

AN IT EXECUTIVE'S OVERVIEW OF THE SARBANES-OXLEY ACT OF 2002

Requirements for IT Compliance

Presented by:



Requirements for IT Compliance
Presented by
SoftLanding Systems, Inc.

CONTENTS

Executive Summary.....	2
Introduction.....	3
The Sarbanes-Oxley Act.....	4
Impact of SOX on Corporate Governance.....	5
SOX Mandates on IT.....	8
SOX Sections 302 and 404 Explained.....	9
Guidlines Towards SOX Compliance.....	11
COSO.....	12
COBIT - IT's COSO.....	13
Suggested Course of SOX Compliance Action.....	14
SoftLanding iSeries Products Pertinent to COBIT Objectives.....	15
A Sampling of COBIT Control Objectives Associated with Change Control and Project Management.....	16
Pertinent Products from SoftLanding.....	17
A Sampling of COBIT Control Objectives Associated with Security Auditing and Controls.....	18
Pertinent Products from SoftLanding.....	19
Summary.....	20
Reference URLs.....	21
Appendix A: CoBIT Objectives Relevent to Sarbanes-Oxley IT Compliance	
Figure 1: SOX Section 302 & 404 Overview.....	10

AN IT EXECUTIVE'S OVERVIEW OF THE SARBANES-OXLEY ACT OF 2002

Requirements for IT
Compliance
Presented by
SoftLanding Systems, Inc.

EXECUTIVE SUMMARY

At the beginning of this millennium, investors in U.S. stock markets lost \$35B, caused in part by illegal manipulation of corporate financial reporting. This resulted in a continual parade of C-Level executives through various criminal courts and the passage of the Sarbanes-Oxley Act of 2002 (SOX).

The Sarbanes-Oxley Act:

- Prohibits CEOs/CFOs from altering corporate financial reports for their own personal gain through previously questionable, but now specifically illegal actions.
- Requires CEOs/CFOs to implement financial/IT controls to prevent or detect any attempted financial manipulation. CEOs/CFOs are to certify on a quarterly basis that financial/IT controls are in place and are effective.
- Requires outside auditors to attest to the accuracy of the CEOs/CFOs certifications.

This white paper provides readers with:

- An overview of the SOX act, highlighting the permanent changes in corporate culture and governance required for public corporations to become SOX compliant.
- Explanations of the Act's provisions that are applicable to IT.
- The strategy that internal auditors have concluded to be most effective for moving IT toward SOX compliance, which involves:
 - a) Assessing current IT controls against established COBIT standards, then
 - b) Upgrading any IT controls identified as deficient to a COBIT maturity level 3.
- A list of iSeries-based products from SoftLanding Systems supporting SOX-applicable COBIT objectives.

As a provider of IBM-certified software management and security tools for iSeries computers since 1989, SoftLanding Systems offers a suite of software products that support 61 of the 164 SOX related COBIT objectives. A tabular listing of the COBIT Control Objectives and the SoftLanding tools that support them can be found in the attached appendix. These SoftLanding Systems products include TurnOver Change Management; TestBench; TurnOver PDQ; SoftMenu; PowerLock NetworkSecurity, SecurityAudit and FlashAudit; and VISUAL Control Center, VISUAL Message Center, and VISUAL Security Suite.

INTRODUCTION

During the 1990s, the United States witnessed unprecedented capital appreciation in the stock markets. Much of the investment excitement at the time was based on emerging new-economy firms attempting to capitalize on new industries in e-business, biotechnology, and wireless or broadband communications.

Without established industry precedents, sustained quarter-to-quarter double-digit growth for these new economy firms appeared believable. Indeed for many firms, it was being documented as such. However in many cases, the continued success stories were simply not true.

Quarterly and annual reports for many post-IPO new-economy firms (as well as for some old-economy firms attempting to compete) often included earnings management, revenue manipulation, out-of-period sales, and sales channel stuffing. All of this creative accounting, compounded by "the buzz" from marketing presentations and press releases provided to analysts and the press, perpetuated an unrealistic increase in both stock valuations and stockholder expectations.

This unprecedented capital appreciation was tacitly endorsed, and rarely questioned, by much of the accounting industry, investment banks, and financial or technology analysts. At the time, everyone benefited, to the ultimate misfortune of Joe and Jane Investor.

What originally was hailed as the successful execution of brilliant new business plans was often just egregious financial misreporting. The new economy investment bubble ultimately burst. Between 1999 and 2002, investors lost \$35 billion in U.S. stock markets.

THE SARBANES-OXLEY ACT

The ultimate financial disclosures of several major corporations typified what new-economy accounting had wrought. As a response, the U.S. Congress implemented a far-reaching law intended to restore the public confidence in capitalism - The Sarbanes-Oxley Act of 2002.

Sarbanes-Oxley (SOX) is a series of specific mandates requiring public firms operating in the United States to re-establish stockholders as the primary corporate beneficiaries, above all other company stakeholders. Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) are now beholden, by law, to their corporate boards of directors. These boards, in turn, are distanced from the corporate executives and are directly responsible to company stockholders.

The board of directors must now include a higher percentage of outside directors. The board must take a more active role in corporate governance and oversight, especially during annual financial audits. The board's audit committee is now exclusively responsible for the selection, the initial direction, and the ongoing management of the outside auditors.

The outside auditing firms must also be more distanced from corporations they are selected to audit. Auditing firms can no longer provide additional value-added, non-auditing services to firms they are auditing that year. They must also be pre-certified by the newly-formed Public Company Accounting Oversight Board (PCAOB) created by the SOX Act.

SOX financial reporting requirements are comprehensive and thorough. The law is an attempt to force corporate executives and boards of directors to reaffirm the original premise of corporate governance.

As Commissioner Paul S. Atkins of the U.S. Securities and Exchange Commission said in a speech to the University of Cologne, Germany on February 5, 2003:

"Fundamentally, the (Sarbanes-Oxley) Act acknowledges the importance of stockholder value. Without equity investors and their confidence, our economic growth and continued technological innovations would be slowed. Sarbanes-Oxley strengthens the role of directors as representatives of stockholders and reinforces the role of management as stewards of the stockholders' interest."

IMPACT OF SOX ON CORPORATE GOVERNANCE

The Sarbanes-Oxley Act of 2002 is comprised of eleven main titles, further divided into sixty-six sections. It details the legal expectations in the governance of public firms doing business in the U.S. Many sections should be recognizable as direct consequences of the abuses wrought by the corporate executives and audit firm partners who achieved prosecutorial prominence between 2000 and 2003. Examples of such sections include:

Section 203 - Rotation of Audit Partners. Requires the lead and concurring outside auditor partners to leave a company's audit program after five years, for a period of five years. Other partners who are part of the engagement team must rotate out after seven years, for a period of two years.

Section 204 - Specific Reports and Responsibilities. Requires the external auditor to report all financial information passed to the outside auditors by the corporation's finance department before and during the audit process to the audit committee appointed by the company's board of directors before filing the financial report.

Section 206 - Prohibition of Conflicts of Interest. An accounting firm cannot audit a company if the company's CEO, CFO, controller, chief accounting officer or any person in an equivalent position was employed by that audit firm and participated in the company's audit during the one-year period immediately preceding the initiation of the audit.

Section 301(2) - Audit Committee Selection and Oversight of Independent Auditor. A company's board-of-director-appointed audit committee is responsible for the appointment, compensation and oversight of the independent, external auditor. This includes the resolution of disagreements between the independent auditor and management regarding financial reporting. The Audit Committee is authorized to, and must be afforded adequate resources to engage independent counsel and other advisors. The Audit Committee must establish procedures for the receipt, retention and treatment of complaints regarding accounting, controls, or auditing matters and for confidential submission of employee concerns.

Section 303 - Improper Influence on Audits. Company executives cannot fraudulently influence, coerce, manipulate, or mislead the independent external auditor for the purpose of rendering the financial statements materially misleading.

Section 304 - Forfeiture of Bonuses and Profits. If a company must restate its financial reports because of material non-compliance in any area due to misconduct, the CEO and the CFO will be required to reimburse any bonus or other incentive-based or equity-based compensation he/she received, as well as any profits realized from the sale of the company's securities during the 12 months following the filing of the non-compliant financial statements.

Section 305/1105 - Prohibition of Service As Director or Officer. The SEC can obtain a court order to bar an individual from serving as a director or officer when the SEC feels the individual has violated general anti-fraud provisions of the securities laws and the court finds that their activities show them to be "unfit."

Section 306 - Trading Restrictions. No director or executive officer will be allowed to trade stock during any 401(k) plan "blackout period."

Section 307 - Responsibilities of Legal Counsel. Attorneys representing public companies before the SEC will be required to report "evidence of" material violations of securities laws.

Section 401(a) - Off-Balance Sheet Transactions. All material off-balance sheet transactions, arrangements, obligations, and other relationships with unconsolidated entities or persons that might materially affect the company's financial condition must be publicly disclosed.

Section 401(b) - Use of Pro Forma Financial Information. Restricts the use and disclosure of "pro forma" financial information (such as non-GAAP information) in SEC filings, press releases, or other public disclosures. This is to ensure that the company's financial information is presented in a manner that does not mislead investors.

Section 402(a) - Prohibition on Loans and Credit to Directors and Executives. Prohibits any manner of extending, maintaining, arranging, or guaranteeing personal loans to corporations' executive officers.

Section 403 - Accelerated Reporting of Insider Stock Transactions. Directors and executive officers are required to report stock transactions within two business days.

Section 406 - Senior Management Code of Ethics. Requires corporations to disclose periodically that a code of ethics for the principal financial officer and the principal accounting officer has been adopted and that these officers are complying with it.

Section 407 - Audit Committee Expertise. Corporations must disclose in periodic reports whether the audit committee includes at least one member who is a "financial expert" and, if not, the reasons why.

Section 802 - Criminal Penalties. A person who destroys, alters, or falsifies records with the intent to obstruct a governmental investigation is subject to a fine and imprisonment for up to 20 years.

Section 802 - Criminal Penalties. The knowing and willful destruction of audit records (such as work papers, correspondence, communications, memoranda), which must be kept for five years, may result in a fine or imprisonment for up to ten years.

Section 806 - Protection of "Whistle Blowers." It is unlawful to discharge, demote, suspend, threaten, harass, or discriminate against in any other manner any employee who provides information regarding conduct the employee reasonably believes constitutes financial fraud or a violation of the securities laws.

Section 906 - CEO/CFO Certification of Annual and Quarterly Reports. CEOs and CFOs must certify that quarterly and annual reports fully comply with Sec. 13(a) or 15(d) of the '34 Act and that information contained in those reports fairly presents, in all material respects, the financial condition and results of operations of the company. A CEO or CFO who knowingly submits a wrong Sec. 906 certification is subject to a fine of up to \$1 million and imprisonment for up to ten years. If the wrong certification was submitted "willfully," the fine can be increased to \$5 million and the prison term can be increased to 20 years.

While IT directors and managers reading this paper have little reason to memorize every section detailed above, they should be very cognizant of the message the U.S. Congress and the SEC is sending to all corporations conducting business in America. It is illegal for C-level executives to attempt personal gain from their actions in corporate governance at the expense of other company stakeholders, primarily the individual stockholders. Any attempt to do so, or to conceal such efforts, will result in personal penalties akin to those issued for felonies and capital crimes.

SOX MANDATES ON IT

Four sections of the Sarbanes-Oxley Act, based on these mandated new governance standards, will require the active efforts of the IT department. These include:

Section 302 - CEO/CFO Certification of Annual, Semi-Annual, and Quarterly Reports. Company CEOs/CFOs must certify that:

- (a) they have reviewed the report,
- (b) the report does not contain any misrepresentation,
- (c) the financial information in the report is fairly presented,
- (d) they are responsible for "disclosure controls and procedures,"
- (e) they have reported any deficiencies in internal controls and fraud involving management to the audit committee, and
- (f) they have indicated any material changes in internal controls.

Section 404(a) - Internal Control Reports. Each annual report must include an "internal control report" stating that management is responsible for an adequate internal control structure and an assessment by management of the control structure's effectiveness.

Section 404(b) - External Auditor Attestation Related to Internal Controls. The registered accounting firm must attest to, and report on, management's assertions regarding its assessment of the effectiveness of the company's internal controls.

Section 409 - Real-Time Disclosure. Corporations will be required to disclose, on a rapid and current basis (48 hours), additional information concerning material changes in its financial condition or operations.

Section 1102 - Corporate Fraud Accountability: Tampering with Evidence. Whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding, shall be fined \$5M and/or imprisoned up to 20 years.

Sections 302 and 1102 are in effect today. Section 404 is to be effective for the first annual reports for the fiscal year ending after November 15, 2004 for all public companies with capital valuations greater than \$75M US. For public firms valued less than \$75M US, the effective date for Section 404 is for annual reports after July 15, 2005. At the time of this writing, the effective start date for Section 409 has not been determined.

SOX SECTIONS 302 AND 404 EXPLAINED

A founder of CARDdecisions (www.carddecisions.com) has created an excellent graphical representation of SOX Sections 302 and 404 requirements (See figure 1, p.10). He is allowing use of this representation in this report.

By law, U.S. public companies must generate quarterly and annual standardized financial reports (10Qs and 10Ks). The target reading audiences for these reports include company stockholders, the board of directors, and federal regulators (Key Disclosure Stakeholders).

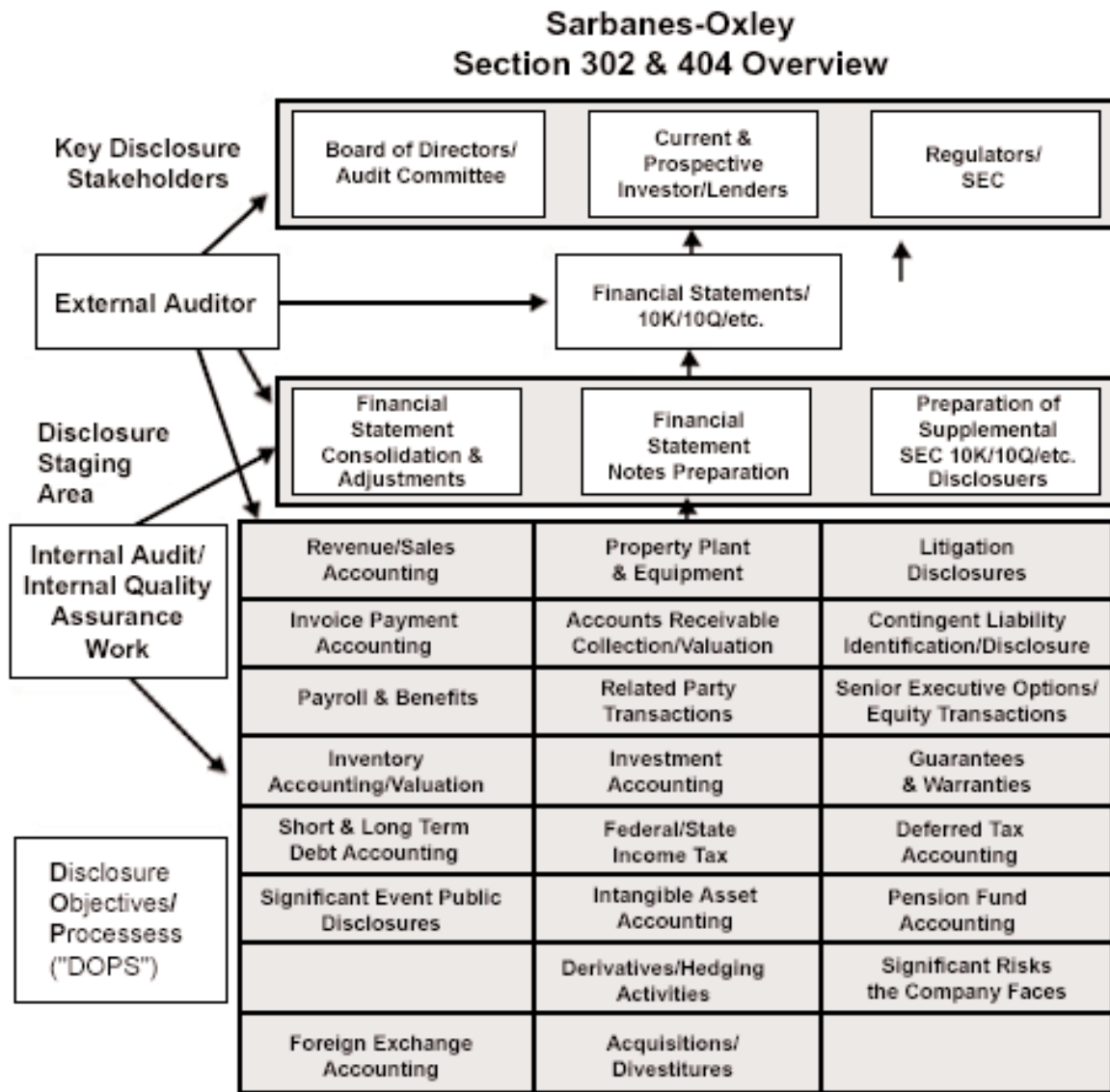
The 10Q and 10K reports are the aggregate summary of all company Disclosure Objectives/Processes (DOPs). All DOPs that have any bearing on the company's financial performance must be included in the financial reporting.

Most DOP information is quantitative in nature. However, some DOPs provide mostly qualitative information, such as the Litigation Disclosures and Significant Event Public Disclosures. The quantitative DOP information is typically from the outputs of business software applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Sales Automation, Supply Chain Management (SCM), and Human Resource Management (HRM), based on multitudes of data streams, including sales, production scheduling, employee payroll, and valuation of inventories.

Internal auditors are to take the quarterly and annual summary outputs of all DOPs to the Disclosure Staging Area, then produce aggregated results - the financial reports of the company. The methodology internal auditors use in these processes is to be readily identifiable and easily repeated by the follow-on external auditors.

AN IT EXECUTIVE'S OVERVIEW OF THE SARBANES-OXLEY ACT OF 2002

SOX Sections 302 and 404 now require company CEOs and CFOs to ensure that all publicly released financial reports accurately and completely document the financial condition and performance of the company. It is now their responsibility to attest that an adequate control structure is in place and operational, ensuring that the output data from each financially significant DOP is current and accurate for the specific audit date.



© 2003 CARDdecisions, Inc. Reprinted by permission¹

Figure 1: A visual overview of Sections 302 and 404 of the Sarbanes-Oxley Act

¹Leech, Tim J., FCA-CIA, CCSA, CFE. Sarbanes-Oxley Sections 302 & 404: A White Paper Proposing Practical, Cost Effective Compliance Strategies. CARDdecisions, Inc., Mississauga, Ontario, Canada: April 2003.

Additionally the financial statements emerging from the Disclosure Staging area are themselves complete and accurate to the correct DOP input data.

It will be the Financial and IT departments' responsibilities to make this adequate control structure happen.

GUIDELINES TOWARDS SOX COMPLIANCE

The Sarbanes-Oxley Act defines what needs to be achieved in corporate financial reporting (transparent reporting) and specifies what is not to be done, or even considered, in corporate governance. However, there are no clear directions as to how the required transparent financial reporting is to be achieved.

The SOX regulations were intentionally written this way.

Because of the broad range of corporate financial structures in place for the wide variety of industries in existence, there is no single formula for compliance that could fit every affected public company. However, there exist general corporate control guidelines companies should use to determine their necessary courses of action for complying with SOX.

Per the PCAOB briefing paper for their July 29, 2003 Roundtable on Internal Control:

"The SEC's final rules specified that management must base its evaluation of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework that is established by a body or group that has followed due-process procedures, including the broad distribution of the framework for public comment. The SEC's final rules do not mandate use of a particular framework, but the Committee of Sponsoring Organizations of the Treadway Commission's ("COSO") framework is explicitly identified as satisfying the SEC's criteria.

"The SEC recognizes that other evaluation standards exist outside of the United States and identifies the *Guidance on Assessing Control*, published by the Canadian Institute of Chartered Accountants, and the *Turnbull Report*, published by the Institute of Chartered Accountants in England and Wales, as examples of suitable criteria. Management's report must identify the evaluation framework used to assess the effectiveness of internal control."

COSO

During the late 1980s, the National Commission of Fraudulent Financial Reporting, known today as the Treadway Commission, was tasked with identifying the causal factors of fraudulent financial reporting by public corporations beginning to become apparent at that time. After their initial research report, the commission, comprised of members from national accounting, internal auditors, and financial executive associations was chartered to make recommendations about ways for reducing corporate financial fraud.

In September 1992, the Treadway Commission's Committee of Sponsoring Organizations (COSO) released its "Internal Control - Integrated Framework." This is a standardized description of internal business controls. It unified the many existing definitions and business control processes then used in accounting, finance, government, and academia.

The Internal Control - Integrated Framework, also simply referred to as COSO, is applicable to business organizations of all sizes and types, in all industries. COSO provides the guidelines businesses can use to effectively manage three specific control objectives: effective and efficient management of operations, accurate financial reporting, and compliance to all applicable laws and regulations.

The internal control system spelled out for these objectives consists of five inter-related components: control environment, control activities, risk assessment, monitoring, and communication and information. For businesses to incorporate the COSO framework into their own enterprises, they must first audit the three control objectives against each of the five control components. These control components are broken into 18 aspects and then into more than 100 additional sub-aspect details.

Auditing a company against the COSO internal control model will produce a highly detailed assessment of the company's existing internal control structure. It will identify for management the specific internal control strengths that exist, as well as the areas of control weakness the company must address to successfully meet SOX mandates.

The COSO model often will have interrelated controls, which are applicable concurrently to several objectives. Graphically, the COSO model can best be described in terms of a three-dimensional matrix. Often, assessments of the five control components, or any of the aspects, will apply to several objectives. Because of the many complexities in today's business control processes, no two businesses should ever have identical internal control frameworks according to the COSO model.

COBIT - IT'S COSO

The COSO framework (or a similar international standard) provides corporate finance departments with guidance for developing the SOX-mandated internal controls over the financial applications used in company DOPs and in the Financial Staging Area processes. However, all of these financial processes reside on a company's IT enterprise. This led to the recognition of corporate IT's need for a COSO-style control framework to help management identify the specific IT upgrades needed for SOX compliance.

The Control Objectives for Information and related technology (COBIT) fill this need. COBIT, also released in 1992, is the IT equivalent to finance departments' COSO guidelines. Conducting an IT audit using the COBIT control framework will identify to IT management the company's IT enterprise control strengths and shortcomings, just as the COSO audit does in operations, finance, and compliance controls. The parallels between the audit guidelines and control cultures emanating from both are striking.

COBIT is an amalgam of many existing IT technical control frameworks, written from a business management perspective. It is independent of any IT platform(s) adopted by a corporation. It provides companies with the same high-level IT control guidance, regardless of which IT platforms (Unix, Linux, Windows, iSeries, etc), are in use.

The COBIT framework specifies 34 high-level control objectives, broken down into 318 detailed objectives, for a complete IT governance control program. During its initial ramp-up for the coming SOX IT audits, a major IT auditing organization identified 164 of these 318 control objectives relevant to SOX compliance. This should not imply that companies need only address these 164 COBIT objectives; however, if a company did so, many of the remaining objectives not relevant to SOX would already be met.

SUGGESTED COURSE OF SOX COMPLIANCE ACTION

There are many SOX compliance solutions now being actively promoted. However, according to experts in the audit industry, there is no single offering providing companies a complete turnkey SOX solution. And, because of the wide variety of business models, types, and sizes, there likely never will be a one provider solution.

An oft repeated recommendation for companies to meet SOX compliance is to rebuild and reformat existing internal business and IT controls in all business areas relating to financial processing and monitoring, using both the COSO and COBIT frameworks. This includes all of the DOPS and every process within the Disclosure Staging Area.

To initiate both these frameworks, key segment managers in operations and finance delegated to SOX compliance first need to be educated in COSO. IT managers should do the same with COBIT, as well as becoming somewhat knowledgeable of COSO. Once the "SOX compliance team" is satisfactorily knowledgeable of the COSO and COBIT frameworks, internal audits of the company's current business and IT controls, using the COSO and COBIT frameworks as the reference standards, need to be administered. When these audits are complete, current IT control strengths and deficiencies will readily be identified. Management can then determine and initiate the corrective controls that are required for compliance.

Before SOX took effect, the Boeing Company undertook an initial internal COSO framework audit. The audit is now an ongoing process at Boeing. At the onset, the company decided to use a binary judgment process (satisfactory or unsatisfactory) in assessing their then-current controls to the COSO framework's components, aspects, and details. The company intentionally set very high specifications for their "satisfactory" ratings.

Another option for use in internal COSO/COBIT audits is employing, as an assessment ranking, the maturity models defined for both frameworks. These models are very similar to the Software Engineering Institute's (SEI's) "Capability Maturity Model Integration" (CMMI) models found at <http://www.sei.cmu.edu/cmmi/models/>.

COSO Maturity Model

1. Unreliable
2. Informal
3. Standardized
4. Monitored
5. Optimized

COBIT Maturity Model

0. Non-Existent
1. Initial / Ad Hoc
2. Repeatable but Intuitive
3. Defined Process
4. Managed and Measurable
5. Optimized

Both COSO and COBIT frameworks provide documentation detailing explicit criteria required to meet these maturity levels for the numerous objectives and components.

The consensus among internal control auditors for first year SOX Section 404 certifications and attestations, which are due beginning November 15, 2004, is that companies must have their internal financial process controls in place and operational, at minimum, to both the COSO and COBIT maturity levels of three.

FACTS PERTINENT

Of the 164 identified COBIT objectives relating to SOX compliance, many are based on strategic IT planning, implementation and adherence to established company policies, as well as ensuring physical security for IT facilities. No stand-alone software tool can meet these objectives. To meet these objectives, IT executives and operations must impose active, standardized procedural processes. However, there are many other COBIT objectives pertaining to SOX compliance that can pass muster only through the implementation of mature, best-practices software tools.

Consider the following detailed control objective under the "Planning & Organization" section of COBIT:

PO7.8 Job Change and Termination: Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Clearly, COBIT objective PO7.8 calls for a procedure to be set in place to avoid disruptions and potential security lapses when key personnel change job function or leave the company. A software tool is not likely to apply in this case.

Now consider the following objective under the "Acquisition & Implementation" section of COBIT:

A13.6 System Software Change Controls: Procedures should be implemented to ensure that system software changes are controlled in line with the organization's change management procedures.

In this case, a Change Management tool could define a controlled and repeatable process for software development. Its use would be highly effective in meeting COBIT objective A13.6.

As a provider of software management and security tools for IBM iSeries computers, SoftLanding Systems offers a suite of software products that address 66 of the 164 identified SOX related COBIT objectives. A tabular listing of these 164 objectives, identifying those that map to specific SoftLanding products, can be found in the attached appendix.

Sample lists of COBIT objectives, broken down into Change Control and Project Management items, as well as Security Auditing and Control items, are presented on the following pages along with the pertinent SoftLanding products.

A SAMPLING OF COBIT CONTROL OBJECTIVES ASSOCIATED WITH CHANGE CONTROL AND PROJECT MANAGEMENT

Below is a partial list of summarized objectives stemming from COBIT that pertain to change management:

- Software changes must be controlled in accordance with the organization's change management procedures. (A13.6)²
- Procedures should be in place to control the handover of software from development to test to production environments. (15.12)
- Development personnel are prohibited from migrating applications and data from the test environment to production. (A13.4)

²Reference to relevant COBIT detailed control objective.

- A similar software management process should be observed whether developing a new application or modifying an existing application. (A12.2)
- Procedures should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the system. (A16.2)
- The release of software should be governed by formal procedures that ensure sign-offs or approvals. (A16.7)
- Installation of software changes must address data conversion.
- Changes must be tested by a development-independent group before installation into the production environment. (A15.7)
- Back-out plans for software changes should be in place. (A12.14, A15.7)
- Internal control measures should ensure distribution of the correct software element to the right place, with integrity and adequate audit trails. (A16.8)
- The software management framework should require that a test plan be created for every development, implementation, and modification project. (PO10.11)

PERTINENT PRODUCTS FROM SOFTLANDING

TurnOver Change Management provides the necessary controls throughout the entire development lifecycle to reinforce and audit your company's change management procedures for SOX compliance. Specific features include standardized controls for source management, quality assurance, promotion approval, and distribution to the production environment. The built-in Project Management module provides issue tracking, task management, task status notification and access to object history. TurnOver reports that facilitate auditing include: audit history, object history, source checkout history, task activity, and programmer history.

TestBench is a comprehensive iSeries testing tool that uniquely integrates database, screen, and report testing functions. Among its many features is the ability to create test data and test plans. TestBench is integrated with TurnOver, allowing you to associate test plans with specific tasks. As a result, TurnOver can automatically run TestBench tests as part of the promotion process. TurnOver also links TestBench test results to the originating TurnOver task so that you can see all task details, including test history, in one place.

A SAMPLING OF COBIT CONTROL OBJECTIVES ASSOCIATED WITH SECURITY AUDITING AND CONTROLS

Below is a partial list of summarized objectives stemming from COBIT that pertain to security and data integrity:

- Security measures should be in line with business requirements, including translating risk assessment information to the IT security plan. (DS5.1)³
- The use of sensitive software utilities should be controlled, monitored, and logged. (A13.7)
- Security levels for access control should be based on a user's demonstrated need to view, add, change or delete data. (DS5.3)
- Review and confirm access rights periodically. (DS5.5)
- Minimize the need for individuals to use multiple logins. (DS5.2)
- Control and access for remote connection to networks and/or applications is in place. (DS5.2)
- Adequate passwords as well as periodic password changes are required. (DS5.2)
- Establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts. (DS5.4)

³Reference to relevant COBIT detailed control objective.

- Security activity is logged and any indication of a security violation is reported immediately and acted upon in a timely manner. (DS5.7)
- Management should ensure that re-accreditation of security is periodically performed. (DS5.12)
- Logical access to computer resources should be based upon the principle of least privilege. (DS5.10)

PERTINENT PRODUCTS FROM SOFTLANDING

PowerLock FlashAudit can be used to provide an initial assessment of security risks. In just a few minutes, the product provides data that delineates the current state of security on your iSeries. We interpret the data and provide you with a comprehensive report that details the specific risks and includes recommendations for resolution.

PowerLock NetworkSecurity provides iSeries Exit Point auditing and controls to protect the integrity of your data. The product covers numerous exit points that provide access to your iSeries, such as those pertaining to ODBC (Microsoft Excel, Microsoft Access, Client/Access file transfer), FTP, TelNet, Remote Command, Network Neighborhood, DDM, and more. All transactions are stored in a secure, AS/400 journal.

PowerLock SecurityAudit provides over 200 reports for internal OS/400 auditing. SecurityAudit utilizes the OS/400 audit journal and provides reporting for both ad-hoc and scheduled intervals. The Audit Diary feature provides an on-screen summary, listing all changes since the last report was run. This provides administrators with a quick view of system security changes. Audit reports for current and changed values are available for system value and user profile changes, object access, command usage, and more. PowerLock NetworkSecurity audit reports can also be executed and scheduled from SecurityAudit.

VISUAL Security Suite utilizes the OS/400 Audit Journal to capture all messages related to internal OS/400 Security and the Windows Event Log. Its Smart Console offers a graphical interface from which to manage filtering of all messages. Business and enterprise-wide templates provide granularity in views. Pre-configured alarms alert Administrators of sensitive security events and custom-designed action sets determine how the event is handled. For example, if the system security level is unexpectedly changed from

50 to 30, the Security Agent can automatically change the security level back to 50; end the job that made the change; disable the user profile that was used; and send an alert describing what occurred - all within seconds. VISUAL Security Suite also interfaces with PowerLock NetworkSecurity and other iSeries Exit Point software to provide real-time monitoring, alarms, action sets, and messaging for sensitive Exit Point transactions.

SoftMenu is an AS/400 menu management product with which you control access to your applications by user or group. Options can be scheduled in terms of availability, or completely disabled. Reports are included that tell you who used which applications and when, and what users have access to particular applications.

SUMMARY

The Sarbanes-Oxley Act of 2002 mandates all public corporations conducting business in the U.S. move to a higher standard of corporate governance. Beginning in November of 2004, companies must state publicly that they are in full compliance with specific financial controls enacted into law to prevent recurrence of financial improprieties.

There are no quick fixes corporations can employ for SOX compliance. They should first assess their existing internal process controls for financial applications against both COSO and COBIT framework standards. Once the weak links in the chain of current controls are identified, control authorities can be redistributed and current controls can be augmented with additional capabilities, meeting both the targeted COSO and COBIT standards, and therefore meeting SOX mandates.

These are not optional tasks; they are required by law. Companies must distribute funding to initiate and subsequently monitor any required SOX compliance project.

For IBM iSeries machines, SoftLanding Systems offers a suite of software security tools addressing over 40% of the SOX related COBIT IT objectives. These include TurnOver Change Management, TestBench, PowerLock, SoftMenu and the VISUAL Security Suite. SoftLanding products have been promoting mature, best practice IT business processes since the late 1980s.

AN IT EXECUTIVE'S OVERVIEW OF THE SARBANES-OXLEY ACT OF 2002

For IT departments, complying with the new mandates of the Sarbanes - Oxley Act should actually be a blessing in disguise. By being forced to operate at a higher IT governance maturity, IT departments will find they have acquired the necessary methodologies for the selection, installation, and maintenance of ever more sophisticated IT business functions. This should elevate the entire department from a tactical corporate cost center, to a strategic corporate resource.

REFERENCE URLS

The Sarbanes-Oxley Act

<http://www.law.uc.edu/CCL/SOact/soact.pdf>

COBIT

http://www.isaca.org/template.cfm?section=about_isaca

COSO

<http://www.coso.org/>

(for the white paper about Boeing's pre-SOX COSO internal audit, click "articles" on the top left side.)

CARDdecisions, Inc.

<http://www.net4solutions.com/clients/CARDdecisions/website/CARDWebDownloads.nsf/>

Software Engineering Institute's (SEI's)

Capability Maturity Model Integration (CMMI) models

<http://www.sei.cmu.edu/cmmi/models/>

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
Planning and Organization		
PO4 – Determine the IT Organization and Relationships		
PO4.1 – IT Planning or Steering Committee	The organization’s senior management should appoint a planning or steering committee to oversee the IT function and its activities. Committee membership should include representatives from senior management, user management, and the IT function. The committee should meet regularly and report to senior management.	---
PO4.4 – Roles and Responsibilities	Management should ensure that all personnel in the organization have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organized and undertaken to increase awareness and discipline.	---
PO4.6 – Responsibility for Logical and Physical Security	Management should formally assign the responsibility for assuring both the logical and physical security of the organization’s information assets to an information security manager, reporting to the organization’s senior management. At a minimum, security management responsibility should be established at the organization-wide level to deal with overall security issues in an organization. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.	---
PO4.8 – Data and System Ownership	Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
PO4.10 – Segregation of Duties	<p>Senior management should implement a division of roles and responsibilities that should exclude the possibility for a single individual to subvert a process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between the following functions:</p> <ul style="list-style-type: none"> - Information systems use - Data entry - Computer operation - Network management - System administration - Systems development and maintenance - Change management - Security administration - Security audit 	---
PO5 – Manage the Information Technology Investment		
PO5.1 – Annual IT Operating Budget	Senior management should implement a budgeting process to ensure that an annual IT operating budget is established and approved in line with the organization’s long- and short-range plans as well as with the IT long- and short-range plans. Funding alternatives should be investigated.	---
PO5.2 – Cost and Benefit Monitoring	Management should establish a cost monitoring process comparing actual to budgets. Moreover, the possible benefits derived from the IT activities should be determined and reported. For cost monitoring, the source of the actual figures should be based upon the organization’s accounting system and that system should routinely record, process, and report the costs associated with the activities of the IT function. For benefit monitoring, high-level performance indicators should be defined, regularly reported, and reviewed for adequacy.	---
PO5.3 – Cost and Benefit Justification	A management control should be in place to guarantee that the delivery of services by the IT function is cost justified and in line with the industry. The benefits derived from IT activities should similarly be analyzed.	---
PO6 – Communicate Management Aims and Direction		
PO6.1 – Positive Information Control Environment	In order to provide guidance for proper behavior, remove temptation for unethical behavior, and provide discipline, where appropriate, management should create a framework and an awareness program fostering a positive control environment throughout the entire organization. This should address the integrity, ethical values and competence of the people, management philosophy, operating style, and accountability. Specific attention is to be given to IT aspects, including security and business continuity planning.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
PO6.5 – Maintenance of Policies	Policies should be adjusted regularly to accommodate changing conditions. Policies should be re-evaluated, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management should provide a framework and process for the periodic review and approval of standards, policies, directives, and procedures.	---
PO6.6 – Compliance with Policies, Procedures, and Standards	Management should ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that policies and procedures are being followed. Compliance procedures for ethical, security, and internal control standards should be set by top management and promoted by example.	---
PO6.8 – Security and Internal Control Framework Policy	Management should assume full responsibility for developing and maintaining a framework policy that establishes the organization’s overall approach to security and internal control to establish and improve the protection of IT resources and integrity of IT systems. The policy should comply with overall business objectives and be aimed at minimization of risks through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration. Measures should be based on cost/benefit analyses and should be prioritized. In addition, management should ensure that this high-level security and internal control policy specifies the purpose and objectives, the management structure, the scope within the organization, the definition and assignment of responsibilities for implementation at all levels, and the definition of penalties and disciplinary actions associated with failing to comply with security and internal control policies. Criteria for periodic re-evaluation of the framework should be defined to support responsiveness to changing organizational, environmental, and technical requirements.	---
PO7 – Manage Human Resources		
PO7.8 – Job Change and Termination	Management should ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.	---
PO9 – Assess Risks		
PO9.2 – Risk Assessment Approach	Management should establish a general risk assessment approach that defines the scope and boundaries, the methodology to be adopted for risk assessments, the responsibilities and the required skills. Management should lead the identification of the risk mitigation solution and be involved in identifying vulnerabilities. Security specialists should lead threat identification, and IT specialists should drive the control selection. The quality of the risk assessments should be ensured by a structured method and skilled risk assessors.	PowerLock

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
PO9.3 – Risk Identification	The risk assessment approach should focus on the examination of the essential elements of risk and the cause/effect relationship between them. The essential elements of risk include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences, and likelihood of threat. The risk identification process should include qualitative and, where appropriate, quantitative risk ranking and should obtain input from management brainstorming, strategic planning, past audits, and other assessments. The risk assessment should consider business, regulatory, legal, technology, trading partner, and human resources risks.	PowerLock
PO9.4 – Risk Measurement	The risk assessment approach should ensure that the analysis of risk identification information results in a quantitative and/or qualitative measurement of risk to which the examined area is exposed. The risk acceptance capacity of the organization should also be assessed.	---
PO9.5 – Risk Action Plan	The risk assessment approach should provide for the definition of a risk action plan to ensure that cost-effective controls and security measures mitigate exposure to risks on a continuing basis. The risk action plan should identify the risk strategy in terms of risk avoidance, mitigation, or acceptance.	---
PO9.6 – Risk Acceptance	The risk assessment approach should ensure the formal acceptance of the residual risk, depending on risk identification and measurement, organizational policy, uncertainty incorporated in the risk assessment approach itself and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.	---
PO9.7 – Safeguard Selection	While aiming for a reasonable, appropriate and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The control system also needs to balance prevention, detection, correction and recovery measures. Furthermore, management needs to communicate the purpose of the control measures, manage conflicting measures and monitor the continuing effectiveness of all control measures.	---
PO9.8 – Risk Assessment Commitment	Management should encourage risk assessment as an important tool in providing information in the design and implementation of internal controls, in the definition of the IT strategic plan and in the monitoring and evaluation mechanisms.	---
PO10 – Manage Projects		
PO10.1 – Project Management Framework	Management should establish a general project management framework that defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points, and approvals.	TurnOver
PO10.2 – User Department Participation in Project Initiation	The organization’s project management framework should provide for participation by the affected user department management in the definition and authorization of a development, implementation, or modification project.	TurnOver

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
PO10.3 – Project Team Membership and Responsibilities	The organization’s project management framework should specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members.	TurnOver
PO10.4 – Project Definition	The organization’s project management framework should provide for the creation of a clear written statement defining the nature and scope of every implementation project before work on the project begins.	TurnOver
PO10.5 – Project Approval	The organization’s project management framework should ensure that for each proposed project, the organization’s senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project.	---
PO10.6 – Project Phase Approval	The organization’s project management framework should provide for designated managers of the user and IT functions to approve the work accomplished in each phase of the cycle before work on the next phase begins.	TurnOver
PO10.7 – Project Master Plan	Management should ensure that for each approved project a project master plan is created which is adequate for maintaining control over the project throughout its life and which includes a method of monitoring the time and costs incurred throughout the life of the project. The content of the project plan should include statements of scope, objectives, required resources and responsibilities and should provide information to permit management to measure progress.	---
PO10.8 – System Quality Assurance Plan	Management should ensure that the implementation of a new or modified system includes the preparation of a quality plan that is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned.	TestBench
PO10.9 – Planning of Assurance Methods	Assurance tasks are to be identified during the planning phase of the project management framework. Assurance tasks should support the accreditation of new or modified systems and should assure that internal controls and security features meet the related requirements.	TestBench
PO10.10 – Formal Project Risk Management	Management should implement a formal project risk management program for eliminating or minimizing risks associated with individual projects (i.e., identifying and controlling the areas or events that have the potential to cause unwanted change).	---
PO10.11 – Test Plan	The organization’s project management framework should require that a test plan be created for every development, implementation, and modification project.	TestBench
PO10.12 – Training Plan	The organization’s project management framework should require that a training plan be created for every development, implementation and modification project.	---
PO10.13 – Post-Implementation Review Plan	The organization’s project management framework should provide, as an integral part of the project team’s activities, for the development of a plan for a post-implementation review of every new or modified information system to ascertain whether the project has delivered the planned benefits.	---
PO11 – Manage Quality		

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
PO11.12 – Program Testing Standards	The organization’s system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.	---
PO11.13 – System Testing Standards	The organization’s system development life cycle methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.	---
PO11.14 – Parallel/Pilot Testing	The organization’s system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.	---
PO11.15 – System Testing Documentation	The organization’s system development life cycle methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.	---
Acquisition and Implementation		
AI2 – Acquire & Maintain Application Software		
AI2.1 – Design Methods	The organization’s system development life cycle methodology should provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements.	---
AI2.2 – Major Changes to Existing Systems	Management should ensure that in the event of major changes to existing systems, a similar development process is observed as in the case of the development of new systems.	TurnOver
AI2.3 – Design Approval	The organization’s system development life cycle methodology should require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organization’s senior management, when appropriate.	---
AI2.4 – File Requirements Definition and Documentation	The organization’s system development life cycle methodology should provide that an appropriate procedure be applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the data dictionary rules are respected.	---
AI2.5 – Program Specifications	The organization’s system development life cycle methodology should require that detailed written program specifications be prepared for each information system development or modification project. The methodology should further ensure that program specifications agree with system design specifications.	---
AI2.6 – Source Data Collection Design	The organization’s system development life cycle methodology should require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
AI2.7 – Input Requirements Definition and Documentation	The organization’s system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.	---
AI2.8 – Definition of Interfaces	The organization’s system development life cycle methodology should provide that all external and internal interfaces are properly specified, designed, and documented.	---
AI2.10 – Processing Requirements Definition and Documentation	The organization’s system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project.	---
AI2.11 – Output Requirements Definition and Documentation	The organization’s system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project.	---
AI2.12 – Controllability	The organization’s system development life cycle methodology should require that adequate mechanisms for assuring the internal control and security requirements be specified for each information system development or modification project. The methodology should further ensure that information systems are designed to include application controls that guarantee the accuracy, completeness, timeliness and authorization of inputs, processing and outputs. Sensitivity assessment should be performed during initiation of system development or modification. The basic security and internal control aspects of a system to be developed or modified should be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible.	TurnOver
AI2.13 – Availability as a Key Design Factor	The organization’s system development life cycle methodology should provide that availability is considered in the design process for new or modified information systems at the earliest possible stage. Availability should be analyzed and, if necessary, increased through maintainability and reliability improvements.	TurnOver, TurnOver PDQ
AI2.14 – IT Integrity Provisions in Application Program Software	The organization should establish procedures to assure, where applicable, that application programs contain provisions that routinely verify the tasks performed by the software to help assure data integrity, and which provide the restoration of the integrity through rollback or other means.	TurnOver
AI2.15 – Application Software Testing	Unit testing, application testing, integration testing, system testing, and load and stress testing should be performed according to the project test plan and established testing standards before the user approves it. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.	TurnOver, TestBench
AI2.16 – User Reference and Support Materials	The organization’s system development life cycle methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every information system development or modification project.	---
AI2.17 – Reassessment of System Design	The organization’s system development life cycle methodology should ensure that the system design is reassessed whenever significant technical and/or logical discrepancies occur during system development or maintenance.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
AI3 – Acquire & Maintain Technology Infrastructure		
AI3.1 – Assessment of New Hardware and Software	Hardware and software selection criteria should be based on the functional specifications for the new or modified system and should identify mandatory and optional requirements. Procedures should be in place to assess new hardware and software for any impact on the performance of the overall system.	---
AI3.2 – Preventative Maintenance for Hardware	IT management should schedule routine and periodic hardware maintenance to reduce the frequency and impact of performance failures.	---
AI3.3 – System Software Security	IT management should ensure that the set up of system software to be installed does not jeopardize the security of the data and programs being stored on the system. Attention should be paid to set up and maintenance of system software parameters.	---
AI3.4 – System Software Installation	Procedures should be implemented to ensure that system software is installed in accordance with the acquisition and maintenance framework for the technology infrastructure. Testing should be performed before use in the production environment is authorized. A group independent of the users and developers should control the movement of programs and data among libraries.	TurnOver, TestBench
AI3.5 – System Software Maintenance	Procedures should be implemented to ensure that system software is maintained in accordance with the acquisition and maintenance framework for the technology infrastructure.	---
AI3.6 – System Software Change Controls	Procedures should be implemented to ensure that system software changes are controlled in line with the organization's change management procedures.	TurnOver
AI3.7 – Use and Monitoring of System Utilities	Policies and techniques should be implemented for using, monitoring and evaluating the use of system utilities. Responsibilities for using sensitive software utilities should be clearly defined and understood by developers, and the use of the utilities should be monitored and logged.	SoftMenu, PowerLock, VISUAL Security Suite
AI4 – Develop & Maintain Procedures		
AI4.1 – Operational Requirements and Service Levels	The organization's system development life cycle methodology should ensure the timely definition of operational requirements and service levels.	---
AI4.2 – User Procedures Manual	The organization's system development life cycle methodology should provide that adequate user procedures manuals be prepared and refreshed as part of every information system development, implementation, or modification project.	---
AI4.3 – Operations Manual	The organization's system development life cycle methodology should provide that an adequate operations manual be prepared and kept up-to-date as part of every information system development, implementation, or modification project.	---
AI4.4 – Training Materials	The organization's system development life cycle methodology should ensure that adequate training materials are developed as part of every information system development, implementation, or modification project. These materials should be focused on the system's use in daily practice.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
A15 – Install & Accredit System		
A15.2 – Application Software Performance Sizing	Application software performance sizing (optimization) should be established as an integral part of the organization’s system development life cycle methodology to forecast the resources required for operating new and significantly changed software.	---
A15.3 – Implementation Plan	An implementation plan should be prepared, reviewed and approved by relevant parties and be used to measure progress. The implementation plan should address site preparation, equipment acquisition and installation, user training, installation of operating software changes, implementation of operating procedures and conversion.	---
A15.4 – System Conversion	The organization’s system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan.	TurnOver
A15.5 – Data Conversion	Management should require that a data conversion plan is prepared, defining the methods of collecting and verifying the data to be converted and identifying and resolving any errors found during conversion. Tests to be performed include comparing the original and converted files, checking the compatibility of the converted data with the new system, checking master files after conversion to ensure the accuracy of master file data, and ensuring that transactions affecting master files update both the old and the new master files during the period between initial conversion and final implementation. A detailed verification of the initial processing of the new system should be performed to confirm successful implementation. Management should ensure that the responsibility for successful conversion of data lies with the system owners.	TurnOver, TurnOver PDQ
A15.6 – Testing Strategies and Plans	Testing strategies and plans should be prepared and signed off by the system owner and IT management.	TestBench
A15.7 – Testing of Changes	Management should ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins. Back-out plans should also be developed. Acceptance testing should be carried out in an environment representative of the future operational environment (e.g., similar security, internal controls, workloads, etc.).	TurnOver, TestBench
A15.8 – Parallel/Pilot Testing Criteria and Performance	Procedures should be in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance.	TurnOver, TestBench
A15.9 – Final Acceptance Test	Procedures should provide, as part of the final acceptance or quality assurance testing of new or modified information systems, for a formal evaluation and approval of the test results by management of the affected user department(s) and the IT function. The tests should cover all components of the information system (e.g., application software, facilities, technology, user procedures).	TurnOver, TestBench

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
AI5.10 – Security Testing and Accreditation	Management should define and implement procedures to ensure that operations and user management formally accept the test results and the level of security for the systems, along with the remaining residual risk. These procedures should reflect the agreed upon roles and responsibilities of end user, system development, network management and system operations personnel, taking into account segregation, supervision, and control issues.	---
AI5.11 – Operational Test	Management should ensure that before moving the system into operation, the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment.	TestBench
AI5.12 – Promotion to Production	Management should define and implement formal procedures to control the handover of the system from development to testing to operations. Management should require that system owner authorization is obtained before a new system is moved into production and that before the old system is discontinued, the new system will have successfully operated through all daily, monthly, and quarterly production cycles. The respective environments should be segregated and properly protected.	TurnOver
AI5.13 – Evaluation of Meeting User Requirements	The organization's system development life cycle methodology should require that a post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) be conducted to assess whether the users' needs are being met by the system.	---
AI6 – Manage Changes		
AI6.1 – Change Request Initiation and Control	IT management should ensure that all requests for changes, system maintenance, and supplier maintenance are standardized and are subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.	TurnOver
AI6.2 – Impact Assessment	A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.	TurnOver
AI6.3 – Control of Changes	IT management should ensure that change management, software control, and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support the recording and tracking of changes made to large, complex information systems.	TurnOver
AI6.4 – Emergency Changes	IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational, and management assessment prior to implementation. The emergency changes should be recorded and authorized by IT management prior to implementation.	TurnOver
AI6.5 – Documentation and Procedures	The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.	TurnOver

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
AI6.6 – Authorized Maintenance	IT management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.	TurnOver
AI6.7 – Software Release Policy	IT management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.	TurnOver
AI6.8 – Distribution of Software	Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.	TurnOver
Delivery and Support		
DS2 – Manage Third-Party Services		
DS2.1 – Supplier Interfaces	Management should ensure that all third-party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented.	---
DS2.3 – Third-Party Contracts	Management should define specific procedures to ensure that for each relationship with a third-party service provider a formal contract is defined and agreed upon before work starts.	---
DS2.5 – Outsourcing Contracts	Specific organizational procedures should be defined to ensure that the contract between the facilities management provider and the organization is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.	---
DS2.6 – Continuity of Services	With respect to ensuring continuity of services, management should consider business risk related to the third-party in terms of legal uncertainties and the going concern concept, and negotiate escrow contracts where appropriate.	---
DS2.7 – Security Relationships	With regard to relationships with third-party service providers, management should ensure that security agreements (e.g., non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities.	---
DS4 – Ensure Continuous Service		

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS4.3 – IT Continuity Plan Contents	IT management should ensure that a written plan is developed containing the following: <ul style="list-style-type: none"> - Guidelines on how to use the continuity plan - Emergency procedures to ensure the safety of all affected staff members - Response procedures meant to bring the business back to the state it was in before the incident or disaster - Recovery procedures meant to bring the business back to the state it was in before the incident or disaster - Procedures to safeguard and reconstruct the home site - Coordination procedures with public authorities - Communication procedures with stakeholders, employees, key customers, critical suppliers, stockholders, and management - Critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media 	---
DS4.4 – Minimizing IT Continuity Requirements	IT management should establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies, and furniture.	---
DS4.5 – Maintaining the IT Continuity Plan	IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change and management and human resources procedures.	---
DS4.6 – Testing the IT Continuity Plan	To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.	---
DS4.7 – IT Continuity Plan Training	The disaster continuity methodology should ensure that all concerned parties receive regular training sessions regarding the procedures to be followed in case of an incident or disaster.	---
DS4.8 – IT Continuity Plan Distribution	Given the sensitive nature of information in the continuity plan, the latter should be distributed only to authorized personnel and should be safeguarded against unauthorized disclosure. Consequently, sections of the plan need to be distributed on a need-to-know basis.	---
DS4.11 – Back-up Site and Hardware	Management should ensure that the continuity methodology incorporates an identification of alternatives regarding the back-up site and hardware as well as a final alternative selection. If applicable, a formal contract for these types of services should be concluded.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS4.12 – Off-site Back-up Storage	Off-site storage of critical back-up media, documentation and other IT resources should be established to support recovery and business continuity plans. Business process owners and IT function personnel should be involved in determining what back-up resources need to be stored off-site. The off-site storage facility should be environmentally appropriate to the media and other resources stored and should have a level of security commensurate with that needed to protect the back-up resources from unauthorized access, theft, or damage. IT management should ensure that off-site arrangements are periodically assessed, at least annually, for content, environmental protection, and security.	---
DS5 – Ensure Systems Security		
DS5.1 – Manage Security Measures	IT security should be managed such that security measures are in line with business requirements including: <ul style="list-style-type: none"> - Translating risk assessment information to the IT security plans - Implementing the IT security plan - Updating the IT security plan to reflect changes in the IT configuration - Assessing the impact of change requests on IT security - Monitoring the implementation of the IT security plan - Aligning IT security procedures to other policies and procedures 	PowerLock, VISUAL Security Suite
DS5.2 – Identification, Authentication, and Access	The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple logins. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).	PowerLock
DS5.3 – Security of Online Access to Data	In an online IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual’s demonstrated need to view, add, change, or delete data.	PowerLock, SoftMenu
DS5.4 – User Account Management	Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.	SoftMenu, PowerLock
DS5.5 – Management Review of User Accounts	Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.	SoftMenu, PowerLock
DS5.6 – User Control of User Accounts	Users should systematically control the activity of their proper account(s). Also, information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	VISUAL Security Suite

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS5.7 – Security Surveillance	IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.	PowerLock, VISUAL Security Suite
DS5.8 – Data Classification	Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing “no protection” should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived, or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organizations, addressing both security and compliance with relevant legislation.	---
DS5.9 – Central Identification and Access Rights Management	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	SoftMenu, PowerLock
DS5.10 – Violation and Security Activity Reports	IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify, and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.	PowerLock, VISUAL Security Suite
DS5.11 – Incident Handling	Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective, and timely response to security incidents.	PowerLock, VISUAL Security Suite
DS5.12 – Reaccreditation	Management should ensure that reaccreditation of security (e.g., through “tiger teams”) is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.	PowerLock
DS5.13 – Counterparty Trust	Organizational policy should ensure that control practices are implemented to verify the authenticity of the counterparty providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens, or cryptographic keys.	---
DS5.14 – Transaction Authorization	Organizational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user’s claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS5.15 – Non-Repudiation	Organizational policy should ensure that, where appropriate, either party cannot deny transactions, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third parties, with appropriate policies that take into account relevant regulatory requirements.	PowerLock
DS5.16 – Trusted Path	Organizational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords, and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems, and between systems.	---
DS5.17 – Protection of Security Functions	All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security design, but should not base their security on the design being secret.	---
DS5.18 – Cryptographic Key Management	Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure. If a key is compromised, management should ensure this information is propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms.	---
DS5.19 – Malicious Software Prevention, Detection, and Correction	Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting.	---
DS5.20 – Firewall Architectures and Connections with Public Networks	If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.	---
DS5.21 – Protection of Electronic Value	Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees, and validation methods used.	---
DS6 – Identify and Allocate Costs		
DS6.1 – Chargeable Items	IT management, with guidance from senior management, should ensure that chargeable items are identifiable, measurable, and predictable by users. Users should be able to control the use of information services and associated billing levels.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS6.2 – Costing Procedures	IT management should define and implement costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are to be adequately analyzed and reported on to facilitate the cost monitoring. In addition, management should periodically evaluate the results of the IT function's job cost accounting procedures, in light of the organization's other financial measurement systems.	---
DS6.3 – User Billing and Chargeback Procedures	IT management should define and use billing and chargeback procedures. It should maintain user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs. The rate charged should reflect the associated costs of providing services.	---
DS9 – Manage The Configuration		
DS9.1 – Configuration Recording	Procedures should be in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition. These procedures should also provide for the authorized disposal and consequential sale of configuration items. Moreover, procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of changed records.	TurnOver
DS9.2 – Configuration Baseline	IT management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes.	TurnOver
DS9.3 – Status Accounting	IT management should ensure that the configuration records reflect the actual status of all configuration items including the history of changes.	TurnOver
DS9.4 – Configuration Control	Procedures should ensure that the existence and consistency of recording of the IT configuration is periodically checked.	---
DS9.5 – Unauthorized Software	Clear policies restricting the use of personal and unlicensed software should be developed and enforced. The organization should use virus detection and remedy software. Business and IT management should periodically check the organization's personal computers for unauthorized software. Compliance with the requirements of software and hardware license agreements should be reviewed on a periodic basis.	---
DS9.6 – Software Storage	A file storage area (library) should be defined for all valid software items in appropriate phases of the system development life cycle. These areas should be separated from each other and from development, testing, and production file storage areas.	TurnOver
DS9.7 – Configuration Management Procedures	Configuration management procedures should be established to ensure that critical components of the organization's IT resources have been appropriately identified and are maintained. There should be an integrated process whereby current and future processing demands are measured and provide input to the IT resource acquisitions process.	TurnOver

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS9.8 – Software Accountability	Software should be labeled, inventoried, and properly licensed. Library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information, and copies of previous versions.	TurnOver
DS10 – Manage Problems And Incidents		
DS10.1 – Problem Management System	IT management should define and implement a problem management system to ensure that all operational events which are not part of the standard operation (incidents, problems, and errors) are recorded, analyzed and resolved in a timely manner. Emergency program change procedures should be promptly tested, documented, approved, and reported. Incident reports should be established in the case of significant problems.	TurnOver
DS10.2 – Problem Escalation	IT management should define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis. These procedures should ensure that these priorities are appropriately set. The procedures should also document the escalation process for the activation of the IT continuity plan.	TurnOver
DS10.3 – Problem Tracking and Audit Trail	The problem management system should provide for adequate audit trail facilities that allow tracing from incident to underlying cause (e.g., package release or urgent change implementation) and back. It should work closely with change management, availability management, and configuration management.	TurnOver
DS10.4 – Emergency and Temporary Access Authorizations	Emergency and temporary access authorizations should be documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period.	---
DS10.5 – Emergency Processing Priorities	Emergency processing priorities should be established, documented, and approved by appropriate program and IT management.	---
DS11 – Manage Data		
DS11.2 – Source Document Authorization Procedures	Management should ensure that source documents are properly prepared by authorized personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.	TurnOver
DS11.6 – Data Input Authorization Procedures	The organization should establish appropriate procedures to ensure that data input is performed only by authorized staff.	---
DS11.7 – Accuracy, Completeness, and Authorization Checks	Transaction data entered for processing (people-generated, system-generated, or interfaced inputs) should be subject to a variety of controls to check for accuracy, completeness, and validity. Procedures should also be established to assure that input data is validated and edited as close to the point of origination as possible.	---
DS11.8 – Data Input Error Handling	The organization should establish procedures for the correction and resubmission of data which was erroneously input.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS11.9 – Data Processing Integrity	The organization should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.	---
DS11.10 – Data Processing Validation and Editing	The organization should establish procedures to ensure that data processing validation, authentication, and editing are performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved.	---
DS11.11 – Data Processing Error Handling	The organization should establish data processing error handling procedures that enable erroneous transactions to be identified without being processed and without undue disruption of the processing of other valid transactions.	---
DS11.13 – Output Distribution	The organization should establish and communicate written procedures for the distribution of IT output.	---
DS11.14 – Output Balancing and Reconciliation	The organization should establish procedures for assuring that output routinely is balanced to the relevant control totals. Audit trails should be provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data.	---
DS11.15 – Output Review and Error Handling	The organization’s management should establish procedures for assuring that the accuracy of output reports is reviewed by the provider and the relevant users. Procedures should also be in place for controlling errors contained in the output.	---
DS11.18 – Protection of Disposed Sensitive Information	Management should define and implement procedures to prevent access to sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. Such procedures should guarantee that data marked as deleted or to be disposed cannot be retrieved by any internal or third party.	---
DS11.23 – Back-up and Restoration	Management should implement a proper strategy for backup and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan. Procedures should be set up to ensure that back-ups are satisfying the above-mentioned requirements.	---
DS11.24 – Back-up Jobs	Procedures should be in place to ensure back-ups are taken in accordance with the defined back-up strategy and the usability of back-ups is regularly verified.	---
DS11.25 – Back-up Storage	Back-up procedures for IT-related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS12 Manage Facilities		
DS12.1 – Physical Security	Appropriate physical security and access control measures should be established for IT facilities, including off-site use of information devices in conformance with the general security policy. Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system’s operation. Access should be restricted to individuals who have been authorized to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism.	---
DS12.3 – Visitor Escort	Appropriate procedures are to be in place ensuring that individuals, who are not members of the IT function’s operations group, are escorted by a member of that group when they must enter the computer facilities. A visitor’s log should be kept and reviewed regularly.	---
DS12.5 – Protection Against Environmental Factors	IT management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat, and humidity). Specialized equipment and devices to monitor and control the environment should be installed.	---
DS13 – Manage Operations		
DS13.1 – Processing Operations Procedures and Instructions Manual	IT management should establish and document standard procedures for IT operations (including network operations). All IT solutions and platforms in place should be operated using these procedures, which should be reviewed periodically to ensure effectiveness and adherence.	---
DS13.2 – Start-up Process and Other Operations Documentation	IT management should ensure that the operations staff is adequately familiar and confident with the start-up process and other operations tasks by having them documented, periodically tested and adjusted when required.	---
DS13.3 – Job Scheduling	IT management should ensure that the continuous scheduling of jobs, processes and tasks is organized into the most efficient sequence, maximizing throughput and utilization, to meet the objectives set in service level agreements. The initial schedules, as well as changes to these schedules, should be appropriately authorized.	VISUAL Control Center
DS13.4 – Departures from Standard Job Schedules	Procedures should be in place to identify, investigate and approve departures from standard job schedules.	VISUAL Control Center
DS13.5 – Processing Continuity	Procedures should require processing continuity during operator shift changes by providing for formal handover of activity, status updates, and reports on current responsibilities.	---
DS13.6 – Operations Logs	Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing and the other activities surrounding or supporting processing.	VISUAL Message Center
DS13.7 – Safeguard Special Forms and Output Devices	Management should establish appropriate physical safeguards over special forms, such as negotiable instruments, and over sensitive output devices, such as signature cartridges, taking into consideration proper accounting of IT resources, forms or items requiring additional protection and inventory management.	---

Appendix A: CobiT Objectives Relevant to Sarbanes-Oxley IT Compliance

Detailed Control Objective	Detailed Control Objective Description	SoftLanding Supporting Tool
DS13.8 – Remote Operations	For remote operations, specific procedures should ensure that the connection and disconnection of the links to the remote site(s) are defined and implemented.	---
Monitoring		
M2 – Assess Internal Control Adequacy		
M2.1 – Internal Control Monitoring	Management should monitor the effectiveness of internal controls in the normal course of operations through management and supervisory activities, comparisons, reconciliations, and other routine actions. Deviations should evoke analysis and corrective action. In addition, deviations should be communicated to the individual responsible for the function and also at least one level of management above that individual. Serious deviations should be reported to senior management.	Supported by all SoftLanding tools
M2.2 – Timely Operation of Internal Controls	Reliance on internal controls requires that controls operate promptly to highlight errors and inconsistencies, and that these are corrected before they impact production and delivery. Information regarding errors, inconsistencies, and exceptions should be kept and systematically reported to management.	VISUAL Security Suite
M2.3 – Internal Control Level Reporting	Management should report information on internal control levels and exceptions to the affected parties to ensure the continued effectiveness of its internal control system. Actions should be taken to identify what information is needed at a particular level of decision-making.	---
M2.4 – Operational Security and Internal Control Assurance	Operational security and internal control assurance should be established and periodically repeated, with self-assessment or independent audit to examine whether or not the security and internal controls are operating according to the stated or implied security and internal control requirements. Ongoing monitoring activities by management should look for vulnerabilities and security problems.	PowerLock, VISUAL Security Suite





84 Elm St. • Peterborough, NH 03458
603/924-8818 • 800/545-9485 • fax: 603/924-6348 • www.softlanding.com • info@softlanding.com
© 2003 SoftLanding Systems, Inc.