



Achieving Sarbanes-Oxley Act Section 404 Compliance with Check Point Solutions

Contents

- Executive summary 3
- Purpose 3
- Background 3
- Essential components of effective internal control 4
 - Control environment 4
 - Risk assessment 4
 - Control activities 4
 - Information and communication 4
 - Monitoring..... 5
- Analysis 5
- Mapping COBIT High-Level Objectives to Check Point solutions 5
- Conclusion 12

Executive summary

Regulatory compliance is a hot topic and costly challenge for most organizations not only because it influences businesses as a whole, but it also can affect executive officers. Increasingly, regulations are being established to require companies to provide evidence that they can protect the privacy and ensure the secure access and integrity of their information resources for consumers and commercial businesses. The regulation that has caught the most attention is the Sarbanes-Oxley Act of 2002 (SOX). SOX was enacted to protect shareholders and the public in the face of several high-profile financial scandals. The act mandated a number of reforms to enhance corporate responsibility, improve the integrity of financial disclosures, and combat corporate and accounting fraud.

Businesses are quickly realizing that SOX compliance is not just about process management and documentation of their financial operations. IT security has become an important part of meeting these new demands placed on businesses by SOX. Significant time and money are being spent on security technology, tools, and resources to ensure SOX compliance. Check Point security solutions offer the most proven unified security architecture for both protecting information resources and complying with SOX.

Purpose

This white paper provides a brief background on Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) and shows how Check Point solutions meet SOX requirements, using the process control objectives from COBIT – the accepted standard for best practices for IT security and control. Please, note that there is no straightforward methodology for achieving SOX Section 404 compliance. Instead, companies certify their compliance status – via mutual agreement between senior management and an external auditor – that they have performed due care in ensuring the integrity of their financial reporting.

Background

SOX consists of several sections designed to improve the quality and integrity of financial reporting. The section that closely affects IT functions is Section 404, “Management Assessment of Internal Controls.” Section 404 requires that a corporation annually report the following:

- Management’s responsibility to establish and maintain adequate internal control over financial reporting
- The framework used as criteria for evaluating the effectiveness of the company’s internal control over financial reporting
- Management’s assessment of the effectiveness of internal company control over financial reporting and disclosure of any material weaknesses

Section 404 also requires that external auditors certify the accuracy of these statements, which have been signed by the CEO and CFO of the company.

An internal control for SOX is a process that provides reasonable assurance that financial reporting and preparation of financial statements for external purposes are in accordance with generally accepted accounting principles (GAAP). Controls include recording of transactions, maintenance of transaction records, and acquisition, use, or disposition of assets that could be considered “material” to reporting. Specific controls directly affect these actions. General or “pervasive” controls impose generic rules applicable to all actions. Pervasive controls include controls over IT security—general functions and controls that are not specific to financial reporting but act as a control to ensure the integrity of information.

The United States Securities and Exchange Commission (SEC) states that a suitable and recognized framework, having been established through public due process, must be used to evaluate internal controls. It points out that COSO Internal Control—Integrated Framework is one framework that meets the criteria.

With far-reaching reliance on IT for financial and operational management systems, it is important to demonstrate how IT controls support the COSO framework. An organization should have IT control competency in all COSO components.

Essential components of effective internal control

COSO identifies the following five essential components of effective internal control:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

Control environment creates the foundation for effective internal control, establishes the “tone at the top,” and represents the apex of the corporate governance structure. The issues raised in the control environment component apply throughout an organization.

Risk assessment involves the identification and analysis by management of relevant risks to achieving predetermined objectives, which form the basis for determining control activities.

Control activities are the policies, procedures, and practices that ensure business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified.

Information and communication is needed at all levels of an organization to run the business and achieve its control objectives. Determining what information is required to achieve control objectives and communicating it in a form and time

frame that allow people to carry out their duties are essential to support the other four components of the COSO framework.

Monitoring assesses the quality of the internal control performance over time. It covers the oversight of internal control by management through continuous and point-in-time assessment.

IT in general and IT security in particular play an important part in establishing internal controls to meet SOX requirements. However, neither SOX nor COSO provide insight into how a company should establish internal controls with IT security. This requires that a secondary framework be used in conjunction with COSO. Two examples for this framework include the Control Objectives for IT (COBIT) 4.1 Edition and ISO/IEC 27002: Code of Practice for Information Security Management.

COBIT is an IT governance model that provides both company- and activity-level objectives along with associated controls. Using COBIT, an organization can design a system of IT controls to comply with Section 404.

Analysis

For the purpose of this white paper, we will focus on the Control Objectives as stated in COBIT because it is a recognized standard for most IT organizations.

Remember, that none of the above frameworks or documents offer guaranteed methodologies toward SOX compliance. In fact, most companies—in agreement with their external auditors—will use a customized framework tailored to their specific financial-reporting processes.

In the following section, certain COBIT Control Objectives have been restated along with specific Check Point security solutions that can contribute to fulfilling these objectives.

Mapping COBIT High-Level Objectives to Check Point solutions

The following chart illustrates how an organization can map Check Point solutions to applicable COBIT High-Level Objectives, specifically for Delivery and Support: Ensures Systems Security (DS5) and Monitoring (M) sections. It is important to note that because every environment is different, companies should evaluate their risks and controls to determine specific requirements for SOX compliance.

COBIT Control Objective	Check Point solution
<p><i>DS5.3 Identity Management</i></p> <ul style="list-style-type: none"> • Ensure that all users are uniquely identifiable. Enable user identities via authentication mechanisms • Maintain user identities and access rights in a central repository • Deploy cost-effective technical and procedural measures and keep them current to establish user identification, to implement authentication, and to enforce access rights 	<p>Access control is an essential element of all Check Point security solutions. Check Point network security, data security, and endpoint security solutions allow for the creation of granular access and authorization rules. VPN-1® and InterSpect™ enforce access policies at the perimeter and on the internal network. Connectra™ and VPN-1 enforce access policies when providing remote access to users outside the perimeter. Check Point Endpoint Security uses desktop firewall rules and network zones to limit PC access to network resources and segments. These access policies define what resources an individual, group, or department is authorized to view.</p> <p>Full-disk encryption uses driver-based preboot access control to completely separate logical access to the encrypted file system from the native operating system.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to help an organization deploy and configure Check Point solutions so that cardholder data access is restricted as required in section DS5.3.</p>
<p><i>DS5.4 User Account Management</i></p> <ul style="list-style-type: none"> • Address requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges with a set of user account management procedures • Perform regular management review of all accounts and related privileges 	<p>Check Point management tools allow administrators to create policies, including the mapping and assignment of groups (of users and endpoints) to resources. All Check Point products can log and report user access across Check Point gateways as well as log and report administrator changes on Check Point systems. Organizations can view this data in SmartViewTracker™ and in reports from Eventia™ Reporter™.</p> <p>Authentication is an essential part of all Check Point solutions, including Check Point VPN solutions, as well as user authentication for VPN-1. VPN-1 supports multiple databases for authentication, including an internal database, Microsoft Active Directory, and OPSEC-certified LDAP and RADIUS databases.</p> <p>Check Point IPS-1™ may be configured to provide inline, real-time password policy validation for password length or alphanumeric requirements.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to help an organization define an ID program that can assign users unique IDs for use with Check Point solutions.</p>

COBIT Control Objective	Check Point solution
<p><i>DS5.5 Security Testing, Surveillance, and Monitoring</i></p> <ul style="list-style-type: none"> • Proactively test and monitor the IT security implementation • A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed 	<p>Check Point Endpoint Security enables enterprises to centrally monitor and report on antivirus, endpoint, remote access, and NAC events alongside network firewall and IPS events from a single management interface.</p> <p>Check Point SmartCenter™ and Eventia® Suite™ — Eventia Reporter and Eventia Analyzer™ — centralize logging, updates, monitoring, and reporting of system events and activity, enabling enterprises to gain a holistic view of their security- and network-activity trends. The consistent presentation of data across the enterprise enables more effective data collection, analysis, and response.</p> <p>Eventia Suite collects, audits, correlates, and reports on logs and event activity across all Check Point products and across a diverse range of third-party products. Eventia Reporter gathers information to report on cross-product attacks, blocked traffic, login activity, and network activity.</p> <p>Eventia Reporter includes centralized reporting of Check Point Endpoint Security data on compliance violations, firewall events, blocked programs, spyware, and client errors. Eventia Reporter also provides reports on antivirus activity, Connectra, InterSpect, and VPN-1 Power VSX™ log reports.</p> <p>IPS-1 Dashboard features an integrated vulnerability browser that maintains a current ranking of all operating system (OS), application server, and network device vulnerabilities at the version/patch-level. This vulnerability listing is continually updated via SmartDefense™ protections and IPS-1 passive OS fingerprinting.</p> <p>Eventia Suite enables enterprises to build audit trails of user access to cardholder data, administrator actions, invalid logical access attempts, and much more. Eventia Analyzer supports the initialization of audit logs, secure access to audit information, and allows for creation and deletion of system-level objects. In addition, Eventia Analyzer provides alerts when the audit logs are initialized and when system objects are created and deleted.</p>

COBIT Control Objective	Check Point solution
<p><i>DS5.6 Security Incident Definition</i></p> <ul style="list-style-type: none"> Clearly define and communicate the characteristics of potential security incidents so that they can be properly classified and treated by the incident and problem management process 	<p>SmartDefense and Web Intelligence™ technologies perform intrusion prevention as part of Connectra, Check Point Endpoint Security, and VPN-1 products. SmartDefense Services allow enterprises to keep intrusion prevention engines updated.</p> <p>Check Point Endpoint Security provides enterprises with a single agent that detects potential security threats, blocks unwanted and malicious contents, and remediates infected systems quickly and easily. The Check Point Endpoint Security central management system allows administrators to define security incidents and policy, monitor potential security incidents, and report on the compliance of endpoint systems to the defined security policy.</p> <p>Eventia Analyzer provides comprehensive support for the identification, handling, and reporting of security incidents. It analyzes log data in near real-time from Check Point solutions and commonly used security devices to identify significant threats across the network. Upon the detection of a security event, Eventia Analyzer can be preset to generate alerts or reports or to take appropriate action to mitigate the detected threat. Eventia Reporter enables real-time, historical, and trend reporting of security events.</p> <p>IPS-1 is a dedicated intrusion prevention system that delivers mission-critical protection and granular forensic analysis capabilities and flexible deployment. N-Code™, the threat description language at the heart of IPS-1 solutions, has uncommon capabilities for inspecting and correlating protocol and application elements using compound logic to reduce complex inspections to simple, high-performance rules adding extensibility and flexibility to IPS-1 solutions from Check Point.</p> <p>IPS-1 Dashboard, operating either as a powerful browser-based management tool or as a tabbed component in SmartCenter, provides a comprehensive view of all intrusion-related events, weighted using integrated vulnerability assessment tools. The IPS-1 Dashboard delivers a high-level, network-wide timeline and facilitates drill-down to investigate patterns and suspicious activity at the packet or rule level.</p>

COBIT Control Objective	Check Point solution
<p><i>DS5.7 Protection of Security Technology</i></p> <ul style="list-style-type: none"> • Make security-related technology resistant to tampering 	<p>Access control is an essential element of all Check Point security solutions. Check Point network security, data security, and endpoint security solutions allow for the creation of granular access and authorization rules. VPN-1 and InterSpect enforce access policies at the perimeter and on the internal network. Connectra and VPN-1 enforce access policies when providing remote access to users outside the perimeter. Check Point Endpoint Security uses desktop firewall rules and network zones to limit PC access to network resources and segments. These access policies define what resources an individual, group, or department is authorized to view.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to help an organization deploy and configure Check Point solutions so that security-related technology is resistant to tampering as required in section DS5.7.</p>
<p><i>DS5.9 Malicious Software Prevention, Detection, and Correction</i></p> <ul style="list-style-type: none"> • Put preventive, detection, and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam) 	<p>The VPN-1 family provides integrated gateway-based antivirus within its VPN-1 gateway and UTM-1 appliance solutions. This supplements the deployment of antivirus solutions on individual PCs and servers and enhances the coverage against threats.</p> <p>Check Point Endpoint Security includes high-performance antivirus technology to detect and eliminate viruses and other related malware from endpoint PCs. Virus detection is based on a combination of signatures, behavior blockers, and heuristic analysis that together enable your network environment to attain one of the industry's highest detection rates. A dedicated, global team of experts delivers proactive 24/7 threat response, including hourly signature updates.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to deploy Check Point solutions that address the requirements of this section, as well as interoperate with any antivirus solution that may already be deployed.</p>

COBIT Control Objective	Check Point solution
<p><i>DS5.10 Network Security</i></p> <ul style="list-style-type: none"> • Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks 	<p>As the industry's number one stateful firewall solution, VPN-1 (which includes FireWall-1®) sets the standard for the very best first line of defense. VPN-1 supports firewall requirements, including the ability to establish proper configuration standards. These capabilities include granular logical management of network components, internal-network-zone segmentation to protect components or segments from other portions of the network, assignment and documentation of ports, firewall configuration policy setting, audit and reporting requirements, and the ability to display network connectivity.</p> <p>Using Check Point Security Management Architecture (SMART™), administrators can centrally manage, approve, view network topology, and verify all external network connections and changes to the firewall configuration. SMART management enables administrators to list and review firewall security policies, protocols, and rule sets as well as to manage and deploy a centralized firewall policy to an unlimited number of VPN-1 gateways.</p> <p>SmartDefense Services, Web Intelligence technology, Eventia Suite, and IPS-1 perform intrusion prevention. These products work alone or together to monitor network traffic and alert personnel to suspicious activity and suspected compromises.</p>
<p><i>DS5.11 Exchange of Sensitive Data</i></p> <ul style="list-style-type: none"> • Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt, and non-repudiation of origin 	<p>Check Point Endpoint Security Full Disk Encryption delivers the highest level of data security by providing a strong, full-disk encryption solution for PCs and laptops as well as access control. Full-disk encryption enables the secure exchange of sensitive data by ensuring the integrity and authenticity of data at rest.</p> <p>Check Point secure remote access solutions, VPN-1 and Connectra, provide strong encryption for data during transmission over open networks using standards-based encryption protocols. VPN-1 supports SSL- and IPSec-encrypted communication protocols. Connectra supports SSL- and TLS-encrypted communication protocols. In addition, both products support the MD5 and SHA-1 protocols to ensure the integrity of secure transmissions involving cardholder data.</p> <p>IPS-1 Sensors offer inline detection and alerting on defined data structures such as personal identification numbers, personal health information, or files watermarked as confidential.</p> <p>Check Point VARs, SIs, and business partners can provide consulting services to deploy Check Point solutions within an organization to enable the secure exchange of data.</p>

COBIT Control Objective	Check Point solution
<p><i>ME1.4 Performance Assessment</i></p> <ul style="list-style-type: none"> Periodically review performance against targets, analyze the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root-cause analysis across deviations 	<p>Check Point SmartCenter and Eventia Suite— Eventia Reporter and Eventia Analyzer— centralize logging, updates, monitoring, and reporting of system events and activity, enabling enterprises to gain a holistic view of their security- and network- activity trends. The consistent presentation of data across the enterprise enables more effective data collection, analysis, and response.</p>
<p><i>ME1.5 Board and Executive Reporting</i></p> <ul style="list-style-type: none"> Develop senior management reports on IT's contribution to the business Provide the report to senior management and solicit feedback from management's review 	<p>Eventia Suite collects, audits, correlates, and reports on logs and event activity across all Check Point products and across a diverse range of third-party products. Eventia Reporter gathers information to report on cross-product attacks, blocked traffic, login activity, and network activity.</p>
<p><i>ME1.6 Remedial Actions</i></p> <ul style="list-style-type: none"> Identify and initiate remedial actions based on performance monitoring, assessment, and reporting 	<p>Eventia Reporter endpoint security reports include centralized reporting of Check Point Endpoint Security data on compliance violations, firewall events, blocked programs, spyware, Malicious Code Protector outcomes, and client errors. Eventia Reporter also provides reports on antivirus activity, Connectra, InterSpect, and VPN-1 Power VSX log reports.</p> <p>Eventia Suite enables enterprises to build audit trails of user access to cardholder data, administrator actions, invalid logical access attempts, and much more. Eventia Analyzer supports the initialization of audit logs, secure access to audit information, and allows for creation and deletion of system-level objects. In addition, Eventia Analyzer provides alerts when the audit logs are initialized and when system objects are created and deleted.</p>



Conclusion

SOX Section 404 provides a turning point for most IT organizations in their efforts to develop and document the IT security controls and processes needed to support financial reporting. Protecting the integrity of information and controlling access to resources are not only essential elements for the preservation of a company but are also requirements for compliance. Check Point security solutions can be leveraged to help fulfill many specific COBIT Control Objectives that will form the foundation for compliance with requirements set forth in SOX Section 404. With Check Point, you can rest assured with the most proven unified security architecture that provides a robust infrastructure from the perimeter to the endpoint.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.