



Netswitch™ Technology Management

# SOX COMPLIANCE READINESS



## The SOX Landscape

In the United States, the Sarbanes-Oxley Act of 2002 imposes stringent requirements on public companies and their executives to ensure the integrity of financial statements and filings. Outside the US, many countries are moving toward the adoption of similar regulations. Regardless of their location companies increasingly face laws designed to ensure and certify the accuracy of their financial processes.

Most companies' financial processes are embedded in computer systems, so complying with SOX, and SOX-like, regulations ultimately sets standards for these systems. The computer systems themselves must be structured and managed to prevent fraud, detect error and ensure completeness and accuracy. NTM can assess the adequacy of the IT control structures underlying your financial processes to confirm that they meet these standards and satisfy SOX.



## The Cost of non-Compliance

There are severe penalties for failure to comply with the requirements set by Sarbanes-Oxley. Regulatory sanctions may include fines in the millions of dollars and imprisonment. In addition, regulators may require regular, and bothersome and expensive, review by independent auditors of your program of protections. In many jurisdictions and industries there are additional laws and standards that establish comparable requirements and bring penalties for analogous failures. Third-party lawsuits for mis-representation, negligence and exposure of confidential information are increasingly common. Even simple publication of these failures can seriously damage a firm's image destroying customer and partner confidence, reducing market valuations, diminishing a brand franchise and embarrassing executives.

## What Does SOX Actually Require?

Four sections of the law set requirements that may affect a firm's computer systems. Of these, the most commonly cited is Section 404. Section 404 makes management responsible for providing an adequate internal control structure for financial reports and requires that an outside auditor review and offer an opinion on management's assessment of the control structure.

- Are all relevant transactions captured and reported accurately?
- Are unauthorized transactions prevented or detected?
- Do change management procedures ensure that any changes in processes are proper and authorized?

## How is SOX Compliance Related to Technology Infrastructure?

The linkage is clear –

- SOX requires that financial reports issued by a firm be accurate and complete;
- Today financial reports are typically derived from computer systems;

- Therefore the computer systems underlying the financial processes must satisfy a set of standards that ensure their integrity.

What management must assure, and what the auditor must verify, is that the computer systems at the center of the financial reporting processes are designed, implemented, secured and operated under a set of principles that ensure the accuracy of the results. So, for example, the requirement that unauthorized transactions are prevented or detected means that the network must be protected from outside "hackers" and that the permissions allowed internal users must be carefully controlled. The issues are the same whether the systems are ERP components or a suite of independent applications.

## Achieving Compliance

The rules implementing Sarbanes-Oxley require that the internal control procedures associated with the processes producing statements of financial results and condition be assessed against a "structured framework of controls." But this control structure is does not result from unique IT management approaches: it is realized by customary Best Practice IT techniques. SOX compliance simply requires that your financial systems conform to good procedure and solid IT management practices.

## How Can Netswitch Help?

Most management teams, and indeed many auditors, lack the technical expertise and experience needed to assess IT control structures. Netswitch is equipped to judge your IT infrastructure and management procedures against a set of Best Practice standards that establish the structured framework of controls demanded by SOX. Our assessment procedure involves extensive testing against these standards: we are able to confirm compliance or to identify deficiencies that must be corrected to enable your management, and your auditor, to attest to the adequacy of your control structure. We fully document the corrective actions needed to bring your systems, technical environment and management practices into compliance. The NTM Readiness Assessment will prepare you to successfully undergo a SOX Compliance Audit.



## The Netswitch Control Framework

SEC rules implementing Sarbanes-Oxley require that internal control procedures be assessed against a structured framework of controls. COBIT, Control Objectives for Information and Related Technology, defines an appropriate set of standards and is compliant with the COSO framework noted by the SEC in its regulations implementing SOX. Netswitch applies the COBIT framework of controls for its SOX Readiness Assessment.

## 1 Assess the IT environment

Our first step is to assess the overall IT environment: what is the technical infrastructure, what is the general technology "maturity level" and what are the relevant applications. This assessment includes management interviews and the use of questionnaires.

## 2 Select Appropriate Controls and Tests

Based on the environment assessment, we define a set of Control Objectives, Controls and Control Tests. COBIT provides the framework, but our approach is tailored to each client's environment.



## The Netswitch Process

COBIT defines a series of Business Processes that describe the IT environment. For each of these processes, a Control Objective targeting Sarbanes-Oxley compliance can be defined. Depending on the client environment, Netswitch determines one or more Controls to measure achievement of each Control Objective. Then we define a series Control Tests to assess satisfaction of each of these Controls. NTM executes this very carefully structured testing program to determine if the IT control structure is sufficient to comply with the requirements mandated by SOX.

## 3 Test

A schedule is set, the defined tests are executed and the findings documented.

## 4 Analyze Test Findings

The findings are reviewed and an analysis prepared and reviewed with management. Management comments are recorded and adjustments incorporated as appropriate.

## 5 Conclusion

The information is compiled in a formal report which includes recommended changes to correct deficiencies and achieve compliance. Reviews are conducted and the proposed changes discussed and clarified as necessary.

## Sample Framework Components

Business Process	COBIT Control Objective	Sample NTM Control	Sample NTM Control Te
<b>Ensure Systems Security</b>	Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.	Procedures are defined and observed to authenticate all users to support the validity of all entered transactions	<ul style="list-style-type: none"> <li>• Test a sample of financial applications to attempt to gain unauthorized access and to enter transaction types inappropriate to the User ID and Password</li> <li>• Review recent password changes and verify that they were made in accordance with the procedure</li> <li>• Review the Password Policy to verify that password specification results in sufficiently complex passwords</li> </ul>
		Where network connectivity is used, appropriate controls are deployed	<ul style="list-style-type: none"> <li>• Review system logs to verify that passwords are changed regularly as required by the procedure</li> <li>• Test the network security provisions to verify that outside parties cannot access financial systems.</li> <li>• Determine the sufficiency of perimeter security controls including firewalls, intrusion prevention and detection tools</li> <li>• Determine if antivirus systems are in place and updated regularly</li> <li>• Determine if management has obtained an independent assessment of the vulnerability of the network to attack in the past year and review the report to assure that necessary corrective action has been taken</li> </ul>
<b>Manage Data</b>	Controls provide reasonable assurance that data recorded, processed and reported remain complete, accurate and valid	A strategy for regular backup of data and programs has been implemented	<ul style="list-style-type: none"> <li>• Determine if the organization has procedures in place to back up data and programs based on IT and user requirements</li> <li>• Select a sample of data files and programs and determine if they are being backed up as required</li> </ul>
<b>Manage Changes</b>	Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production.	Requests for program changes, system changes and maintenance (including changes to system software) are documented and subject to formal change management procedures	<ul style="list-style-type: none"> <li>• Evaluate the process used to control and monitor change requests.</li> <li>• Consider whether change requests are properly initiated, approved and tracked.</li> <li>• Determine whether program modification is performed in a segregated, controlled environment</li> </ul>
<b>Manage Problems and incidents</b>	Controls provide reasonable assurance that any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution	A security incident response process exists to support timely response and investigation of unauthorized activities	<ul style="list-style-type: none"> <li>• Review the log of unauthorized activities and verify that a sample of incidents was researched and resolved in a timely and comprehensive fashion</li> <li>• Discuss incidents with a sample of users and verify that the incidents were recorded in the log</li> </ul>

Netswitch brings passion to the achievement of our mission:

"To improve our clients' business performance through cost-effective application of technology."

Our Clients, from small businesses to large enterprises, have seen the results...



**Adobe Systems Incorporated**

*Cyndi Rainey, Global Safety & Security Manager*

"Netswitch delivers a high level of service that provides global expertise, strategic project management, and cost savings. These tangibles support all the key necessities for a successful project and their commitment is invaluable."



**The Hong Kong & Shanghai Hotels Limited – Peninsula**

*Shane Izaks, General Manager, Information Technology*

"With regard to the Vulnerability Assessment, as a consequence of the potential vulnerabilities [Netswitch] identified and the corrections you proposed, we have made several changes and we are now completely confident that our hotels' network security ensures the confidentiality, integrity and availability of our IT systems."



**Vodafone Americas, Inc.**

*Robert Chu, Director of Support Services*

"Netswitch has added tremendous value to our IT/Telecom support with the array of services they provide. Their knowledge and experience was the catalyst in my decision making to entrust them with our past and future projects. In addition, their expertise and presence in Asia Countries is beneficial to my supporting region. I look forward to a strong and successful partnership."



**Verizon Wireless**

*Kelly Perry, Senior Telecommunications Engineer*

"Netswitch provided incredible service. They were always available for me -- before and after the project ended. Great support! I would definitely call on them again for another project."



**Nan Yang Textile Group**

*Ben Tuangsitthisombat, President*

"Netswitch has provided our IT Team an opportunity to review our IT strategy and also the high level skill required to secure and improve our network infrastructure. I am also impressed with your personal approach to handle our concerns and the willingness to commit to ensure our objectives are accomplished. It is these values you have demonstrated given us the confidence to continue to trust Netswitch."

[info@netswitch.net](mailto:info@netswitch.net) | [www.netswitch.net](http://www.netswitch.net)



**USA Headquarters**  
400 Oyster Point Blvd., Ste. 226  
So. San Francisco, CA 94080, USA

**China Office**  
Level 2501, Bank of China Tower  
1 Garden Road, Central, Hong Kong

**Thailand Office**  
Level 11 Zone B Thaniya Plaza Building  
52 Silom Road, Suriyawongse, Bangrak  
Bangkok 10500 Thailand

Main: +1-415-566-6228 Fax: +1-415-566-4226

Main: +852-2251-8826 Fax: +852-2573-8911

Main: +662 231 2635 6 Fax: +662 231 2637