



Bsafe Information Systems White Paper “Get SOX Compliant, Fast, with Bsafe/Enterprise Security”

Recommended Best Practices for the IBM iSeries Platform

Introduction

This is a brief, no-nonsense, list of directions to get compliant with Sarbanes Oxley compliance requirements, using Bsafe/Enterprise Security.

Frequently Asked SOX Compliancy Questions

What to Do?

How do I get to log the activity on the iSeries from the network and internally?	See stages 1, 2, 3 and 5 below
How do I implement access control to be sure that any user without specific permission to an application server cannot get access?	See stage 4, below
How do I set up and manage a security policy?	See stages 4 and 5, below.
How do I monitor changes in data?	See stage 6, below.
How do I produce audit reports on demand?	See stage 7, below.
Is there a way of being alerted the moment an intrusion or unauthorized access attempt occurs?	Yes. See stage 8, below.
How can I force an automatic timeout for user sessions?	See stage 9, below.
Is there a way I can protect resources like files, application servers and functions, from power users?	Yes. See stages 4 and 10, below.
How can I investigate suspected cases of careless or intentional corruption of data?	See stages 5, 6 and 7, below.

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be reproduced or duplicated without the permission of Bsafe Information Systems. www.bsafesolutions.com

Updated 12 June 2006

Tel: +1-201-5030021 +972-9-9610400 (all regions).



Step by Step Path Towards SOX Compliance

Stage 1. Install Bsafe/Enterprise Security

Until the product is installed, you are far away from compliancy. Follow the detailed installation instructions on the Bsafe website.

What you will have achieved upon completion of stage 1:

The logging of accesses to your iSeries from the network, and signon monitoring. This activity will be kept in the Application Audit and will be available for review and analysis. You have taken the first step towards compliancy.

Stage 2. Activate Bsafe/Enterprise Security protection for all Application Servers

Now you have installed the product, you should expand the range of application servers protected, one by one until all are active. Carefully follow the instructions and safeguards for Bsafe activation in the Implementation Instructions on the Bsafe website.

What you will have achieved upon completion of stage 2.

Monitoring of all access to your iSeries from the network - you will have a far more complete picture of the activity in your system. This picture will include information of users, IP addresses, application servers, times, actions and objects accessed.

Stage 3. Switching off Optimize

The product comes with a powerful built-in feature to minimize overheads and maximize system performance – the Optimizer. It is switched on by default for certain application servers (DDM, database, data-queue and file server) but when switched off, it gives a higher level of logging detail. Once your system has been running for a few days, switch the optimizer off for these four applications, one by one and checking if performance is affected. If so, Optimize will have to be defined for certain specific (usually I-O intensive) jobs. If not, continue with the next application until the optimizer is off for most or all of the system.

What you will have achieved upon completion of stage 3.

The highest level of logging for optimal use of the powerful auditing tools and graphical analyzer, and a basis on which to move to the next stage – building a policy for the protection of your system.



Before moving to stage 4, let's recap on what the SOX law is and what SOX auditors will be looking out for.

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, i5 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.**

The following stages will show you how to use powerful auditing, protection and access control features you have set up in **Bsafe/Enterprise Security**, above to make a significant contribution towards meeting these conditions and so achieving Sarbanes-Oxley conformity.

Stage 4. Completing Implementation

This is where you create permissions definitions based on the logged activity and your policy conception. Carefully follow the instructions and safeguards for Bsafe activation in the Implementation Instructions on the Bsafe website. The final stage of implementation is to lock down defaults access so that authorized users can access the iSeries only in the ways you have permitted.

What you will have achieved upon completion of stage 4.

Protection and access control of all applications - no unauthorized users will have access to the network or other exit point protected applications.



Stage 5. System Audit.

If you have never set up a system journal on your system, you have nothing to fear. Bsafe/Enterprise Security will do all the work for you and even pre-define the policy to log a wide scope of system events. If already setup, you will have control over the policy and information you'd never have imagined.

What you will have achieved upon completion of stage 5.

A thorough and detailed audit of all system activity with the ability to fine-tune the policy or, in other words, the kind of system activity you want logged and available for auditing. The activity logged here will be available for use in the dozens of ready-defined system journal reports shipped with the system, not to mention instant alerts and on-line inquiries. Examples of these reports include unsuccessful login attempts, object authorization violations and usage of adopted authority.

Stage 6. File Audit

Through file Audit, you will be able to view database changes which have taken place in your system. For files already journaled this is instantly available whereas files not yet journaled can be journaled in moments.

What you will have achieved upon completion of stage 6.

A field level view of database changes, additions and deletions whether done in native environment or from the network.



Stage 7. Run audit reports

Now everything is setup, you can sit back and enjoy the power of dozens of auditing reports and on-line inquiries.

What you will have achieved upon completion of stage 7

Instantly available detailed reports whenever you need them, covering network access, system activity, database changes, summaries and policy definitions. Alongside the audit reports, the interactive filtering and graphical tools will be available to investigate activity in depth.

Stage 8. Setup Alerts

It is now time to make use of the advanced features of the product. Setup instant alerts for selected events.

What you will have achieved upon completion of stage 8

You will be able to know the moment an intrusion, unauthorized access attempt or specific system event occurs, without having to discover it in audit reports later on.

Stage 9. Setup Session Timeout

Implement session timeout to suspend or end jobs which have been left unattended.

What you will have achieved upon completion of stage 9

Unattended Telnet signon sessions will no longer be left open for users to take advantage of the opportunity. This provides an added layer of security where policies and controls cannot always be trusted to users.

Stage 10. File Protection

Limit access to your most sensitive files to specified users only.

What you will have achieved upon completion of stage 10

Power users (ie those with *allobj authority or QSECOFR) will no longer have uncontrolled access to any object. This level of protection adds to the security afforded by OS/400 object authority.



Summary Table
Bsafe/Enterprise Features and SOX Requirements

Stage	Auditing Capability	Protection Capability
1	Auditing of network access and signon	
2	Improved network access and native environment auditing	
3	Maximum network and native environment auditing. Full use of inquiries and reports and graphical analysis tools	
4		Access control and protection
5	System activity auditing and system policy definition. Use of stock audit reports for reporting of activity	
6	Field-level database change audit	
7	Full auditing and analysis capabilities	
8	Instant alerts for selected access and system events	
9		Disconnection of unattended signon sessions
10		Protection of database files from all unnecessary users including power users