



Version: 4

Sarbanes-Oxley: Implications For Using Spreadsheets

Remediation of the significant risks inherent in the widespread use of spreadsheets for financial reporting and operational processes.

This document is proprietary, company confidential, and access restricted. It may not be copied except with written permission of Pinion Software, Inc. The document is Copyright© 2005, Pinion Software. Pinion™ and the Pinion logo are trademarks of Pinion Software. All rights are reserved. All other trademarks, registered trademarks, service marks, and registered service marks are property of their respective owners.

Spreadsheets and users have become more sophisticated, and are now used by many companies to support complex business functions and financial models.

A significant percentage of spreadsheets, estimated as high as 90%, contain errors.

Because spreadsheets can be easily changed, they are subject to increased risk and error.

Errors in relatively simple spreadsheets can result in potential material misstatements in a company's financial results.

Public companies today are faced with a growing body of regulation that are intended to protect consumers, investors, and the companies themselves from fraudulent management, governance, and various forms of loss. One in particular that is having a dramatic impact on the collection, management, and dissemination of business information throughout the enterprise is the Sarbanes-Oxley Act. More specifically, Section 404 of the Act defines requirements for establishing and maintaining an adequate internal control structure and procedures for financial reporting.

To date, the efforts by companies to comply with Section 404 have focused on assessing existing processes and controls. Included in this assessment are what processes and tools provide the most vulnerability, identifying the type and level of controls that are needed, and the associated costs of compliance. One of the vulnerabilities that have been identified is the extensive use of spreadsheets as both an operational and financial reporting tool by many companies.

Price Waterhouse Coopers recently published a white paper titled *The Use of Spreadsheets: Considerations for Section 404 of the Sarbanes-Oxley Act*. PWC found that spreadsheets are used by many companies and have become an integral part of the information and decision making process. A summary of key findings is included in the box above.

The requirements contained within Section 404 of the Sarbanes-Oxley Act increase the focus on controls needed for the development and maintenance of spreadsheets used for financial reporting and operational processes. The ability to control and tamper-proof critical spreadsheets is particularly important in light of the ubiquity of spreadsheet applications within the majority of companies. Nearly every PC asset in most companies is equipped with the application, enabling virtually any user to modify spreadsheet data.

Remediation of Spreadsheet Vulnerabilities

Appropriate control over spreadsheets is a critical element of compliance with Sarbanes-Oxley Section 404. To help mitigate the risks inherent in the use of spreadsheets, companies should implement controls that address such items as change control, access

control, version control, and provide for security and integrity of data. Among the approaches that support a company's efforts to comply with these control requirements are new technology solutions that secure, protect, or otherwise tamper-proof spreadsheets and other forms of sensitive information.

Pinion Software's information security solutions provide comprehensive, continuing in-use protection for spreadsheets, as well as any other type of digital file, which are shared both inside and outside the corporate firewall. In-use protection enables companies to control access, use, and prevent modification of spreadsheets by setting permissions that are appropriate to the sensitivity or value of the information. Protections include:

- Tamper-proof files by prohibiting modifications.
- Specify a date the recipient may first access the information.
- Select date after which the data will be removed, or shredded from the recipients PC.
- Prohibit printing, cut and paste, and screen capture tools.
- Prohibit saving, copying, and forwarding.
- Attach a password to the protected information.
- Force authentication of recipient each time the information is accessed.
- Update permissions as business conditions change.
- Permanently remove data / files from recipients PC upon expiration of permissions.

Pinion Software's solutions include:

- SecureMail™** — protects information sent by email, including the email body and file attachments. Integrated easily and seamlessly with leading email systems such as Microsoft Outlook and Lotus Notes, users follow the same process they would when attaching any other file.
- SecureShare™** — protect digital files distributed internally and externally through file sharing systems such as the corporate intranet, business portals, and document management systems.
- SecureCD™** - protect files distributed on CD-ROMs.

How It All Works – Pinion Software Technology

Pinion Software's solutions are comprehensive enterprise applications that are comprised of three components that together deliver multiple layers of defense for both in-transit and in-use protection.

- ❑ Pinion Publisher – allows users to assign in-use permissions to email messages and files that are to be sent by email or posted to a file sharing system for either internal or external distribution. Email messages and / or files are then sent to the Pinion Secure File Server.
- ❑ Pinion Secure File Server - this server-based application packages and encrypts email messages and files with assigned permissions and sends a link to the recipient. The server communicates with the Pinion Receiver to deliver protected content.
- ❑ Pinion Receiver - a one-time install, freely downloadable application that creates the secure environment where files and permissions are saved. Pinion Receiver controls access to the files, enforces permissions, and completely removes the files upon expiration.

About Pinion Software

Founded in 1998 and privately held, Pinion Software is a leader in the emerging market for Enterprise Rights Management solutions. Pinion Software enables companies to share information with confidence by providing continuous control over how the information may be used. Our flagship system, Pinion Secure Enterprise, protects information both inside and outside the corporate firewall—whether shared by email, corporate intranet, business portals, or document-management systems. For more information, visit our website at www.pinionsoftware.com.