SECURE AUDITOR – SOX COMPLIANCE STATEMENT

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

In this era every financial institution, Government, private business, military, corporations & hospitals collect a great deal of confidential information about their employees, customers, products, research, and financial status. A large amount of this information is now collected, processed and stored on electronic computers and transmitted to other networks and computers.

In order to get customer's trust & maintain a long term relationship with customers & partners, it is very important to ensure them the confidentiality, integrity & security of their data.

Sarbanes-Oxley Act has made it mandatory for organizations to make sure that their financial information accurate and the systems generating the information are reliable. Management is required to undergo assessment of internal controls over financial reporting. Internal control over financial reporting should be accessed by Management

SOX compliance will significantly impact the IT based organization of most public companies. However there is one enormous problem that there is no specific standard mentioned in Section 404 in order to comply with SOX. Different companies use different standards like COSO, Six Sigma and COBIT for defining and documenting its internal controls. These days majority of auditors have adopted COBIT to fulfill SOX Compliance requirements. Secure Auditor also uses COBIT guidelines for SOX compliance.

Secure Auditor helps to manage internal controls in order to facilitate compliance with Section 404, a major provision of the Sarbanes-Oxley Act, requiring that management report annually on the effectiveness of internal controls for financial reporting and that external auditors confirm management's assessment.

Following reports are embedded within Secure Auditor that are required as part are the Sarbanes-Oxley audit process:

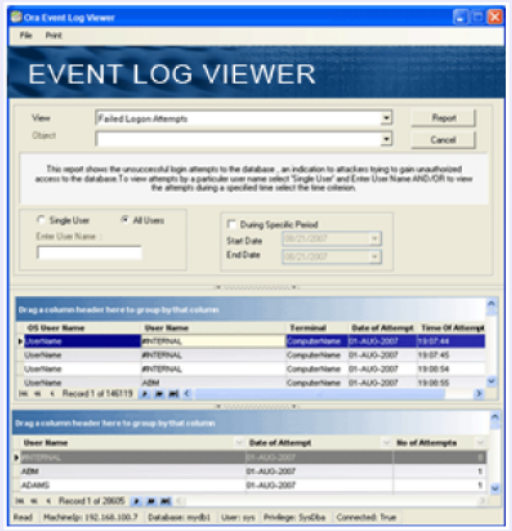
- Access Control
- System Integrity
- User Rights
- Information Disclosure
- User Privileges
- Audit policies
- Remote Access

For compliance with SOX, Auditors should care about

- User's Access Rights
- User's Privileges
- Remote Access to the systems
- Latest Patches
- Vulnerability Assessment

Benefits of Secure Auditor's SOX Compliance

- Ability to meet SOX requirements and avoid fines.
- Provides detailed solutions to the identified risks, timely reporting of Mis-configurations.
- Less chances of exposure to risk of breach through vulnerability exploitation.
- Avoid cost from network outages/downtime from security breach.
- Reduces spending on outside consultants.
- Create a safer environment for your customers.
- Get Customer's and partner's trust & satisfaction.
- Up-to-date security.



SECURE BYTES

Secure Auditor's Purposed Solution Matrix

Secure Auditor with 30 embedded utilities offers the services that have been designed to help organization to comply PCI compliance.

COBIT Clause No.	COBIT Clause	Compliance statement
ME1.6	Remedial actions	The remedial actions to strengthen IT performance are clearly demonstrated through Secure Auditor reports and step by step solutions. Secure Auditor identifies vulnerabilities and suggests methods to rectify the identified vulnerabilities. The best part of the Secure Auditor functionality is that it not only identifies the problem but also suggest solution to identified problems.
ME2	Monitor and evaluate internal control.	Internal Controls are an effective measure to strengthen an organizational IT and security efforts. Secure Auditor clearly checks the effectiveness of internal controls like access rights, event logs, network and system inventory management, password policies etc through its in-depth audit and embedded utilities. Using Secure Auditor facilitates the monitoring and evaluation process of Internal controls in an automated way.
ME2.1	Monitoring of internal control framework	Secure Auditor supports vulnerability benchmarking against standards and frameworks like COBIT and SOX in detailed reports to control the IT environment of an organization. Secure Auditor supports exception control through the ignore vulnerability function on a host-by host basis. This information can be made available across users. Secure Auditor also provides subscription based timely security notification about emergency threat detections.
PO2.4	Integrity management	Secure Auditor ensures security and integrity of Information assets of an organization by proactive scanning and vulnerability management. It ensures integrity of the systems and network assets because it identifies the vulnerabilities in the system that facilitates the process of safeguarding system's integrity.
ME2.4	Control self-assessment	Secure Auditor facilitates the process of control self assessment as it provides an automated tool to assess implemented control in organizational management. IS and Internal Auditors could evaluate their own systems and network assets with Secure Auditor to proactively identify any control or compliance flaws.
ME2.5	Assurance of internal control	Secure Auditor provides assurance to internal control through its monitoring and evaluation techniques for performing vulnerability assessment, risk assessment and audit. If no vulnerability is identified in a particular category then it ensures that that particular control is designed and implemented properly so that it fulfills its purpose.

COBIT Clause No.	COBIT Clause	Compliance statement
ME2.7	Remedial actions	Secure Auditor not only identifies issues but it also suggests methods for the remedy of the identified vulnerabilities. Complete remedial actions are provided by Secure Auditor to ensure that risk is mitigated proactively.
ME3	Ensure compliance with external requirements.	Secure Auditor provides assurance for compliance with external requirements of internationally proclaimed framework and standards like HIPAA, SOX, PCI and COBIT. Once an audit is conducted against a specified embedded profile like SOX then it identifies compliance gap between current and organizational state and minimum requirements defined by the standards and framework. If all vulnerabilities identified by Secure Auditor are fixed then it ensures that the gap between compliance requirement and current organizational stage has been filled.
ME3.3	Evaluation of compliance with external requirements	Secure Auditor evaluates the compliance of IT policies and procedures,
PO3.4	Technology standards	Positive assurance of compliance is ensured by Secure Auditor as it provides embedded profiles for compliance standards. If an audit is conducted against a specific compliance profile like SOX and COBIT and no vulnerability is identified then it gives positive assurance to an organization that a compliance standard has been followed properly through control measures.
ME3.4	Positive assurance of compliance	Secure Auditor provides integrated reporting facility to users through its embedded reporting console. It helps an organization to keep records of changes in an integrated manner. Compliance reports are also part of Secure Auditor's integrated reporting management system.
ME3.5	Integrated reporting	With the enforcement of technology standards like COBIT, SOX, ITIL, HIPAA etc, it becomes difficult for organizations to enforce and implement compliance within limited budgets. Secure Auditor provides compliance with all standards like SOX, HIPAA, FISMA, COBIT etc.
ME4	Provide IT governance.	Secure Auditor provides embedded solutions for IT governance as it allows an organization to conduct audit against embedded profiles like SOX, PCI/DSS, HIPAA etc. These profiles are based on checklists defined in accordance with the compliance and governance standards. Once an audit is conducted against these standards, it identified vulnerabilities that define weaknesses in implemented controls and deficiencies to become compliant with standards and frameworks. Once fixes for vulnerabilities are identified by Secure Auditor will be implemented then an organization becomes compliant with standards with effective IT governance.

COBIT Clause No.	COBIT Clause	Compliance statement
ME4.1	Establishment of an IT governance framework	Secure Auditor establishes an IT governance framework that is essential for maintenance of effective and efficient control environment in an organization. Control measures are essential in efficient and effective application of IT governance framework. Secure Auditor ensures control measures taken by an organization and performs a critical part in the establishment of an IT governance framework.
ME4.2	Strategic alignment	IT security and organizational strategy are aligned with Secure Auditor because it ensures compliance and effective controls that becomes the most critical part of an organization.
ME4.5	Risk management	Secure Auditor facilitates risk management efforts of an organization by segregating the identified risk into categories on the basis of its impact.
ME4.7	Independent assurance	Secure Auditor is a third party software that provides independent audit and assurance to an organization through automated audit lifecycle management. It gives an independent assurance that specified control measures are implemented to ensure compliance enforcement.
PO4.6	Establishment of roles and responsibilities	Establishment of roles and responsibilities is among the foremost requirements for defining access rights Secure Auditor provides facility to enumerate and audit role based access rights granted on Oracle and MSSQL server. It helps an administrator in identifying and rectifying access rights issues and vulnerabilities over the network that will cause serious issues and security breaches.
PO4.11	Segregation of duties	Segregation of duties is done through proper allocation of rights and responsibilities. Secure Auditor facilitates in assigning duties with respect to the assigned roles, with the help of Secure Auditor's Access right auditor. It is a true companion of an administrator in defining and segregating the duties in accordance with roles and responsibilities. It also helps in identifying issues in segregation of duties through conducting proper audit for allocated access rights.

COBIT Clause No.	COBIT Clause	Compliance statement
DS5	Ensure systems security.	Secure Auditor ensures system security with the help of its auditing tool and embedded utilities. The following tools provide facilitation in compliance with DS5 like: * MSSQL Event Log Viewer * Windows Event Log Viewer * Oracle Access Rights Auditor * MSSQL Access Rights Auditor * Oracle Password Auditor * Cisco MD5 Password Auditor * MSSQL Password Auditor * Windows Password Auditor * Cisco Type 7 Password Decryptor * Cisco Config Manager * Windows System Inventory Viewer * Windows Software Inventory Viewer * SNMP Browser * Port Scanner * Trace Route * SNMP Brute Force Attacker * MSSQL Brute Force Attacker * FTP Brute Force Attacker * HTTP Brute Force Attacker * Oracle Brute Force Attacker * SNMP Scanner * Oracle Default Password Tester * MSSQL Default Password Tester * Oracle SID Tester * Oracle TNS Password Tester * Oracle Query Analyzer * MSSQL Query Analyzer * IP Calculator * Mac Detector * DNS Auditor * DNS Lookup * Whois

COBIT Clause No.	COBIT Clause	Compliance statement
DS5.1	Management of IT security	Secure Auditor assesses and manages IT security risk through auditing and vulnerability assessment. It also facilitates in managing IT security risk by providing step by step solutions of the identified risk to mitigate the overall impact of risk.
DS5.4	User account management	Secure Auditor checks account policies, account lock out duration , enabled and disabled accounts of the users by conducting the auditing according to the IT & compliance standards like ISACA, SANS, CIS, SOX, and PCI DSS.
DS5.5	Security testing, surveillance and monitoring	Secure Auditor clearly identifies the existence of malwares, spywares and Trojans on the specific system that has been audited. Compliance with DS 5.9 becomes easy with Secure Auditor without conducting extra scans over the network for the malicious software prevention, detection and correction.
DS5.9	Malicious software prevention, detection and correction	Secure Auditor clearly identifies the existence of malwares, spywares and Trojans on the specific system that has been audited. Compliance with DS 5.9 becomes easy with Secure Auditor without conducting extra scans over the network for the malicious software prevention, detection and correction.
DS5.10	Network security	Secure Auditor is a network auditing and security tool that automates the process of network security. It reduces manual work of network security because it performs a comprehensive function as a network security tool. Secure Auditor provides an opportunity to proactively secure network by conducting audits and identifying vulnerabilities associated with network assets.
PO6.1	IT policy and control environment	Secure Auditor facilitates control framework enforcement by defining enterprise IT risks. Organizations define their IT policy and control environment in accordance with compliance standards enforced on their industry and specific line of business. Secure Auditor also provides facilitation in enforcing compliance regulation that defines policy and control infrastructure of an organization.
PO6.2	Enterprise IT risk and control framework	Secure Auditor identifies vulnerabilities to define a risk posture of an organization. It strengthens enterprise security by categorizing risk according to the severity of impact. Secure Auditor serves as an effective tool in efficiently enforced controlled environment within an organization.

COBIT Clause No.	COBIT Clause	Compliance statement
DS7	Educate and train users.	Secure Auditor facilitates the process of educating and training the users. It provides options for self study regarding security vulnerabilities through detailed vulnerability specifications. It also provides options to create on job training options by reading and implementing fixes for vulnerabilities identified through Secure Auditor.
PO9	Assess and manage IT risks.	Secure Auditor assesses and manages IT risk through auditing and vulnerability assessment. It also facilitates in managing the IT risk by providing step by step solutions of the identified risks to mitigate the overall impact of risk.
PO9.1	IT risk management alignment	Secure Auditor provides its customers a method of assessing risks within their environment based on COBIT and by allowing each customer to create an individualized value matrix for the identified risks. It aligns overall IT objective in context with the risk of an organization that makes it possible for management.
PO9.3	Event identification	Secure Auditor's event log viewer provides facility to view logs of any event and identify events for security, penetration testing and forensics purposes.
PO9.4	Risk assessment	Risk assessment is the foremost priority of an organization. Secure Auditor assesses security risk and categorizes them according to their severity of impact. It is a fundamental tool to conduct risk assessment of an organization.
PO9.5	Risk response	Determining the exact response to an identified risk is the most difficult decision for management. Due to unavailability of qualified resources, auditors select risk avoidance and transference as a response strategy rather than risk mitigation of the identified vulnerabilities. Secure Auditor provides exact solution to mitigate risk of identified threats that makes it possible for management to select a mitigation risk response strategy even with minimum resources.
DS11.6	Security requirements for data management	Data management could become handy with Secure Auditor as it performs efficient access rights auditing through its embedded tools and automated audit. For the security of data, it is extremely important to secure where data is being kept. Secure Auditor ensures database security through its audit and vulnerability identification process. Secure Auditor also checks that wether transported data has been encrypted or not.
AI4.2	Knowledge transfer to business management	Secure Auditor provides multiple reports according to the needs and distinguishes requirements of various management cadres. These reports contain details regarding the risk and security posture of an organization and provide facility to transfer knowledge regarding vulnerabilities, compliance and security status in a less technical manner.

COBIT Clause No.	COBIT Clause	Compliance statement
AI4.4	Knowledge transfer to operations and support staff	Secure Auditor provides detailed vulnerability description along with specifications, sources defined and step by step solution to provide knowledge transfer regarding various security and compliance concerns to operation and support staff that will be managing and fixing information assets vulnerabilities.
AI6	Manage changes.	Secure Auditor manages and reports changes into the system through its comparative and competency reports. All changes occurres into the system can be identified by comparing reports of two audits conducted at a certain time interval. Secure Auditor is a comprehensive tool regarding identification of changes occurring in the information assets.
AI6.2	Impact assessment, prioritization and authorization	Secure Auditor facilitates risk assessment and change impact analyses by categorizing the risk associated with changes on the basis of their impact on the organizational information assets. It helps in authorization of responsibilities regarding IT and security risk to the concerns people.
AI6.4	Change status tracking and reporting	Secure Auditor provides reporting facility to track change status tracking facility. If a user compare two reports of an audit conducted by Secure Auditor after a particular interval then he can easily identify the changes occurred in the information systems.