How to establish a SECURITY AUDIT for DB2 z/OS

– A TEMPLATE for DBAs

By Dave Beulke

Data security is on everyone's mind. With all the types of hacking and information theft going on these days, recent studies from Verizon, FireEye, 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?

As a data scientist, database administrator, or management professional you realize a positive perception of your company and its brand is paramount to success in today's world. Data security is the critical centerpiece component of that perception. Customer trust and social reputation depend on your company's transparency and adherence to the always evolving and tightening PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NIST, and other industry compliance standards. Properly standardized security, audit procedures, and efficient processing are the foundation needed for your enterprise system's long-term organizational success.

"Properly standardized security, audit procedures, and efficient processing are the foundation needed for your enterprise system's long-term organizational success."

Security Audit Mindset

Through my consulting engagements, examining systems, databases and applications during security audits offers many challenges because each company's situation is unique and has distinctive data security requirements. The following categories and considerations highlight the many areas that need evaluation when starting security audits, different aspects of data security compliance audits, and the implementation of a long-term solution for constant vigilance against hackers through a comprehensive security audit plan.

Each company has unique data security and compliance requirements because of their industry, the variety of computing platforms, mix of homegrown and purchased applications, and the diversity of programming languages and data interfaces. These distinctive, unique areas create huge challenges that are similar to the extensive unique disaster recovery procedures which require a constant vigil of an extensive dedicated staff to safeguard business continuity. The same dedicated resources to security and compliance are needed to keep your data safe. The scope of critical business issues is very similar and upper management commitment needs to be firmly established for the time, resources, and tools necessary to defend your business and brand.

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

> "Auditing and governance for these environments is a time consuming and recurring compliance reporting requirement."

Ease of Implementation and Use

Today's dynamic robust systems, database and application environments also requires that security and audit procedures and tools be extremely easy to implement and use. Speed of implementation, standard audit procedures, quick time to answer interfaces and robust reporting are critical for responding to the dynamic complex systems environments' security situations.

Within the industry's security and audit tools there are many options and implementation strategies. Specialized security, audit infrastructure definitions and maintenance are burdensome to implement, maintain and upgrade. The best solution is for all aspects of a security and audit frameworks to utilize the existing database's native instrumentation, logging and interfaces to monitoring data usage and management of the database infrastructure. Using these many native integrated database instrumentation, logging and other interfaces your security and auditing activities are assured to get the complete view. These built in facilities provide all the access activity information, are able to provide dynamic alerts and provide details needed to proactively protect your data.

As complex as the environments and data management issues can be, the implementation of security and audit features needs to be quickly and easily setup from samples, templates and previous defined configurations. These configurations should then be customizable for easy collaboration with auditors and customizable to supply detail information for potential threats and security exposures.

Dynamic Security Audits Are Critical

Often the security audit and compliance requirements are assigned to the understaffed and overburdened security department which is usually busy with daily operations and new projects. By performing only static periodic security audits and compliance review activities, their finalized stagnant audit definitions leave systems and database security vulnerable to the latest hacking methods. In today's dynamic landscape, static security audits are not effective for constantly changing systems, applications and hacker techniques.

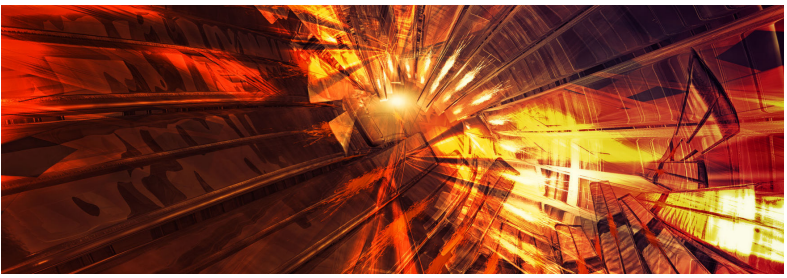
System and application changes need constant security auditing that quickly analyze, identify, and defend from penetration testing of hackers. Dynamic hacking techniques and constant research of systems and database vulnerabilities easily circumvent static security techniques and audit practices. Today's business is online 24x7x365, and your security auditing and procedures need to be as dynamic and robust as the constant poisonous penetration probes that are attacking your systems.

> “Audit and reporting expertise and effective use of proper security and audit tool solutions focus compliance efforts quickly.”

Fulfill Today’s Dynamic Needs

Experienced consultants using industry tools who understand the recurring reporting compliance and governance business requirements are vital. These partners and tools can help your company develop comprehensive multi-dimensional solutions to satisfy security audit and compliance requirements of your industry, your company’s specific applications, and overall compliance reporting requirements. This can be a very complex task since there are so many different documentation requirements for inside stakeholders and outside auditors. In addition, your company may need to produce specialized compliance reports for industry, government agencies, and other outside auditors. To obtain tools that exploit best practices, evaluate compliance automation tools for their ease of use and the ability to provide all types of extremely detailed security audit information as well as summary level material based on any type of reporting or timeframe requirement.

Over time spent performing company security and overall audits, security practices and their compliance are improved and sharpened. Compliance expertise with the different industry types and audit details can quickly speed up the time to compliance and make a crucial difference in your company’s governance and compliance success. Audit and reporting expertise and effective use of proper security and audit tool solutions focus compliance efforts quickly. This focus helps everyone to 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 detailed information presents comprehensive Use Case Views of 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.



Expandable for Tomorrow

Extensibility and expandability are two additional areas to assess when evaluating any security audit compliance reporting and automation tool. Assess the ease or difficulty of adding new security audit areas, new applications, or new data files into the assortment of your compliance reporting. Also, evaluate the variety of report types that your tools can produce from the base security auditing information. Make sure to evaluate producing standard compliance reports, spreadsheets, and specific detailed security subarea reports.

Also, gauge the ease of producing charts, pie graphs, and pivot tables of your compliance and security activity information. During your initial evaluation efforts, try to produce all the security audit and compliance reports you believe your company will need on a regular basis or estimate the development time of the various security audit and compliance reports required immediately for industry groups, inside auditors, and different levels of management.

Once the standard security audit and compliance reports are checked out, try to extend the various reports to include another area or security situation. Determine if extending the data and reporting processes is easy and how difficult it is to produce a compliance report for an ad hoc security emergency type request.

Next, analyze how easily the report timeframe details can be adjusted from reporting on standard periods to flexible timeframes, extending or compressing audit report scopes. The security timeframe reporting aspect is very important because it helps everyone understand the recent security approval changes done, their impact on access over time, and their effect on the system or application area activities.

> “The security timeframe reporting aspect is very important because it helps everyone understand the recent security approval changes.”

Multi-layer Approach

Having a security strategy and compliance reporting system with a multi-dimensional approach and multiple layers of protection and comprehensive reporting is critical to protecting your data. Your company needs a complete picture of its security challenges. The best technique is to capture and track all access of different types of interfaces via the system and the applications' SQL access. Documenting, analyzing, and including all the ad hoc database access and all the database utility usage also needs to be complete in the security and audits compliance reports.

Another layer for security audits is the database and file objects' security protection profiles. Detailing the different users and ids that have different read and/or update access to various database objects and files is another layer of analysis for your security and audit reports. The object security definitions along with their application information need to be analyzed to understand any overlaps or user security ids that have cross database or application definitions that can sometimes be a security risk.

The next layer is the analysis of elevated users within various systems, databases, and applications. These elevated ids need extra attention as the powerful nature that lets them update critical data elements and usually configurations may inadvertently loosen security defined within application environment.

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 auditor or tool. Having a reporting tool and consultant who understands and has extensive background with these reporting needs is vital for minimizing and streamlining audit costs. Staff and auditors need to leverage industry compliance templates to build a repository of security compliance settings over time to produce all types of security profile compliance delineated timeframe reports.

Some security and audit tools are cumbersome and have extensive overhead which can present performance issues while monitoring security compliance. Manageable methods to get answers and speed to achieve compliance solutions are paramount for regular reporting and are especially critical for expedited research of irregularities and exceptions. Evaluate and classify the security audit tool's overhead, time for implementation, and overall manageable/usage for constant monitoring, reporting, and protecting your data assets.

Security Measurement, Analysis and Improvement Procedures

When starting a security audit initiative, it is paramount to implement a full 360° view of the security perimeter for your organization: its systems, application, and personnel. Driving the development of the initial security requirements through the most active and revenue related application is usually a good starting point. Collecting its general security and audit requirements, then capturing all of its database and personnel related security activities is very enlightening for all the technical and management participants.

The initial security data collection establishes a baseline and beginning of the security audit and reporting procedures. Hopefully, the information gathering does not surprise anyone with its variety and large number of accesses and users. Grouping the access types and classifying the users is the first step in corralling the security around the diversity of the system, database, application, and associated file usage.

Next comes the monitoring and measurement phase where the security grouping and numbers within the initial analysis are validated. Do the user types, number of accesses through the day, or usage pattern change? If usage fluctuates, could there be better security definitions or security groupings for better management within reasonable tolerances? Evaluating these security and audit questions needs to be done first for the most important PII, HIPPA, and proprietary data that justified the security and audit activities in the first place, and then for each of the less important data objects within the other systems, databases and applications.

"When starting a security audit initiative, it is paramount to implement a full 360° view of the security perimeter for your organization."

Then evaluating the baseline usage against the business, the deviation of the number of accesses, and the types of users' needs to be audited. If the number of users or types of users deviation from the normal usage is greater than reasonably expected, or if a new single unexpected user is in the usage it may identify a research hacker probe within your system, database, or application. Based on security audit findings, next best actions can be as extreme as a shutdown of the entire system, database, or application or as mild as general questions to end users. Monitoring security access to the data, redefinition of the security profiles, or other notification to management of the anomaly situations needs to be developed into standard escalation procedures for different types of data security situations.

These anomaly situations can lead to a large number of discussions of internal audit result findings. The key is to evaluate the security landscape of your system, database, and application activities and then develop the proper level of scrutiny, skepticism, and curiosity to separate the justified proper access against the malicious probes of someone planting a Trojan horse process within your overall company enterprise architecture.

Next, the internal audit evaluation then needs to determine the level of tolerance and level of action that needs to be taken against these different situations no matter how big or how small the security anomaly is within the security landscape. How much security control do each of the situations warrant within in the realm of protecting and securing your data? How does the business value, react, and provide access without further risking other accesses of other corporate data? These considerations can lead to deep concerns and wide-ranging security questions given the millions of dollars at stake with a potential breach of the PII and other critical data within the organization.

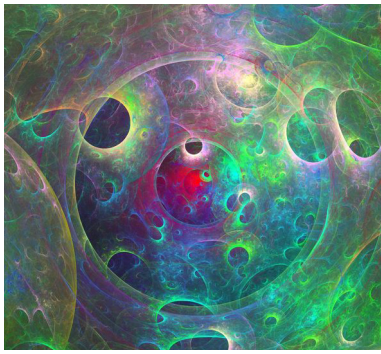
Next, preventative and corrective action needs to be established for a consistent and planned procedure within the company so all the systems, databases, and applications can be controlled, corrected, and standardized for future security and audits. The original goals of providing the best access and security to the proper business function are critical for the business. Security tightening actions and discussions need to focus on the anomalies and corrective actions to enhance trusted users while isolating the anomalies for further detailed scrutiny until verification of all users and their access is complete and trusted.

All these security audit actions and procedures are only a first step in the ongoing procedures to repeat every day, week, and quarter for every changing database or application within your organization. Security configurations and users always present new and interesting challenges to your ability to keep security and audit activities analysis and correction procedures fine-tuned for all data management areas and all your data secure.

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.