



Enterprise Random Password Manager

Maintaining Compliance with the Sarbanes-Oxley Act

The Sarbanes-Oxley Act was signed into law in 2002 in response to a number of major corporate accounting scandals that cost investors billions of dollars. The most prominent area of the regulation is Section 404, which requires management to establish and report on the company's internal controls over sensitive data.

These controls are primarily implemented within a company's IT infrastructure, so compliance with Sarbanes-Oxley requires meticulous detail in maintaining security best practices. Compliance is at risk if security measures are compromised and data is lost or inappropriately disclosed.

Common problems facing organizations in their Sarbanes-Oxley compliance efforts are:

- Securing access control and user management
- Ensuring individual identities for each user
- Creating audit-ready security reports

THE SOLUTION

With Lieberman Software's **Enterprise Random Password Manager** you can automatically discover, update, store, and recover every privileged account password in the network. It regularly creates unique, complex local and domain passwords for each account in the enterprise, and then propagates the password changes to all of the services, tasks, and applications that reference those credentials.

You maintain fully audited control over which local passwords a user can access and for what length of time. You also have access to a historic audit trail of password changes.

Specifically, Enterprise Random Password Manager helps organizations maintain compliance with Sarbanes-Oxley by providing the following controls:

ERPM FEATURE

SARBANES-OXLEY COMPLIANCE BENEFIT

Frequently randomize local administrator and root account passwords on every system	Protect private data by preventing one decrypted local password from providing unrestricted network access
Create unique local passwords for every system	Correlate unique IDs to each user to prove who accessed an account and when
Grant delegated users the ability to recover current local passwords	Control administrative privileges and ensure that only authorized users can access sensitive data
Log all password operations including logons, recoveries, and changes	Generate, analyze, and share audit-ready security reports
Secure passwords with SSL encryption of data to the browser, AES-256 encryption of data in the database, and optional hardware-based encryption	Prevent administrator and root passwords from being accessed and utilized by unauthorized users
Verify that the local passwords assigned to each system are still functional	Conduct periodic audits of user privileges