



White Paper: Bsafe/Enterprise Security and The Sarbanes-Oxley Act of 2002



The Sarbanes-Oxley act of 2002 was passed following the spate of cases involving misleading representation of corporate financial status and manipulation of company books, which came to light over the previous two to three years. The most notable cases were the Enron crisis, WorldCom and Tyco.

The primary aim of the bill was to protect investors through improving the accuracy and reliability of corporate disclosures and placing accountability for this on the organization's executives. Formulated in United States federal law, the bill has spurred similar initiatives in Europe and at this time (mid 2004) the European Union and a number of European countries are working towards similar legislation.

The act, known also as SOX, implements tight controls in corporate financial and accounting processes, considerably affecting how companies go about their business.

The Sarbanes-Oxley act obligates eleven broad areas of responsibility as follows:

- I. Public Company Accounting Oversight Board
- II. Auditor Independence
- III. Corporate Responsibility
- IV. Enhanced Financial Disclosures
- V. Analyst Conflict of Interest
- VI. Commission Resources and Authority
- VII. Studies and Reports
- VIII. Corporate and Criminal Fraud Accountability
- IX. White-collar Crime Penalty Enhancements
- X. Corporate Tax Returns
- XI. Corporate Fraud and Accountability

Most of these areas define controls and practices to be followed by senior management, financial officers and accountants. The controls and practices are varied and cover such areas as penalties, fraudulent activity, improper influencing, conflict of interests, qualifications of personnel and more.

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It is a partial explanation of the Sarbanes-Oxley Law of 2002 as understood by Bsafe Information Systems and prepared for the convenience of our customers only. It is by no means a legal reference and must not be considered as such. Bsafe Information Systems takes no responsibility for the accuracy of the contents of this document.



While many of these have nothing to do with information technology or computer security, some of them have a direct connection to the organization's information systems and so there is an important part to be played by the company IT department. The main categories of concern to the Information Technology Manager and Security Administrator are:

III – Corporate responsibility

Specifically, Section 302 - Corporate responsibility for financial reports.

IV – Enhanced Financial Disclosures

Specifically, Section 404 - Management assessment of internal controls.

XI – Corporate Fraud and Accountability.

Specifically, Section 1102 – Tampering with a record or otherwise impeding an official proceeding.

Additionally there is some significance for IT departments in category **I - Public Company Accounting Oversight Board** and category **VIII – Corporate and Criminal Fraud Accountability** which details the punishment in law for the changing and deleting of records.

After making a detailed study of these sections, the bottom line for the IT manager and security administrator in an organization using IBM iSeries or AS/400 computers may be summarized quite simply. They must do everything in their power to ensure the following two conditions are met:

1. Data must be protected against unlawful change or removal.
2. Changes in data must be logged and available for auditing to a reasonable degree.

Bsafe/Enterprise Security for iSeries includes powerful auditing and access control features which make a significant contribution towards meeting these conditions and so achieving Sarbanes-Oxley conformity. The list on the following page outlines the relevant Bsafe/Enterprise Security features which, together, constitute the answer to this conformity requirement.



A Mapping of Bsafe/Enterprises Security's Features Against SOX Requirements.

Function of Bsafe/Enterprise Security Covering the Act	How this Function Contributes Towards Sarbanes-Oxley Conformity
The Application Access Control	Restricts access to the iSeries through the network for each user according to definitions given by the security administrator. Anyone not granted specific permissions has no access whatsoever.
The Application Audit	Makes a detailed log of network events including detailed of user, time and type of access, SQL statement and advanced filtering capability to narrow down and identify specific events.
The Application Analyzer and Network Log Reports	A set of graphs and reports of the network events recorded in the Bsafe log. By identifying exceptions in network activity their use can pinpoint attempted breaches.
The IDS (intrusion detection system).	Sends instant alerts of breaches from outside or internal unauthorized activity
System Audit	Simplified but powerful management of the iSeries system journal including audit policy definition, ready-defined reports, system audit report generator and management of receivers. The system journal display allows filtering by many different criteria facilitating the investigation of security breach attempts and simplifying an otherwise complex and time-consuming task.
File Audit	Monitors and records changes in the iSeries database at user, application and even database field-level.
Internal OS/400 Security Manager	Allows operation of OS/400 internal security functions through an easy-to-use GUI. It includes user profile management,



OS400 object authority management and port restrictions.

Field Encryption/Masking

Masks actual values in selected sensitive fields.

File Protection

Protects files from power users, even QSECOFR.

Session Time Out

Considerably reduces the chance of an uninvited user working on another user's session.

Account Swapping

Switching of one user by another at session connect, adopting authorities without knowing the password of the other user. Full audit trail.

Central Audit

History of system activity and database access showing field level values for every record read by each user.

For additional information, please contact your local representative or visit the Bsafe Information Systems website at www.bsafesolutions.com

USA New Jersey	Canada	Europe & R.O.W.
Tel: 877-237-8024 toll free Fax: 775-593-4464 itay@bsafesolutions.com	Tel: 905-9434042 info-ca@bsafesolutions.com	Tel: (+972) 9-9610400 Fax: (+972) 9-9610408 chaya@bsafesolutions.com

Local resellers worldwide are listed on the Bsafe Information Systems website www.bsafesolutions.com

Copyright 2000-2006 Bsafe Information Systems Ltd.
 All rights and privileges reserved.
 All trademarks are property of their respective owners.
 Bsafe/Enterprise Security Analyzer patent 1326452
 Bsafe/Enterprise Security registered as IBM product no. 5620DLJ

IBM Product No. 5620DLJ
Analyzer: patent 1326452



© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It is a partial explanation of the Sarbanes-Oxley Law of 2002 as understood by Bsafe Information Systems and prepared for the convenience of our customers only. It is by no means a legal reference and must not be considered as such. Bsafe Information Systems takes no responsibility for the accuracy of the contents of this document.