helpsystems

CHECKLIST *(Cybersecurity)*

Sarbanes-Oxley (SOX) Requirements Checklist

REQUIREMENT	HOW WE CAN ASSIST

Section 302 – Corporate Responsibility for Financial Reports

Signing officers (CEO, CFO) must certify that financial reports are completed and accurate.

Signing officers must certify that they have implemented and evaluated all internal controls around financial reporting within the previous 90 days. Reports should include an assessment of these internal controls.

While there is no specific list of which internal controls must be used, information security tools are generally considered a required part of these controls.

Use **Core Privileged Access Manager (BoKS)** to enforce staff login with their own accounts on SOX infrastructures and limit privileges to financial data to only staff requiring access.

Use **Powertech Event Manager** to monitor logs and security events pertaining to financial data. Integrate pertinent financial software to centralize monitoring and allow for event correlation.

Use **Powertech Security Auditor** to enforce security policy adherence and prevent security misconfiguration.

Use **Powertech Antivirus** to provide protection for enterprise servers that store sensitive financial information.

Section 404 – Management Assessment of Internal Controls

Organizations must provide a top-down risk assessment report of their internal controls to an external auditing firm.

External auditors must determine the effectiveness of the organization's internal controls based on this report.

While there is no specific list of which internal controls must be assessed, cybersecurity efforts geared towards preventing insider and external threats are generally considered a required part of these controls.

Use **Core Privileged Access Manager (BoKS)** to log keystrokes, providing full visibility of your environment. Automatically generate event and audit logs, with user ID and user group fields in each log record.

Use **Powertech Event Manager** to generate automatic reports that can show logs for all event and incident response activity, as well as security posture performance over time.

Use **Powertech Security Auditor** to provide reports containing logs of new systems added, out-of-compliance settings, and remediation.

Use **Powertech Antivirus** to generate reports of scanning activity, infections found, and malware removal. All malware scanning activity is recorded in the system audit journal and syslog archive.