



Is 339° Security Audit Sufficient?

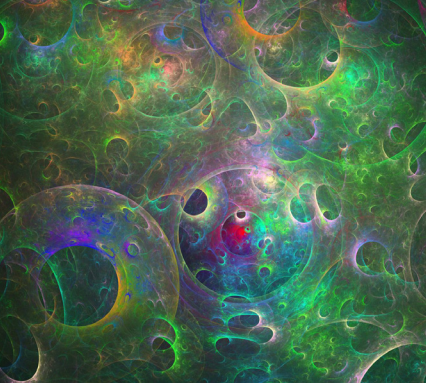
– A Whitepaper for CTOs and CEOs

By Dave Beulke

From your boardroom to your living room, everyone wants to know if their personal information is secure in your company. All types of hacking are prevalent, from stealing information, to a process to destroy industrial machines, to a weapon to change governments by exposing political secrets. Recent studies from Verizon (<http://www.verizonenterprise.com/DBIR/2015/>), FireEye (<https://www.fireeye.com/current-threats/threat-intelligence-reports.html>) and others have calculated that last year over a half a billion data records were stolen from files and databases around the world. These hacking exposures have cost companies hundreds of millions of dollars in fines, penalties, and business losses. Does your company appear vulnerable?

A positive perception of your company and its brand is paramount to success in today's world. Data security is a critical component of that perception. Customer trust and social reputation depend on your company's transparency and adherence to the many PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NIST, and other compliance standards. These different industry standards each provide detailed guidelines for confidentiality, integrity and protection of private customer data. Properly standardized security, audit procedures, and efficient processing are the foundation needed for your enterprise system's long-term organizational success.

“Data security is a critical component of perception.”



Enterprise Complexity Hinders Success

Legacy applications, heterogeneous, and the constant development of new environments provide complex compliance challenges. Auditing and governance for these environments is a time consuming and recurring ordeal. The standardization of policies and overall security procedures needs to be continuously streamlined for efficiency and cost containment as new systems come online to ensure regularly scheduled compliance. The recurring expenses of compliance efforts steal resources and precious time away from the real profitability goals of your organization.

The Security Audit Difference

You need a partner with experience to help you with the constant data access activity analytics and industry standards reporting requirements. Today's audit solutions need to use existing integrated DB2 infrastructure, quickly analyze data access and to simplify the complexity of security audit tasks. Any security audit solution needs to quickly address recurring compliance and governance business requirements and provide a comprehensive multi-dimensional solution to satisfy the many different documentation requirements of inside stakeholders and outside auditors. State of the art security audit compliance activities document system, database and application areas and have the ability to provide all types of extremely detailed information as well as summary level material based on any type of reporting requirement.

“This security and audit compliance can be developed in-house but its time consuming maintenance is not a match for the vendor tools that are available.”

After many years serving customers, I have honed expertise on the compliance and audit details that can make the crucial difference in your company's governance and compliance success. Our audit and reporting solutions concentrate on delivering a comprehensive view of the security protecting your data, who is accessing it, what access method is being used, how was it accessed, and when was it accessed. This information presents comprehensive Use Case views of the security authorization practices, the data workload, and any ad hoc access within your environment, alerting you to any security problems before they become a crisis.

Having a security strategy and compliance reporting system through a multi-dimensional approach with multiple layers of protection and comprehensive reporting is critical to protect your data. A complete picture of your security data protection with compliance standards customized to your regulations can be easily developed by tracking all types of access within the system, SQL access through the applications, and object security profiles. This security and audit compliance can be developed in-house but its time consuming maintenance is not a match for the vendor tools that are available.

“The best tools leverage the existing DB2 infrastructure to get SQL activity and application data access.”

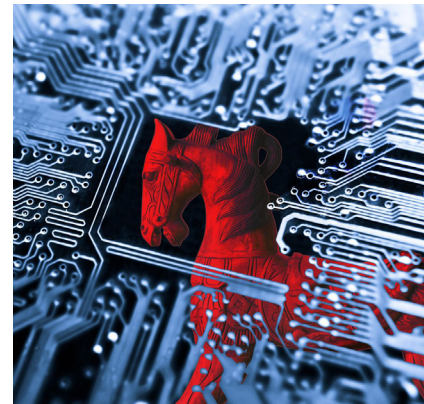
Support for Your Team

By leveraging tools, many with easy and straightforward GUI interfaces, your team can navigate, understand, and maintain their security perimeter more efficiently. Security auditors really appreciate using a tool with a good architecture and easy-to-use design to quickly develop compliance reports, document security privileges, and understand object security profiles. Having an easy to learn GUI interface tool your technical and business users quickly understand their security compliance considerations and can quickly document their security audit id activities.

Evaluation of the security and audit tools must identify any extensive overhead or cumbersome interfaces that can present performance issues while monitoring security compliance. The best tools leverage the existing DB2 infrastructure to get SQL activity and application data access. Tools integrated into the existing infrastructure, can get compliance answers quickly for regular reporting and report solutions for especially critical expedited research of irregularities and exceptions. Having a security audit tool that has almost no overhead, making implementation and use manageable for constant monitoring, reporting and protecting your data assets is the state of art solution.

History of security privileges, security settings, and the ability to report on past security compliance can be a major effort for any audit and compliance reporting. Having a tool and partner who understands and has extensive background with these reporting needs is vital for minimizing and streamlining audit time and costs. Through an integrated security audit tool, your staff and auditors can follow previously developed templates to build a repository of security compliance information for all industry type standard reporting requirements, exception reporting for quick diagnosis of exception security situations

In addition, some tools provide a historical SQL access and security details repository that can supply a variety of benefits from capturing all historical active access to your databases to analyze all the access in detail, or in aggregation for compliance reporting, usage pattern analysis, or charting security or audit metrics. Through the SQL access security repository, developing overall compliance documentation inspections can be researched over any timeframe for all types of security and auditor details to efficiency and effortlessly fill any compliance requirements. This compliance reporting capabilities can inspect today's, last month's or any previous timeframe for all security compliance aspects. This security compliance historical research ability lets security and compliance auditors create reports dynamically to enhance their specific research and security audit compliance efforts.



In this new digital world economy, data is the most critical asset of your company and its security is vital to your enterprise's bottom line success. Securing it, protecting access to it, and having transparent security and audit compliance reporting helps all your stakeholders have confidence in your company as a trustworthy business partner.

Through my years of audits, I understand these security requirements, compliance-reporting capabilities, and audit functionality details. Having experience and capabilities that provide a comprehensive solution for securing your data and compliance reporting for tomorrow's challenges today save time and money.

A solution I can recommend is WorkloadExpert Audit for DB2 z/OS from SEGUS/ SOFTWARE ENGINEERING. It gives you the benefits:

- Quick to learn and easy to use
- Low to no overhead
- Serves all levels of users with their desire level of reporting
- Comprehensive compliance reporting of activity, privileges against all your data
- SQL repository to report any compliance timeframe desired

“In this new digital world economy, data is the most critical asset of your company and its security is vital to your enterprise's bottom line success.”

Links to Reports reference above:

<https://www.fireeye.com/current-threats/threat-intelligence-reports.html>

<http://www.verizonenterprise.com/DBIR/2015/>

About the Author Independent consultant Dave Beulke is a system strategist, application architect, security auditor and performance expert specializing in Big Data, data warehouses, and high performance internet business solutions. He has been an IBM Gold Consultant since 1998, one of the first IBM Information Champions, President of DAMA-NCR, former President of International DB2 User Group, and frequent speaker at national and international conferences on data management topics. His architectures, designs, audits and tuning techniques help organization better protect their information assets and help them save millions in processing costs.

© 2016 Copyright Pragmatic Solutions, Inc.