WHITE paper

Keeping Up Your SOX Compliance

And Turning IT into a High Performer by Improving Change Control

By Dan Swanson

Forward

Organizations are exposed to governance, compliance and ethical risks daily. Coupled with the current economic, regulatory and social climate, these risks have propelled corporate governance, compliance management, and information security to be key business priorities.

Tripwire is the world's leading change auditing software vendor. The company has a clear mission: helping organizations gain control over IT. Tripwire's enterprise-strength change auditing solutions lower the risk of regulatory violations, business disruptions, security breaches, and loss of customer confidence. Tripwire software reduces operational risk and ensures the security and availability of your networks. By establishing a baseline of data in its desired state, and detecting and reporting changes to that baseline, Tripwire ensures rapid discovery and remediation when an undesired change occurs. Over time, by using Tripwire, stretched IT staffs gain increased visibility and control over change and establish a foundation for stable IT operations and systems security.

It gives me great pleasure to publish this new white paper to help you improve your governance practices and to get "IT under control."This paper provides guidance to improve your Sarbanes-Oxley program efforts and highlights key information on Tripwire and to the many ways we can support your efforts.

Regards,

Gene Kim
CTO, Tripwire

Executive Overview

Sarbanes-Oxley Program Efforts Must be Sustainable

The Sarbanes-Oxley Act (SOX) has significant information security implications for companies governed by the regulation. Sections 302, 404 and 409 of SOX, and corresponding SEC Rules and Regulations, have tremendous ramifications for information technology (IT) in the areas of control (internal controls), evaluation (governance, measurement and recordkeeping), and disclosure (reporting and certification). These "control, evaluate and disclose" elements must work together as integral parts of the SOX compliance process. To meet the challenges of SOX compliance, companies need to adopt changes to corporate governance and a process of change auditing.

Achieving Control of IT

IT is pervasive in today's world. These days, an effective IT solution is required for every key organizational initiative. The IT solution (i.e., its design) is also one of the key cost drivers that will impact long term success. Therefore, the IT infrastructure and its suite of applications has become a prized corporate asset that must be managed (controlled) and "protected".

In 2000, Gene Kim and Kevin Behr began a long term research effort to develop a clear understanding of what makes certain organizations "high-performers". They studied high-performing IT operations and security organizations to understand their processes and implementations. As a result, the Visible Ops methodology was developed.

The Visible Ops Handbook: Implementing ITIL® in 4 Practical and Auditable Steps reflects the lessons learned about how leading organizations work and describes a control-based entry point into the world of ITIL. Organizations can use Visible Ops to springboard their own process improvement efforts.

In order to understand how high-performing organizations manage IT and achieve their business objectives, the IT Process Institute conducted the IT Controls Performance Study in the Fall of 2005 (**www.itpi.org/home/performance_study.php**). The goal was to identify the unique practices of top performing organizations, and determine the operational improvements enabled by IT control activities.

These high performing IT organizations, representing 13% of the study respondents, support and deliver:

- 8x more projects
- 5x more applications and software
- 5x more IT services
- 7x more business IT changes
- and overall better security measures spanning loss, detection, correction and prevention

Consequently, these organizations have higher user satisfaction and their IT budget is 3x higher than their industry counterparts.

The top two controls that were almost universally present in the high performers were:

- Monitoring systems for unauthorized changes
- Having defined consequences for intentional, unauthorized changes

When looking beyond the controls and metrics analyzed in the ITPI study and into the generally acknowledged practices, here's how the high performers really set themselves apart:

1. They place significant emphasis on their change management process. In fact, high performers see their change management as a key capability that makes them high performers.

2. They place high value on understanding why change happened and what exactly happened. In order to do this, they monitor, audit, and document all changes to the infrastructure.

3. They consider the only acceptable number of unauthorized changes in a change management system is ZERO. We've heard time and time again that high performers recognize that they are only one change away from being a low performer and that unauthorized changes can have catastrophic impact if they're left unattended.

4. They send the right cultural message within the organization, implement the right controls to hold people accountable for adhering to policies, and exercise appropriate disciplinary actions for non-compliance.

5. They test all changes in a preproduction environment. This discipline fosters introducing changes into the production environment in a reliable, predictable manner.

6. They have established ways of analyzing the impact of IT change before and after it occurs, allowing them to deal with incidents more effectively.

7. They track and analyze change successes and failures to capture lessons learned, share best practices, and prevent recurrence of an undesirable change incident.

A Compelling Business Case for Change Management

There is a substantial and growing body of evidence that "change management" is a key success factor in the implementation of efficient, effective and secure IT Operations. Because every "IT risk" creates some degree of business risk, it is important that executives thoroughly understand change management issues.

Change and patch management is defined here as the set of processes executed within the organization's IT department and designed to manage the enhancements, updates, incremental fixes and patches to production systems. These include:

- Application code revisions
- System upgrades (applications, operating systems, databases, etc.)
- Infrastructure changes (servers, cabling, routers, firewalls, etc.)

Collectively, most organizations refer to these as "IT changes." All organizations have to deal with IT changes effectively, because technology is an integral part of business. When changes fail or are poorly controlled, the impact on the business can range from minor inconvenience to events that hinder the achievement of business objectives, including the ability to comply with the growing body of regulation.

Poor Change Management can be Identified Quickly

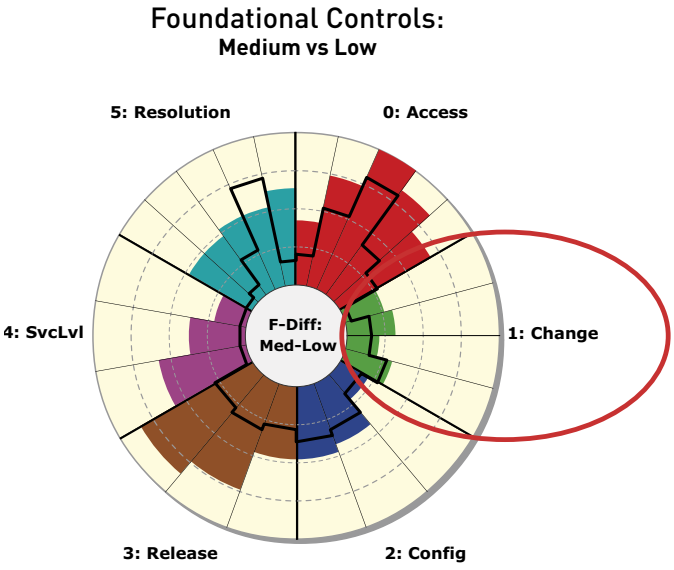
The IIA change management guide was developed to help auditors and managers ask IT organizations the right questions to assess their change management capability. To help you quickly assess the overall level of process risk and determine whether a more detailed process review may be necessary, this guide also provides expected answers to these right questions.

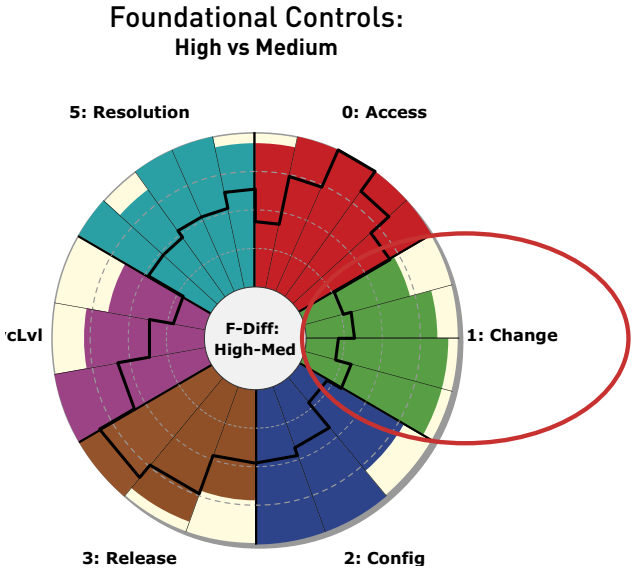
The Top Five Risk Indicators of Poor Change Management:

- Unauthorized changes (above zero is unacceptable)
- Unplanned outages
- Low change success rate
- High number of emergency changes
- Delayed project implementations

Moving IT From Good to Great

The IT Controls Performance Study by ITPI reveals some interesting results. Key findings indicate that a set of 21 control activities, what the ITPI calls Foundational Controls, have the broadest impact on key performance results.





We Need to Take a Long-Term View Regarding IT Controls

Change has become the business norm and improving your IT solutions has become a business priority. To achieve compliance in today's business environment, we need to have effective IT control. To achieve such control, enforcing change policy with change auditing has become an absolute necessity.

Organizations also need to develop ways to keep the assessment of internal controls current over time. In fact, according to SOX 302, the evaluation process must be conducted at least quarterly. This requires that IT be involved in the day-to-day SOX compliance efforts. If your internal controls are established with the appropriate tests and you have change auditing in place to ensure that controls are operating as intended, then you are well on your way to a sustainable compliance environment.

Implementing robust change management practices has numerous benefits. These include the strengthening of IT Operations and information security programs, and perhaps most important, ensuring management can demonstrate to the board and key stakeholders that they are serious in achieving "operational excellence" and in implementing strong governance practices. Over time, achieving these goals helps create a strong competitive advantage.

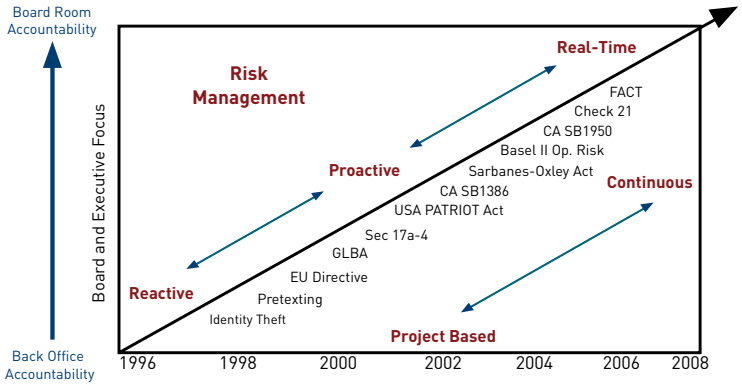
Chapter 1 – History

"Quality is not a sprint; it is a long-distance event." — DANIEL HUNT

Governance, compliance, and information security practices have been "ramping up" for many years. At the turn of the century, significant and massive failures in financial reporting and governance practices in general created the need for sustainable improvement and made it a number one business priority. Improving compliance programs became paramount. Efforts to do so included enhancing ethics efforts and results; establishing a formal "Whistle-Blower Hot-Line;" increased auditing of financial reporting, disclosures and IT controls in general; and implementing sound governance practices.

The Compliance Decade

The passage of information security and technology laws and rules over the past 10 years has affected most industries and companies. The "Compliance Decade" chart shows a graphical summary of the number of laws that have been passed that require today's corporations to adopt a culture of operational excellence. In response to these laws, management must be more accountable and aware of the need for a continuous and proactive operational risk management environment that recognizes the links between its technology infrastructure, business processes, reputation, compliance, and internal controls. This decade of heightened compliance is driving major corporate initiatives for greater transparency, governance, accuracy and accountability throughout the enterprise. Each company must identify, track and validate all business processes to ensure that its operations are compliant.



The Compliance Decade

SOX Year 1 – The Rush to Compliance

The insight provided below was taken directly from CICA's Information Technology Advisory Committee paper entitled *The Role of Information Technology in Sustained Regulatory Compliance (2006)*.

"For many organizations, Year 1 of SOX can perhaps be referred to as 'the rush to compliance.' The principal objectives, at least initially, were to complete the assessment of the company's internal control over financial reporting as well as of disclosure controls and procedures, to complete any necessary remediation activities in time to allow management to assert the effectiveness of controls, and to permit the company's external auditor to reach an opinion that supported both management's assertion of control effectiveness as well as its assessment process. For many, 'success' was defined as management's ability to assert that controls were operating effectively and as the external auditor's ability to issue a clean audit opinion.

"In this 'rush to compliance' decisions may have been made to maximize the likelihood of achieving short-term "success" with comparatively less focus on the consequences of these decisions on overall costs or the longer-term efficiency and effectiveness of these activities. For example, 'certification project management offices' and 'certification project teams' were established, typically leveraging external consultants, to develop the documentation, identify and assess the controls, and test them for effectiveness. For the sake of expediency, and in the absence of proven automated solutions, these teams may have captured this corporate knowledge using first-wave tools with which they were already familiar, such as word processors and spreadsheets. Often there was simply no time to investigate or develop more robust knowledge-management solutions, and to train the teams of consultants on how to use them. As a consequence of this initial focus on achieving 'success,' in many cases the solution implemented may have been sub-optimal. While for the most part the initial objective of Year 1 compliance was achieved, the process has created a number of problems as we look forward to Year 2 compliance and beyond."

Operational Excellence Needs to be a Way of Life

With the increased privacy and security awareness among consumers, businesses and our elected officials, traditional best practices are being incorporated into new laws and regulations that define higher operating, security, and risk management standards for organizations. Industry best practices of yesterday are being replaced with legal mandates for ensuring that most organization's corporate governance, internal controls, network infrastructure, business processes, and operations are safe, sound and secure. New laws and regulations now dictate how businesses must govern, work, communicate and securely interact throughout the organization and with external parties such as customers and strategic partners. Such mandates impose obligations on Directors and Senior Executives to ensure prudent governance, security, business processes, and controls are established.

Operational excellence is no longer just a prudent business decision. It now needs to be a way of life.

Chapter 2 – Overview of SOX

SOX requires publicly held companies to implement internal controls over financial reporting (ICFR), to evaluate the strengths and weaknesses of these internal controls in official documents filed with the SEC and to make regular disclosures concerning the viability of these controls and potential fraud or losses that may affect the company's financial position. Because most companies' financial reporting and operations depend heavily on IT, and because many corporate assets now exist in the form of critical data, SOX has significant information security implications for companies governed by the law.

SOX was Passed to Re-establish "Accountability" and Restore Investor Confidence

Responsibility, penalties, enforcement and deadlines—the drafters of SOX sought to ensure enforceability. To that end, the law contains significant penalties, an international scope, and strict deadlines. The pattern of compliance prosecutions by the SEC prior to SOX demonstrates that the law will likely become the basis for a growing number of SEC prosecutions.

The question "Who's responsible?" is often the first one asked when a new law is passed. SOX places compliance responsibility squarely at the highest levels: the CEO and the CFO. The internal controls, evaluation and disclosure requirements under 302, for example, are required to be certified in writing by no less than the principal executive officer and principal financial officer of the company. These are also the officers that face the stiffest penalties and to date have been the targets of most SEC prosecutions.

This responsibility does not stop at the U.S. borders. The law extends to overseas operations of companies publicly traded on U.S. exchanges. The internal controls required by SOX must be implemented worldwide for affected companies, which may prove challenging for some organizations given cultural and legal differences overseas.

Section 302 is to Improve Quarterly Financial Reporting Disclosure

Perhaps the most talked-about requirements of SOX are the ones related to internal control over financial reporting. Section 302 of SOX and the SEC Regulations that were passed to implement it require corporations to put into place strong internal controls over financial reporting and disclosure controls. Specifically, Section 302 requires a company's CEO and CFO to certify in quarterly and annual reports to the SEC that:

- They are responsible for establishing and maintaining internal controls;
- They have designed internal controls to ensure that material information [about the company and its subsidiaries] is made known to them;
- The financial report does not contain any untrue statement of a material fact or omit to state a material fact ;
- The financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations;
- They have disclosed to the auditors and the audit committee all significant deficiencies and material weaknesses in internal controls and fraud that involves management or employees with a significant role in internal controls; and
- They have indicated in the report whether or not there were significant changes in internal controls.

Although this sounds complicated, it boils down to creating a process to ensure that top management receives truthful information about the company's finances, operations, control deficiencies, and fraud from subordinates and reports it to the SEC. The goals are to: (a) ensure that financial results reported to shareholders are accurate, and; (b) place responsibility for ICFR and disclosure controls on top management.

Section 404 is to Improve Financial Reporting

Section 404 of Sarbanes-Oxley required the SEC to develop and publish rules for management to assess ICFR and for external auditors to render an opinion on this assessment. Those rules were completed in June 2003, and the PCAOB followed with its Auditing Standards (AS) 2, which was approved by the SEC in June 2004.

Together, they require that:

- Management performs a formal assessment of ICFR, including testing to confirm both the design and operating effectiveness of the controls.
- Management include in its annual report on Form 10-K an assessment of ICFR.
- The external auditors provide three opinions as part of a single integrated audit of the company, instead of the one previously provided. This includes:
  — An opinion on management's assessment
  — An independent opinion on the effectiveness of the system of ICFR
  — The traditional opinion on the financial statements

The SEC rules are worth reviewing carefully. They "require a company's annual report to include an internal control report that contains:

- A statement of management's responsibility for establishing and maintaining adequate ICFR for the company.
- A statement identifying the framework used by management to conduct the evaluation of the effectiveness of ICFR.
- Management's assessment of the effectiveness of the company's ICFR as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's ICFR is effective. The assessment must include disclosure of any "material weaknesses" in the company's ICFR identified by management. Management is not permitted to conclude that the company's ICFR is effective if there are one or more material weaknesses in its ICFR.
- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's ICFR."

Sarbanes-Oxley Section 404: A Guide for Management by Internal Control Practitioners published by The IIA is based on "lessons learned" by internal auditors and other control practitioners, and reflects the latest SEC and PCAOB guidance.

The final rules also require a company to file, as part of the company's annual report, the attestation report of the registered public accounting firm that audited the company's financial statements.

SOX Efforts Must be Cost Effective, Risk-Based, Business Driven

An organization's SOX compliance efforts must meet the requirements of the Act and the rules set by the SEC and PCAOB. The SOX program must also be driven by management and the board (not the external auditor) and reflect the risks facing the organization. That is, SOX efforts should reflect the organization's strategic goals and objectives, as well as ensure accurate financial reporting, and transparent and timely disclosures.

Many "lessons learned" resulted from the first year's implementation of SOX. Numerous public roundtables were held, such as ones held by the SEC and PCAOB (see their web sites for summaries of this extensive public debate). Many webcasts and other public events by FEI, NACD, IIA, and numerous other organizations have featured extensive debate on enhancing the SOX implementation on a go-forward basis.

An IIA research study entitled *Sarbanes-Oxley Section 404 Work — Looking at the Benefits* (**www.theiia.org/download.cfm?file=343**) provides an extensive summary of some of the key benefits from SOX implementations, along with extensive discussion regarding the high first year costs involved in meeting the requirements of the Act and its related SEC rules.

The IIA research study presented three major themes:

First, there are significant benefits associated with the control identification, documentation, and testing process. The evaluation process has led to improvements in basic internal controls such as reconciliations and segregation of duties. Substantial improvements in the control environment have resulted from the process. Many companies have recognized they have vulnerabilities in the Information Technology (IT) area and will be devoting more resources to improving and evaluating IT controls as they move forward. Companies are gaining more confidence in their control structure and are evaluating accounting risks, which should enable investors to have more confidence in the reliability of unaudited data furnished to the securities market.

Second, the prognosis is that the future costs associated with Section 404 will decrease substantially as we look forward three years. Much of the initial cost came about because controls had not been systematically documented or evaluated prior to the Section 404 requirements. Chief Audit Executives (CAEs) see the process as becoming more systematized. The authors believe companies will see significant efficiencies as they fully implement the information, communication and monitoring concepts embedded in COSO's *Internal Control Integrated Framework.*

Third, there is uncertainty about the future role of internal auditing with respect to Section 404 work. The majority of CAEs want to maintain a strong presence in the risk and control arena. They recognize the need to perform more operational auditing and that it continues to add value to the organization. The majority of the respondents recognize a need to invest resources in IT auditing. Most CAEs see themselves playing a major role in ongoing monitoring and testing activities associated with Section 404 work.

Leading Control Improvements From First Year SOX Efforts

There were many control improvements and they are described in detail in the actual IIA research report. A summary of the control improvements is presented below. This top 10 list can also help companies when they evaluate their own progress towards a robust control environment.

1. A more engaged control environment with active participation by the board, the audit committee, and management.

2. More thoughtful analysis of monitoring controls, along with recognition that monitoring is an integral part of the control processes.

3. More structure to the year-end closing process and recording of journal entries, thus recognizing the extent to which these areas have increased in complexity.

4. Implementation of anti-fraud activities with defined processes in place, including responsibility for follow-up by defined parties and resolution approaches.

5. Better understanding of the risks associated with general computer controls, and the need to improve both control and audit procedures to gain assurances that the risks associated with computer systems are mitigated.

6. Improved documentation of controls and control processes that can serve as a basis for training, practical day-to-day guidance, and management evaluation.

7. Improved definition of controls, and the relationship of controls and risk, across the organization.

8. Control concepts becoming embedded into the organization with a broader understanding by operating personnel and management of their responsibility for controls.

The COSO small business task force has issued guidance for smaller public companies regarding internal control over financial reporting. The three volume set of guidance will be helpful for organizations with all size of operations.

9. Improvements in the adequacy of the audit trail as a basis to support operations, as well as to support audit assessment of control adequacy and financial reporting.

10. Re-implementation of basic controls (e.g., segregation of duties, periodic reconciliation of accounts, and authorization processes) that had been eroded as organizations downsized or consolidated operations.

Chapter 3 – We Need to Ensure IT is in Control

The management team should ensure sufficient attention is given to the identification of key IT controls by individuals with a broad understanding of the business and the overall SOX program effort. Failures to effectively link IT risks and controls to an organization's overall, top-down SOX risk assessment process and identification of key controls are common.

Controls fall into two broad categories. *Preventive controls* are intended to eliminate lapses, either intentional or inadvertent. An example would be the segregation of duties in an IT department so that one person approves an change, another implements it, and a third checks that the change has been properly made. In this way an unauthorized or incorrect change is prevented. *Detective controls* are designed to identify errors and irregularities that have already occurred. A software product that monitors servers or other devices for changes is a good example. An essential element of any compliance program is the testing of controls.

To achieve a world-class business operation, IT operations and IT in general needs to operate within a very strong "control environment" and IT needs to be in control.

All IT Changes Need to be Auditable

Changes to a server, network devices, or directory servers can have a major impact on the security, level, and quality of IT services delivered. The question is what kind of impact? As enterprise network infrastructures become geometrically more complex, IT teams are burdened with increased demands, reduced budgets, rising costs, and increased operational risks. IT teams need to know when change occurs and whether it's desired, not desired, accidental, benign, malicious, intentional, or originating from inside or outside, in order to address the resultant risks.

Tripwire's change auditing solutions deliver visibility into service-affecting changes, as well as the capabilities to quickly detect change, assess its impact, and mitigate risk. As a vital component of IT operational best practices, Tripwire solutions integrate with a wide range of enterprise management systems to close the verification loop on change management, and in the process, enable organizations to increase security, instill process accountability, and improve system availability.

The *Managing Change in IT Infrastructures* white paper by Tripwire highlights:

- The biggest causal factors of IT downtime
- Seven benefits of change management
- How to establish a change management process
- How Tripwire software can help create a closed-loop change management process

All Changes Need to be Authorized

Network administrators and IT managers know that the ramifications of one small change to a company's critical servers or network devices (such as routers, switches and firewalls) depend on whether the change is desired or not. Change auditing solutions allow companies to reconcile detected changes with those previously authorized. They give the organizations greater control over service-affecting changes and provide the foundation of a layered security strategy. Tripwire change auditing software monitors key files and configurations of servers, desktops, network devices, directory servers and databases, detecting externally and internally originating changes, alerting IT staff, and providing detailed reports for rapid restoration of systems to a known good state.

The *What's Good for Security is Good for Operations* whitepaper by Tripwire presents:

- How Tripwire software assures the integrity and security of servers, desktops, network devices, directory servers and more by addressing the three key elements of change auditing
- How change auditing solutions can help demonstrate IT compliance to regulations and policies, enhance security, and increase IT availability
- How change auditing helps conserve the IT organization's most valuable resource—its staff

All Unauthorized Changes Must be Investigated

To establish a robust and effective change management program, managers and staff need to know that unauthorized activities will be detected and investigated. Building the "fence" around your IT infrastructure and systems includes determining when someone has broken a board and taking appropriate disciplinary and corrective actions so the fence will continue to have the necessary integrity to protect your key assets.

Tripwire and Visible Ops: A Four-Phase Approach to Instituting Change Management, a white paper by Tripwire, presents "lessons learned" from several years of research at leading IT organizations and will help put getting your IT under control on the fast track.

Chapter 4 – Sustainability

(And Making Your SOX Efforts a Source of Long-Term "Competitive Advantage")

Companies faced with SOX clearly need to adopt a compliance process that addresses the control, evaluation and disclosure elements of Sections 302, 404 and 409. Because IT is crucial to support and enables financial reporting and other company operations, security technologies and measures must be adapted to meet these requirements.

Because the law and a company's operations will change over time, companies that adopt a change auditing approach that includes strong IT governance measures are best positioned to equip the CEOs and CFOs with the tools to implement and certify the existence of ICFR and meet the evaluation and disclosure requirements of SOX.

During the first year of SOX implementation, many organizations and their auditors tested an unnecessarily large number of controls. To reduce the compliance burden, some organizations now conduct a top-down assessment to determine which accounts and supporting processes and systems are most susceptible to error or abuse that will cause a material misstatement.

Key controls for these significant accounts and supporting processes and systems are tested more frequently; less essential ones may fall outside the scope of testing entirely. Many organizations have achieved cost savings without any reduction in control assessment effectiveness by rationalizing their control testing in this manner. Some questions to consider when evaluating IT control relevance include:

- Is the Data Center responsible directly/indirectly for producing the financial reports?
- Is an IT activity connected with an important account?
- Is an IT process critical to financial reporting?
- Are there known deficiencies or material weaknesses in a technology?
- Is the financial application linked to other system interfaces?
- Is the application shared by many business units across the enterprise?

Questions such as these can help rationalize your control testing and place relevance boundaries around your IT infrastructure.

For further reading, the *Darning SOX* whitepaper by Tripwire presents:

- The SEC definition of "internal controls" as they apply to SOX
- The relevance of COSO and COBIT in SOX compliance initiatives
- Guidelines for ongoing evaluation of internal controls
- SOX disclosure guidelines
- Responsibilities, penalties, enforcement, and deadlines relevant to SOX compliance

Importance of Keeping the Overall Process Current

Organizations need to develop ways to keep the assessment of internal controls current over time. In fact, according to SOX 302, the evaluation process must be conducted at least quarterly. This requires that IT be involved in the day-to-day SOX compliance efforts. If your internal controls are established with the appropriate tests and you have change auditing in place to ensure that controls are operating as intended, then you are well on your way to a sustainable compliance environment.

How well you track, manage and document changes goes a long way towards determining how consistent, relevant, costly and efficient your compliance effort will be. Understanding your existing systems significantly improves your planning and management of your IT infrastructure. This is where detailed documentation is extremely beneficial.

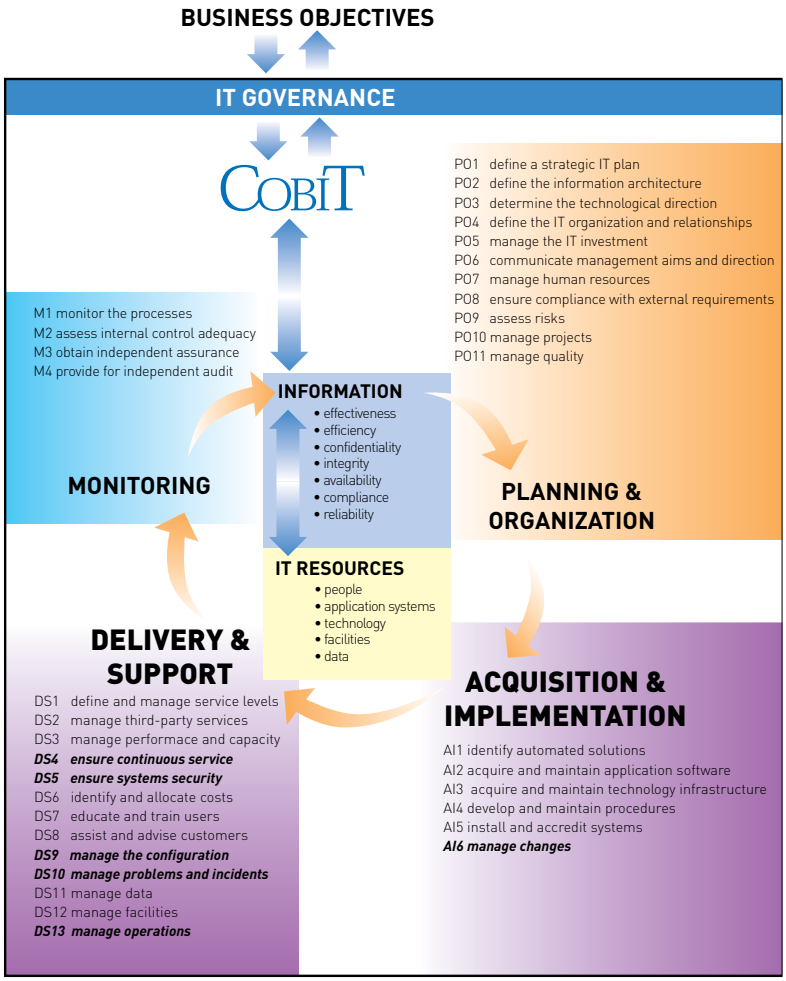
Good IT documentation lets you create audit-ready documents on demand, which is an essential component for SOX compliance. It also enables you to understand dependencies across your entire IT infrastructure and helps you optimize network and system configuration, standardize configuration settings, and accelerate problem resolution and trouble-shooting.

Regular testing and validation of security systems is a primary requirement to maintain reasonable network security. This translates to documenting processes and systems, risk analysis and mitigation controls, as well as key control test strategies for IT systems that impact financial reporting.

Keeping the overall process current is foundational for managing your entire IT infrastructure and maintaining value in your security, compliance and policy implementation.

IT General Controls for SOX

Tripwire can be implemented and configured to promote achievement of COBIT control objectives that are commonly adopted for SOX compliance efforts. The COBIT table defines a series of control objectives and identifies where Tripwire can help validate the effectiveness of a control. This also shows how Tripwire can help you pinpoint compliance gaps, as well as summarize evidence of deficiencies.



Tripwire provides essential preventive and detective controls within COBIT's **Delivery & Support** *and* **Acquisition & Implementation** *domains.*

Fitting Tripwire into Your SOX Sustainability Strategy

Gaining control of IT requires an effective combination of people, processes and technology. Business process owners, IT staff, security personnel, and auditors must work together to define and enforce change policies and processes. Once policies and processes are defined, they can be enforced with technology.

Tripwire Enterprise change auditing software enables you to prove that all authorized change is properly implemented and that no unauthorized change goes undetected. Detailed change audit trails prove that IT process controls are effective, that the IT infrastructure is secure, and that your change management policy is enforced and supports compliance with Sections 302 and 404.

Change detection so that every change is auditable

Tripwire Enterprise provides an independent, single point of management control for enterprise-wide change monitoring of IT systems. This includes directory servers, file servers, desktops, databases, middleware applications, and a broad range of network devices, including network switched, routers, firewalls, and Virtual Private Network (VPN) systems. Within these systems, Tripwire monitors service elements—such as file systems and their attributes, configuration settings, users, and permissions—and even systems from a variety of vendors.

Tripwire detects change relative to a specific, trusted state (known as a baseline) against which any change is automatically compared and logged. This ensures that every change is auditable. Further enhancing auditability, only users with appropriate permissions are able to accept detected changes and include them in the current baseline if the changes are desired and authorized.

Change reconciliation ensures all changes are authorized

Determining which of an IT organization's thousands of changes are authorized—and which are not—is a task for technology. Tripwire's change reconciliation capabilities enable IT organizations to institute a variety of manual and automated techniques to separate appropriate changes from unauthorized changes that may negatively affect enterprise compliance, security, or service quality.

Reconciliation also accelerates identification of unauthorized changes and facilitates investigation of these changes. Tripwire Enterprise change auditing helps IT management define change processes, enforce them, and document when these processes are circumvented so that the enterprise can mitigate risk and avoid negative consequences.

Change reporting substantiates change policy effectiveness

Tripwire Enterprise provides a wide range of customizable reports and online dashboards to highlight IT infrastructure changes anywhere in the enterprise. With report linking features, managers can drill down into underlying details and metrics. For example, a report could illustrate the change rate of selected systems for the past year; a manager could drill down to view changes for a specific quarter, month, or week. Real-time status reports facilitate incident management and help staff determine root causes of outages.

Tripwire reporting features deliver high visibility into operations, enable management to foster process improvement, and integrate change auditing capabilities with security, compliance and system availability initiatives.

Chapter 5 – Other Considerations

Other IT Efforts That IT Management Should be Planning For

- Investment in continuous improvement of IT operations, including:
  - — Helping business management to reduce use of spreadsheets by integrating these functionalities into existing or new applications
  - — Implementing ongoing monitoring tools to identify control deficiencies
  - — ITIL staff training
  - — Strengthening the control environment

  - — Continuing to improve documentation
  - — Standardizing processes
  - — Strengthening weak links
  - — Systematic reduction in unplanned work
  - — Establishing metrics (if you can't measure it, you can't improve it)
- Investment in IT flexibility (e.g., to handle more acquisitions)
- Investment in other improvement efforts for IT Operations and IT management (e.g., acquisition and implementation of IT management software)

We Need to Take a Long Term View Regarding IT Controls

Change has become the business norm and improving your IT solutions has become a business priority. To achieve compliance in today's business environment, we need to have effective IT controls. To achieve control of IT, enforcing change policy with change auditing is critical.

Why IT is Worth It

Getting control of IT and enforcing change management processes pays off in greater auditability, service quality, efficiency, and IT infrastructure integrity. Because IT is crucial to support and enables financial reporting and other company operations, information security technologies and measures must be adapted to continue to meet SOX Sections 302 and 404. Change auditing reduces the cost and difficulty associated with audit preparation and makes it easier to pass internal and external audits.

If all authorized system changes can be documented, then once IT elements are configured, tested and deployed into production, they will continue to operate appropriately unless changed. Strong internal change controls provide management and auditors the confidence and supporting evidence that security measures are effective and IT systems operate with integrity. They mitigate the risk of malicious changes and provide security staff with a reliable, objective view of change across an enterprise.

1. To attest that the change management process is in control, auditors need to confirm that all changes are detected, reviewed and tied to authorized requests for change. Furthermore, auditors need to confirm that unauthorized changes are detected, reviewed and resolved by corrective actions.

2. Having IT personnel aware that all changes will be detected and disciplinary action taken for unauthorized changes, an organization's culture shifts from a cowboy mentality to one of compliance with processes. During this shift, the benefits of a well-designed and implemented change management process will become apparent as the infrastructure stabilizes and unplanned corrective work decreases.

3. As unplanned work decreases, the ability of the organization to work on planned projects increases. This shift of resources away from nonproductive work to productive work is catalytic both for IT and the organization as focus is directed towards the achievement of objectives and goals.

4. As planned changes are communicated in advance and detected changes reported, organizations have a powerful ability to answer the question of "What changed?" immediately in the incident lifecycle. This ability to know what changed as the first step of the incident allows for a movement away from emergency phone calls, pages and emails to one of knowing what caused an incident without even logging onto the system in question. As a result, the Mean Time To Repair (MTTR) is lowered and overall availability increases.

— Musings by George Spafford, Principal Consultant, Pepperweed Consulting

Appendix A: References

Learning From Others

Extensive resources are available from various professional associations, research organizations, vendors, and your peers. In today's competitive environment, every opportunity to leverage lessons learned and best practices should be exploited. The resources highlighted in this white paper have all been reviewed by the writer. They will help you plan and implement various initiatives, and improve your operational excellence and the likelihood of success in your governance, compliance, security and other initiatives.

Key Resources

There are many sources for valuable material and informative guides regarding governance, implementing robust change management processes, and getting "IT under control." In addition to the various white papers already highlighted throughout this paper, links are provided below to further leading guidance and key resources that will help you meet your compliance, service quality, and information security requirements.

1. Operational Excellence: Linking Your Business, Compliance, Operations, and Security. A tactical guide enabling organizations to take action and achieve operational excellence.
   www.tripwire.com/promos/61/cio/index.cfm

2. The IIA's Expressing Opinions on Internal Control Resource repository. Provides extensive guidance on topics ranging from corporate governance to risk management.
   www.theiia.org/index.cfm?doc_id=5317

3. The IIA's Change and Patch Management Controls: Critical for Organizational Success (GTAG). This guide will help readers to counsel their boards about change management risks and controls and help their organizations comply with constantly changing regulatory requirements.
   www.theiia.org/index.cfm?doc_id=5167

4. The IIA's Information Technology Controls (GTAG). Covers technology topics, issues, and audit concerns as well as issues surrounding management, security, control, assurance, and risk management.
   www.theiia.org/index.cfm?doc_id=5166

5. The Visible Ops Handbook. Visible Ops illustrates how organizations might replicate key processes of these high-performing organizations in just four steps.
   www.itpi.org/home/visibleops2.php

6. The OCEG Internal Audit Guide (IAG) – Evaluating Your Compliance and Ethics Program. This 88-page guide provides a roadmap for internal auditors to audit a compliance and ethics program. It is also be useful for people charged with governance responsibilities.
   www.oceg.org/landing/IAG.aspx

7. CICA's Information Technology Advisory Committee paper entitled: "The Role of Information Technology in Sustained Regulatory Compliance (2006)."
   www.cica.ca/

8. Bill 198 and Internal Controls for Technology (white paper by Tripwire).
   www.tripwire.com/files/literature/white_papers/Tripwire_Bill_198_WP.pdf

Leading Web Sites:

Compliance

Tripwire – **www.tripwire.com**

The Open Compliance and Ethics group (OCEG) – **www.oceg.org**

Expressing Opinions on Internal Control – (IIA resource repository) – **www.theiia.org/index.cfm?doc_id=5317**

Audit

Tripwire – **www.tripwire.com**

Internal and IT Audit guidance – The Institute of Internal Auditors, Inc. (IIA)
www.theiia.org/guidance and www.theiia.org/technology

IT Audit and Control – Information Systems Audit and Control Association (ISACA) – **www.isaca.org**

Federal Financial Institutions Examination Council (FFIEC)
www.ffiec.gov/ffiecinfobase/resources/re_01.html
www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

American Society for Quality (ASQ) – **www.asq.org**

U.S. General Accountability Office (GAO) – **www.gao.gov/aac.html**

Auditing System Conversions article – **www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5495**

IT Operations

Tripwire – **www.tripwire.com**

The Visible Ops handbook – **www.itpi.org/home/visibleops2.php**

Change and Patch Management Controls: Critical for Organizational Success – **www.theiia.org/technology**

Information Technology Process Institute (ITPI) Reading Room – **www.itpi.org/home/articles.php**

What's Good for Security is Good for Operations: Why Change Auditing is Key to Operational Stability
www.tripwire.com/solutions

20 Questions Directors Should Ask of IT (CICA) – **www.cica.ca/index.cfm/ci_id/1000/la_id/1.htm**

Security

Tripwire – **www.tripwire.com**

Governing for Enterprise Security – **www.cert.org/governance/ges.html**

Management Guide for IS Security Auditing – **www.gao.gov/special.pubs/mgmtpln.pdf**

Information Technology Controls (IIA GTAG) – **www.theiia.org/technology**

Series of three IIA security guidance reports completed for CIAO

Information Security Management and Assurance: A Call to Action for Corporate Governance

Information Security Governance: What Directors Need to Know

Building, Managing, and Auditing Information Security
www.theiia.org/index.cfm?doc_id=3061

Auditing Information Security – **http://infosecuritymag.techtarget.com/articles/october00/features3.shtml**

SANS "What Works" Repository – **www.sans.org/whatworks**

International Systems Security Engineering Association (ISSEA) – **www.ISSEA.org**

CISSP Study Web Site – **www.cccure.org**

Professional Security Testers Web Site – **www.professionalsecuritytesters.org**

IT

Tripwire – **www.tripwire.com**

The Institute of Internal Auditors technology guidance – **www.theiia.org/technology**

The IT Process Institute (ITPI) – **www.itpi.org/home**

The Carnegie Mellon Software Engineering Institute (SEI) – **www.sei.cmu.edu**

ITIL (the IT Infrastructure Library) – **www.itil.co.uk**

SANS Reading Room – **www.sans.org/reading_room**

OGC's Successful Delivery Toolkit – **www.ogc.gov.uk/sdtoolkit**

Forrester – **www.forrester.com**

U.S. General Accountability Office (GAO) – **www.gao.gov/special.pubs/cit.html**

The U.S. CIO Council – **www.cio.gov**

Internal Control and Risk Management related resources

IT Control Objectives for Sarbanes-Oxley (by ISACA)
http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/IT_Control_Objectives_for_Sarbanes-Oxley1.htm

Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control – Integrated Framework (IC-IF) – Executive Summary.
www.coso.org/publications/executive_summary_integrated_framework.htm

COSO"Enterprise Risk Management—Integrated Framework (ERM-IF)".
www.coso.org/publications.htm

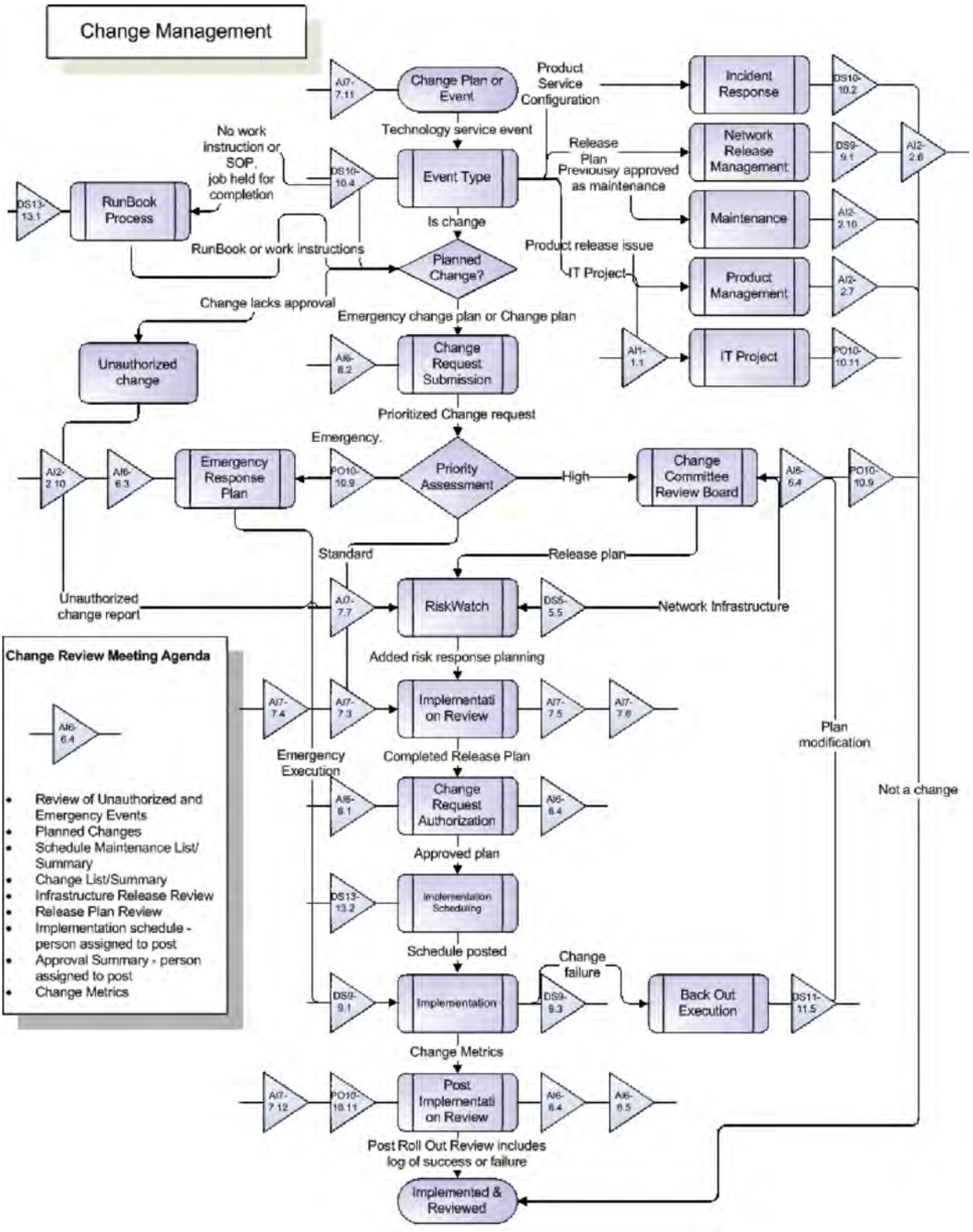
The Role of Internal Auditing in Enterprise-wide Risk Management (PDF)
www.theiia.org/iia/download.cfm?file=283

Other COSO Related Resources
www.theiia.org/?doc_id=4884 and www.coso.org

FAQs for COSO's Enterprise Risk Management—Integrated Framework (ERM-IF)
www.theiia.org/?doc_id=4883

Revenue recognition issues.
www.revenuerecognition.com

Appendix B: Change Management "Overview" Pictorial



This overview was developed by Robin Basham (President and Founder, Phoenix Business & Systems Process, **www.pbandsp.com**) to present a high level pictorial of the many activities, processes, and stakeholders in a typical change management program.

About the Author

Dan Swanson, CMA, CIA, CISA, CISSP, CAP
President and CEO, Dan Swanson & Associates

Dan Swanson is a 22-year internal audit veteran who most recently was director of professional practices at the Institute of Internal Auditors. Prior to the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing at the federal, provincial and municipal levels, and the rest in the private sector (chiefly financial services, transportation, and health).

Swanson has completed 100 internal audits in his career including: operational audits, system audits, financial audits, value-for-money audits, comprehensive audits, and more. He has completed 50 IT audits and a dozen comprehensive audits of the information technology function. He is the author of more than 70 articles on internal auditing and numerous other management topics and currently a freelance writer and independent management consultant. He can be reached at **www.securitybenchmark.com**.

Swanson recently led the writing of the OCEG internal audit guide for use in internal audits of compliance and ethics programs (**www.oceg.org**) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (**www.coso.org**). He is also a regular columnist for the Compliance Week magazine and the IT Compliance Institute (ITCI).