t e l e r a n.
Data Visibility and Protection

Authored by Robert Schnitzer and Jeff Devlin

Meeting Risk and Compliance Requirements While Expanding the Business Value of Data-Intensive Applications

An Information Management Perspective

Executive Summary

This paper, written by two Information Management executives, describes how a Fortune 100 financial services company addressed data audit, risk and compliance issues while at the same time improving the business value and efficiency of data-intensive enterprise applications. External auditors identified security risks and compliance gaps associated with the company's enterprise data warehouse, widely used CRM systems, and other data-driven analytical applications. The central issue identified by the auditors was that these systems, supported by very large databases, were used by thousands of employees across the organization, allowing potential misuse or theft of sensitive business data and personally identifiable customer information (PII).

At the same time, as these systems had grown larger and more critical to the operations of the company, Information Management recognized the need to have a deeper understanding of how the business was using the data in these very large systems. They were seeking greater usage visibility to better support the business objectives, improve the value of these business-critical systems, and to ensure ongoing system cost efficiency and performance.

The authors partnered with their company's internal Audit, Risk, and Compliance groups to address the data compliance and security requirements, while improving the visibility of these applications with data visibility and protection software from Teleran. With a deeper understanding and context of the business usage patterns, Information Management worked with Risk and Compliance to configure the system to deliver more effective protection and compliance. It resulted in lower audit costs and reduced audit exceptions by over 30%. It also enabled them to deliver back to the business increased system performance, better service, and improved system efficiency.

Audit, Risk, Compliance and Information Management Challenges

As a Fortune 100 financial services firm specializing in retirement funds for people who work in academic, research, medical and cultural fields, the company had to meet stringent internal governance rules, increasingly complex regulatory compliance mandates, and escalating data security standards. Large and critical database applications needed greater oversight, better transparency into what data was used, and more comprehensive data usage protection to prevent harmful breaches and compliance violations.

Specifically these systems allowed in many cases unfettered access to vast amounts of company data, including sales revenue data, sensitive customer information (PII), and other operational data. PCI-DSS, SEC, Sarbanes Oxley (SOX), SAS70 and other regulations all require monitoring and control of the access and use of the company's sensitive data.

The Audit, Risk, and Compliance departments needed to partner with the Information Management team to ensure ongoing data integrity, compliance and protection of their critical applications and data. At the same time Information Management recognized that it needed to have a deeper understanding of how the business was using the data in these large systems. They were seeking greater visibility for three reasons: 1) to better support the business objectives of these critical systems, 2) to improve their business value, and 3) to ensure ongoing system performance and efficiency.

There were particular challenges with the company's enterprise data warehouse, CRM system and analytical applications: the usage was highly dynamic, query patterns were complex and constantly changing, there were thousands of users from a broad range of departments and functions using many different reporting and analysis tools accessing and using the data in different ways. In addition, the databases contained hundreds of terabytes of data and were constantly expanding and adding new data. This made it challenging to understand, audit, monitor, and manage the use and access to these large systems to meet data compliance and protection requirements while ensuring the business value and consistent performance.

Working together, the teams developed a combined set of requirements. The system needed to:
- Continuously monitor and report on access to sensitive and non-sensitive data
- Deliver granular access controls to enforce data security and compliance requirements on sensitive database tables and columns by user, user groups and applications
- Provide detailed data usage visibility and compliance reporting
- Provide analytics to enable a deeper visibility into dynamic and complex data usage patterns
- Combine application usage metrics, including the application users, with data usage tracking
- Integrate with the company's Security Information and Event Management (SIEM) solution
- Deliver comprehensive visibility on application performance and efficiency
- Minimize implementation effort and ongoing administrative overhead

The Audit, Risk, and Compliance groups as well as IT initially reviewed tools that were being used internally by the company. It soon became apparent that these tools were inadequate for the problems at hand. Native database monitoring tools were designed for database administration and management and no longer appropriate for ongoing compliance and security monitoring, nor did they provide the depth of visibility for Information Management to better understand the business use of the data. In addition the native database tools needed to be managed by DBA's, violating auditors' "separation of duties" requirements. They also consumed a material amount of database resources if they were used continuously, putting at risk service level agreements and increasing demands on already strained IT infrastructure resources.

As a result, an analysis of current tools in the marketplace was conducted. Teleran's software product suite was identified as the one that would best satisfy the requirements of Audit, Risk, and Compliance. At the same time, it would also deliver the data usage visibility Information Management was seeking to improve support of the data warehouse and the CRM reporting and analysis process and enable them to enhance the business value of those systems.

Product Selection Criteria

The teams chose Teleran's solution based on these criteria:
- Fulfilled granular data monitoring, reporting and control for both compliance and data protection
- Highly scalable, unobtrusive architecture supporting high volume applications and large databases
- Visibility on complex querying behavior of data across user groups and applications
- Identified the users in their organizational and functional context
- Integrated with BI and analytical tools for visibility across both the data and application layers
- Real-time query and access controls that were easy-to-implement and adapt
- Integrated reporting and analysis including ready-to-go compliance reporting modules
- Ease of installation and ongoing administration
- Separation of duties from DBA teams
- Support for both on premise and public cloud or hybrid model
- Strong vendor references and track record with large, complex database applications

Teleran Product Suite

Teleran's solution provided three software products that delivered the data visibility, compliance and protection the company required.

iSight is a query and data usage monitor. It continuously and unobtrusively captures who is running what queries and reports against what data with what application. It delivers three critical visibility enhancing capabilities which are very valuable to the company and distinguished it from the competition:

1) The **Identity Persistence** feature ensures that all users are identified, despite the use of connection pooling, single sign-on or proxy database IDs that mask the actual users' identity accessing the database. This was a critical capability for the company considering the wide range of users and methods for logging into applications and systems. Tracking the actual user back to their specific transactions enables more accurate compliance and more effective data protection.

2) **Business Context** associates users with their specific organizational context like location, geography, role, department and functional area for deeper insight into identifying appropriate and inappropriate behavior and delivering a business context for IT support. This feature enables the company to put usage in the context of the business and create controls appropriate to the role and function, thus enabling effective compliance and protection while not impeding business use of the data.

3) **Applications Integration** builds broader usage context and protection by associating application level metrics including user ID, application names, report names, and application server activity

with database transactions. This capability gives auditors and compliance teams a combined view of both the application layer and the data layer, providing a comprehensive visibility to ensure data compliance and protection. It also significantly enhanced Information Management's understanding of the business use of the applications and data.

iSight Analytics is the reporting and analysis engine that delivers audit, risk, and compliance reporting, as well as data usage visibility. Its reporting highlights overall risks, inappropriate or suspicious activities and identifies user behaviors that reduce performance and efficiency. iSight Analytics is designed for use by non-technical roles such as auditors, compliance and security staff and application managers.

iGuard is a query policy action engine, a SQL firewall if you will, that prevents users or applications from launching unauthorized or inappropriate queries against sensitive data. It also prevents inefficient queries from degrading database performance. iGuard operates in-memory within the Teleran network agent. Its patented high speed, artificial intelligence (AI) rule engine allows it to operate automatically without human intervention in determining what queries can pass to the database and which ones violate active policies and are blocked. If a query is blocked, a user message is passed by iGuard to the user's application informing the user that they attempted to violate a compliance or governance policy.

Implementation

One of the benefits of the Teleran system is its ease of implementation. The software is logically very straightforward. A proxy listener is installed on the network between the applications and the backend databases, typically on the same physical server as the database. A secure repository is set up in a relational database on the internal network. An analytical server is also installed to analyze and report on what is captured and stored in the repository. Installing and configuring the software typically took two hours per database system. Generating meaningful monitoring reports began almost immediately, within a few hours of installation.

Teleran's patented network agent monitors and controls access at the database protocol layer (layer 7 of the OSI model) on the TCP-IP network. Because Teleran's agent does not rely on in-the-database functions such as triggers, traces or transaction logs, it does its job of continuous monitoring without affecting database performance or stability. Ongoing management and administration of the software is minimal and did not require additional staff hires.

Network-based Architecture
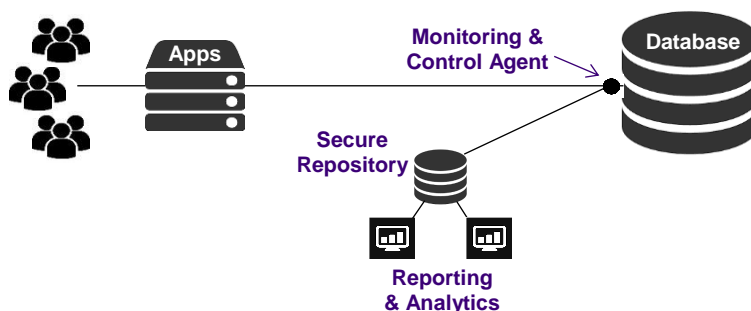
Meeting Audit, Risk, and Compliance Requirements

Teleran's products, once implemented, provided a level of audit and compliance monitoring and control unmatched by previous attempts with other products. Both internal and external auditors were highly satisfied with the compliance and security audit results that were demonstrated. For the first time they had a centralized system that provided a comprehensive, accurate, and consistent single point of truth for their audits and compliance reporting on these complex and dynamic systems. The Audit and Compliance teams were relieved of tedious efforts in meeting the demands to attest to and document compliance across the wide range of internal data governance and privacy policies as well as state and federal regulatory mandates. The Teleran iSight compliance reporting included a wide range of standard compliance report templates that were easily customized to meet the needs of compliance staff and auditors. Teleran's contribution to the enterprise audit process was recognized as a strong success.

One key measure, the number of audit exceptions, was significantly improved; after the implementation of the Teleran suite, audit exceptions compared with the prior period were down by over 30%. The company was able to put in place a process and technology to meet increasingly stringent data audit requirements and also lower the cost of audits and associated remediation going forward.

Sensitive Table and Column Access Audit Report
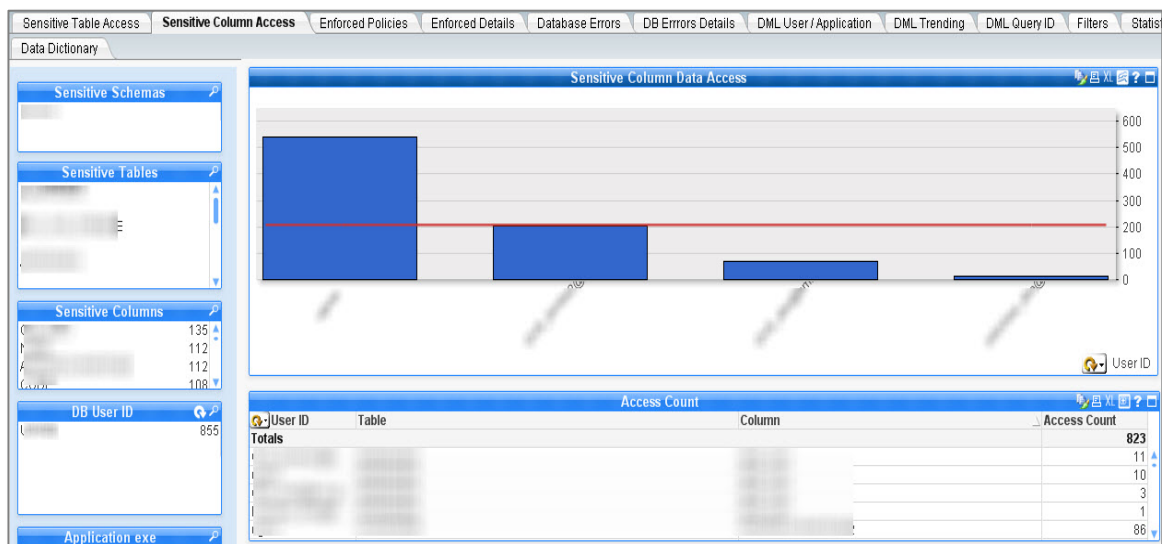
Auditors and compliance staff utilized reports like this and others to ensure that the access and use of sensitive data is in compliance with internal audit and regulatory compliance policies.

Drill-Down to Detail SQL Query Audit Report

The Teleran system also captures and reports on data manipulation activity by providing a detailed look into what DML (data manipulation language) is being executed by whom, with what application and on what data. Auditors required this information to document that sensitive data protection and integrity policies were being enforced.

**Data Integrity (DML) Reporting by Applications and Users**
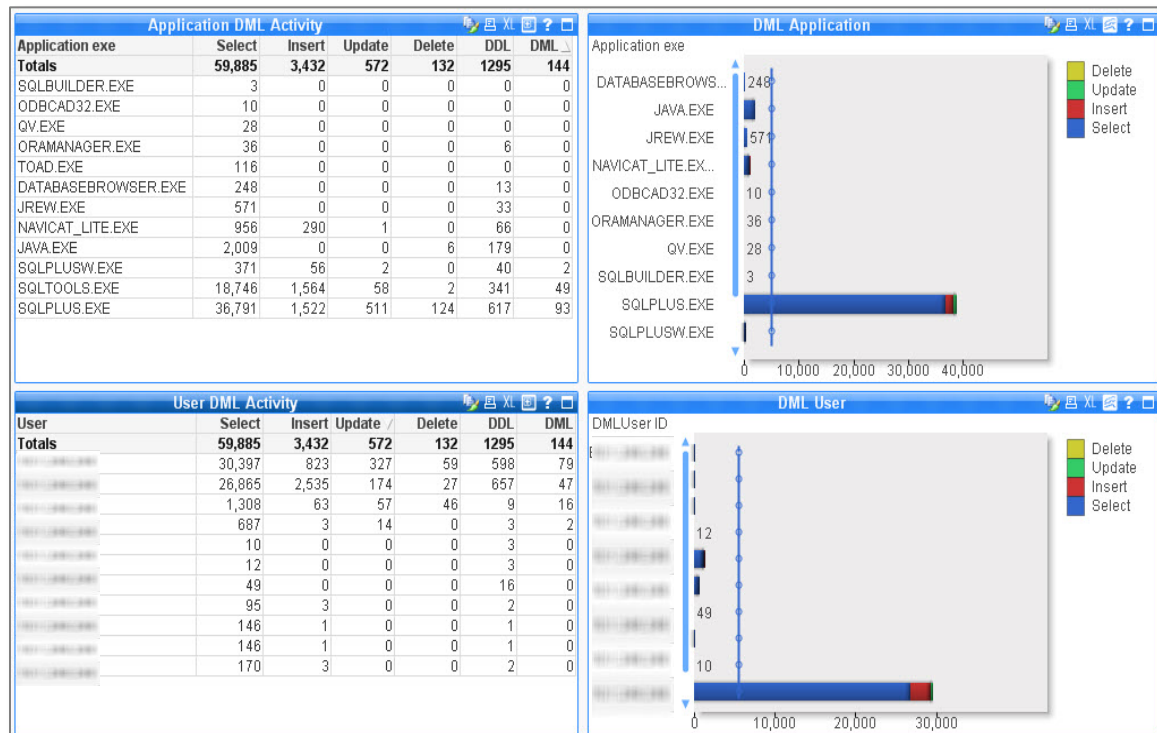
Detailed Data Integrity Audit Report

Business context is critical in data audit, compliance and protection. Profiling data usage by identified users in their departments, functional areas, roles, and locations enabled the company to establish context-aware baseline activity and identify inappropriate or suspicious data usage behavior that requires further analysis or monitoring.

Transaction Analysis in Context of the Business
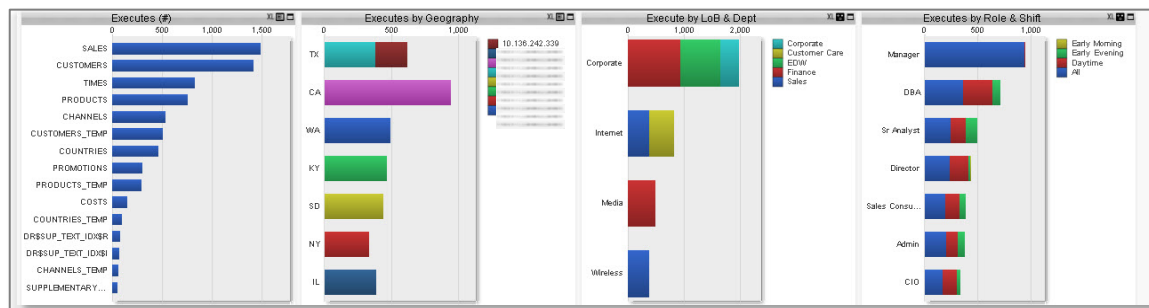
Delivering Data Protection

The Audit, Risk, and Compliance staff as well as the Information Management team deployed the iGuard data protection solution to address the need for greater data access and usage controls. Because the data warehouse and CRM systems was very dynamic and accessed by many different software applications, building consistent controls at the application layer was not feasible. iGuard fulfilled the need to deliver consistent and granular data usage controls independent of the database and the applications. iGuard policies can be customized and applied using an intuitive point-and-shoot interface. In addition, iGuard comes with over 70 policy templates that can be easily customized to address a wide variety of unique policy requirements.

iGuard Data Protection Policy Selector

| iGuard Candidates Detail | iGuard Policy Selector | iGuard Policy Categories | iGuard Policy Variables | Enforced iGuard Policies ● | Enforced iGuard Policies Detail | Filters | Data Dictionary |

Statistics | Configuration

Compliance		Shift Needed?		Datasource		Relational Operator		INSERT		CREATE		GRANT	
no	27	no	12	no	14	no	47	no	49	no	49	no	50
yes	25	yes	38	yes	38	yes	4	yes	3	yes	3	yes	2

Application Need...: maybe 2, no 8, yes 10

Performance		Table		Numeric Value		UPDATE		DROP		SELECT (Read)	
no	20	no	14	no	41	no	48	no	49	no	48
yes	32	yes	38	yes	11	yes	4	yes	3	yes	4

< Value Need   Variables >

Usage		DB Specific		Column		DDL/DML (Write)		DELETE		ALTER		Policy Type	
no	38	No	47	no	39	no	41	no	49	no	49	Advanced	6
yes	13	no	2	yes	13	yes	11	yes	3	yes	3	Basic	46
		Yes	3										

Policy Name

- Application Restriction
- BETWEEN Range Limit
- Column Access Restriction
- Column Combination Restriction
- Column Filter Requirement
- Column Restriction
- DDL Restriction
- DML Restriction
- IN List Limit
- Join Limit
- Join Requirement
- Join Restriction
- Large Table Restriction
- NOT IN Restriction
- Partition Access Requirement
- Relational Operator Restriction
- Row Level Restriction
- SELECT Restriction
- Self-join Restriction
- Table Join Requirement
- Table Requirement
- WHERE Requirement
- z.not in use

Policy Groups and Descriptions

Policy Name	Policy Description	Use Case(s)	User Message
Application Restriction	This policy prevents queries from executing on <TABLE> without a filtering condition unless the query is issued by <APPLICATION> by <USER> and <DATA SOURCE>.	Use this policy to prevent inefficient queries from access tools like MS Access in which users can easily launch queries with no conditions.	In order for your query to run faster, you must use a condition (against <TABLE>.
BETWEEN Range Limit	This policy prevents queries from executing on <TABLE> filtering on <COLUMN> using a range of values (using BETWEEN or NOT BETWEEN) where the interval of the range of values is larger than (or smaller than) a specified <NUMERIC LITERAL> value by <USER> and <DATASOURCE>.	Use this policy to limit the size of the results set returned when filtering on a range of data for a specific column.	Your query has been cancelled. You must limit the range of BETWEEN or NOT BETWEEN to x.

Here are some of the query policies the company applied using iGuard:

- White listing authorized applications. All other applications or data access tools were blacklisted and blocked by iGuard
- Allowing only selected privileged users to update or change data using DML. All other authorized users are designated "read only" users and limited to "SELECT" queries
- White listing authorized users to allow access to sensitive data tables and columns. All other users' access to sensitive data are blocked
- Preventing users from joining certain data tables that enable them to infer sensitive information
- Preventing certain users from accessing detailed customer records and allow them to view only summarized customer data tables

iGuard controls as well as the iGuard reporting on the controls are auditable and attestable, a key requirement for both internal and external auditors.

iGuard Active Data Protection Audit Report

| Dashboard | Comparison | Time | Time Comparison | Applications | User | Instances | SQL Status ● | Errors | DDL-DML | Query ID | Query ID Details | iGuard Candidates |
| iGuard Candidates Detail | iGuard Policy Selector | iGuard Policy Categories | iGuard Policy Variables | Enforced iGuard Policies ● | **Enforced iGuard Policies Detail** | Filters | Data Dictionary |

Statistics | Configuration

Enforced Policy Details

Application exe	POLICY_ID	Policy Message	SQL Status ●	SQL Text	Complex SQL	Standard App	SELECT *	SELECT DISTINCT	WHERE ?	Total Execu...	Total Response...
SQLPLUS	384	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	Yes	NO	YES	1	0
SQLPLUS	384	There is no WHERE clause in this SQL statement. Please add a filtering criterion.	Query Cancelled by Teleran	s	NO	NO	Yes	NO	YES	3	0
SQLPLUS	384	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	Yes	NO	YES	2	0
SQLPLUS	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	Yes	NO	YES	2	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran fr	s	NO	NO	No	NO	YES	1	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran fr	s	NO	NO	No	NO	YES	2	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	No	NO	YES	7	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	No	NO	YES	1	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	No	NO	YES	2	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	No	NO	YES	2	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	NO	NO	No	NO	YES	2	0
NQSSERVER	388	There is no WHERE clause in this SQL statement.	Query Cancelled by Teleran	s	YES	NO	No	NO	YES	2	0
		There is no WHERE clause in this SQL	Query Cancelled by	s								

iGuard allows audit and compliance staff to easily customize, test and apply policies. Policies can be applied to prevent access to any database table, view or column, by user or user group, and application. iGuard messages are fully customizable to ensure the users are informed and in compliance.

iGuard Data Protection Policy Enforcement Report
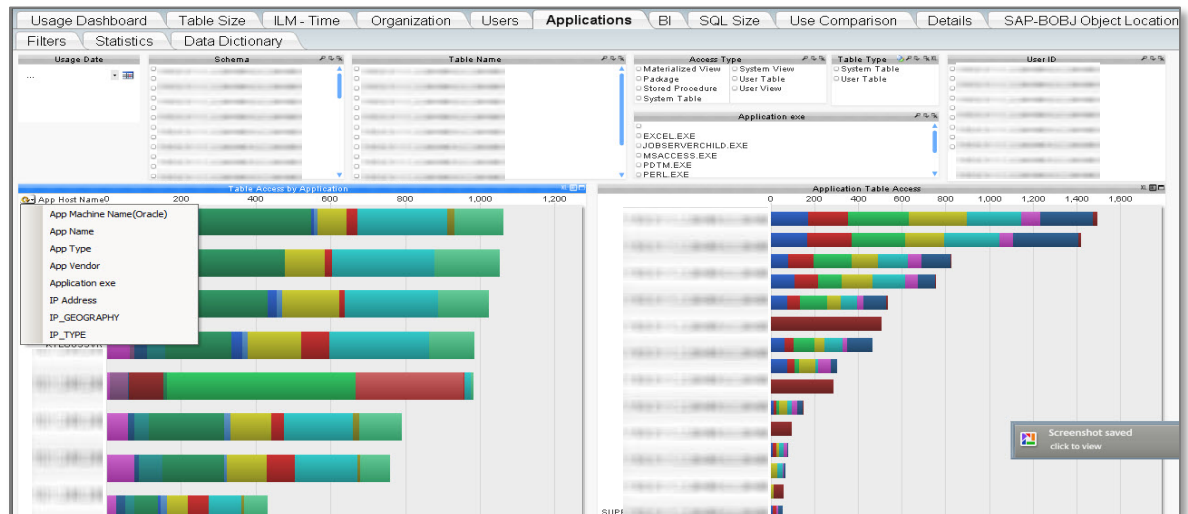

Information Management: Delivering Business Value

The Information Management team was seeking to better track and understand from a business user perspective how the data in the data warehouse and CRM systems were being used, by whom and with what applications. With this knowledge they could better understand why and how the various business departments and functions were using the applications and data. This information enabled them to effectively engage with the business to improve the value, performance and cost efficiency of these critical systems. With iSight and iSight Analytics, the Information Management team was able to identify all the applications in use, identify those that were being used inappropriately and wasting costly IT system resources. Information Management met with the business users to recommend more effective analytical tools, improve query performance, and reduce wasteful querying behavior. This process significantly improved user satisfaction and productivity and improved the overall effectiveness of the applications. It was recognized as a strong win-win for both Information Management and the business users.

Here are some examples of how the Information Management team was able to improve the value and efficiency of the data warehouse, CRM systems, and other analytical applications:

- Uncovered and corrected application errors that resulted in misleading results and increased business operating risks
- Identified little used batch reporting applications that were consuming large system resources Most of the reports were not used and retired, while active reports were converted to a more efficient and widely used tool
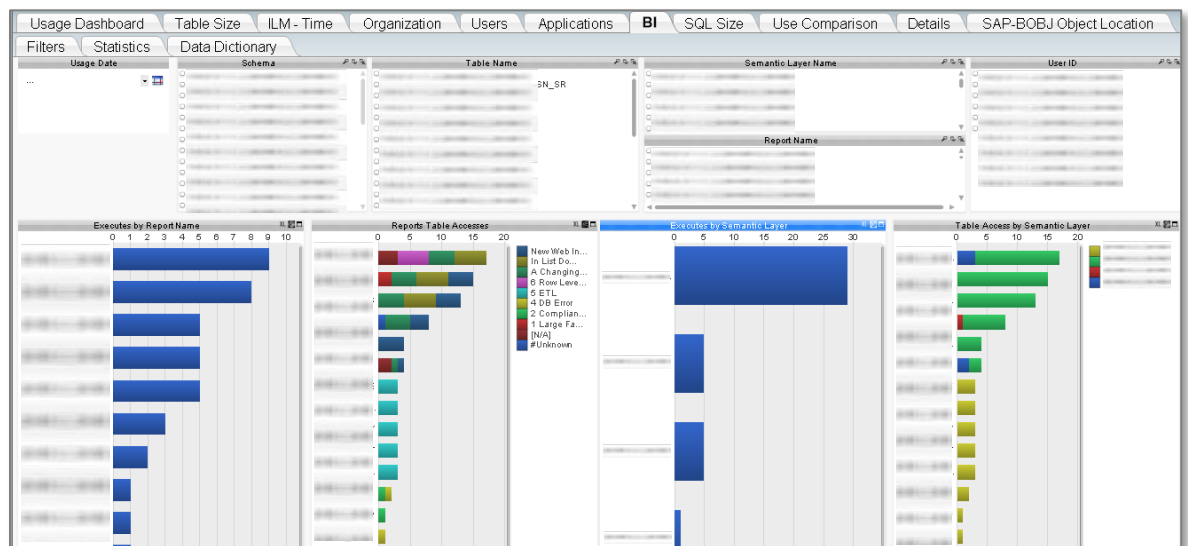
- Uncovered downstream data marts that could be consolidated into the enterprise data warehouse to improve both security and compliance and lower data management and storage costs
- Discovered dormant data that was rarely or never used and could be retired or archived to reduce data storage and handling costs

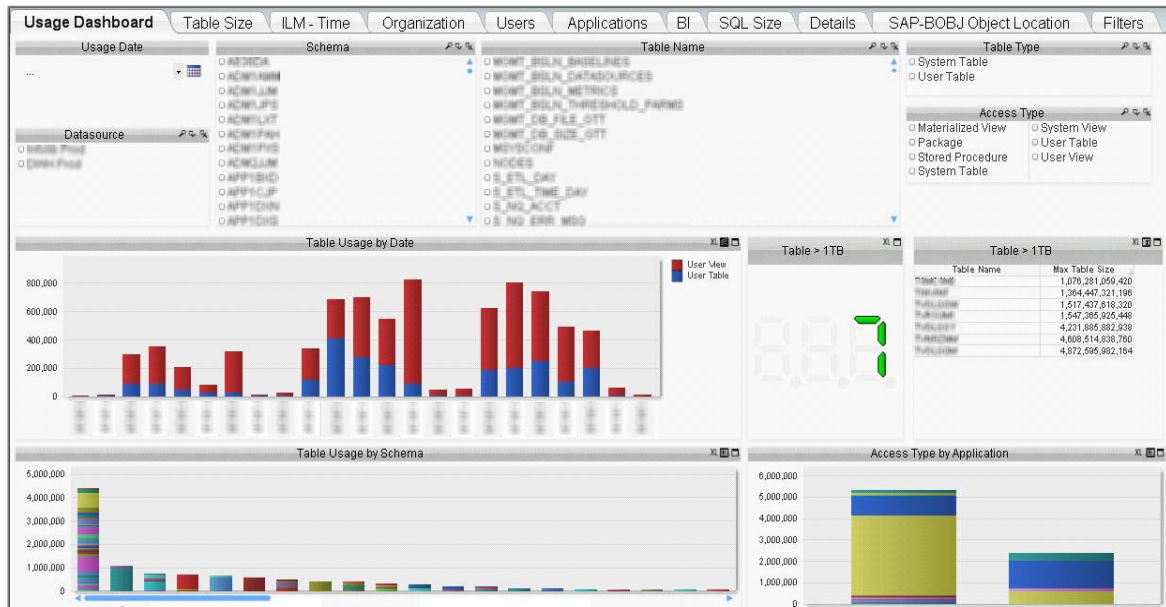**Application and Data Usage Analysis**

Information Management staff was able to gain deeper visibility into the business intelligence applications to identify what BI reports were being run against what data, how frequently and by whom. Dormant reports were identified and retired while long-running reports were optimized to improve performance or batched for greater resource efficiency.

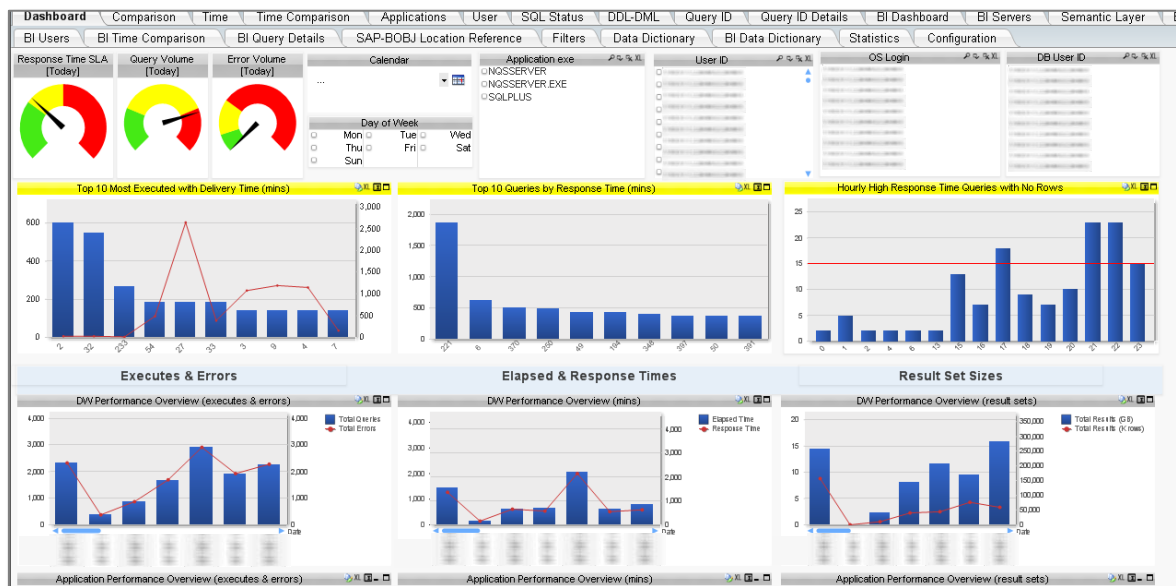**Data Usage by Named Business Intelligence Application Report and User**

Tracking what data was used, when and for what purpose enabled Information Management to archive or dispose of unused data, generating significant resource savings and improving IT staff productivity.

Data Usage Dashboard

Visibility and performance analyses enabled Information Management to diagnose and address application and database performance issues not visible via database administration tools to improve overall performance and service to the business.

Application Visibility and Performance Dashboard

Conclusion

The highly dynamic and complex usage patterns of the enterprise data warehouse and CRM systems used by 1000's of users were challenging to monitor and understand. It also made it challenging to apply the appropriate policies to protect the data without interfering with the analytics and business process. Working together Audit, Risk, Compliance, and Information Management groups were able to address these data monitoring and protection challenges using Teleran's solution. The company quickly implemented both Teleran's granular compliance monitoring and reporting as well as real-time data protection with no disruption to production systems.

The results were significant: Audit costs were materially lowered, audit exceptions were reduced by over 30% and both internal and external company auditors were satisfied with the compliance monitoring and protections put in place for these large and complicated systems. In addition, Information Management was able to better understand the business users' interaction and use of both the business intelligence and analytical applications and their interaction with the back end databases. With this insight they were able to effectively engage with the business to improve the value, performance and cost efficiency of these critical systems.

_____

About the Authors

Robert Schnitzer has over 25 years of experience managing a wide variety of IT functions including enterprise systems management, database administration, quality control, and problem management at leading financial services companies including Bankers Trust Company, Deutsche Bank, TIAA-CREF, Guardian Life Insurance, JP Morgan Chase, and the Federal Reserve Bank of NY. He is currently consulting at a major New York bank. In a recent engagement at a large financial services organization he was responsible for developing an IT governance, risk and compliance program and team. This project included developing an assessment of the existing state of governance maturity and then assisting with the creation IT governance capabilities including implementing a CIO Balanced Scorecard. Rob also identified the need and then implemented the Teleran products at two financial institutions to ensure best practices for data use as well as federal and state compliance regulations.

Jeff Devlin is an expert in building, deploying and protecting database applications in large organizations. He has built successful Information Management organizations which have implemented enterprise governance, risk and compliance solutions, as well as establishing data architectures, data quality programs, and data warehouse and database standards. Jeff has also established GRC maturity models and lean program implementations at leading financial institutions. He has successfully deployed the Teleran product suite in a highly complex regulatory environment, which has led to effective security, audit and compliance systems addressing both federal and state regulations. Jeff has held IT management positions at Bankers Trust Company, AXA Financial and TIAA-CREF. He is currently consulting with a major US bank.

For more information on Teleran's Data Security and Compliance Solution visit www.teleran.com or call +1.973.439.1820, ext. 203.