sentrigo

Achieving Database Compliance with Sarbanes-Oxley Using Sentrigo Hedgehog

Sarbanes Oxley and Databases – a Moving Target

The Sarbanes-Oxley act (aka "SOX") was introduced in 2002, but for most IT organizations it is still a moving target. External auditors keep changing the methods and requirements, and IT organizations are struggling to meet new requirements.

Databases are often a major focus of the SOX audit because they hold volumes of sensitive financial data and are by and large unprotected and not adequately monitored.

A key change has been the adoption of AS5 (Auditing Standard No. 5) by external auditors. One of its effects is the use of less prescriptive language by auditors as well as a risk-based approach. When it comes to database compliance this means that IT managers are no longer faced with check lists of all the measures and audit tasks they need to implement at the database level. Instead, they are tasked with implementing controls on financial data and other sensitive data, based on their particular business, applications, and data structure.

Faced with the new requirements, IT managers are looking for a database security and audit solution that will allow them to easily create the necessary controls at the database level, based on the auditors' requirements.

Existing Solutions – Native DBMS Tools

Most enterprises turn first to native DBMS audit tools and database triggers as a primary solution for their compliance needs. However, they soon find out the excessive administrative challenges that using native DBMS tools entails, as well as the severe negative impact on database performance. In some DBMSs the audit facilities do not exist at all, or require the use of tools that were intended for database troubleshooting and are not adequate for the task of complying with SOX.

Enterprises need a solution that will provide an easy translation of the auditor's requirements into a clear security policy, and easily implement the policy on the in-scope databases without impact on database performance or legitimate accessibility.

Hedgehog Database Security and Audit – The Easy Way to Translate Auditor Requirements to Policy

Hedgehog Enterprise, a host based software solution, monitors database activity and protects sensitive data from attacks, helping customers comply with both Sections 302 and 404 of the Sarbanes-Oxley Act.

By monitoring all access to data in the database, including access of privileged inside users (such as DBAs and other IT personnel), Hedgehog allows customers to monitor all access to sensitive data in a way that satisfies external auditors.

Once the auditors identify the sensitive data (financial and other), in a matter of minutes and without any interruption to the database or to other applications, Hedgehog is installed on the database host and soon begins monitoring all access to sensitive data. Hedgehog can also prevent attacks and other actions that could result in data loss or internal fraud, thus providing the highest possible level of database security for SOX compliance.

The Hedgehog SOX module – Database SOX Compliance in Minutes

When using Hedgehog the only preparation that you will need to undertake is to gather the locations of sensitive tables and several details that are usually readily available (e.g. the authorized applications, IP subnets that are authorized to access the database and so on). Once the data is collected a wizard interface walks you through the creation of the SOX policy for your databases, based on prudent best practices garnered from the experience of many customers and auditors.

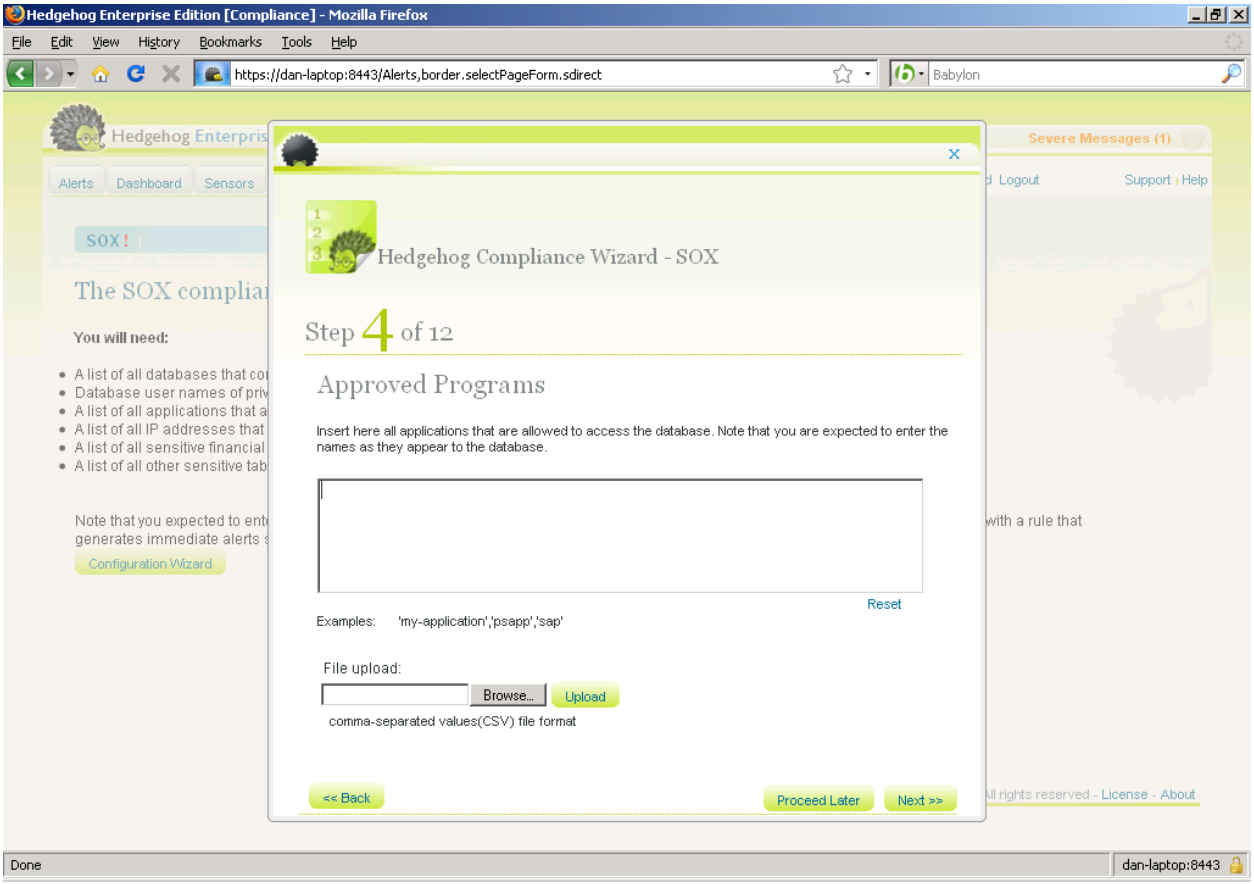

ILLUSTRATION 1 – HEDGEHOG SOX COMPLIANCE WIZARD

Once you have finished using the SOX Compliance Wizard, the in-scope databases are monitored immediately and you will be able to easily review your audit trails, as well as run ready-made reports.

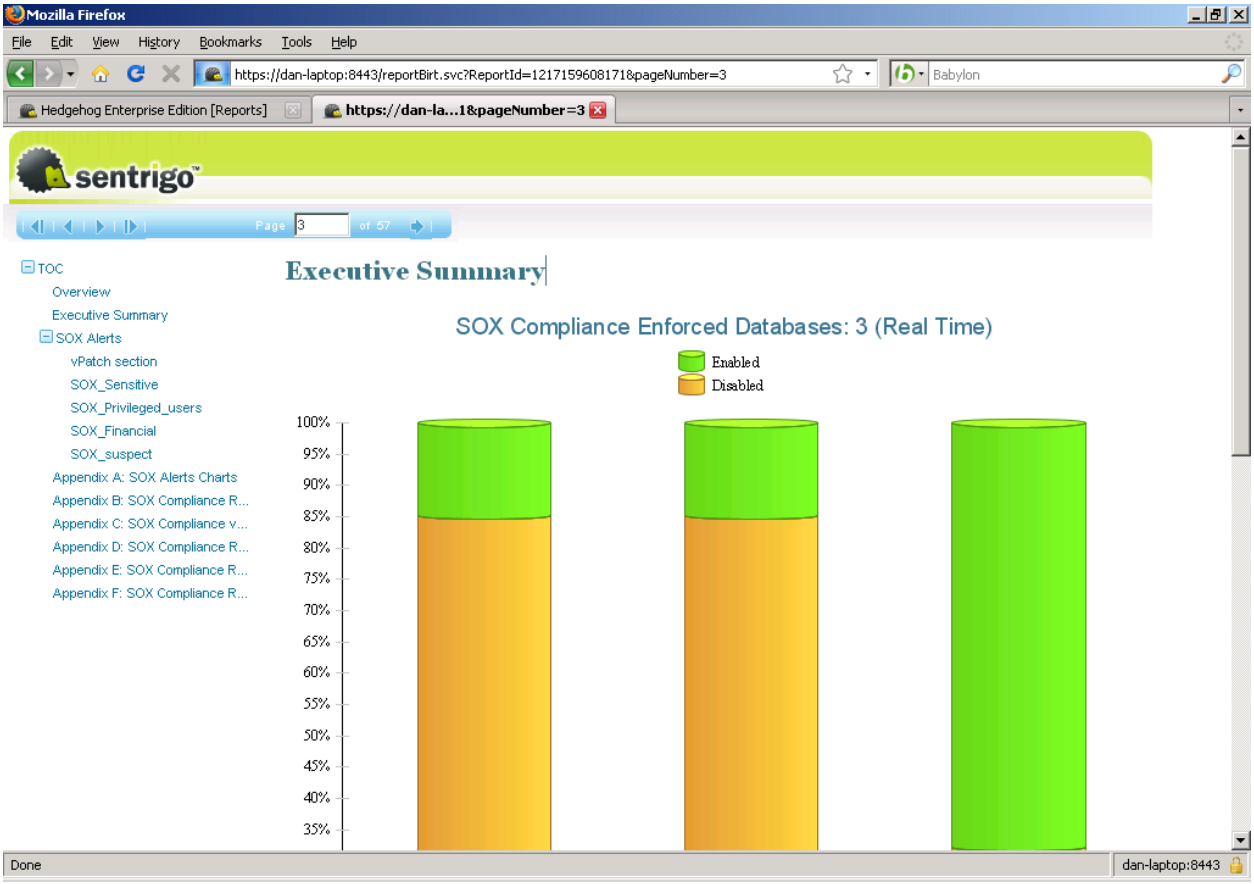

ILLUSTRATION 2 – SOX COMPLIANCE REPORT

Running the Sarbanes Oxley Wizard and the Resulting Policy

The Sarbanes-Oxley (SOX) Wizard requires the following data:

- A list of all in-scope databases that contain sensitive financial data as well as other data with which you associate high risk
- Database user names of privileged users, their OS user names and a list of application users
- A list of all applications that are permitted to access the in-scope databases
- A list of all IP addresses that are permitted to access the in-scope databases
- A list of all sensitive financial reports-related tables
- A list of all other sensitive tables where loss of data or its illegitimate access are considered high risk

When the information has been imported into Hedgehog, monitoring of the following begins on all in-scope databases:

1. Audit of all access to financial data.
2. Audit of all access to other sensitive data.
3. Audit of all transactions initiated by privileged users.
4. Audit of all transactions by suspect users and applications.

In most cases the policy will satisfy all of the auditor's requirements. In the event that the auditor requires further actions, you can easily fine-tune rules and add new rules, as well as create and schedule dynamic reports. If and when auditors' requirements change, Hedgehog's flexible policy creation tools make it easy to adapt to the new requirements by going through the same process of changing current rules, easily changing the monitored objects (e.g. sensitive financial tables) or adding new rules where necessary.

Summary

Sarbanes-Oxley compliance is a moving target for many IT and compliance managers, and the current tools are by and large inadequate in meeting the ever changing requirements for database SOX compliance.

Hedgehog Enterprise provides an easy-to-implement policy that monitors all in-scope databases from a single central management system, and allows customers to easily respond to auditor requirements as well as to change the policy whenever the requirements change.