

**Q. What is Sarbanes Oxley?**

- A.** The Sarbanes Oxley Act of 2002 is legislation designed to restore confidence in the equity markets and in the integrity of financial reporting after several corporate scandals. Sarbanes Oxley consists of several sections designed to improve the quality of financial reporting. The section that most closely impacts IT functions is Section 404, developed by the Securities and Exchange Commission (SEC).

Section 404 governs “management assessment of internal controls,” stating that a corporation must state what internal controls are in place to protect the integrity of the financial reporting mechanism and what the quality of those controls are. External auditors must then attest to the accuracy of these statements which have been signed by officers of the company.

**Q. What penalties are in place for non-compliance?**

- A.** The penalty for misstating the status of internal controls is the same as for filing wrong information – possible civil or criminal penalties. The penalties for not putting controls in place and reporting that proper controls are not in place is most likely loss of confidence in the value of the company.

**Q. What is meant by internal control?**

- A.** An internal control for Sarbanes Oxley is a process designed to provide reasonable assurance that financial reporting and the preparation of financial statements for external purposes are in accordance with generally accepted accounting principles. They include the maintenance of records of transactions, the recording of transactions, and the acquisition, use or disposition of assets that could be considered “material” to reporting.

These controls include specific controls that directly affect these actions but also include what is known as “pervasive” controls. Pervasive controls include such controls as IT security. IT security is a general function and control that is not specific to financial reporting but acts as a control to ensure the integrity of information.

**Q. Who is affected by Sarbanes Oxley?**

- A.** Sarbanes Oxley affects companies that are required to file with the SEC. This will include public companies over a certain market capitalization and other companies such as banks and savings association.

**Q. Are foreign companies affected by Sarbanes Oxley?**

- A.** Yes, if they are categorized as an “issuer” under SEC rules. In other words, if they are required to report with the SEC regularly, they must comply with Sarbanes Oxley.

**Q. What does Section 404 of Sarbanes Oxley require?**

**A.** Section 404 requires two basic elements that are related:

- The reporting of internal controls, signed by management and attested to by external auditors.
- The establishment of a framework for internal controls. Section 404, as published by the SEC, states that this framework must be suitable and recognized, having been established through public due process. It goes on to point out that COSO Internal Control – Integrated Framework is one framework that meets the criteria. Other frameworks may meet the requirements as well.

**Q. What is COSO?**

**A.** COSO, or Committee of Sponsoring Organizations, is an organization formed in 1985 to improve the quality of financial reporting. It is sponsored by organizations such as the American Accounting Association, the Institute of Internal Auditors, and others.

One of COSO's documents, first published in 1992, is Internal Controls – Integrated Framework. This document outlines three dimensions to internal controls: Objectives, Entity- or Activity-Level Evaluation, and five components of internal controls.

Under the Integrated Framework, the objective are to effectiveness and efficiency of operations, financial reporting reliability, and compliance with regulations. Each of these may have sub-objectives.

Each of the objectives must be evaluated at the entity-level and the activity-level. For instance, is the organization meeting the objective? Is this certain process – the booking of sales – meeting the objectives?

The five components that make up internal controls are the Control Environment component, the Risk Assessment component, the Control Activities component, the Information and Communication component, and the Monitoring component.

For more information on how the Internal Controls – Integrated Framework operates, please visit the COSO website at <http://www.coso.org>.

**Q. What is the place of network security within Sarbanes Oxley and COSO?**

**A.** Without a doubt, network security in particular and IT in general will play an important part in establishing internal controls. However, neither Sarbanes Oxley not COSO provide insight into how to establish internal controls with IT security. To do that requires a secondary framework grafted onto COSO.

Two possibilities for this framework include the Control Objectives for IT (COBIT) 3<sup>rd</sup> Edition and ISO 17799: Code of Practice for Information Security Management. COBIT can be found at <http://www.isaca.org> and ISO 17799 can be found <http://www.iso.org>.

**Q. How can I apply an IT framework to COSO?**

**A.** To apply an IT framework to COSO, it is vital to think of where IT processes fit into each of the three dimensions of the COSO framework. For instance, network security could fit under three separate components: control activities, information and communications, and monitoring. For COBIT, much of the mapping has been done in "IT Control Objectives for Sarbanes Oxley," a paper by the IT Governance Institute and the Information Systems Audit and Control Association. It can be found at <http://www.isaca.org>.

**Q. How do I match up Check Point security solutions to Sarbanes Oxley?**

**A.** Below you will find Check Point’s solutions mapped to the COBIT guidelines, specifically sections of DS5, or Delivery and Support: Ensure Systems Security. This chart is meant as an example of how an organization can map Check Point solutions. However, because every environment is different, it is important to evaluate your organization’s risks and controls.

COBIT Objective	The Check Point Solution
<b>DS1: Define and Manage Service Levels</b>	
<b>DS1.4: Monitoring and Reporting</b> Management should appoint a manager who is responsible for monitoring and reporting on service performance criteria and all problems encountered.	<i>SmartCenter</i> and <i>SmartCenter Pro</i> include <i>SmartView Status</i> and <i>Tracker</i> to provide detailed logs and visual tracking of security incidents. <i>SmartView Reporter</i> enables managers to quickly turn this information into actionable reports.
<b>DS2: Manage Third-Party Services</b>	
<b>DS2.8: Monitoring</b> There must be a process for monitoring service delivery from third-party vendors.	Organizations can ensure that a third-party managed security organization that uses <i>Provider-1</i> to manage their security infrastructure complies with agreed-to security policy.
<b>DS5: Ensure System Security</b>	
<b>DS4.11: Back-up Site and Hardware</b> Management must ensure that continuity plans incorporate alternatives including back-up sites and hardware.	Check Point’s VPN solutions, including <i>VPN-1 Pro</i> , <i>VPN-1 Express</i> , and <i>Connectra</i> , include multiple options for high availability, including stateful failover, ISP redundancy, and the ability to have multiple entry points for VPNs.
<b>DS5.1: Manage Security Measures</b> IT security should be managed in line with business objectives.	<i>SmartCenter</i> and <i>SmartCenter Pro</i> enable organizations to easily translate a written security policy into an actionable policy for Check Point solutions.
<b>DS5.2: Identification, Authentication and Access</b> Logical access to resources must be restricted with identification, authentication, and authorization mechanisms.	Check Point’s solutions support a number of methods – including certificates, tokens, passwords, biometrics, and more – to ensure that the proper security policy is applied, restricting a person’s access to authorized resources.  Check Point solutions also support common user databases such as Active Directory, LDAP, or NDS.
<b>DS5.3: Security of Online Access to Data</b> There must be controls in place to provide access based on a person’s need to view, add, change, or delete data.	With Check Point <i>SmartCenter</i> and <i>SmartCenter Pro</i> , administrators can be limited to specific security tasks.  Also, using Check Point solutions enables an organizations to develop granular access controls based on a person’s identity – supplementing application-level access control.
<b>DS5.4: User Account Management</b> An organization should have controls in palce to quickly add, suspend or close user accounts.	All <i>SmartCenter</i> management solutions provide centralized management of user accounts. With <i>SmartCenter Pro</i> , network security accounts can be integrated with existing user databases such as Active Directory or LDAP directories.
<b>DS5.7: Security Surveillance</b> The IT department should ensure that security activity is logged and potential security violations result in alerts and actions.	Check Point solutions enable administrators to configure a variety of actions, ranging from logging to alerts to self-defined steps like paging an administrator, to provide proper monitoring of the security policy.
<b>DS5.9: Central Identification and Access Rights Management</b> Controls are in place to ensure centralized management of identification and access rights	Check Point <i>SmartCenter</i> solutions enable organizations to centrally administer access rights as well as user profiles.

<p><b>DS5.10: Violation and Security Activity Reports</b> IT administration needs to ensure the violation and security activity is logged, reported and reviewed. Security logs should be treated as “need-to-know.”</p>	<p>Check Point enables administrators to granularly determine what activities need to be logged and, when reports are needed, <i>SmartView Reporter</i> provides actionable reports on security.</p> <p>Access to security logs can be configured by designated administrators.</p>
<p><b>DS5.11: Incident Handling</b> Organizations needs an incident handling capability with a centralized platform.</p>	<p>With Check Point's <i>SmartCenter</i> solutions, a company's security staff can quickly address security incidents with one centralized management platform.</p> <p><i>InterSpect</i> enables organizations to quarantine internal hosts suspected of an attack until the incident handling team has taken action.</p>
<p><b>DS5.12: Reaccreditation</b> An organization must regularly ensure that security is enforced as needed – both in terms of defined security policy and in terms of acceptable risk.</p>	<p>Check Point <i>SmartDefense Service</i> provides updated protection against new attacks – enabling organizations to stay current against new risks.</p> <p>With <i>SmartCenter's</i> centralized management, security teams can quickly ensure that all Check Point security solutions are enforcing a consistent, correct security policy.</p>
<p><b>DS5.13: Counterparty Trust</b> Organizations need a method of verifying the authenticity of electronic instructions or transactions.</p>	<p>With Check Point VPN solutions, organizations can choose from passwords, tokens, certificates, or other authentication mechanisms to establish trust.</p>
<p><b>DS5.14: Transaction Authorization</b> Where appropriate, cryptographic techniques should be used to validate a user's identify.</p>	<p>By using accepted cryptographic algorithms such as AES and DES, Check Point VPN solutions enable an organization to validate identities.</p>
<p><b>DS5.15: Non-Repudiation</b> When appropriate, techniques should be used to guarantee that neither party to a transaction can deny its part.</p>	<p>Check Point's standards-based encryption technologies enable organizations to gain non-repudiation of transactions when necessary.</p>
<p><b>DS5.16: Trusted Path</b> Organizational policy should require sensitive transaction data to travel over a trusted path.</p>	<p>Check Point's VPN solutions provide a trusted path both externally and internally to the network.</p> <p><i>VPN-1</i> also enables VLAN-tagging for establishing trusted paths between external and internal sources and destinations.</p>
<p><b>DS5.18 Cryptographic Key Management</b> Organizations must define and implement procedures for the proper management of cryptographic keys.</p>	<p><i>VPN-1</i> provides and internal certificate authority for the management of cryptographic keys used for site-to-site and remote access VPNs. It also supports the use of third-party PKI solutions.</p>
<p><b>DS5.19: Malicious Software Prevention, Detection and Correction</b> Organizations must taken proper measures to protect against worms, viruses or trojan horses.</p>	<p><i>VPN-1</i>, <i>InterSpect</i>, and <i>Connectra</i> protect against the spread of worms and other attacks.</p> <p><i>Connectra</i>, <i>Integrity Clientless Security</i>, <i>Integrity</i>, <i>Integrity SecureClient</i> and <i>VPN-1 SecureClient</i> can be used to ensure that anti-virus is present and up-to-date before allowing computers to access network resources.</p>
<p><b>DS5.20: Firewall Architectures and Connections with Public Networks</b> If there is a connection to the Internet or any other public network, firewalls should be used to prevent unauthorized access and denial-of-service.</p>	<p><i>VPN-1</i> provides the most intelligent firewall security with Stateful Inspection, Application Intelligence, and Web Intelligence. The <i>VPN-1</i> family line provides solutions for small offices, branch offices, mid-sized business, and corporate headquarters.</p>

<b>DS7: Educate and Train Users</b>	
<p><b>DS7.2: Security Principles and Awareness Training</b> All personnel must be trained and educated in system security principles.</p>	<p>Check Point solutions such as <i>VPN-1 SecureClient</i>, <i>InterSpect</i>, and <i>Connectra</i> can be used to provide instant feedback messages when a user's system does not meet adequate security levels.</p>
<b>DS9: Manage the Configuration</b>	
<p><b>DS9.5: Unauthorized Software</b> An organization should have clear policies restricting the use of personal or unlicensed software.</p>	<p>Check Point solutions such as <i>VPN-1 SecureClient</i>, <i>Integrity SecureClient</i>, <i>Connectra</i>, and <i>Integrity Clientless Security</i> can check for unauthorized software and deny access based on the security policy.</p>
<b>DS10: Manage Problems and Incidents</b>	
<p><b>DS10.3: Problems Tracking and Audit Trail</b> An organization's problem management system should provide an adequate tracking and audit function that allows for tracing the incident back to original cause.</p>	<p>Check Point <i>SmartCenter</i> solutions allow for policy version rollback to previous versions to determine the root cause of a problem.</p>
<b>DS11: Manage Data</b>	
<p><b>DS11.17: Protection of Sensitive Information During Transmission and Transport</b> Sensitive information should be protected during transmission and transport.</p>	<p>Check Point's VPN solutions provide protection against unauthorized access or modification through standards-based encryption technologies.</p>
<p><b>DS11.27: Protection of Sensitive Messages</b> Sensitive information sent over the Internet or a public network should have protection to ensure integrity, confidentiality, and non-repudiation.</p>	<p>Check Point VPN solutions such as <i>VPN-1</i> and <i>Connectra</i> provide this protection through standards-based encryption.</p>
<b>DS13: Manage Operations</b>	
<p><b>DS13.8: Remote Operations</b> Procedures should exist to control the connection and disconnection of links to remote sites.</p>	<p>Check Point solutions require remote users to re-authenticate at administrator-determined times.</p>