Forrester Consulting

HELPING BUSINESS THRIVE ON TECHNOLOGY CHANGE

FORRESTER®

Prepared for Guardium, Inc.

January 2008

The Total Economic Impact™ Of Guardium Database Security, Monitoring, And Auditing

For A Global Consumer Products Company

Project Director: Jeffrey North, Principal Consultant

FORRESTER®

Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA

Tel: +1 617/613-6000 • Fax: +1 617/613-5000 • www.forrester.com

TABLE OF CONTENTS

Executive Summary

In 2007, Guardium commissioned Forrester Consulting to examine the financial impact and potential return on investment (ROI) that enterprises can realize by deploying Guardium's product for real-time database security, monitoring, and auditing.

Guardium's appliance-based product uses policy-based controls and anomaly detection to prevent unauthorized changes and access to sensitive data by privileged insiders, potential hackers, and end-users of enterprise applications such as Oracle Financials, PeopleSoft, and SAP. The product also provides a suite of security and compliance applications, with preconfigured reports and built-in workflow automation that allow organizations to simplify and automate many of their corporate compliance and governance processes.

Monitoring and controlling access to databases has become a critical component of information security strategies because it forms the last line of defense for enterprise data, typically one of the most sensitive and valuable corporate assets. This has become even more challenging in recent years as a result of the rapid growth of information that is available online, the complexity and heterogeneity of modern data center infrastructures, and the demands of regulations like Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI-DSS), HIPAA, and the Graham-Leach-Bliley Act (GLBA).

Forrester estimates the value of the database auditing and real-time protection market, which includes new licenses, support, and services, at approximately $450 million, and Forrester expects it to double by 2010 as enterprises look to automate and secure even more of their enterprise databases.[1]

To address the challenge of effectively securing enterprise data, companies need to define and adhere to comprehensive policies regarding access to sensitive data and changes to database schemas. Adherence to these policies needs to be ensured by monitoring and auditing all attempts to update, delete, insert, or view important data and database structures in real-time. Due to the large amount of people, systems, data, and transactions involved, this can create a very significant burden on those responsible for building and supporting these application and database infrastructures. If not implemented properly, it can also have a significant impact on the performance of the databases involved as well as on the corresponding application stacks built upon these databases, because the databases must now perform twice as many write operations in order to log the occurrence of each action.

Forrester conducted in-depth interviews with three Guardium customers in different industries and found that these companies significantly improved real-time protection of their enterprise data while avoiding the substantial labor and capital costs that would otherwise have been required for database auditing, reporting, and management oversight demanded by SOX and other compliance regulations. The Guardium product also helped these customers optimize the performance and availability of their critical business applications by capturing detailed transaction information that helped to identify and address elusive database errors that were being generated by these applications. All of this was accomplished without any compromise in the performance or stability of their business applications.

Purpose

The purpose of this study is to provide readers with a framework for evaluating the potential financial impact of the Guardium product on their organizations. Forrester's aim is to clearly show all calculations and assumptions used in the analysis. Readers should use this study to better

understand, develop, and communicate a business case for investing in the Guardium product compared with developing their own in-house solutions that rely on native, database-resident logging and/or auditing tools.

Methodology

Guardium selected Forrester for this project because of its industry expertise in database security and auditing and for its Total Economic Impact™ (TEI) methodology. TEI not only measures technology costs and cost reductions (areas that are typically accounted for within IT), it also takes into account the ability of technology to improve the efficiency and effectiveness of the business.

For this study, Forrester employed four fundamental elements of TEI in modeling the financial impact of Guardium's database monitoring and security and auditing product.

1. Costs.

2. Benefits to the entire organization.

3. Flexibility.

4. Risk.

Given the increasing sophistication of the IT investment analyses being used by enterprises, Forrester's TEI methodology serves a useful purpose by providing a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Approach

Forrester used a four-step approach for this study:

1. Forrester gathered data from existing Forrester research relevant to the Guardium product specifically and database security and auditing in general.

2. Forrester interviewed senior representatives from Guardium to fully understand the potential value proposition of its products.

3. Forrester conducted a series of in-depth interviews with three companies that are currently using the Guardium product. Forrester focused on one of these customers to feature in this study, and leveraged the data shared by the other two customers to validate the study findings.

4. Forrester constructed a financial model representative of one customer's implementation, and used information and insights from the other two Guardium customers to validate and support the financial results exhibited herein. This model is described in the TEI Framework section below.

Key Findings

> *Since we installed the Guardium solution, there's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers. Perhaps because people know that audit capabilities are automated, they maintain greater awareness of the need to oversee and enforce change ticketing procedures, for example. We now have a clearer focus on security and compliance, promoted in large part by the presence and operation of the Guardium product.*
>
> — Lead Security Analyst

Forrester's study yielded the following key findings:

- The Guardium product provides a cost-effective solution for addressing the database security, monitoring, and auditing aspects of SOX compliance for the three companies interviewed for this study. For example, the system captures all database transactions and automates the creation of reports comparing all detected database changes with approved change requests in their corporate ticketing systems. This process, known as "change control reconciliation," is increasingly required by auditors to tighten internal controls around critical financial systems.

- The product also helps customers rapidly identify and proactively address security policy incidents. For example, the system's real-time alerting capability is now being used to address a request by the business to immediately inform specific people of any changes to certain database tables.

- Native auditing tools were considered inadequate for the purposes of SOX compliance because these tools: 1) do not fully support all requirements for audit data capture and reporting; 2) have a deleterious effect on database performance; and 3) collect too much data that subsequently requires a great deal of manual labor to sort and evaluate.

- Transaction log auditing was also evaluated and determined to be generally less flexible, and it did not capture certain kinds of database activities, including "SELECT" (read) operations.

- The primary quantifiable benefit for the customers interviewed for this study was avoiding significant labor and capital costs that would have otherwise been required to collect, analyze, and distribute database access and change records for SOX audits if the native logging capabilities of database platforms were used.

- A secondary benefit of the Guardium implementation was valuable insight into runaway processes and/or problems with authorized and unauthorized applications accessing databases in "rogue" fashion. This improved the productivity, performance, and security of the company's financial and ERP systems.

- These customers were able to meet their compliance needs without risking the performance and availability of their critical financial and business applications.

- The customer featured in this case study also found that its interactions with auditors were greatly simplified by using a purpose-built product for database activity monitoring, security, and auditing. Once the auditors were shown Guardium's capability to continuously monitor

and audit database accesses in real-time, they were comfortable that it addressed the related needs for SOX compliance.

Table 1 illustrates the original and risk-adjusted cash flow for the customer interviewed for this study, based on data and characteristics obtained during the interview process. Forrester risk-adjusts these values to take into account the potential uncertainty that exists in estimating the costs and benefits of a technology investment. The risk-adjusted value is meant to provide a conservative estimation, incorporating any potential risk factors that may later impact the original cost and benefit estimates.

Table 1: Summary Of Financial Calculations

Summary financial results	Original estimate	Risk-adjusted
ROI	259%	239%
Payback period (months)	5.7	5.9
Total costs (PV)	$256,000	$260,333
Total benefits (PV)	$918,511	$883,570
Total (NPV)	$662,511	$623,238

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

- The study was commissioned by Guardium and is being delivered by the Forrester Consulting group.
- Guardium reviewed and provided feedback to Forrester, but Forrester maintained editorial control over the study and its findings.
- The customers for the interviews were provided by Guardium.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive with the Guardium product. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in the Guardium product.
- This study is not an endorsement by Forrester of the Guardium product.
- The study is not meant to be used as a competitive product analysis.

Guardium Product Overview

According to Guardium, the product provides a scalable enterprise security platform for ensuring the integrity of enterprise information and preventing information leaks from the data center.

By continuously tracking all DBMS traffic at both the network level and on database servers themselves — across all major DBMS platforms, OS platforms, and applications — the Guardium product provides 100 percent visibility into all database activities without impacting the performance of business-critical applications and databases.

Managing The Entire Database Security Life Cycle

Guardium provides a suite of enterprise applications for managing the entire database security, risk management, governance, and compliance life cycle, including:

- Discovery and classification of sensitive data.
- Assessing and hardening of database environments, such as vulnerability assessment, configuration change tracking, and automated baselining.
- Monitoring and enforcing access to sensitive data with policy-based actions, anomaly detection, real-time prevention, and granular access controls.
- Auditing and reporting via centralized aggregation of audit data in a secure repository, preconfigured compliance reporting (for SOX, PCI, and data privacy laws), automated sign-off management and escalations, incident management, data mining tools and database-focused analytics for forensics, and efficient long-term retention of audit data for compliance.

The Guardium Architecture

Guardium's product consists of a modular software suite that is built on a hardened Linux kernel and delivered as a series of self-contained, preconfigured appliances. The appliance itself is a 1U, rack-mountable unit built on a high-performance, industry-standard server platform.

In smaller environments or where only a subset of database traffic is being audited, a single Guardium appliance is usually sufficient. In enterprise data center environments, multiple appliances are typically deployed in a clustered, multi-tier topology. In this case, a central management appliance aggregates and normalizes audit data, applies advanced database-focused analytics, distributes reports, and manages enterprise-wide security policies.

Database traffic is continuously monitored either via passive network SPAN ports and/or lightweight probes called S-TAPs (software taps) that are installed on database servers.[2] S-TAPs capture all local activities by privileged users (such as console access, shared memory, and named pipes) as well as all networked access to databases. This additional flexibility is advantageous when no SPAN ports are available, or where the database team prefers to control the deployment rather than involving network operations. S-TAPs can also eliminate the need for dedicated appliances in remote locations such as outsourcing facilities.

TEI Framework

From the information provided in the interviews, Forrester has constructed a TEI framework for those organizations that are evaluating an investment and implementation of the Guardium product. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that impact the investment decision.

The Customer And The Guardium Implementation

> *"The ability to associate changes with a ticket number makes our job a lot easier," reported one customer staff member. "The other products didn't have that capability to automatically put in an associated ticket number with the activity that was going on within the database, which is something the auditors ask about."*
>
> — Lead Security Analyst

The Guardium customer featured in this study is a Fortune 500 global manufacturer and marketer of consumer food and beverage products with more than 50,000 employees and $15 billion in revenue. The company's brands are household names known around the world.

Prior to the implementation of the Guardium product, the customer did not have a standardized mechanism for enforcing database security policies and did not conduct consistent auditing of database activities across the different database environments. In some areas, only changes to the schema were being captured; capturing changes to the data would have required a very high volume of data collection and would have adversely affected the performance of the databases. In other areas, native tools and some custom scripts were employed. The Guardium product now allows the customer to centrally maintain consistent audit data capture and practices across all databases.

The customer's database security team evaluated the use of the native audit logging capability of its database platforms along with software tools that ran on the database servers to analyze the logs. This option would have required additional hardware and labor. Adding an additional audit process on top of the existing server load would have pushed a number of the databases out of acceptable limits for response times. Labor requirements for such an initiative would also have been considerable because native DBMS audit capabilities are seldom end-user friendly. The team determined that native tools contain little or no intelligence, consume CPU cycles and disk space, and reduce the performance of the database. Labor is required to sort out relevant events from the massive log that would be generated. These costs, which are avoided with the use of the Guardium product, are described in the financial framework section below.

The team also evaluated a number of other potential database security and auditing products. Guardium was selected for its ease of use and implementation and because the product would have minimal impact on the performance of its database servers. In addition, with some auditing products that rely on native logs, a database administrator is able to turn off the auditing and has access to the logs. The Guardium product eliminates this security exposure.

The company requires security and auditing capabilities for its financial databases to effectively and efficiently comply with the auditing requirements demanded by Sarbanes-Oxley. These databases are accessed by five database administrators (DBAs) and 24 applications including SAP, Siebel, Manugistics, and others. All attempts to access financial data must be logged; questionable access requests must be analyzed to ensure that they are consistent with defined policies. All network and local traffic is monitored by the Guardium system.

The customer's database environment is heterogeneous. The IT group at this consumer products company manages three database platforms: Microsoft SQL Server, Oracle, and IBM DB2 on Windows and AIX. An enterprise information security team is responsible for monitoring the databases, operating systems, and applications that would be involved in any changes made to financial records.

In 2005, the company purchased three Guardium appliances to monitor all of the accesses and modifications that involve all of the database servers that are relevant to SOX. The customer also purchased Guardium's AuditGuard application to automatically distribute daily reports to the oversight team.

The implementation required no modifications to the databases in order to monitor and control access. Further, none of the enterprise applications required any modification. The team simply installed the S-TAP on its database servers, defined aliases, and began monitoring all database traffic. The setup provides real-time alerting, using SNMP and SMTP mechanisms, for any and all changes to production data by privileged users with administration or security officer access.

Each change to a database is tied to an approved change management ticket, a feature that was another determinant in the company's decision to invest in the Guardium product.

The system conducts daily archive and backup, purging the data after three months.

Since installing the Guardium system, this Guardium customer has successfully completed four internal and external SOX-related audits. The database administration and security teams have also found that their interactions with the SOX auditors were simplified because Guardium's product was specifically built to address the security and auditing requirements of SOX and other similar regulations. SOX auditors were impressed with the output and organization of the audit reports produced by the Guardium system as well as by the real-time controls that it provides.

The financial model presented below looks at the quantifiable benefits and costs of this implementation compared with developing an in-house solution.

Benefits

> *The auditors were very impressed with the Guardium product; they were impressed by the way we have it set up — the alerts, rules, and reports. There hasn't been a case where they've found something that wasn't covered by an approved change ticket.*
>
> — Lead Security Analyst

From its investment and deployment of the Guardium solution, this customer has gained greater efficiency and effectiveness in its database security, auditing, and reporting capabilities required for SOX compliance. The customer explained that discussions with the auditors have been simplified using a purpose-built product for SOX auditing, avoiding what would likely have been challenging discussions about the completeness of the audit data provided and verification of actions taken to meet compliance.

Another benefit of the Guardium product has been the detailed insight the product provides regarding database usage — which is being employed for troubleshooting problematic applications and improving application performance. Development, operations, and security teams can use the Guardium-generated reports to determine precisely who (or which application) is accessing each database, when they are accessing them, and how they are accessing them. This functionality can provide an efficient alternative to labor-intensive tasks. For example, one of the customers interviewed for this study must manage the disparate database environments that have come under

the team's purview as the result of corporate acquisitions. As one DBA explained, "There are processes that are running on our boxes that people don't know about. There could be a batch job that someone wrote ten years ago that still runs every day or every month. We've uncovered those by using Guardium. We have been able to track a lot of legacy stuff that's just out there running that shouldn't be."

The profiled customer estimated the labor and capital costs that would have been required to develop a manual, in-house solution for database auditing and database-related troubleshooting and performance improvement capabilities in order to quantify the financial benefit. The "alternative option" used for the comparison was based on the native logging capabilities provided by the database platforms (for capturing and storing the audit logs) as well as new software and scripts that would be developed in-house for analyzing and reporting on this information, and then distributing the reports to those doing the audits and others with oversight responsibilities.

It is important to note that an in-house solution would not have provided the real-time security controls provided by the Guardium product due to the batch nature of logging utilities. It also could not provide the same level of automated functionality for change control tagging and reconciliation.

Three areas of costs were identified for building and operating this alternative option:

- Labor costs for developing and updating the secure logging, storage, analysis, reporting, and distribution capability.
- Labor costs associated with the ongoing use and maintenance of the developed capability to support SOX auditing and the troubleshooting, performance optimization, and security of the database applications.
- Capital costs associated with the incremental hardware required to support the additional processing and storage demands of native database logging and analysis.

The costs *avoided* for each of these three areas are shown in Table 2.

Table 2: Benefit Of Implementing Guardium

Benefits	Initial	Year 1	Year 2	Year 3	Total
Resources for developing SOX auditing capability	48,000		24,000		72,000
Labor cost savings: ongoing support of in-house SOX auditing		300,000	315,000	330,750	945,750
Capital purchases of processing and storage		50,000	15,000	15,000	80,000
Total	$48,000	$350,000	$354,000	$345,750	$1,097,750

Source: Forrester Research, Inc.

Resources For Developing In-House Database Monitoring And Auditing Capability

The customer estimates that an eight-week effort by three resources (i.e., developer, security administrator, DBA) would be required to develop, test, and deploy the required functionality for securely logging, storing, analyzing, and reporting on the database audit access information. The fully burdened annual cost of each of these resources is assumed to be $100,000, or $2,000 per

week. Each would have been utilized for 40 days out of a 250-day work year. This expense would be incurred in Year 0 (i.e., the start of the project). A similar effort requiring half of this level of expense would then be required in Year 2 to provide enhancements. This calculates as $48,000 initially (Initial, Year 0) and $24,000 in Year 2.

Ongoing Support For Database Monitoring And Auditing Requirements

When the alternative option would have been developed, the customer estimates that three resources would be required to use and maintain it over time. The first resource would be a dedicated DBA responsible for providing ongoing database support for the storage and analysis of the logging/auditing data while also being responsible for the reporting of all database access by DBAs.

Given the design of the alternative option, it would be important that this be a dedicated resource in order to meet the need for "separation of duties" required by auditors — the person auditing the logging of the data should not have direct access to the databases for which access is being audited. In the case of the Guardium product, the auditors are comfortable with a member of the DBA team having access to the production databases while also managing the Guardium system due to the fact that the system is self-contained and that this DBA does not have any direct access to Guardium's internal database and therefore cannot make changes to the actual audit data that is collected. The DBA can make changes to the reports and alerts, but all changes made are captured in a secure audit log.

The second and third ongoing support resources would be two application support specialists responsible for ongoing auditing and reporting of all non-DBA (applications and non-DBA power users) access to the databases while also providing the database error diagnosis, troubleshooting, and performance improvement support that is enabled by the Guardium system currently.

These three resources are assumed to be compensated at an average fully loaded (includes benefits) rate of $100,000 per year. The costs avoided for ongoing auditing support are therefore assumed to be $300,000 per year, with an annual increase for raises and cost of living adjustments of 5% per year.

Capital Purchases Of Processing And Storage

The database server configuration currently being monitored by the Guardium system includes multiple servers that support the company's financial databases. The customer estimates that an initial investment in processing and storage of at least $50,000 would be needed to support database audit logging for the alternative option while maintaining acceptable response time and availability of critical applications. At least $15,000 would be required in each subsequent year to support growth. The current Guardium appliances are able to support this growth. Additional Guardium appliances may be required by this customer in the future — but only to support other needs such as monitoring of other key databases in the customer's environment.

Real-Time Database Security Benefits

The Guardium system has helped the customer identify and proactively address security policy incidents — another valuable byproduct of its auditing capabilities. The real-time alert capability of the system is also being used to address a request by the business to immediately inform specific people of any changes to certain database tables.

Finally, the Guardium customer described one more important "people and process" benefit: there is a sharper focus on database security within the organization. Security is more top-of-mind among IT and other staff. Perhaps because people know that audit capabilities are automated, they maintain greater awareness of the need to oversee and enforce ticket procedures, for example. The

customer described a new, clearer focus on security and compliance within the IT organization, promoted in part by the presence and operation of the Guardium system.

Costs

A comprehensive review of IT costs is undertaken with the TEI methodology to determine the total investment required to achieve the benefits outlined in the previous section. This includes all incremental investments in hardware and software, and the internal and external resources used. The costs are summarized in Table 3.

Table 3: Costs Of Implementing Guardium System

Costs	Initial	Year 1	Year 2	Year 3	Total
Guardium appliances	150,000				150,000
Annual maintenance fee			27,000	27,000	54,000
Guardium professional services	14,400				14,400
Implementation labor costs	39,000				39,000
Hardware costs	10,000				10,000
Total	$213,400		$27,000	$27,000	$267,400

Source: Forrester Research, Inc.

The purchase price of the Guardium product for this implementation is $150,000 for three appliances. This price includes support for the first year. Note that pricing of Guardium products varies based on the number of databases being monitored, the types of databases involved, the throughput of those databases, and the amount of audit information that needs to be captured and analyzed.

The annual maintenance for these appliances is $27,000 beginning in Year 2. The customer purchased $14,400 worth of Guardium Consulting Services (9 days x $1,600 per day). The customer also had to purchase a network SAN storage and archiving device costing $10,000 and used $39,000 worth of internal labor on the installation, testing, and development of reports using data from the Guardium system (five full-time equivalents x $50 per hour x 6 hours per week x 26 weeks). The actual physical implementation took approximately three days, although testing was conducted over a six-month period. Guardium delivered and racked the equipment, worked with the client to install local software “taps” (to monitor local access), and then configured the system to start collecting data. The customer then had to train people on reports and administration, create the reports, and design all of the review processes.

Risk

Risk is the third component within the TEI model; it is used as a filter to capture the uncertainty surrounding different cost and benefit estimates. If a risk-adjusted ROI demonstrates a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as "realistic" expectations, since they represent the expected values considering risk. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. In this case, the scenario works in an opposite manner; the risks of *avoided* project costs and schedule overruns appear in the benefit category.

In this case, Forrester does not risk-adjust the cost assumptions (with the exception of implementation labor costs). This is done: a) for clarity; b) because the nature, scope, and magnitude of these costs are relatively simple to assess prior to an implementation; and c) because the precise amounts for most hardware, software, and many services costs can be set contractually prior to project engagement.

The TEI model uses a triangular distribution method to calculate risk-adjusted values. To construct the distribution, it is necessary to first estimate the low, most likely, and high values that could occur. The risk-adjusted value is the mean of the distribution of those points.

For example, in the case of the benefit of avoiding the cost of deploying resources to develop database auditing capability that would be required in the absence of the Guardium product, the original assumption of eight weeks worth of effort from three staff used in this analysis can be considered the "most likely" or expected value. Yet this amount could vary significantly if unexpected complexities are uncovered in mid-project. This variability represents a risk that is captured as part of this study. Forrester uses an assumption of twelve weeks on the high end, eight weeks as the most likely, and seven weeks on the low end. Each of these is multiplied by the fully loaded annual compensation amount of $2,000 per three staff per week. Since this is an estimate of a cost avoidance and costs are more likely to be revised upward than downward, this has the effect of increasing the benefit. Forrester then creates a triangular distribution to reflect the range of expected benefits, with 9.0 as the mean.

Table 4: Risk Adjustment — Labor Costs Avoided For Developing Database Monitoring And Auditing Capability

Ref.	Metric	Calc	Initial/ Year 0	Year 1	Year 2	Year 3	Total
A1	Number of workers (saved)		3				
	Weeks — Low		7				
A2	Weeks		8				
	Weeks — High		12				
A3	Weekly rate per worker		$2,000				
	Equation — Low		$42,000				
At	Resources for developing SOX auditing capability	A1*A2*A3	$48,000				

	Equation — High		$72,000				
Ato	Total — Original		$48,000	$0	$24,000	$0	$72,000
Atr	**Total — Risk-adjusted**		$54,000	$0	$27,000	$0	$81,000
Atl	Total — Low		$42,000	$0	$21,000	$0	$63,000
Ath	Total — High		$72,000	$0	$36,000	$0	$108,000

Source: Forrester Research, Inc.

In the example above, the risk adjustment method actually raises the amount of the benefit in this category, based on the inherent uncertainty in estimating that amount of labor cost (and here the labor cost *avoided*).

Another example can be seen in the risk treatment of the labor costs for the Guardium implementation. The customers interviewed for the study explained that there is some uncertainty around the amount of internal labor and time to complete the project. In order to capture this uncertainty, Forrester begins with an original estimate of 6 hours per week for five staff as the original assumption. The high end assumes the project ultimately requires 10 hours per week per staff. The lower variable is assumed to be a 4 hour per week requirement. The mean of these assumptions is 6.67 hours per week, thereby increasing the risk-adjusted amount modestly upward.

Table 5: Risk Adjustment — Implementation Labor Cost

Ref.	Metric	Calc	Initial/ Year 0	Year 1	Year 2	Year 3	Total
A1	Number of people		5				
A2	Hourly rate per person		$50				
	Hours — Low		4.0				
A3	Hours		6.0				
	Hours — High		10.0				
A4	Weeks		26				
	Equation — Low		$26,000				
At	Implementation labor costs	A1*A2*A3*A4	$39,000				
	Equation — High		$65,000				
Ato	Total — Original		$39,000	$0	$0	$0	$39,000
Atr	**Total — Risk-adjusted**		$43,333	$0	$0	$0	$43,333

Atl	Total — Low		$26,000	$0	$0	$0	$26,000
Ath	Total — High		$65,000	$0	$0	$0	$65,000

Source: Forrester Research, Inc.

A third example is shown for the benefit calculation of the cost avoided for ongoing support in the absence of the Guardium product For this benefit category, Forrester sets the low and original estimates at three FTEs. The high estimate, however, assumes that only 2.5 FTEs would be required, thereby reducing the risk-adjusted benefit amount, as shown in Table 6.

Table 6: Risk Adjustment — Labor Cost Avoided: Ongoing Support For Database Monitoring And Auditing

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total
	Variable — Low		3.0			
A1	Number of DBA/application support staff		3.0			
	Variable — High		2.5			
A2	Annual salary and benefits per worker		$100,000			
	Equation — Low		$300,000			
At	Labor cost savings: ongoing support of in-house SOX auditing	A1*A2	$300,000			
	Equation — High		$250,000			
Ato	Total — Original		$300,000	$315,000	$330,750	$945,750
Atr	Total — Risk-adjusted		$283,333	$297,500	$312,375	$893,208
Atl	Total — Low		$300,000	$315,000	$330,750	$945,750
Ath	Total — High		$250,000	$262,500	$275,625	$788,125

Source: Forrester Research, Inc.

For those estimating expected costs and benefits, the following areas of potential uncertainty should be taken into consideration:

- The “people and process” aspects of the overall solution. The ability of the Guardium product to identify inappropriate database access is dependent on agreement among the various organizations (business owners, internal auditors, application developers, and database and network administrators, etc.) regarding clear policies about appropriate business and IT processes. The organization must also assign personnel to be trained, and it must implement the policies and automated reporting processes as well as manage the

system on an ongoing basis. Lack of attention to these critical aspects will typically introduce additional risk into the project and may impact the benefits gained.

Flexibility

Flexibility, as defined by Forrester's TEI methodology, represents an investment in additional capacity or agility today that can be turned into future business benefits at some additional cost in the future. This provides an organization with the "right" or the ability to engage in future initiatives — but not the obligation to do so. For this study, the potential options for flexibility are identified and described qualitatively.

Flexibility options with the Guardium product for this customer include the following:

- Using the platform to enable compliance with any future regulations, such as privacy laws, that also require auditing of databases. Two of the three customers interviewed for this study described plans to employ the Guardium product for this purpose in the near future.

- Using the platform to monitor other databases for SOX compliance, as auditors gradually broaden their definition of which applications and databases are considered key financial systems.

- Using the monitoring capability of Guardium to help with the troubleshooting, diagnoses, and performance management of other databases that are outside of the purview of SOX. Given the value that has been demonstrated by the use of Guardium for the financial-related databases, the DBA and application support teams are considering using the technology to monitor and analyze accesses to databases in other application areas.

TEI Framework: Summary

Considering the financial framework constructed above, the results of the costs, benefits, and risk, sections using the representative numbers can be used to determine a return on investment, net present value, and payback period.

Tables 7 and 8 show the risk-adjusted values after applying the risk-adjustment method indicated in the Risk section above.

Table 7: Risk-Adjusted Costs

Costs	Initial	Year 1	Year 2	Year 3	Total	Present value
Guardium appliances	150,000				150,000	150,000
Software maintenance			27,000	27,000	54,000	42,600
Guardium professional services	14,400				14,400	14,400
Implementation labor costs	43,333				43,333	43,333
Hardware costs	10,000				10,000	10,000
Total	$217,733		$27,000	$27,000	$271,733	$260,333

Source: Forrester Research, Inc

Table 8: Risk-Adjusted Benefits

Benefits	Initial	Year 1	Year 2	Year 3	Total	Present value
Resources for developing SOX auditing capability	54,000		27,000		81,000	76,314
Labor cost savings — ongoing support of in-house SOX auditing		283,333	297,500	312,375	893,208	738,135
Capital purchases of processing and storage		50,000	15,000	15,000	80,000	69,121
Total	$54,000	$333,333	$339,500	$327,375	$1,054,208	$883,570

Source: Forrester Research, Inc.

Note that Forrester makes no assumptions as to the potential return that other organizations will receive within their own environment. Forrester strongly advises that readers use their own estimates within the framework provided in this study to determine the expected financial impact of implementing the Guardium product.

Study Conclusions

Forrester's in-depth interviews with Guardium customers yielded several important observations:

- The customers interviewed for this case study were very pleased with the overall ROI from Guardium's product.
- The consumer products company featured in the case study was able to quickly and cost-effectively address an important aspect of its compliance with SOX regulations — including not just reporting but also enhanced real-time controls around database security — without risking any major impact to the performance or availability of its business-critical financial applications.
- Customers also gained the unintended but valuable additional benefit of enhanced awareness of database security issues within the organization.
- A secondary benefit was the improved efficiency and effectiveness of those responsible for supporting database application development. This was achieved via Guardium's ability to provide continuous, granular visibility into all transactions occurring in customers' application and database environment, which they did not have previously.

The financial analysis provided in this study illustrates the potential way an organization can evaluate the value proposition of the Guardium product. Based on information collected during in-depth customer interviews, Forrester calculated a three-year risk-adjusted ROI of 239% with a payback period of less than six months. All final estimates are risk-adjusted to incorporate potential uncertainty in the calculation of costs and benefits.

The net present value (NPV) provides insight into the overall magnitude of the expected return. The payback period indicates the expected amount of time before the net returns from the use of Guardium first exceed the investment in the product. The ROI shows what the expected return would be, in percentage terms, relative to the upfront investment.

Table 9: Summary Of Financial Calculations

Summary financial results	Original estimate	Risk-adjusted
ROI	259%	239%
Payback period (months)	5.7	5.9
Total costs (PV)	($256,000)	($260,333)
Total benefits (PV)	$918,511	$883,570
Total (NPV)	$662,511	$623,238

Source: Forrester Research, Inc.

Forrester believes that for many organizations, using a financial framework based on the model presented in this study, a compelling business case exists for investing in the Guardium product.

The NPV provides insight into the overall magnitude of the expected return. The payback period indicates the expected amount of time before the net returns from the use of the Guardium product

first exceed the investment in the product. The ROI shows what the expected return would be, in percentage terms, relative to the upfront investment.

Appendix A: Total Economic Impact™ Overview

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The TEI methodology consists of four components to evaluate investment value: benefits, cost, risk, and flexibility.

Benefits

Benefits represent the value delivered to the user-organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room for analysis of the impact of the technology on the entire organization. The TEI methodology and resulting financial model places equal weight on the measure of benefits and costs, allowing for a full examination of the impact of the technology on the entire organization. Calculation of benefits estimates involves a clear dialogue with the user organization to understand the specific created value. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefits estimates after the project has been completed. This ensures that benefits estimates tie back directly to the bottom line.

Costs

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs. These may be in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment due to ongoing costs associated with the implementation. All costs must be tied to the created benefits.

Risk

Risk is the fourth component of the TEI methodology. Risk is a measurement of the uncertainty of benefits and costs estimates contained within the investment. Uncertainty is measured in two ways: the likelihood that the costs and benefits estimates will meet the original projections and the likelihood that the estimates will be measured and tracked over time.

TEI applies a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the underlying range around each cost and benefits estimate. The expected value — the mean of the distribution — is used as the risk-adjusted costs or benefits number. The risk-adjusted costs and benefits are then summed to yield a complete risk-adjusted summary and ROI.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary justification of a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if it is activated. The collaboration can only be used with additional investment in training at some future point in time.

However, having the ability to capture that benefit has a present value that can be estimated. The flexibility component of TEI captures that value.

Appendix B: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Although the Federal Reserve Bank sets a discount rate, companies often set a discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their organization to determine the most appropriate discount rate to use in their own environment.

Present value/net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). Present value often refers to individual cost and benefit cash flows, and NPV is the sum of the present values. A positive NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total net present value of cash flows.

Payback period: The breakeven point for an investment, or the point in time at which net benefits (benefits minus costs) equal initial investment or cost. Other things being equal, the better investment is usually the one with the shorter payback period. The example below illustrates the concept.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A Note On Cash Flow Tables

The following is a note on the cash flow tables used in this study (see the Example Table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in Years 1 through 3 are discounted using the discount rate (10% in this case) at the end of the year. Present value (PV) calculations are calculated for each total cost and benefit estimate. Net present value (NPV) calculations are not calculated until the summary tables and are the sum of the initial investment and the discounted cash flows in each year.

Example Table

Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.

Appendix C: Supplemental Material

Related Forrester Research

"The Future Of DBMS Technology," September 29, 2005, by Noel Yuhanna.
http://www.forrester.com/Research/Document/0,7211,37181,00.html

"Trends 2006: DBMS Security," November 29, 2005, by Noel Yuhanna.
http://www.forrester.com/Research/Document/0,7211,38298,00.html

"Sarbanes-Oxley Compliance Software 2006: Momentum Will Shift To Controls Optimization," March 9, 2006, by Paul D. Hamerman.
http://www.forrester.com/Research/Document/0,7211,39049,00.html

"Sarbanes-Oxley Compliance 2006: Taking Internal Controls To The Next Level," March 9, 2006, by Paul D. Hamerman.
http://www.forrester.com/Research/Document/0,7211,39052,00.html

"Assessing SOX's Impact on IT," November 29, 2006, by Michael Rasmussen, Paul D. Hamerman.
http://www.forrester.com/Research/Document/0,7211,40775,00.html

"Enterprise Databases Need Greater Focus To Meet Regulatory Compliance Requirements," January 24, 2007, by Noel Yuhanna.
http://www.forrester.com/Research/Document/0,7211,40551,00.html

"Guardium Is A Leader In Enterprise Database Auditing And Real-Time Protection," October 26, 2007, by Noel Yuhanna.
http://www.forrester.com/Research/Document/0,7211,43643,00.html

Appendix D: About the Project Director

Jeffrey North, Principal Consultant

Jeffrey North is a principal consultant with Forrester's Total Economic Impact (TEI) consulting practice. The TEI methodology focuses on measuring and communicating the value of IT and business decisions as well as providing a business case based on the costs, benefits, flexibility, and risk of investments.

Jeff came to Forrester with consulting and operating experience, notably working with fast-growth companies. He was a founding member of the digital strategy practice at Cambridge Technology Partners, where he specialized in business value justification of technology investments and customer advocacy. As a director in the international and catalog business units at Staples, Jeff built and managed metrics and reporting programs in North America and Europe as the company experienced significant growth. He has also consulted in a business-IT capacity to retailers and life sciences companies.

Jeff holds a B.A. from St. Lawrence University and an M.B.A. with concentrations in international management and finance from the Thunderbird School of Global Management.

Appendix E: Endnotes

[1] For more information, see the October 26, 2007, "The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007" report.

[2] S-TAPs have minimal impact on performance because they passively monitor database traffic in OS memory at the Inter-Process Communication (IPC) level, rather than by collecting information from native DBMS transaction or audit logs. Also, S-TAPs don't perform any local processing but merely forward a copy of database traffic to Guardium appliances for analysis, storage, and reporting.