NAI
Nouri Associates Inc.
"where experience counts"

Technology Solutions for Regulatory Compliance

"How to Reduce the Cost of Compliance"

Change and Release Management Processes

July 2005

Author: Hamid Nouri
1 (888) 556-3618 Ext. 612

Compliance Research White Paper – ITIL Focus Series

Table of Contents

1.0 Executive Summary

Regulatory compliance is having a profound impact on how organizations manage risk and exercise due care going forward. For many, the administrative burden will be unbearable. For organizations in highly regulated industries such as financial services, healthcare and telecommunications managing compliance with diverse regulatory requirements from a number of national and international sources is extremely expensive and is starting to affect the available budget for legitimate business opportunities that can help the organization compete more effectively within its industry.

In the last five years, we've observed substantial discussions on impact of regulations, driven largely by the U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002. Other regulations with a significant impact include:

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,
- The Gramm-Leach-Bliley Financial Services Modernization Act,
- The New Basel Capital Accord (Basel II),
- Title 21 Code of Federal Regulations (21 CFR) Part 11, and
- The Health Insurance Portability and Accountability Act (HIPAA)

These regulations and a number of others will increasingly expose IT operations to a variety of interested stakeholders.

This white paper will discuss the impact of the regulatory requirements on local and global organizations, whether organizations can afford to ignore or delay compliance with the new regulatory demands, and how IT organizations can best support the compliance initiatives using their engineering know-how, technology tool box, and relationship management skills.

2.0 Compliance Challenges and Best Practices

Many of the recent regulations demand that the IT environment be able to provide evidence of its own integrity, maintain audit trails associated with change and security, and identify accountability associated with “material” IT systems. The new laws and regulations will require intense enterprise attention to understanding and managing the components that make up the IT environment, as well as alterations to that environment, increasing the demands made on IT operational groups' capabilities.

Some of the most common regulatory challenges include:

- Consequence of non-compliance (prison, heavy fines)

- Multiple rule sources (SEC, EU, FDA, Feds, etc.)
- Monitoring responsibilities associated with the regulations
- Ongoing responsibility for testing
- The perpetual nature of regulations.

Some of the best practices in achieving compliance include:

- Establishing an enterprisewide compliance office or officer
- Developing clear communication channels and protocols
- Filing electronically, whenever possible
- Involving as many stakeholders as you can, including regulators
- Leveraging technology to manage content, events, tasks and approvals
- Selection of comprehensive control frameworks
- Senior Management to lead by example and set the tone

3.0 Sarbanes-Oxley Overview

The Sarbanes-Oxley Act demonstrates firm resolve by the US Congress to improve corporate responsibility. The Act was created to restore investor confidence in US public markets, which was damaged by business scandals and lapses in corporate governance. Although the Act and supporting regulations have rewritten the rules for accountability, disclosure and reporting, the Act's many pages of legalese support a simple premise: good corporate governance and ethical business practices are no longer optional niceties.

The Sarbanes-Oxley Act has fundamentally changed the business and regulatory environment. The Act aims to enhance corporate governance through measures that will strengthen internal checks and balances and, ultimately, strengthen corporate accountability. However, it is important to emphasize that section 404 does not require senior management and business process owners merely to establish and maintain an adequate internal control structure, but also to assess its effectiveness on an annual basis. This distinction is significant. The following is a high level overview of SOX implications:

- Holds the CEO and CFO personally responsible for restatements due to misconduct
- Imposes new obligations and responsibilities on audit committees
- Requires process control and documentation
- Strengthens penalties for corporate fraud
- Requires rules to address securities analyst conflict of interest.

Figure 1. SOX – Who Is Responsible For What

Section 302: Ultimate responsibility	*What:* Sign accounts, ensure accuracy and disclose anomalies *Who:* Board of Directors, CEO, CFO
Section 204: Penultimate responsibility	*What:* Understand controls, test and attest *Who:* External auditors and audit committee
Section 103: Standards	*What:* Demonstrate compliance with accounting standards, identify gaps and remediate *Who:* Auditors, CIO, chief counsel and compliance officer
Section 404: Report on internal controls	*What:* Process control, automation and documentation *Who:* IT managers, internal auditors, Controller, process specialists and IT systems
Section 409: Rapid disclosure	*What:* Operations, financial reporting and compliance *Who:* Accountants, controllers, records managers, security and IT managers

Source: Gartner

Sarbanes-Oxley was fashioned to protect investors by requiring accuracy, reliability, and accountability of corporate disclosures. It requires companies to put in place controls to inhibit and deter financial misconduct. And it places responsibility for all this – unambiguously – in the hands of the CEO.

Section 404 is concerned with the general controls that maintain the integrity of processing and reporting of financial data. Any process or system that could influence the integrity of transaction processing or data must be examined, and controls must be in place to ensure overall process and system integrity. A company's financial reporting processes rely on financial applications, which rely on computer systems. Many different systems, in different parts of the organization, can materially affect financial reporting.

Human resources, payroll, inventory, accounts payable, accounts receivable, purchasing, order entry and custom applications are all common, and often independent, systems that can materially affect major financial accounts. In today's highly automated business environment, IT-related risks and controls must be considered in any overall evaluation of internal control over financial reporting. The Public Company Accounting Oversight Board (PCAOB), which was established by the Sarbanes-Oxley Act to oversee the audits of public companies, specifically mentions the importance of IT systems and IT general controls in its auditing guidelines dated March 9, 2004. Because external auditors will follow PCAOB guidelines during the audit process, companies need to document and evaluate the IT systems and controls that contribute to the financial reporting process. A

company cannot pass an audit and demonstrate control of its financial reporting process without control of the underlying systems.

3.1 What is Internal Control?

Internal control is broadly defined as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

For those organizations that have begun the compliance process, it has quickly become apparent that IT plays a vital role in internal control. Systems, data and infrastructure components are critical to the financial reporting process. PCAOB Auditing Standard No. 2 discusses the importance of IT in the context of internal control. In particular, it 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.

3.2 Consequence of Non-Compliance

In some organizations there is a view that SOX is fundamentally a set of regulations that have to be complied with and provided IT Directors and CIOs 'check the various boxes' SOX compliance is assured. This is a perilous position because SOX is different from other forms of regulations in a number of ways:

1. External people such as auditors and regulatory bodies check to ensure that controls are in place not only on paper but are being used as well.
2. This legislation has significant penalties and fines built into it. CEOs and Finance Directors can be fined up to $20 million and serve up to 10 years in prison under the Act.
3. Material weaknesses have to be reported publicly in financial statements, the impact on share prices for non-compliance with SOX is hardly likely to be positive.

Most organizations cannot afford to ignore or underestimate SOX.

4.0 Impact of Regulatory Compliance Mandates on IT

IT systems are the foundation for a cost effective and affordable compliance framework. Many of the necessary IT components (document management, content management, workflow management and IT service management) are in place in many organizations, however experience shows that they must be standardized and integrated across the enterprise. There must also be a repository that contains details of every process, internal controls and risk. Access to this content will ensure that everyone knows who owns each element and will facilitate the auditors' ability to quickly access the needed information while increasing their confidence in the controls in the environment.

IT systems must be able to deliver relevant compliance tasks to the appropriate owners. Therefore IT has a special responsibility to work with finance, internal audit and the CFO to reduce the compliance burden on the organization. This can be achieved by automating manual process controls and, over time, eliminating process controls by following a compliance architecture approach to create inherent system controls. In year one of SOX, a great majority of organizational controls involve manual operations. Most organizations have declared their intentions to automate these controls during the next several years. However, since there's no such thing as a comprehensive off-the-shelf compliance technology, the only way they'll be able to achieve this is by taking available technologies and integrating them to create a compliance infrastructure. The IT function must be able to lead the integration effort, because those appointed as chief compliance officers aren't likely to have IT backgrounds, or sometimes much experience as IT users.

Regulations, due to their necessarily broad scope, tend not to be very prescriptive. Regulators need to leave the requirements very broad to make them withstand the test of time and relevance. Any attempt to make them concise and detailed will make them obsolete before the ink on the page is dry. IT's support for the compliance initiatives will be greatly affected by this lack of specificity (Are we compliant yet?) and is exacerbated by the fact that the requirements are usually not defined by technologists. As a result, the IT community usually has varying interpretations of what constitutes compliance with a given regulation. In terms of Sarbanes-Oxley, everything in IT potentially impacts financial reporting. The key word in the regulations is "material," both individually and in aggregate. Therefore, to focus on those items that are material, IT organizations must be careful to refine their corresponding operational processes accordingly.

IT must proactively work with the regulatory affairs and internal audit to identify which regulatory requirements are relevant to the organization and to interpret those requirements in terms of the organization's comfort with documentation, risk and adherence to processes. These interpretations will drive the appropriate levels of technology support for the compliance initiative.

5.0 CIO's Role in Compliance Initiatives

CIOs can help business process owners determine their organizations' greatest areas of risk so they can be addressed first. Often, CIOs have led the organization's effort to determine the greatest areas of exposure through Business Continuity, IT Service Continuity or Project Portfolio Management initiatives. With these skills comes the ability to focus and champion the automation of internal controls and contribute significantly to reducing the organization's overall compliance burden. Other corporate stakeholders will tend to want a comprehensive solution involving every IT system, control and process.

In many organizations funding is a zero sum game. Resources directed to compliance efforts will reduce organization's resource to deal with other high priority requirements. The CIO must proactively work with business leaders to manage and contain the scope of compliance efforts so the IT organization only has to work on elements that relate directly to compliance requirements — for example, financial systems in the case of Sarbanes-Oxley. In some cases the investments in improving controls can result in operational cost savings and/or improvements in quality of systems. CIOs should be focused on identifying these opportunities and demand the right performance indicators for technology projects in support of compliance, and ask for verification of results from these investments.

If managed correctly, *compliance efforts can result in significant performance improvements in IT operations if they are combined or coordinated with IT process and service transformation initiatives using industry best practices*. This however is a challenging endeavor in that service transformation and changing organizational behavior is fraught with risks and challenges of culture change management. CIOs should be prepared to invest large amounts of managerial time to make this happen.

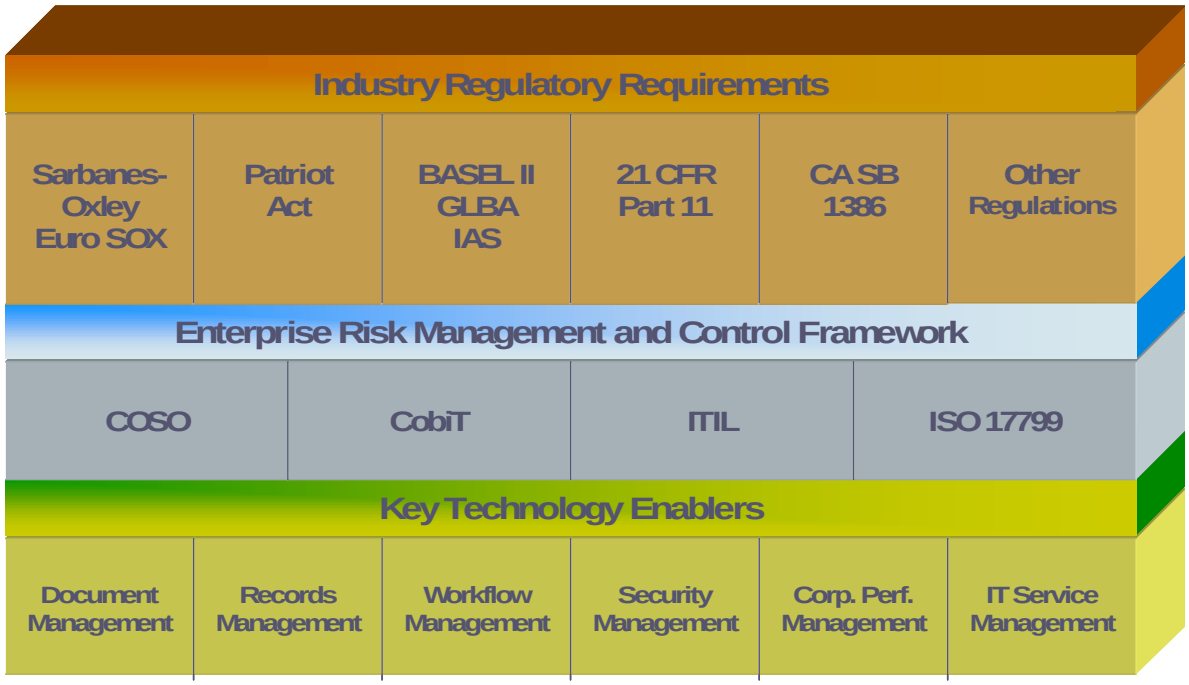
6.0 Compliance Management Architecture

Complying with the latest regulatory requirements does not have to be a burdensome one off activity. There are a number of common themes that run through most regulations. By using a Compliance Management Architecture framework organizations can save significant time and energy in meeting their compliance objectives.

A Compliance Management Architecture Framework enables a comprehensive approach to managing an organization's compliance efforts.

According to Gartner, "by 2006, public companies that do not adopt a compliance management architecture will spend 50 percent more annually to achieve SOX compliance (0.8 probability). Companies that choose one-off solutions to each regulatory challenge they face will spend 10 times more on compliance projects than their counterparts that take a proactive approach (0.9 probability)."

Figure 2. Compliance Management Architecture



6.1 Compliance Management Architecture Overview

Compliance Management Architecture is a set of internal controls for managing organizations. The recommended Architecture above focuses on IT and technology controls. There are four compatible frameworks within the Architecture:

- **COSO (Committee of Sponsoring Organizations' Enterprise Risk Management Framework)** – Scope is organization wide controls,
- **COBIT (Control Objectives for Information and Related Technologies)** – Satisfies and extends COSO controls related to Information Technology,
- **ITIL (Information Technology Infrastructure Library)** – Satisfies and extends COBIT controls relating to IT Service Management (Problem Management, Change Management, Release Management, etc.),
- **ISO 17799** – IT Security Controls to meet and extend COBIT Security.

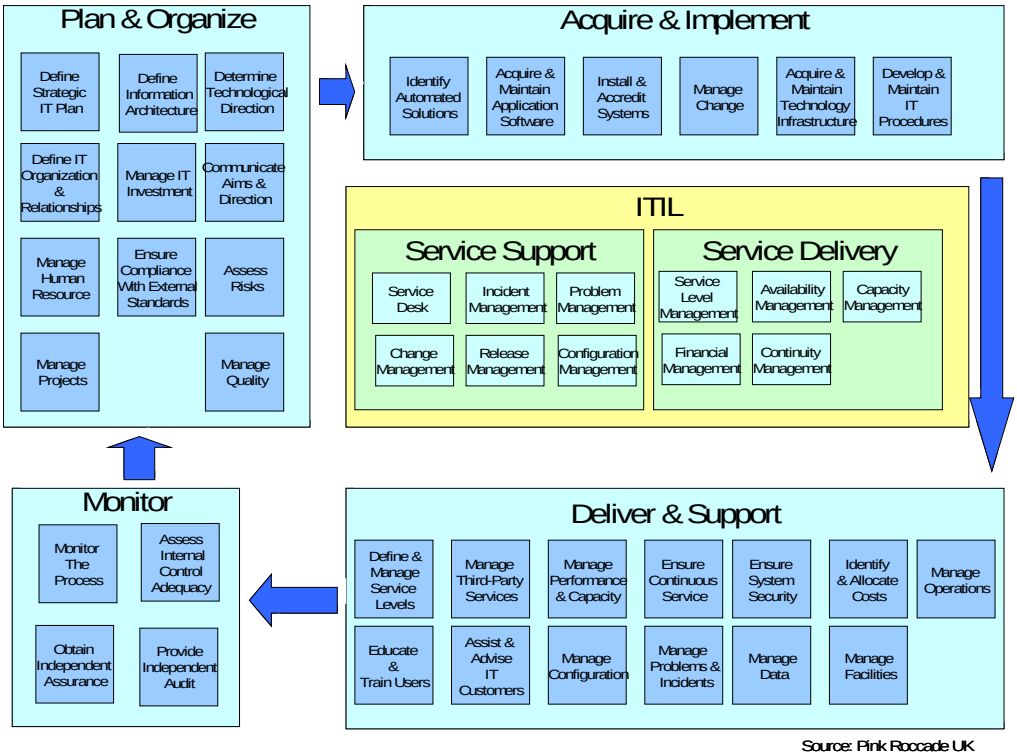
COBIT is based on established frameworks, such as the Software Engineering Institute's Capability Maturity Model, ISO 9000 and ITIL. However, COBIT does not include control guidelines or practices, which are the next level of detail. Unlike ITIL, COBIT does not include process steps and tasks because it is a control framework rather than a process framework. COBIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is auditors, senior business management and senior IT management.

COBIT and ISO 17799 health checks are used to determine current status and identify weaknesses in processes and controls. ITIL is used to improve IT processes and controls, and ISO 17799 is used to improve security processes and controls. ITIL is also used to determine technology requirements. ITIL can also assist in identifying possible organizational structures, roles and responsibilities. COBIT is used to assist in defining metrics and key performance indicators. In the U.S. COBIT has become the de facto standard for evaluating IT controls in support of SOX.

ITIL is based on defining best-practice processes for IT service delivery and support, rather than defining a broad-based control framework. It focuses on the method. ITIL has a narrower scope than COBIT because of its focus on IT service management, but it defines a more comprehensive set of processes within that narrower field of service delivery and support. ITIL is more prescriptive about the tasks involved in those processes and, as such, its primary target audience is IT and service management.

ITIL is strong in IT Operational processes, but is limited in security and application development. COBIT is strong in IT controls and IT metrics, but does not say how (i.e. process flows) to implement a process and is not strong enough in security. ISO 17799 is strong in security controls, but does not say how (i.e. process flows) to implement the specific processes. There are no contradictions or overlaps within the overall architecture and by combining the frameworks organizations are able to ensure comprehensive review of all critical control issues.

Figure 3. Role of COBIT and ITIL Within the Architecture



Source: Pink Roccade UK

There are 34 process domains defined within the COBIT framework as highlighted in the above graphics. Based on practical experience, there are 17 processes that have direct relevance to SOX compliance efforts:

Table 1. COBIT Processes Relevant to SOX Compliance Initiatives

Compliance Management Imperatives	COBIT Processes
Manage Operations	DS 2 — Manage third-party services DS 7 — Educate and train users DS 13 — Manage Operations
Manage Risk and Controls	PO 9 — Assess risks PO 8 — Ensure external compliance M1 — Monitor M2 — Assess internal control adequacy
Manage Reliability	DS 5 — Ensure system Security DS 10 — Problems and incidents
Manage Systems	PO 5 — Manage the IT investment AI 4 — Develop and maintain procedures DS 9 — Manage the configuration
Manage Change	PO 11 — Manage quality AI 5 — Install and accredit systems AI 6 — Manage change
Manage Records and Data	PO 2 — Define IT Architecture DS 11— Manage data

The technology enablers portion of the framework identifies key technology solution categories that are required for the overall compliance effort. In many cases these tools already exist in the current environment and have to be properly deployed in support of the standard processes or required support for the compliance effort. However in many cases organizations can greatly benefit from the acquisition and deployment of tactical and strategic tools and technology frameworks in support of their compliance initiatives.

6.2 Benefits of Compliance Management Architecture

There are a number of benefits to utilizing a Compliance Management Architecture:

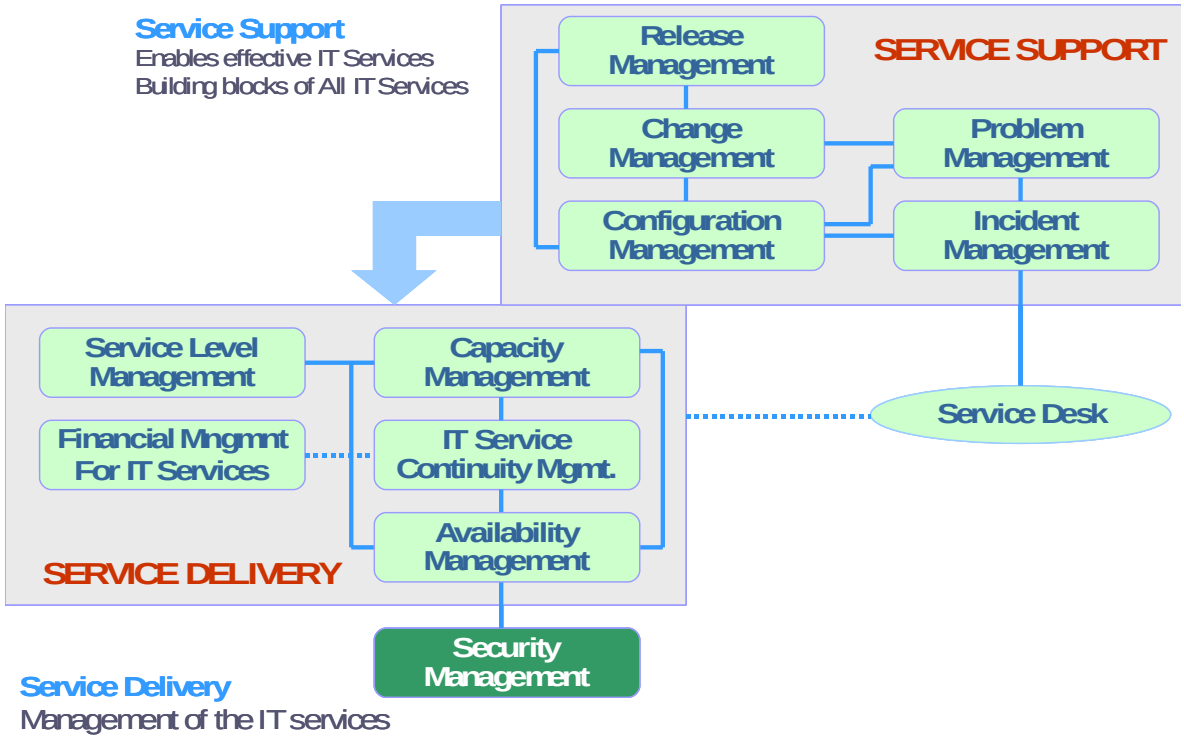
- Security and privacy regulations typically have common concerns and requirements
  - As much as 80% overlap in functional requirements
  - Therefore an organization can use one approach for all

- Compliance Management Architectures are based on standard auditor recommendations and regulator expectations
  - "Here's what we'd like to see..."
- Compliance Architecture strategy can be based on industry best practices
  - Industry best practices have been tried and tested in many organizations
  - Efficient and effective (can result in competitive advantage)
  - Support materials available off the shelf
    - Procedures, policies, role descriptions
    - Don't have to spend staff and management time creating equivalent processes.

7.0 Role of ITIL in Achieving Compliance

IT Infrastructure Library (ITIL) was developed by the Central Computing and Telecommunications Agency for the U.K. government and is now part of the Office of Government Commerce (OGC). It offers a set of best practices in 11 service delivery and IT service support areas, including Service Level Management, Financial Management, Capacity, Availability and Service Continuity Management, Service Desk, Incident Management, Problem Management, Change, Release and Configuration Management.

Figure 4. IT Infrastructure Library Framework



Primary motivation for the development of the framework came from the OGC, which wanted process standards that all government agencies could use to manage their complex IT worlds. However, a government's requirements do not necessarily reflect those of the commercial world. To address this, OGC put together a working relationship with various non-government groups and organizations to test and modify ITIL. From this, a nonprofit foundation and review board, IT Service Management Forum (itSMF), was created. ITIL has now been consolidated into seven books that provide guidance around successful deployment of ITIL in an organization. The primary process framework is covered in 2 of these books, Service Delivery and Service Support.

ITIL provides best practices guidance on how to implement the General IT Controls required by COSO within the IT infrastructure. It prescribes a specific definition and scope for each of the Service Delivery and Support process domains, and identifies key activities, roles and responsibilities for all stakeholders involved.

In the next section we will take a deeper look into the Change and Release Management processes as defined by ITIL. Change and Release Management are a critical part of the General IT Controls required by the COSO framework. These two domains are generally a very challenging area for organizations to standardize and automate, in light of the growth of more sophisticated next generation Web and Composite applications.

8.0 ITIL Change and Release Management

Managing Change is one of the key process domains and control objectives required by the COBIT framework. Poor Change and Release Management processes are the root cause of many production related problems experienced by corporations worldwide. Over a number of years, we have found that in more than 80% of engagements where service availability and reliability is the issue defined by the client management team, poor change and release management processes have been directly responsible for somewhere between 30-40% of problems experienced in production. SOX is now mandating that organizations demonstrate due process and adequate controls on how changes to financial reporting and supporting application systems and IT infrastructure are handled within the environment. ITIL guidance around the role of Change and Release Management, and the best practices for defining and controlling the process in the organization will enable enterprises to effectively address this requirement.

8.1 Goal of ITIL Change Management

Changes can arise as a result of Problems, but many Changes come from proactively seeking business benefits such as reducing costs or improving services. The goal of the Change management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization.

Effective response to a Change request entails a considered approach to assessment of risk and business continuity, Change impact, resource requirements and Change approval. This thorough approach is essential to maintain a proper balance between the need for Change against the impact of the Change. It is particularly important that Change Management processes have high visibility and open channels of communication in order to promote smooth transitions when Changes take place.

8.2 Goal of ITIL Release Management

Many service providers and suppliers may be involved in the Release of hardware and software in a distributed environment. Good resource planning and management are essential to package and distribute a Release successfully to the Customer. Release Management takes a holistic view of a Change to an IT service and should ensure that all aspects of a Release, both technical and-non-technical, are considered together.

The goals of Release Management are:

- To plan and oversee the successful rollout of software and related hardware
- To design and implement efficient procedures for the distribution and installation of Changes to IT systems
- To ensure that hardware and software being changed is traceable, secure and that only correct, authorized and tested versions are installed
- To communicate and manage expectations of the Customer during the planning and rollout of new Releases
- To agree the exact content and rollout plan for the Release, through liaison with Change management
- To implement new software Releases or hardware into the operational environment using the controlling processes of Configuration Management and Change Management – a Release should be under Change Management and may consist of any combination of hardware, software, firmware and document Configuration Items (CIs).
- To ensure that master copies of all software are secured in the Definitive software library (DSL) and that the Configuration management database (CMDB) is updated
- To ensure that all hardware being rolled out or changed is secure and traceable, using the services of Configuration Management.
- The focus of Release Management is the protection of the live environment and its services through the use of formal procedures and checks.

Release Management works closely with the Change Management and Configuration Management processes to ensure that the shared CMDB is kept up-to-date following Changes implemented by new Releases, and that the content of those Releases is stored

in the DSL. Hardware specifications, assembly instructions and network configurations are also stored in the DSL/CMDB.

Today, in many organizations, the process for handling change requests and change deployment for application systems and infrastructure are very much an inconsistent, manual and laborious set of processes. Most IT organizations are overwhelmed with the volume of changes thrown at them continuously. Web-enabled applications and next generation Composite Applications that are designed by combining multiple legacy, new and off-the shelf applications further exacerbate the problem for many organizations.

If there is a Change Advisory Board (CAB) in place, it is very difficult for the participants to understand and comprehend the nature and the impact of changes being proposed. It is usually the problem investigation conducted after a failure in production that reveals the true impact of the change that was authorized. For many the Release Management process itself is the source of some of the problems experienced in production. Again, the statistics show that over 30-40% of production related issues are due to poor change and release management processes. Consequently there is a great need and opportunity for standardizing these processes using the ITIL best practices framework and leveraging technology to automate these two critical process areas.

9.0 Technology Solutions for Change and Release

A number of technology vendors offer life cycle function tools for server provisioning, application provisioning, modeling and repurposing. There is no single tool that fully automates the entire lifecycle of changes across a heterogeneous IT infrastructure. However a number of vendors have started to combine key functionality around automated provisioning with robust workflow and auditing capabilities to deliver a more comprehensive solution for SOX compliance initiatives.

The key features and functionality to look for in solutions that automate the Change and Release Management processes include:

- Automated aggregation, packaging and deployment
- Automated rollback of production environment to a known good state
- Robust workflow engine
- Capturing audit trail of all approvals
- Deployment Logs & Reporting
- Email notification for testing and approval
- Integration with Service Desk
- Support for any source(s) to any destination(s) deployment
- Support for Record Retention

- Synchronization of code and content for Web applications and infrastructure
- Version runtime web applications

Vendors approach the market from a number of different angles. Some are focused on automated server provisioning and configuration management, others focus on Application Provisioning, yet a third category primarily focuses on robust patch management functionality. Multi-platform or Windows only support is another key differentiator. Some of the vendors with credible and proven offerings in this segment include:

- BladeLogic
- BMC
- HP
- IBM
- Interwoven
- Opsware
- Sun
- Veritas
- and a number of other specialist players.

One of the critical success factors for Change and Release Management processes is the concurrent deployment of a Configuration Management initiative which encompasses the use of automated solutions that enable the Change Management process to evaluate the impact of a proposed change on all the components of an IT Service. A number of innovative startups have started to offer tools to enable this capability.

9.1 Benefits of Deploying Technology Solutions in Change and Release

Besides the obvious benefit of achieving compliance, there are a number of other benefits that can be had by deploying the right technology solutions focused on specific pain points:

- **Cost Savings** – Organizations have reported savings in the range of 30-50% compared to a manually controlled Change and Release Management processes,
- **Increased Customer Satisfaction** – Our clients report observable increases in customer satisfaction due to improved communication and collaboration amongst internal and external stakeholders,

- **Production Environment Stability** – A 15-20% decrease in the number of change related incidents in the production environment,
- **Reduction in Deployment Time** – Many organizations report their lead time to production deployment and time in the queue being cut by 50 to 70% after implementation of best practices supported by automation,
- **Support for Corporate Quality Initiatives** – Organizations can use their technology tool set to support their internal corporate quality initiatives such as Six Sigma, TQM, Operational Excellence, and others by optimizing their continuous process improvement initiatives.

10.0Conclusion

Compliance efforts are costly and ongoing endeavors that can create a significant administrative burden for the organization. A siloed and independent approach to each of the regulations affecting an organization will further exacerbate this problem. Through the use of a Compliance Management Architecture organizations can take a holistic and efficient approach to their compliance efforts.

COBIT and ISO 17799 are effective frameworks for evaluating an organization's internal IT controls. ITIL provides prescriptive guidance for implementing best practices in IT infrastructure operations. Standardized Change and Release Management are the foundations for effective internal controls and IT Operations. It is imperative that organizations address these two processes in early stages of any compliance effort. Organizations can gain significant benefits by leveraging technology solutions to help automate their Change and Release Management processes.

11.0About NAI

Nouri Associates, Inc. (NAI) is an international Information Technology Management Consultancy based in Northern California. NAI focuses on solving challenging IT related issues faced by an organization's senior management team. We specialize in providing highly experienced and expert talent to their global client base in a number of key practice areas such as IT Strategic Planning, IT Service Transformation, Compliance and Risk Management, Enterprise Architecture, IT Optimization and Sourcing Strategies.

Nouri Associates, Inc.
One Embarcadero Center Suite 500
San Francisco, CA 94111
Voice: (888) 556-3618
Fax: (415) 267-6127
Email: info@nouriassociates.com
http://www.nouriassociates.com/