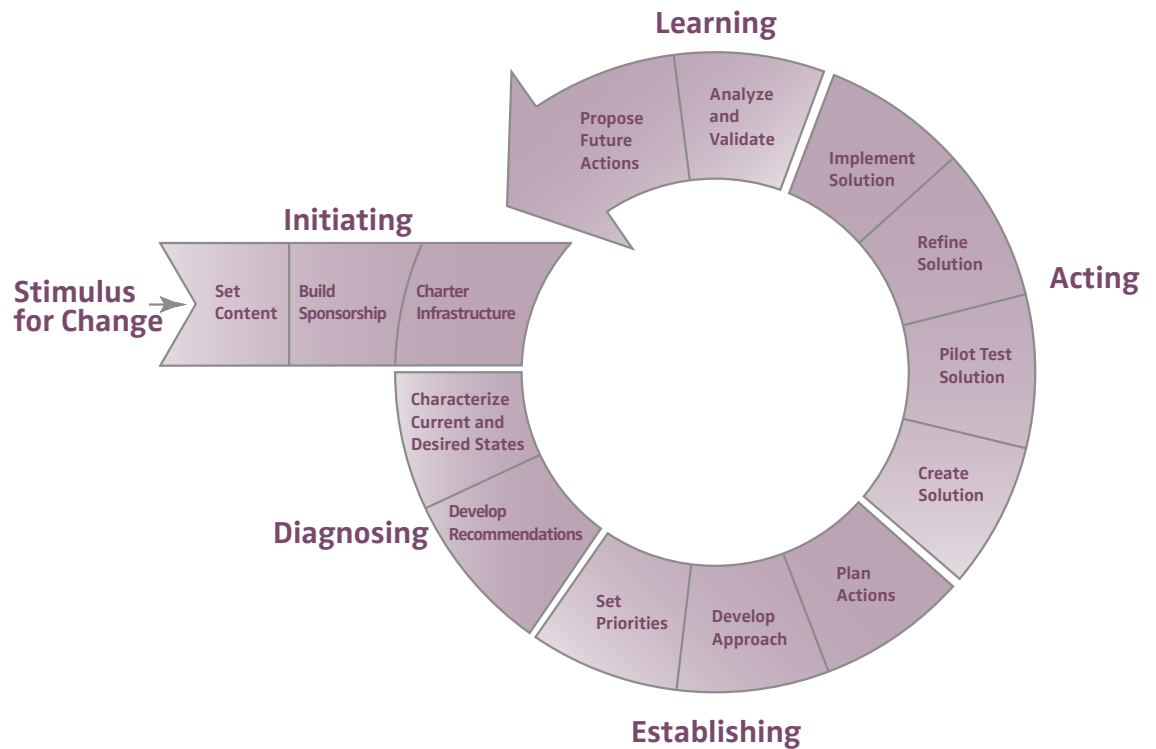
The concept of the PDCA Cycle was originally developed by Walter Shewhart, the pioneering statistician who developed statistical process control in the Bell Laboratories in the US during the 1930s. It was taken up and promoted very effectively from the 1950s by the famous Quality Management authority, W. Edwards Deming, and is consequently known to many as 'the Deming Wheel'.

The PDCA cycle is an iterative approach where each cycle leads closer to the desired objectives. It is one of the oldest methodologies provided and has been used as the basis for many of the more recent improvement methodologies in the industry. The following stages make up each cycle:

- 1. Plan** to improve your operations first by identifying the problems faced, such as poor profitability or slow response to customers. Next, develop ideas for solving or improving these problems.
- 2. Do** implement ideas on a small scale first. This minimizes disruption to routine activities while determining whether the changes will work.
- 3. Check** whether the experimental changes are achieving the desired result by measuring results using the same performance indicators or measurements used in the planning stage. Continuously check key activities to ensure that you know what the quality of the output is at all times, and to identify any new problems as they arise. This requires ongoing monitoring of the above measurements and indicators.
- 4. Act** to implement changes on a larger scale if the experiment is successful. Make the changes a routine part of the organization's activity, and involve others—departments, suppliers, or customers—whose cooperation you need to implement the changes on a larger scale.

THE IDEALSM MODEL

With the expertise gained from the PDCA cycle, the Software Engineering Institute (SEI) developed the **IDEAL Model**. This is an organizational improvement model that serves as a roadmap for initiating, planning, and implementing actions to improve some aspect of the business' operations. IDEAL is an acronym of the five phases the model describes: initiating, diagnosing, establishing, acting, and learning. The model forms an infrastructure to guide organizations in planning and implementing an effective software process improvement program in five phases:



- 1. Initiating:** laying the groundwork for a successful improvement effort. In this phase, organizations clearly articulate the business reasons for undertaking the effort. They identify contributions to business goals and objectives, and relationships with the other work within the organization. This is key because when the business reasons for change are evident, there is greater buy-in throughout the organization and therefore greater chance for success.
- 2. Diagnosing:** determining where you are relative to where you want to be. Characterizing the current and desired states can be done more easily using a reference standard such as the CMM for software development.
- 3. Establishing:** developing a detailed work plan of how to reach the destination. The organization sets priorities that reflect the recommendations made during the diagnosing phase, as well as the organization's broader operations and the constraints of its operating environment.

4. Acting: implementing the work that has been conceptualized and planned in the previous three phases. This phase will typically consume more calendar time and more resources than all of the other phases combined. Several iterations of the Test-Refine process may be necessary to reach a satisfactory solution. A solution should be workable before it is implemented, but waiting for a “perfect” solution may unnecessarily delay the implementation.

5. Learning: the learning phase completes the improvement cycle. One goal of the IDEAL Model is to continuously improve the ability to implement change. In the learning phase, the organization reviews the entire IDEAL experience to determine what was accomplished, whether the effort accomplished the intended goals, and how the organization can implement change more effectively in the future.

The IDEAL Model is documented on the SEI website, and the latest developments will be available there at www.sei.cmu.edu.

SIX SIGMA

A third popular improvement methodology is **Six Sigma**, which was originally defined as a process variation that would produce no more than 3.4 defects per million parts (or “opportunities”). Six Sigma is a quality management program that identifies and eliminates “defects” in manufacturing and service-related processes. Rigorous and disciplined, this methodology uses data and statistical analysis to measure and improve a company’s operational performance. It was pioneered at Motorola in the mid-1980s by Bob Galvin, head of the company, and Motorola engineer Bill Smith. It has since spread to many other manufacturing companies, including General Electric (GE), Honeywell, Raytheon, Seagate Technology, and Microsoft. However, it can be applied to any industry that wants to control variation. Recently, the service industry has begun to adopt Six Sigma.

In an article that describes the financial benefits of implementing Six Sigma, Charles Waxer investigated Motorola, Allied Signal, GE, and Honeywell. These companies invented and refined Six Sigma, and they are also the most mature in their deployments and culture changes. The companies in this study showed savings as a percentage of revenue of between 1.2 percent to 4.5 percent, indicating that Six Sigma savings can clearly be significant to a company. He also noted that companies shouldn’t expect to do more than break even in the first year of implementation. Six Sigma is a “get rich slow” methodology, meaning that its benefits accrue only over a long period of proper planning and consistent execution.

Six Sigma comprises two methodologies, DMAIC and DMADV.

DMAIC is designed to improve existing processes and is an acronym for:

- define the out-of-tolerance range
- measure the key internal processes critical to quality
- analyze why defects occur and explore opportunities for improvement
- improve the process to stay within tolerance
- control the process to stay within goals

DMADV is designed to introduce new processes and is an acronym for:

- define the process and where it would fail to meet customer needs
- measure and determine if the process meets customer needs
- analyze the options to meet customer needs
- design changes to the process to meet customers' needs
- verify the changes result in a process that meets customer needs

Six Sigma is about “managing by fact.” Most process problems are the result of a lack of facts. All Six Sigma solutions are based on obtaining, analyzing, and acting on facts, instead of on fault-finding, finger-pointing, or mass executions.

Lack of data *is* data. No data just means the project has unquantified variables. That, in turn, means management must resort to a tool that will allow the modeling of the potential consequences of a range of possibilities. Even when no one knows the appropriate value to assign to a variable, experts within the company can usually come up with worst-case, best-case, and most-likely values, perhaps with a probability distribution. This is enough to model the range and probability of potential outcomes.

With a better understanding of models used to improve aspects of IT provided in this section, the next section will take a closer look at why Change Governance Series: organizations are looking for these improvements.

BUSINESS DRIVERS

There are three main drivers for organizations to adopt improvement processes or best practices: essential external requirements (what they must do), strong internal or external needs (what they need to do), and internal preferences (what they want to do).

“MUST” DRIVERS (EXTERNAL)

Sometimes, a business has no choice about starting a change or improvement process. If the company must comply with governmental regulations, then failure to do so can result in penalties ranging from fines to imprisonment.

External regulations impose actions and investments that are often not in line with the company’s core business goals, but they often have a positive impact on the organization. Take for example the following quote from Jeffrey Immelt, Chairman & CEO of GE, taken from his “Letter to Stakeholders,” GE 2004 Annual Report, in February 2005:

“None of us likes more regulation, but I actually think SOX 404 is helpful. It takes the process control discipline we use in our factories and applies it to our financial statements. Implementing SOX 404 cost GE \$33 million in 2004. But we think it is a good investment ... Investors should demand high standards of governance and great performance. Some managers failed investors in the late ‘90s. Companies were destroyed, value was lost, and billions are being paid because of fraud. This happened. SOX 404 is by no means perfect, but it is a price we are willing to pay to restore investor trust.”

Regulations impacting IT will be discussed in the next section.

“NEEDED” DRIVERS (INTERNAL/EXTERNAL)

This second category of business drivers is much broader, and it can be internal or external in nature. Unlike the previous category, these drivers are optional; an organization does not have to implement any of the industry best practices or frameworks such as CMM, ITIL, or ISO. Non-compliance has no repercussions for the organization other than a possible loss of business. A company’s choice is influenced by:

- External pressure. Market demands can drive the adoption of best practices or regulatory compliance, even if the company is not obliged to do so. For example, partner or subsidiary companies based in different countries will often choose to comply with the other company’s best practices or regulatory commitments in order to ensure compliance and end-to-end auditability. Similarly, if consulting firms want to bid for any project at the Department of Defense, they should have a CMM Level 3 certification or Change Governance Series: equivalent.

- Internal requirements. Many organizations will aim for an industry certification such as CMM or ISO in order to gain competitive advantage. This has been happening for some time in the non-IT world, especially with regards to ISO 9000 certification.

With CIOs increasingly dependent on outside service providers to help with software projects, some have come to view CMM as a seal of approval for software providers. Consider the following quote from Dennis Callahan, Executive Vice President and CIO of Guardian Life Insurance:

“Level 5 was once a differentiator, but now it is a condition of getting into the game; having said that, there are some Level 3 or 4 start-ups that we might consider, but they have a lot more convincing to do before I would do business with them. They would be at a disadvantage.”

This means that organizations often have little choice other than to make the implementation of an industry best practice and certification process part of their business strategy.

“WANTED” DRIVERS (INTERNAL)

Many organizations have no internal standards or policies for conducting and optimizing their activities, and they ask themselves whether adopting industry standards would help. They look at the experience of other companies and see that successfully implementing an improvement methodology or a best practice can help in achieving objectives such as:

- minimizing the cost of operation
- maximizing software quality
- providing maximum auditability
- increasing levels of service / maximizing client satisfaction
- improving time to market

Regardless of the specific business driver, organizations undertaking these optional best-practice implementations often underestimate the complexity of the change process and its associated human aspects. Depending on the organizational culture and style, implementation strategies will differ. An external change management consultant can help guide the company through the process. Additionally, software solutions can assist in the understanding, orchestration, and enforcement of the processes to be implemented, ensuring consistency and maximizing the auditability of the process. Software can also help companies monitor and measure the performance and improvements of the new process.

Industry Best Practices and Guidelines

This section takes a closer look at the main IT industry best practices or guidelines, each of which was developed with a specific target audience and objective in mind. This section describes each best practice's history, focus, and intended use in order to help organizations choose the most appropriate one.

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

Developed in the United Kingdom in the late 1980s by the Central Computer and Telecommunications Agency (CCTA), which was later subsumed by the Office of Government Commerce (OGC), the IT Infrastructure Library (ITIL) is a customizable framework of best practices that promotes quality computing services within IT. ITIL addresses the structure and skill requirements for an IT organization by presenting a comprehensive set of management procedures with which an organization can manage its IT operations. These procedures are supplier-independent and apply to all aspects of IT infrastructure. Since the mid 1990's, ITIL has become a worldwide de facto standard for IT service management. ITIL is built on a process-model view of controlling and managing operations. The itSMF website (see References section for url) allows organizations to go through self-assessments of important processes in order to establish the extent to which they have adopted the best-practice guidance available from the OGC.

While ITIL has its roots in Europe, implementation of ITIL is quickly becoming a requirement in government and large corporations in the US. In fact, a recent US poll of more than 250 federal, state and local government decision-makers showed that 65% were testing or implementing ITIL.

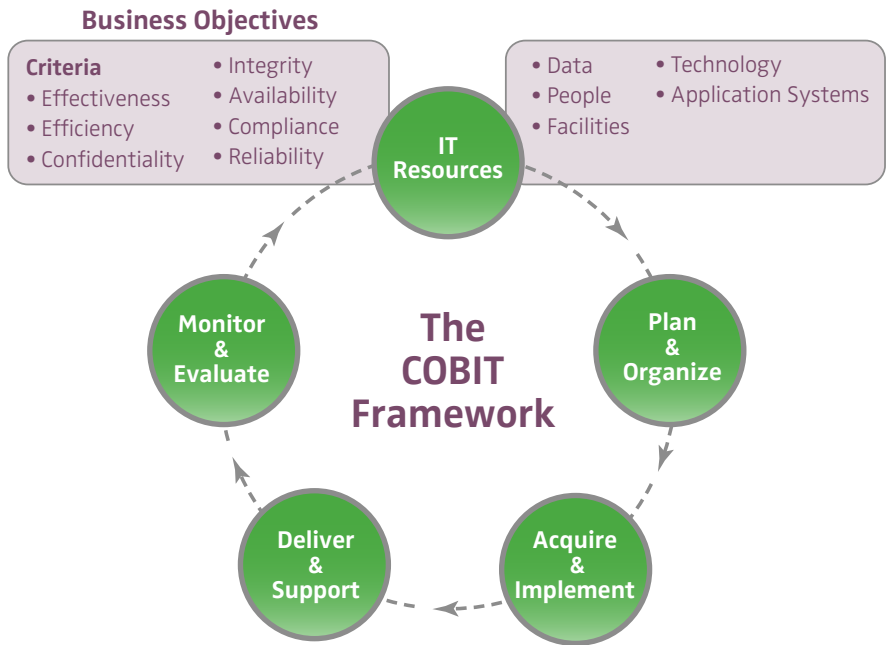
The rapid adoption of and increased interest in ITIL best practices are mostly due to the following characteristics:

- ITIL is open: freely available, non-exclusive, and non-proprietary
- The ITIL "kernel" of seven key volumes consolidates the original 40-volume set and is available at the modest price of approximately \$120 each, so the cost is low
- Competing technology companies, not just individual developers, contributed to the library in the subject areas they know best, so ITIL incorporates the experience of domain experts
- Competing technology companies carefully reviewed one another's work with a keen eye to ensure that rivals did not add proprietary or other self-serving provisions
- An independent, not-for-profit organization maintains and publishes the libraries and administers the related ITIL certification program, which certifies organizations and practitioners but *not* products

ITIL is a theoretical framework, not a complete process solution. Because you choose from among the best practices available, there is much work to be done before, during, and after introducing ITIL. It is not a straightforward process: implementing ITIL also means changing the mindset of employees, for example, pushing technical staff to be more aware of service and business. There are emotions and habits involved. It is neither practical nor desirable to implement ITIL in one fell swoop. Most organizations implement ITIL in phases, beginning with the area of most pain.

CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT)

COBIT is a framework for IT management risks that helps managers, auditors, and users understand their IT systems and develop a governance model that spells out what level of security and control is necessary to protect their companies' assets.



Monitor and Evaluate	Delivery and Support	Plan and Organize	Acquire and Implement
M1 Monitor the process	DS1 Define service levels	PO1 Define a strategic IT plan	A11 Identify automated solutions
M2 Assess internal control adequacy	DS2 Manage third-party services	PO2 Define the Information architecture	A12 Acquire and maintain application software
M3 Obtain independent assurance	DS3 Manage performance and capacity	PO3 Determine the technological direction	A13 Acquire and maintain technology infrastructure
M4 Provide for independent audit	DS4 Ensure continuous service	PO4 Define the IT organization and relationships	A14 Develop and maintain IT procedures
	DS5 Ensure systems security	PO5 Manage the IT Investment	A15 Install and accredit systems
	DS6 Identify and attribute costs	PO6 Communicate management aims and direction	A16 Manage changes
	DS7 Educate and train users	PO7 Manage human resources	
	DS8 Assist and advise IT costumers	PO8 Ensure compliance with external requirements	
	DS9 Manage the configuration	PO9 Assess risks	
	DS10 Manage problems and incidents	PO10 Manage projects	
	DS11 Manage data	PO11 Manage quality	
	DS12 Manage facilities		
	DS13 Manage operations		

Created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992, with the first edition published in 1996, COBIT's mission is "to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors."

In its 3rd edition, COBIT has 34 high-level objectives that cover 318 control objectives categorized in four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. It comprises six elements: management guidelines, control objectives, the COBIT framework, executive summary, audit guidelines and an implementation toolset. All are documented in separate volumes. COBIT is a set of 36 standards that details how to control or audit the effectiveness of IT process controls.

In recent years, increased attention has been devoted to internal control by auditors, managers, accountants, and legislators. Scandals like Enron, Qwest, Worldcom, etc., and the subsequent passage of the Sarbanes-Oxley Act (SOX) have resulted in a recent increase in interest and adoption. In fact, five recently issued documents are the result of continuing efforts to define, assess, report on, and improve internal control. They are the Information Systems Audit and Control Foundation's COBIT (already discussed above), the Institute of Internal Auditors Research Foundation's Systems Auditability and Control (SAC), the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control-Integrated Framework (COSO), and the American Institute of Certified Public Accountants' Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55), as amended by Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (SAS 78).

Because different bodies developed the documents to address the needs of their own audiences, some disparities may exist. Nevertheless, each document focuses on internal control and each audience—for example, internal auditors, management, and external auditors—devotes much time and effort to establishing or evaluating internal controls. Therefore, comparing the internal control concepts presented in these documents may be of interest to members of all three audiences.

This increase in focus on audits and compliancy has also resulted in the ITGI to release in December 2005 its version 4.0 of COBIT. This new release emphasizes on regulatory compliance, helps organizations to increase the value attained from their IT operation, enables business alignment and simplifies implementation of the COBIT framework through presentation of activities in a more streamlined and practical manner. This new version also provides a detailed mapping between COBIT and ITIL, CMM, COSO, PMBOK, ISF and ISO/IEC 17799 to enable harmonization with those standards in language, definitions and concepts.

For more information about this latest update we refer to the ISCA website at <http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>

CAPABILITY MATURITY MODEL (CMM/CMMI)

The Capability Maturity Model is a method for evaluating and measuring the maturity of the software development process of organizations on a scale of 1 to 5. The CMM was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University in Pittsburgh in the mid-1980s. It has been used extensively for avionics software and for government projects. The Software Engineering Institute has subsequently released a revised version known as the Capability Maturity Model Integration (CMMI). The purpose of CMM is to provide guidance for improving an organization's processes and its ability to manage the development, acquisition, and maintenance of products or services.

There are five levels of the CMM.

Maturity Level 1: Initial—processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this, they often produce products and services that work; however, they frequently exceed the budget and schedule of their projects. Maturity level 1 organizations tend to overcommit, abandon processes in the time of crisis, and cannot repeat their past successes.

Maturity Level 2: Repeatable—software development successes are repeatable. The organization may use basic project management to track costs and schedules. Process discipline helps ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans. Project status and the delivery of services are visible to management at defined points such as major milestones.

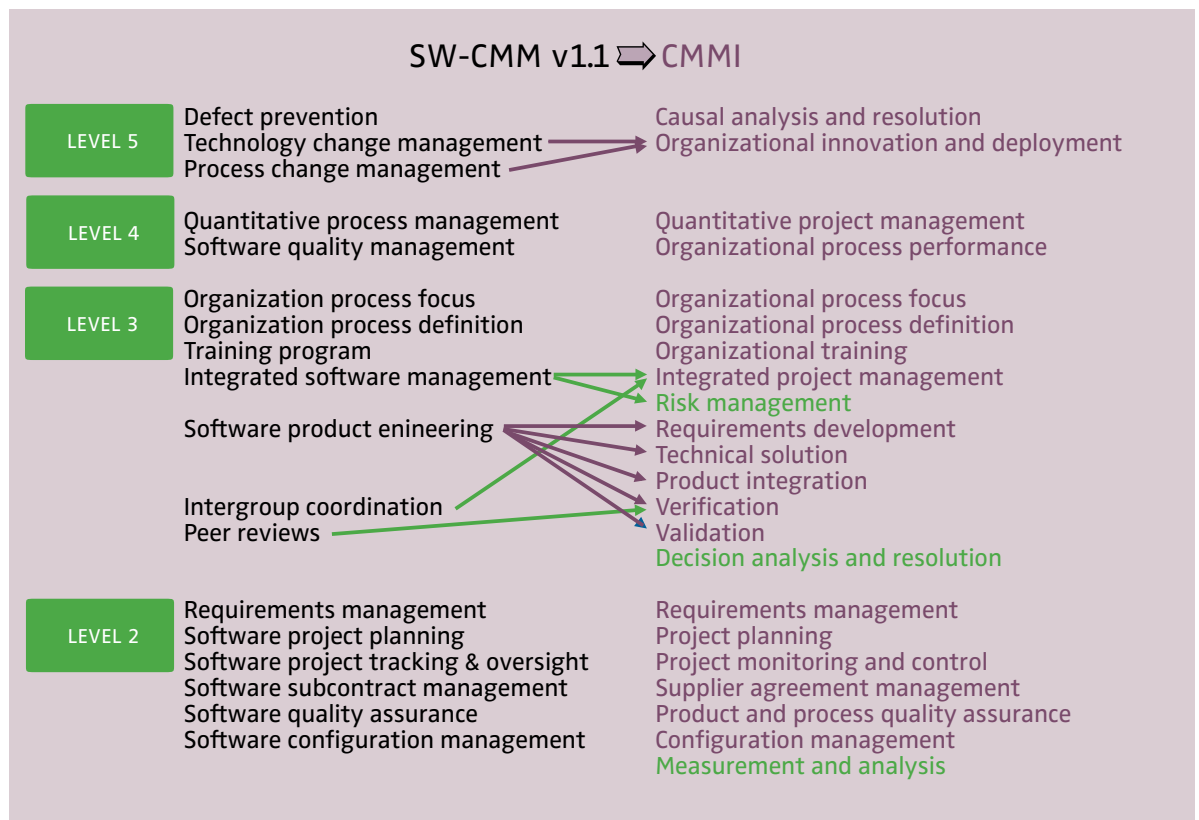
Maturity Level 3: Defined—processes are well characterized and understood, and they are described in standards, procedures, tools, and methods. The organization establishes and improves over time its set of standard processes, which is the basis for level 3. These standard processes help ensure consistency across the organization. Projects abide by defined processes, tailored according to guidelines. While level 2 standards, process descriptions, and procedures may differ from one project to the next, at level 3 the standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit.

Maturity Level 4: Managed—using precise measurements, management can control the software development effort. In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Management selects subprocesses that significantly contribute to overall process performance, and it controls them using statistical and other quantitative techniques.

A critical distinction between maturity level 3 and maturity level 4 is the predictability of process performance. At maturity level 3, processes are only qualitatively predictable, but at maturity level 4, the performance of processes is controlled, using statistical and other quantitative techniques, and is quantitatively predictable.

Maturity Level 5: Optimizing—focuses on continually improving process performance through incremental and innovative technological improvements. The organization establishes quantitative process improvement objectives, continually revising them to reflect changing business objectives, and uses them as criteria in managing process improvement. The organization measures the effects of deployed process improvements and evaluates them against the quantitative process improvement objectives. Both the defined processes and the organization’s set of standard processes are targets of measurable improvement activities. The organization’s ability to rapidly respond to changes and opportunities is enhanced by finding ways to accelerate and share learning. A critical distinction between maturity level 4 and maturity level 5 is the type of process variation addressed. At maturity level 4, processes address special causes of process variation and provide statistical predictability of the results. Though processes may produce predictable results, the results may be insufficient to achieve the established objectives. At maturity level 5, processes are concerned with addressing common causes of process variation and changing the process (that is, shifting the mean of the process performance) to improve process performance (while maintaining statistical predictability) to achieve the established quantitative process improvement objectives.

For CMMI, the successor of CMM, the objective is to integrate competing maturity models (such as SW-CMM, SECM, IPD-CMM, SA-CMM) and to provide a more consistent process improvement model. It results in better integration of the functional disciplines in their application in organizations. It also emphasizes the importance of measurable improvements to achieve business objectives. Also, CMMI addresses some process areas not covered by CMM, such as Engineering Process, Areas, Measurement and Analysis, Risk Management, and Decision Analysis. (See chart on following page.)



The CMM is intended to help assess an organization's software development maturity. This makes it an important tool for outsourcing and exporting software development work. Economic development agencies in India, Ireland, Egypt, and elsewhere have praised the CMM for enabling them to be able to compete for US outsourcing contracts on an even footing.

IBM, Motorola, Logica, BT, and others have discovered the following:

- It takes 18 months on average to move up one SEI level, but it has been done in eight months
- Defect rates can be lowered from 1 per 1,000 lines of code to 1 per 1,000,000 lines, which is roughly Six Sigma quality
- There is no specific evidence for shortening time to market, but there is evidence that at level 1, organizations overrun their estimated completion dates by 75 percent on average, while organizations at level 5 typically meet completion dates, plus or minus 2 percent
- Data on productivity increases is more variable, but at the least, productivity doubles

No external body certifies a software development center as being CMM compliant; it is supposed to be an honest self-assessment. The CMM does not describe how to create an effective software development organization; instead, it describes behaviors and best practices that successful projects have demonstrated. Being CMM compliant is not a guarantee that a project will be successful; however being compliant can Change Governance Series: increase a project's chances of being successful.

Most organizations will end up at either a level 2 or level 3. The following are the most beneficial elements of CMM level 2 and level 3:

- Creation of software specifications, stating what is going to be developed and providing for a formal sign-off, an executive sponsor, and an approval mechanism. This is NOT a living document, but additions are placed in a deferred or out-of-scope section for later incorporation into the next cycle of software development.
- A technical specification, stating how precisely the specified software is to be developed and will be used. This is a living document.
- Peer review of code that provides a formal approval mechanism for completed code. Its metrics also allow developers to walk through an implementation and suggest improvements or changes. The formal approval process avoids potential problems due to code that has already been developed based on a bad design.
- Version control that can provide a formal revision control mechanism and release mechanism. Many organizations lack these key mechanisms.
- The idea that there is a "right way" to build software. CMM promotes the view that development is a scientific process involving engineering design, not just a process in which groups of developers patch together work-arounds for the problem du jour.

ISO STANDARDS

Most ISO standards are highly specific to a particular product, material, or process. However, both ISO 9000 and ISO 14000 are known as generic management system standards because they can be applied to any organization, large or small, whatever its product or service, in any industry, and in any sector (government, business, or non-profit). These management system standards apply to what the organization does to manage its processes and activities, such as satisfying the customer's quality requirements, complying with regulations, or meeting environmental objectives.

In a very small organization, there is probably no system, as such, just "our way of doing things." This is probably not written down, but in the head of the manager or owner. The larger the organization, and the more people involved, the more likely it is that there are some written procedures, instructions, forms, or records. These help ensure that the organization goes about its business in an orderly and structured way, so that it uses time, money, and other resources efficiently.

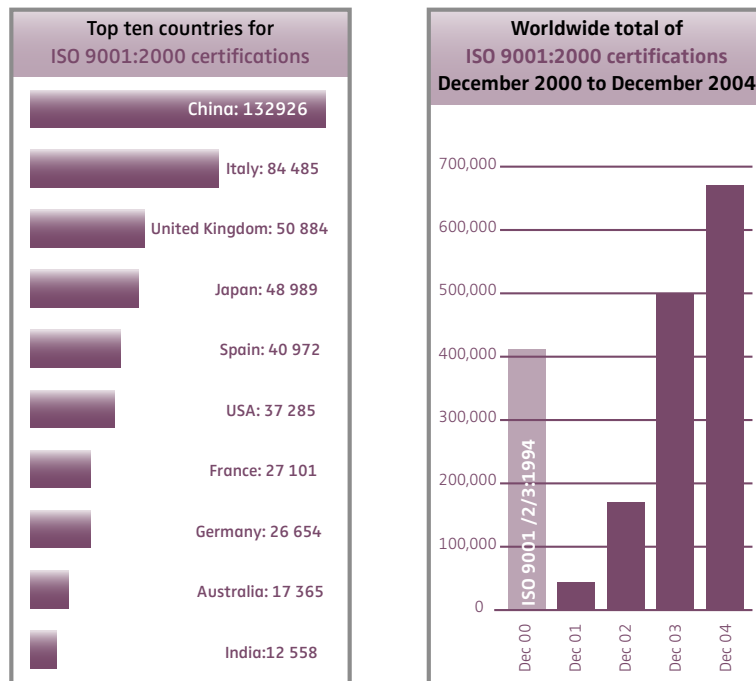
To be really efficient and effective, the organization can adopt a system that manages its way of doing things. This ensures that nothing important is left out and that everyone is clear about who is responsible for doing what, when, how, why, and where.

The ISO 9000 family of standards represents an international consensus on good management practices with the aim of ensuring that the organization can consistently deliver its products or services, meet the customer's quality requirements to enhance customer satisfaction, comply with applicable regulatory requirements, and achieve continual improvement of its performance in pursuit of these objectives. These good practices have been distilled into a set of standardized requirements for a quality management system, regardless of what the organization does, its size, or whether it's in the private or public sector.

Companies should make sure that they are pursuing certification for the right reasons, for example:

- To improve their business processes and save money. Many companies implementing ISO 9000 certification report increases in business process efficiencies, reductions in waste, and improved product quality.
- To qualify for new customers. Many corporations see ISO 9000 certification as an essential requirement for conducting business with a new vendor.
- To enter global markets. Many countries require ISO 9000 standards.

As seen in the associated charts, there has been a year-on-year increase in the number of enterprises adopting the ISO 9000 standards for several years. To date, adoption is far more successful in Europe (Italy, UK, Spain, France, and Germany) and China than it is in North America.



As every business is unique, ISO 9000 lays down what requirements a quality system must meet, but does not dictate how. This leaves great scope and flexibility for implementation in different business sectors, business cultures, and national cultures.

ISO 14000 is primarily concerned with environmental management: what the organization does to minimize harmful effects on the environment caused by its activities.

Both ISO 9000 and ISO 14000 focus on the way an organization goes about its work: they address processes, not products—at least, not directly. Nevertheless, the way in which the organization manages its processes can affect its final product. In the case of ISO 9000, the efficient and effective management of processes is, for example, going to affect whether or not everything has been done to ensure that the product satisfies the customer's quality requirements. This is why most successful organizations that implemented ISO 9000 have implemented proper IT systems in order to help them with the definition, automation, and control of the processes they needed to manage.

In the case of ISO 14000, the efficient and effective management of processes is going to affect whether or not everything has been done to ensure a product will have the least harmful impact on the environment, at every stage in its life cycle, either by pollution or by depleting natural resources. Enforcement of policies and procedures is critical in this case.

A question that regularly comes up is the difference between Sarbanes-Oxley (see section on compliance) and ISO compliance. First, Sarbanes-Oxley is a regulation, which means there are penalties for noncompliance, while ISO has no penalties. They're both very document-centric, but ISO 9000 focuses mainly on manufacturing processes while Sarbanes-Oxley focuses on financial processes. Given their similarities in approach, ISO 9000-certified companies may find it easier to comply with Sarbanes-Oxley, depending on the business processes they have been certified on.

Concerning relationships between Best practices and efforts we want to mention the proposed and upcoming ISO 20000 standard, which will be the next edition of the BS15000 British standard, which was the first standard for IT service management, fully compatible and supportive of ITIL.

SAS 70

The American Institute of Certified Public Accountants (AICPA) developed the Statement on Auditing Standards (SAS) No. 70. To successfully complete an SAS 70 audit, organizations must go through an in-depth audit of their control activities, including controls over IT and related processes.

SAS 70 provides guidance to enable an independent auditor to issue an opinion on a service organization's description of controls through a Service Auditor's Report (see below). SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

SAS 70 data centers have to maintain prescribed levels of data security and redundancy, as well as personnel controls. These requirements include reporting on firewall configuration and access, database access, data transmissions, data backup and recovery, application security, and product development. In addition, data center staff cannot access servers or data without a specific procedure. All access and activity is logged, and all physical access is highly controlled.

The audit output, the Service Auditor's Report, contains the auditor's opinion, a description of the controls in place, and—if it is a Type II report—a description of the auditor's tests of control effectiveness. An SAS 70 Type I analysis does not include testing. Some question the validity of the SAS 70 auditor's opinion, because SAS 70 is not a predetermined set of standards that an organization must satisfy in order to "pass" the audit. In an SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors in user organizations. If an organization does not have a security policy covering a particular area, or has one that allows ineffective security (for example, an organization may not have a policy that prevents the deployment of production servers with default configurations and default passwords), the SAS 70 audit report would contain a favorable opinion because the control activities (none) matched the stated control objectives (none).

As an organization decides to automate some of its controls and processes, especially in the area of product development, auditor reviews will become much easier, and consistent use of processes can be easily enforced.

COSO

COSO (Committee of Sponsoring Organizations of the Treadway Commission) was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. This was an independent private sector initiative that studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.

The COSO framework describes the critical principles and components of an effective enterprise risk management process, including how all important risks should be identified, assessed, responded to, and controlled. It also provides a common language, so that when executives, directors, and others talk about risk management, they are truly communicating.

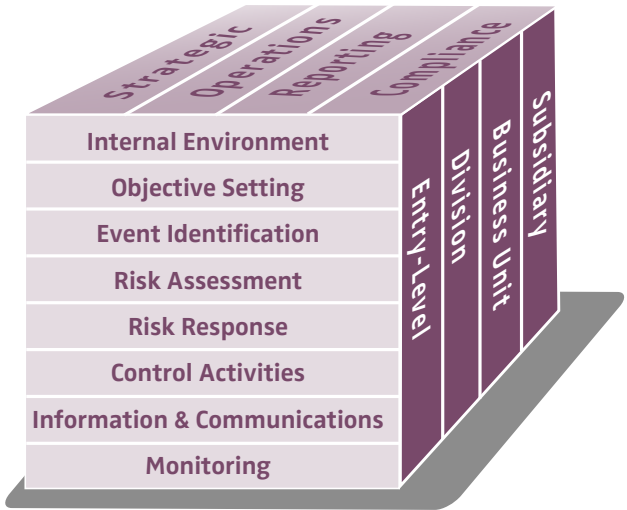
The framework sets forth how a company should apply enterprise risk management in its strategic planning and also describes techniques some companies are using in identifying and managing risk. Importantly, the framework emphasizes how an effective enterprise risk management process identifies not only the downside, but also the upside, or opportunities that can be seized to enhance profitability and return. The framework also describes roles of key players in the enterprise risk management process.

Within the COSO framework, enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process.

These components are:

- **Internal environment:** the internal environment encompasses the tone of an organization, and it sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate
- **Objective setting:** objectives must exist before management can identify potential events affecting their achievement
- **Event identification:** internal and external events affecting achievement of an organization's objectives must be identified, distinguishing between risks and opportunities
- **Risk assessment:** the likelihood and impact of risks are assessed, on an inherent and a residual basis, to determine how they should be managed
- **Risk response:** management selects risk responses, such as avoiding, accepting, reducing, or sharing risk, to develop a set of actions that aligns risks with the company's risk tolerances and risk 'appetite'
- **Control activities:** policies and procedures are established and implemented to help ensure the risk responses are effectively carried out
- **Information and communication:** relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities; communication flows down, across, and up the entity
- **Monitoring:** the entirety of enterprise risk management is monitored through ongoing management activities, separate evaluations, or both, and modifications are made as necessary

IT can play an important role in the implementation of some of the COSO components. Control activities benefit from IT's automated and enforced policies and procedures that reduce risk by maximizing compliance. Information and communication is made easier by using IT systems to record information and communicate electronically. IT supports monitoring by aggregating information through data warehousing, decision support systems, and dashboards, for example.



Regulations and Compliance

There are several major regulations in the market. This section briefly describes the most commonly encountered ones and their implications for the IT organization.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted by the U.S. Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification provisions, required the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. These provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

HIPAA defines three segments of security safeguards for compliance: administrative, physical, and technical. Organizations must ensure they have in place:

- Administrative safeguards through policies and procedures that clearly show how the entity will comply with the act
- Physical safeguards that control physical access to protect against inappropriate access to protected data
- Technical safeguards that control access to computer systems and enable covered entities to protect interception of communications containing personal health information transmitted electronically over open networks

Most medical records are stored within IT systems. Security management in general—whether intrusion detection, data encryption, or access management—is also an area of IT responsibility. Although the definition, implementation, auditing, and change control of policies and procedures does not clearly reference automation systems, the risk of non-compliance to the processes will be significantly higher without such systems, due to the high percentage of human involvement. Automated systems can also help manage the introduction and removal of hardware and software from the network, as part of the physical safeguards.

At present there is no standard process to determine HIPAA compliance, which becomes even more complicated when organizations are evaluated according to different criteria and methodologies. The Corbett Technologies' HIPAA-Capability Maturity Model© (HIPAA-CMM©) is a standard methodology and evaluation model based on proven, valid techniques recognized by the information security community. Based on the CMM framework described in section 2, HIPAA-CMM is proposed as the standard framework for evaluating and ensuring HIPAA compliance.

GRAMM-LEACH-BLILEY FINANCIAL SERVICES MODERNIZATION ACT (GLBA)

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) of 1999 repealed the Glass-Steagall Act, which prohibited a bank from offering investment, commercial banking, and insurance services. The Gramm-Leach-Bliley Act opened up competition among banks, securities companies, and insurance companies, allowing investment and commercial banks to consolidate. The combined industry is known as the financial services industry.

Most of the largest banks, brokerages, and insurance companies supported GLBA. The justification was that people usually put more money in investments in a good economy, but put their money into savings accounts when hard times come. With the new act, financial services institutions could prosper in changing economic circumstances.

The key rules under the act include the Financial Privacy Rule that governs financial institutions' collection and disclosure of customers' personal financial information.

The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information. It also applies to companies, such as credit reporting agencies, that receive such information.

GLBA compliance is not voluntary. Whether or not a financial institution discloses nonpublic information, it must have a policy in place to protect the information from foreseeable threats to security and data integrity.

SARBANES-OXLEY ACT

Probably the regulation with the most impact on IT is Sarbanes-Oxley (SOX), officially titled the "Public Company Accounting Reform and Investor Protection Act of 2002" and signed into law on July 30, 2002. SOX was created to protect investors by improving the accuracy and reliability of corporate disclosures. The act, created in the wake of a series of corporate financial scandals, requires establishment of a public company accounting oversight board, auditor independence, corporate responsibility, and enhanced financial disclosure.

SOX primarily affects public companies with a market capitalization of \$75 million listed on U.S. exchanges. While SOX is strictly focused on financial reporting and does not specifically address IT, companies keep their financial records electronically, which brings the reliability and security of IT systems under scrutiny.

A fundamental difference between SOX and similar requirements in other countries is its requirement for an annual assessment of internal controls (including documentation) and an attestation from an external auditor. A company cannot rely on verbal confirmation any longer; management must provide a body of evidence to demonstrate that controls are working effectively.

Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure. The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared."

Moreover, under Section 404 of the Act, management is required to produce an "internal control report" as part of each annual Exchange Act report. The report must affirm "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting." The report must also "contain an assessment, as of the end of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the Change Governance Series: issuer for financial reporting."

SOX requires companies, for the first time, to demonstrate that they have assessed and proven their internal controls. This presents new challenges to businesses, especially in documenting control procedures related to their IT systems.

The Public Company Accounting Oversight Board (PCAOB) suggests considering the COSO framework in management or auditor assessment of controls. Auditors have also looked to the IT Governance Institute's COBIT for appropriate standards. This framework focuses on IT processes while keeping in mind the big picture of COSO's control activities and information and communication. However, certain aspects of COBIT are outside the boundaries of SOX regulation.

In today's business environment, the financial reporting processes of most organizations are driven by IT systems, so IT plays a vital role in internal control. As PCAOB's "Auditing Standard 2" states:

"The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting."

For most organizations, the role of IT will be crucial to achieving SOX compliance. To support the SOX compliance process, IT must:

- Understand the organization's internal control program and its financial reporting process
- Map the IT systems that support internal control and map the financial reporting process to the financial statements
- Identify risks related to these IT systems
- Design and implement controls to mitigate the identified risks and monitor them for continued effectiveness
- Document and test IT controls
- Ensure that IT controls are updated and changed, as necessary, to correspond to changes in internal control or financial reporting processes
- Participate in SOX project management

The importance of IT as it relates to the overall financial reporting process is highlighted by several sections in PCAOB Auditing Standard No. 2, which discusses the relationship of IT and its importance in testing the design and operational effectiveness of internal controls. An excerpt from the standard states:

"...Controls should be tested, including controls over relevant assertions related to all significant accounts and disclosures in the financial statements." Generally, such controls include (among others) controls, including information technology general controls, on which other controls are dependent."

SOX also specifically addresses IT involvement in each period-end financial reporting process element. In an article by Deloitte, “Under Control,” “sustainable compliance” is encouraged. The article suggests leveraging lessons learned to immediately transition into a long-term strategy. One of the areas described as inhibitors to the process included the underestimation of technology impacts and implications:

“IT is recognized as critical for achieving the goals of the Sarbanes-Oxley Act, and the impact and implications of technology are widely regarded as significant and pervasive. In many year-one projects, organizations focused heavily on business processes and did not consider the broader role that IT plays in managing financial information and enabling controls... IT will make a huge impact on compliance going forward. At a minimum technology investments will be necessary to support sustainable compliance in several areas, including repository, work flow, and audit trail functionality. Technology will also be used to enable the integration of financial and internal control monitoring and reporting — a critical requirement at most large and complex enterprises.”

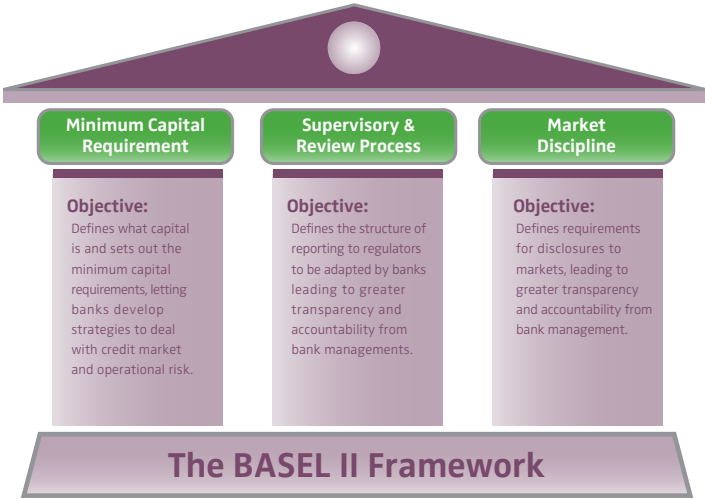
To add to this, a survey carried out by Charles River Associates (CRA) reviewing relevant data for a sample of companies belonging to the Fortune 1000 identified the average number of deficiencies in 2004 to be 348, of which about 77 deficiencies were for subsequent remediation. Of these unremediated deficiencies, almost 96 percent were classified as control deficiencies. The standard defines a control deficiency as “a deficiency when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.” IT can help by providing means to orchestrate and enforce the controls that need to be in place.

Many of the best practices discussed in this paper—ITIL, CMM, and ISO—all define ways of organizing processes, and therefore have a positive effect in achieving SOX compliance as well.

BASEL II

Basel II was devised to improve the soundness of the international financial system by aligning regulatory capital requirements with the underlying risks of the banking industry. Its proposals aim to improve the international consistency of capital regulations, make regulatory capital more risk sensitive, and promote enhanced risk-management practices among large, internationally active banking organizations. Basel II is a key strategic imperative for European banks as risk management strategies play an increasingly critical role in smoothing earnings and winning much-needed investor confidence. Financial institutions should integrate Basel II in their operations by year-end 2006.

Basel II intends to provide more risk-sensitive approaches while maintaining the overall level of regulatory capital within the financial system. This can be achieved through a meticulously designed framework consisting of three mutually reinforcing pillars as summarized in the figure below.



Leveraging information technology assets can help institutions manage risks more efficiently, as outlined by Basel II. The financial sector will, therefore, rely significantly on IT service providers to provide a more coherent architecture for process automation, integration, and cost reduction mechanisms.

However, financial institutions should pause before they buy packaged Basel II solutions to make sure that they fully understand where compliance begins. Basel II compliance is essentially a knowledge issue, requiring data capture, reporting and analysis of credit, market, and operational risk, and then mitigation of perceived risks through business processes, whether automated or performed manually. Organizations must develop a complete understanding of the processes, roles, and skills employed in the operation of the business through business process modeling.

Combining data and business processes together then provides an enterprise architecture, which details not only the processes and data themselves, but also the relationships between them. The most popular description of an enterprise architecture is based on the Zachman Framework, which models how all parts of an organization fit together and provides an 'as-is' diagram of the organization.

Once a financial institution has developed an accurate picture of its organization, it can begin to look ahead and predict future risk scenarios, which will be a valuable tool in Basel II compliance in the long term.

CODE OF FEDERAL REGULATION PART 11 (21 CFR PART 11)

The United States Food and Drug Administration's (FDA's) 21 Code of Federal Regulations Part 11 (21 CFR Part 11) has been in effect since August 1997. This Code defines the criteria under which the FDA will accept electronic records and signatures, and IT covers all FDA-regulated enterprises—including manufacturers of pharmaceutical, medical device, cosmetic, biotechnology, and food and beverage products—as part of a program to identify current good manufacturing practices (cGMP) or more general good clinical, laboratory, manufacturing, and pharmaceutical practices (cGxP). Adoption and focus has been mainly in the pharmaceutical industry.

The Code was created to address FDA concerns about fraud through misuse of electronic signatures and through alterations to database elements without an audit trail recording that changes were made. A move to electronic records and electronic signatures can create tremendous value for companies by enhancing speed, efficiency and accuracy of information. The goal of the Code is to establish a standard that makes these records and signatures trustworthy and verifiable, so that pharmaceutical or medical device companies can confidently use them as a replacement for paper records and handwritten signatures.

The Code outlines the procedural and technical requirements necessary to implement computer systems utilizing electronic records and/or electronic signatures. It is a regulated quality initiative that allows and requires companies to document conditions and events electronically during the manufacturing process to ensure exact manufacturing procedures are followed and to guarantee consistent product quality.

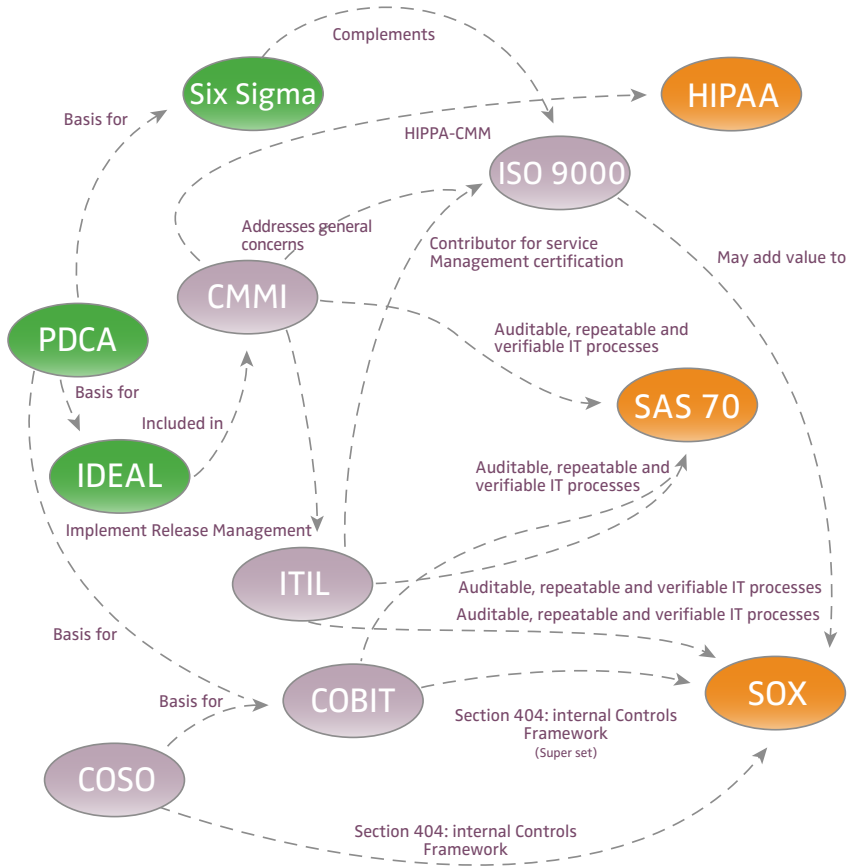
In order for auditors to validate a system, organizations must provide the following documentation:

- Installation qualification, a documented verification that a system was installed in accordance with written and pre-approved specifications
- Operational qualification, a documented verification that a system operates according to a set of written and pre-approved specifications throughout all operating ranges
- Performance qualification, a documented verification that the system is capable of controlling or performing the activities it is required to perform or control, according to written and pre-approved specifications while operating in its specified operating environment

Although the Code has been in place for a while, the FDA is now starting to actively enforce it. The penalties for FDA-regulated companies that fail to comply with 21 CFR Part 11 can range from receiving citations to a full shutdown of operations. The enforcement activities have increased since the passing of the Electronic Signatures in Global Commerce Act on June 30, 2000 (E-SIGN). This law eliminated legal barriers to the use of electronic technology to create, sign, and approve contracts, store documents, and send and receive notices and disclosures. Prior to this law only handwritten signatures or paper, microfilm, or microfiche records were considered 'legal'.

Summary

Many organizations today are either considering or are in the process of implementing an industry best practice, either to achieve internal business goals such as cost reduction, or to meet external demands or regulatory requirements. As this white paper has shown, there is a variety of best practices to choose from, and also a range of regulations that might affect a company.



Regardless of the type of process to be implemented, all implementations assume some sort of improvement over the current situation, so all methodologies require a way to measure and evaluate whether the effort taken is truly resulting in an improvement against the objectives set. The more automated this process of measurement and evaluation, the more accurate its results.

Best practices offer various ways to help organizations comply with regulations, especially when they share the same objectives (see the figure above in this section). Some of the relationships are obvious, for example COSO and SOX are both endorsed by the SEC. Other relationships, such as between ITIL and SOX, are less direct. Lacking SEC guidance for the IT audit in SOX, CIOs have turned to existing IT frameworks, including ITIL, to ensure that processes for supporting financial data are in place and effective—but the best practices in ITIL support only some of the processes required by SOX. SOX is about assessing risk, and while risk assessment is an element of ITIL, it isn't the framework's primary focus. Other frameworks, including ITIL and COBIT, can help companies put in place general controls for IT, but this is much broader than the narrow scope required by SOX, which only requires that companies establish controls over systems relating directly to financial reporting.

Best practices are often complementary, so implementing one best practice can make it easier to implement another. For example, to improve the overall level of IT service to the business, an organization might decide to implement ITIL. If the enterprise is doing its own development, then it needs to align service creation (development) with delivery—its operations. Within the ITIL framework most of the development is done within release management, which requires various types of information, such as the application components and their interdependencies, the planning of the releases of the service, and the required scripts to run before or after deployment. To achieve this, a process needs to exist within service creation as well. This is where CMM comes in: the service creation team should operate in a way similar to the principles of level 3 within CMM.

This white paper provides a basic introduction to key methodologies, best practices, and regulations. Subsequent Serena white papers will explore how to implement industry best practices and apply technology to visualize, orchestrate, and enforce processes so that organizations can more effectively comply with regulations and benefit from best practices.

References

www.govtech.net/magazine/channel_story.php/96490
www.serverwatch.com/tutorials/article.php/2198721
<http://it.safemode.org/>
www.isaca.org/
www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr012.pdf
www.sei.cmu.edu/cmml/
www.tc.umn.edu/~hause011/article/Capability_maturity_models.html
www.cio.com/archive/030104/cmm.html
www.isixsigma.com/
www.iso.org/iso/en/ISOOnline.frontpage
www.iso.org/iso/en/prods-services/otherpubs/pdf/survey2004.pdf
www.federalreserve.gov/generalinfo/basel2/default.htm
<http://itresearch.forbes.com/rlist/term/Basel-II.html>
www.dtic.mil/ndia/systems/Ferguson2.pdf

www.bna.com/webwatch/basel.htm
www.systemexperts.com/tutors/sas70.pdf
www.coso.org
www.hci.com.au/hcisite2/toolkit/pdcacycl.htm
www.sei.cmu.edu/ideal/
www.sas70.com/
www.isixsigma.com/offsite.asp?A=Fr&Url=http://www.sei.cmu.edu/pub/documents/94.reports/pdf/tr12.94.pdf
www.s-oxinternalcontrolinfo.com/pdfs/CRAReport%20-%20404%20Final.pdf
www.pcaobus.org/
www.strategyassociates.cc/articles/hottopics/sixsigma/SixSigmaISO9000.html
www.bitspi.com/newsletter/vol5iss2.htm
www.itil.co.uk/
www.itsmf.com
www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

ABOUT SERENA

Serena Software, the Change Governance™ leader, helps more than 15,000 organizations around the world—including 96 of the Fortune 100 and 90 of the Global 100—turn change into a business advantage. Serena is headquartered in San Mateo, California, and has offices throughout the U.S., Europe, and Asia Pacific.

CONTACT

Learn more about the enterprise-wide power of Serena Industry Best Practices by visiting www.serena.com or contacting one of our sales representatives in your area.

Serena Worldwide Headquarters

Serena Software, Inc.
 Corporate Offices
 2755 Campus Drive
 Third Floor
 San Mateo, California 94403-2538
 United States

800.457.3736 T
 650.522.6699 F
info@serena.com

Serena European Headquarters

Serena Software Europe Ltd.
 Hertfordshire
 Abbey View Everard Close
 St. Albans
 Hertfordshire AL1 2PS
 United Kingdom

+44 (0)800.328.0243 T
 +44 (0)1727.869.804 F
ukinfo@serena.com

Serena Asia Pacific Headquarters

Serena Software Pte Ltd
 360 Orchard Road
 #12-10
 International Building
 Singapore 238869

+65 6834.9880 T
 +65 6836.3119 F
apinfo@serena.com

