Sarbanes-Oxley (SOX) Act Compliance Reference Card

SOPHOS
Security made simple.

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act, was enacted in response to a number of major corporate and accounting scandals. The Act, also known as "SOX," led to a series of regulations imposing strict rules and accountability regarding reporting and record-keeping requirements for all publicly traded companies. SOX mandates that senior executives of these companies take personal responsibility for the accuracy and completeness of the company's financial reports and data. A number of the Act's provisions apply to privately held companies.

Sophos supports companies in their efforts to meet SOX requirements by offering them controls that support authorization, authentication, and security monitoring to ensure security of their systems and financial data.

Security challenge	Sophos Product	How it helps
Enterprise level controls		
User and application level controls	Sophos Firewall/UTM Sophos Endpoint Protection Advanced Sophos Server Protection Sophos Web Gateway	Allows user-based policy control over applications, websites, categories, and traffic shaping (QoS). User-based application policies enables custom-tailored application control to be added to any user, group, or network policy with the option to also apply traffic shaping.
Data security		
Multi-factor authentication to prevent unauthorized access to systems/resources	Sophos Firewall/UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos SafeGuard Enterprise	Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard Enterprise. Supports multi-factor authentication, tokens, and smart cards for user authentication.
Security of data at rest or in motion	Sophos SafeGuard Enterprise	Complete data protection solution across multiple platforms and devices, including mobile devices. Protect data at rest with full disk encryption. Location-based file encryption protects data in motion and follows the file wherever it may go – for example, via email, uploaded to cloud storage, or copied to removable devices. Application-based (synchronized) encryption encrypts data by default as soon as it is created.
	Sophos Mobile	Delivers mobile data protection when integrated with SafeGuard Enterprise to enable access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separate and can be locked down or wiped.
	Sophos Email Appliance	Secures against email threats and phishing attacks; provides advanced DLP and easy policy-based encryption.

Sarbanes-Oxley (SOX) Act Compliance Reference Card (colour light)

Security challenge	Sophos Product	How it helps
Access controls		
Policy controls for data access by privileged users/accounts	Sophos Enterprise Console / Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
	Sophos Mobile	Role-based administration ensures user privacy and appropriate credentials for altering compliance or device/data access.
	Sophos Firewall Manager	Centralized security management with extensive administrative controls; Role-based administration with change control and logging.
Controlled access to data based on need-to-know	Sophos Firewall/UTM	Our patented Layer-8 user-identity technology governs all firewall policies and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
	Secure Web Gateway	Offers control over applications, web surfing, and other network resources by user and group.
Security Intelligence		
Track and monitor all access to network resources and cardholder data	Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
	Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data. Mobile Security Privacy and Security Advisory alert users to apps that try to access the internet and various data sources.
	Sophos Firewall/UTM	Controls remote access authentication and user monitoring for remote access, and logs of all access attempts.
	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
Business continuity		
Uninterrupted Protection	Sophos Email on Sophos Central	In the event of third party cloud email service provider outages: alerts are provided if mail can't be delivered to a server/service, and email is then queued for delivery to ensure no email is lost. Access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is 5 days.
Perimeter defense		
Protect networks from latest and advanced threats with controls such as firewall and intrusion detection	Sophos XG Firewall	Provides all the latest advanced technology to protect your network from botnets, hacks, and advanced threats with Advanced Threat Protection, IPS, Sandboxing, Web and Email Protection.

Specifications and descriptions subject to change without notice. Sophos disclaims in full all warranties and guarantees.
This document and the information in it do not constitute legal advice. Customers are solely responsible for compliance
with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

SOPHOS