

Prepared for Oracle Corporation
November 2008

The Total Economic Impact Of Oracle Identity Manager

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	3
Purpose	4
Methodology.....	4
Approach.....	4
Key Findings	5
Disclosures.....	6
Analysis.....	7
Interview Highlights.....	7
TEI Framework	9
Costs	11
Benefits	14
Risk.....	20
Flexibility.....	22
TEI Framework: Summary.....	24
Study Conclusions.....	25
Appendix A: Composite Organization Description	27
Appendix B: Total Economic Impact™ Overview	30
Appendix C: Glossary.....	31
Appendix D: About The Project Director.....	32
Appendix E: Related Forrester Research.....	33

© 2008, Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Forrester clients may make one attributed copy or slide of each figure contained herein. Additional reproduction is strictly prohibited. For additional reproduction rights and usage information, go to www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Executive Summary

Identity and access management is the entire aspect of maintaining a person's complete set of information, spanning multiple identities and establishing the relationship among these various identities with the goal of improving data consistency, data accuracy, and data systems security in an efficient manner. Identity and access management helps extend business services, improve efficiency and effectiveness, and allow for better governance and accountability. Identity management is critical to ensure compliance with industry regulations, including the Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Basel II. Another benefit is significant reductions in audit compliance costs; an organization's security and compliance efforts are dependent on understanding who has access to what resources and efficiently and effectively managing those relationships. In turn, this contributes to improved business results.¹

In May 2008, Oracle Corporation commissioned Forrester Consulting to examine the total economic impact and potential return on investment (ROI) enterprises may realize by deploying an enterprise identity provisioning platform, more specifically Oracle Identity Manager (OIM). An identity provisioning system administers and maintains users' access rights and privileges throughout the provisioning lifecycle within enterprise IT and other (physical) resources. It helps to answer the critical compliance questions around who has access to which applications and data, for how long, granted by whom, for what reasons, etc., while ensuring immediate provisioning and revocation of user access to and from enterprise resources. This study illustrates the financial impact of implementing OIM in a \$15 billion engineering and manufacturing enterprise with 35,000 employees, 5,000 contractors, and 10,000 partners and vendors.

In conducting in-depth interviews with four existing OIM customers, Forrester found that these companies achieved benefits in the areas of labor cost savings resulting from: 1) fewer help desk calls; 2) reduced account creation time; and 3) fewer manual new account requests via improved account creation processes and automation. Using OIM to create a single, universal source of past, current, and planned user access privilege information leads to lower administration labor costs, and end user productivity improvements result when new hires are provisioned faster and users can reset passwords without help desk assistance. A primary driver for investing in OIM for all companies that Forrester interviewed for this study was business risk reduction — from ghost and orphaned accounts, excessive or erroneous access to sensitive applications, and any other weaknesses that may lead to security leaks. Other benefits include better regulatory and policy compliance, reductions in the numbers of audit findings that require remediation, and lower reporting and attestation costs.

According to Oracle, Oracle Identity Manager is an enterprise identity management system that manages users' access right and privileges, throughout the provisioning life-cycle, within enterprise IT resources. It helps to answer the critical compliance questions of who has access to which applications and data.

Oracle Identity Manager's architecture can handle complex IT and business requirements without requiring changes to existing infrastructure, policies, or procedures. This architecture abstracts core provisioning functions into discrete layers. Changes to workflow, policy, data flow, or integration technology are isolated within the respective functional layers, thus minimizing application-wide impact. All configurations are done via OIM's user interface. The product does not rely on any scripting language for setup, configuration, or process modeling. More information is available at: <http://www.oracle.com/products/middleware/identity-management/identity-manager.html>.

¹ Topic Overview: Identify and Access Management, April 14, 2008

Purpose

The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of OIM 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 and communicate a business case for investing in Oracle Identity Manager. Although this study was conducted with OIM and OIM customers, it is intended to demonstrate the benefit for implementing identity provisioning products in general. The TEI model and resulting ROI should extrapolate well to similar identity provisioning products with comparable feature sets and product maturity as OIM.

Methodology

Oracle selected Forrester for this project for Forrester's expertise in access management and user account provisioning applications, in addition to Forrester's Total Economic Impact™ (TEI) methodology. TEI not only measures costs and cost reduction (areas that are typically accounted for within IT) but also weighs the enabling value of a technology in increasing the effectiveness of overall business processes.

For this study, Forrester employed four fundamental elements of TEI in modeling the financial dimensions of an investment in OIM:

1. Costs.
2. Benefits to the entire organization.
3. Risk.
4. Flexibility

Given the increasing sophistication that enterprises have regarding cost analyses related to IT investments, Forrester's TEI methodology serves a useful purpose by providing a complete picture of the total economic impact of purchase decisions. Please see Appendix B for additional information on the TEI methodology.

Approach

Forrester used a five-step approach for this study:

1. Forrester gathered data from existing Forrester research relative to OIM and the identity and the access management/user account provisioning market in general.
2. Forrester interviewed Oracle product marketing personnel to fully understand the potential value proposition of OIM solutions.
3. Forrester conducted a series of in-depth interviews with four organizations currently using Oracle Identity Manager.
4. Forrester constructed a financial model representative of the interviews. This model can be found in the TEI Framework section below.
5. Forrester created a composite organization based on the interviews and populated the framework using data from the interviews as applied to the composite organization.

Key Findings

Forrester’s study yielded a number of key findings:

- **ROI.** Based on the interviews with four customers, Forrester constructed a TEI framework for a composite organization (see description below and Appendix A), and an associated ROI analysis illustrating the financial impact areas. As seen in Table 1, the ROI for the composite company is 212% with a breakeven point (payback period) of six months after deployment.
 - **NOTE:** If the estimates of productivity improvements are removed from the financial framework described in the study — to present the most conservative scenario — the ROI for the composite company is 16% with a payback period of 24 months.
- **Benefits.** Principal benefits from an investment in OIM include productivity improvements from faster provisioning for new hires and transfers, labor cost reductions on the help desk and for administration of accounts, attestation, and auditing. Additional benefits are seen in the cost of audit remediations. Finally, Forrester believes that an OIM implementation will reduce the risk of a potentially costly security breach by managing the off-boarding and account termination processes for employees, contractors, and external partners and minimizing instances of excessive and erroneous access grants via manual administration.
- **Costs.** The significant categories of costs include license fees and maintenance, hardware, professional services, internal labor for implementation, and ongoing management.

Table 1 illustrates the risk-adjusted cash flow for the composite organization, based on data and characteristics obtained during the interviews. 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. For a more in-depth explanation of risk and risk adjustments used in this study, please see the Risk section.

Table 1: Three-Year ROI, Risk-Adjusted

Summary financial results	Original estimate	Risk-adjusted
ROI	250%	212%
Payback period (months)	5.4	6.1
Total costs (PV)	(\$4,103,186)	(\$4,373,379)
Total benefits (PV)	\$14,346,649	\$13,641,627
Total (NPV)	\$10,243,463	\$9,268,247

Source: Forrester Research, Inc.

Disclosures

The reader should be aware of the following:

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

Analysis

Forrester took a multistep approach to evaluate the impact that implementing OIM can have on an organization:

- Interviews with Oracle product and marketing personnel.
- In-depth interviews of four organizations currently using OIM.
- Construction of a common financial framework for the implementation of OIM.
- Construction of a composite organization based on characteristics of the interviewed organizations.

Interview Highlights

A total of four interviews were conducted for this study, involving representatives from the following companies (Oracle customers which are based in the United States and Europe):

1. Semiconductor manufacturer with 900 users, using OIM since 2006. Oracle Identity Manager eliminated manual processes associated with hiring new employees and contractors, replacing tickets sent to three separated help desks and the HR system, and the upkeep of spreadsheets and manual databases.
2. European bank with 70,000 users, using OIM since 2004. OIM automated a host of manual approval and account creation processes, replaced at least one native tool used to create accounts, and provided a new automated link to the HR system.
3. US-based investment firm with 40,000 users, using OIM since 2003. OIM replaced manual processes and highly disjointed access and identity management practices that varied by department and application.
4. Computer system and software company, with over 8,000 users, using OIM since 2006. OIM replaced a homegrown provisioning system and several point solutions for managing passwords.

The composite organization (see full description below) created from the results of the customer interviews is a US-based electronics design and manufacturing company with 35,000 employees, 5,000 contractors, and 10,000 external vendors/partners. "Intercontinental Manufacturing Group" (IMG) earns \$15 billion in annual revenues from the sale of semiconductors and consumer electronics technology products from operations in Canada, Europe, Australia, and the US. IMG has extensive manufacturing and supply chain partners in multiple countries in Asia.

The interviews uncovered a number of facts and insights that apply to the composite company and also to organizations considering an investment in Oracle Identity Manager, including:

- **Risk reduction.** Risk reduction was a key driver in the OIM investment decision. As one interviewee explained, "If you have horrible controls around your user provisioning, then you absolutely run the risk of people being able to steal equipment and critical data after termination." And as another IT decision maker recounted, "OIM protects us in that we don't

get a contingent [contractor or temporary worker] that left months and months ago who still has an active account and who might be able to gain access and do bad things.”

- **Lack of consistent password policies.** Companies lack any consistent password policies across key applications. “You know, we also had multiple password policies across all these different tools,” according to another interviewee, “and trying to keep those synchronized and people trying to remember passwords for multiple systems without writing them down right — all those scary things drove us to invest in identity management.”
- **Provisioning new employees or contractors in a timely manner.** Provisioning is another driver common to all companies included in the study. Companies lack automated processes and workflow management to support on-boarding and off-boarding their workers, and they are burdened by *multiple* processes for on-boarding and off-boarding employees, temps, and contractors.
 - “On Friday afternoon, a person accepts an offer and they’re coming in Monday. So we would scatter to provision all their accounts. Even so, they’d hit the ground Monday, and they wouldn’t have access to be ready to work. Now, instead, as soon as the hire is processed in HR, within 30 minutes OIM provisioning runs, and it creates all those accounts for them. And it is based on where they’re located, what department they’re in, whether they’re contingent or employee. So it really helps automate and make our processes much, much more efficient.”
- **Too many user names and passwords.** Multiple systems require too many user names and passwords; excessive help desk tickets are created for forgotten passwords or locked accounts. Companies explained that after implementing OIM, help desk tickets decreased by as much as 85%.
- **Lack of single source of identity information.** Efficiency and security are both compromised by the common lack of a centralized data repository for a single source of identity information. As a director of technology services interviewed for this study explained to Forrester, “If you went to Exchange and pulled up people’s information and their phone number and other data, you’d see different data than what was on our portal, which would be different again from what you’d find in HR. And if it was a contractor, where do you go for that data? There could be multiple places for that information depending on what agency, depending on who booked it, and so forth. That lack of a single source of truth was huge for us. And that led to inefficiencies in the administrative processes in general.”
- **Regulatory compliance.** Regulatory compliance, especially Sarbanes-Oxley, is another key driver. Consistent, orderly, and timely de-provisioning of key accounts for SOX auditing was cited by all companies interviewed for this study. “No matter how hard we would try, we’d always find one little slip here or there; maybe we didn’t kill somebody’s AD accounts in time or we killed their Oracle account but not their AD account or vice-a-versa. So that was probably the biggest push for us was to help fix some of those SOX problems,” said one interviewee.
- **Lower attrition rates for IT administration.** Eliminating redundant, repetitive identity support tasks can lead to lower attrition rates. “If you look at a standard IT person,” explained an interviewee, “they like to work on projects. Most of them do not like redundant, repetitive work. They want to learn new technology. That’s why they’re in IT. And if you bombard a person with nothing but repetitive tasks, you’ll lose them.”

Other reasons cited by interviewed customers for investing in the Oracle Identity Manager include the ability to leverage existing investments, a flexible architecture, integration with other Oracle applications, a single vendor for support and maintenance, and a road map that includes customer opinions.

TEI Framework

Composite Organization

In this TEI study, Forrester has created a composite organization, “Intercontinental Manufacturing Group” (IMG), to illustrate the quantifiable costs and benefits, risk and flexibility of implementing Oracle Identity Manager. By aggregating the findings from the four customer interviews and portraying a composite organization that is achieving value from OIM software, this study illustrates the financial impact of an investment in Oracle Identity Manager.

IMG provides semiconductors and consumer electronics technology products with operations in Canada, Europe, Australia, and the US, with an extensive supply chain partner network across Asia. Forrester created this composite company to reflect an organization described as follows:

Organization Size And Dimensions

- Annual revenues of \$15 billion.
- Thirty-five thousand employees, 5,000 contractors, and 10,000 external vendors/partners. Turnover is 10% per year, and the user base is increasing 10% annually.
- Globally distributed IT infrastructure across four locations. Approximately 2,000 target resources and 10 major user repositories. These target resources include multiple instances of SAP for ERP, PeopleSoft for HR, Oracle e-Business Suite for financials and CRM, legacy ordering system deployed on RACF mainframe, an assortment of infrastructure technologies from a multitude of vendors such as Novell eDirectory, a few types of Unix servers, Microsoft Active Directory, Microsoft Exchange, BMC Remedy ARS, RSA SecurID, Oracle Weblogic Application Server, IBM Websphere Application Server, Oracle databases, SQL Server databases, and others. Over half of the 2000 resources are custom homegrown applications, mostly built on Java but also including C and .NET applications. Twenty-four of these applications are Sarbanes Oxley (SOX) sensitive.

Identity Management Environment Prior To Investment

- No enterprise-wide identity management products were employed prior to implementing OIM, with the exception of LDAP directories and Active Directory.
- Manual processes were used for provisioning, using application native tools and admin consoles. The help desk system was leveraged to accept provisioning requests and route tickets for manual provisioning.
- There were no HR event feeds from PeopleSoft or other identity repositories. Multiple legacy HR systems are in place from past acquisitions. HR events are exported to the help desk using a daily flat file dump. Only data on employees was stored in the HR system; contractor data were housed in a custom database.

- There were more than 10 different ways to request access to resources. Users had to figure out how to ask for application access or business functionality (entitlements) in applications.
- Quarterly sweeps of individual systems (although not all) were engaged to confirm current access information. No automated process existed to reconcile this information with HR information.

No logs (past or current) were created of who has/had access to what and why. User access auditing and attestation processes are completely manual, distributed, and cumbersome.

Implementation

- Phase 1 of the implementation required six months starting in 2005 (Year 0 in the financial framework).
- Ten thousand user groups/roles prior to OIM deployment were reduced to 3,000 roles after a role analysis before implementation.
- Simple role-based provisioning policy (similar to minimal standard, or 'birthright' provisioning) focuses on simple roles that apply to a large population of users. Roles like "employee," "contractor," "engineer," etc. The organization currently relies on these simple roles and policies to provision core systems used by all, such as Active Directory, MS Exchange, etc.
- OIM became the aggregation point for user information across all HR and contractor databases. The HR systems send exports to OIM every 4 hours. The contractor database was eliminated and replaced by OIM.
- Eight core systems were provisioned in Phase 1: Active Directory, Exchange, Windows File Share, a variety of Unix systems, Single Sign-On systems (from vendors like Oracle, CA, RSA), and three core business applications (ERP, etc.).
- Phase 2 and Phase 3 involved integrating additional systems, rolling out self-service capabilities, adding more roles and policies, performing periodic attestation of user access, and integrating the identity management framework with the SOA framework.
- Users no longer have to figure out where to go ask for access and permissions; request management has been centralized to OIM's self-service feature.

Initial Reasons For Investment

Based on interviews with actual OIM customers, Forrester assumed that IMG identified the following business drivers for investing in OIM:

- Reduce risk and meet SOX compliance more easily.
- Reduce costs of manual provisioning and help desk resources.
- Terminate access when an employee leaves to eliminate security and information leaks associated with orphan and dormant accounts.

- Increase user productivity on Day 1 by ensuring new employees have immediate access to resources that they need to be productive and do their jobs.
- Reduce help desk call volume and improve user experience with self service (such as password reset) and single request portal.
- Centralize security administration provisioning processes so policy-compliant provisioning and approval workflows are executed, and one-stop for managers, system, and application administrators is available.

Framework Assumptions

Table 2 lists the discount rate used in the present value (PV) and net present value (NPV) calculations and time horizon used for the financial modeling.

Table 2: General Assumptions

Ref.	General assumptions	Value
	Discount rate	10%
	Length of analysis	Three years

Source: Forrester Research, Inc.

Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult with their finance department to determine the most appropriate discount rate to use within their own organizations.

Costs

Costs for the OIM implementation for the composite company encompass Oracle OIM software license fees (A1) and annual maintenance (A2), professional services (B1-B6), internal labor for planning and deployment (C1-C3), and internal resources for ongoing system monitoring and management (D1-D3). Also, Table 7 includes additional hardware costs for development, testing, and production environments.

Software Licenses And Maintenance

Total costs for software over the course of the three years measured in this analysis amounted to just under \$1.4 million. This includes the main license for OIM, an additional license fee for external users, an additional cost for 10 connectors to the key endpoints, and annual maintenance of 22% of the combined license amounts.

Table 3: License And Maintenance Costs

Ref.	Metric	Initial	Year 1	Year 2	Year 3	Total
A1	Software license fees incl. adapters	830,000				830,000
A2	Annual maintenance (22%)	0	182,600	182,600	182,600	547,800

The Total Economic Impact™ Of Oracle Identity Manager

At	Total license and maintenance	\$830,000	\$182,600	\$182,600	\$182,600	\$1,377,800
----	-------------------------------	-----------	-----------	-----------	-----------	-------------

Source: Forrester Research, Inc.

This amount assumes typical pricing for an implementation of this scope and complexity, according to Oracle. Readers of this study should note that pricing varies greatly depending on the specific customer's organization, size, and other factors.

Professional Services

Consulting resources engaged for an initial phase OIM implementation such as this one would require six consultants for six months. Assuming a blended rate of \$1,000 per day produces an amount of \$780,000. Subsequent phases of the implementation would require a third as much in consulting resources for Phase 2 and 3 in Year 1 and Year 2, as show in the table below:

Table 4: Professional Services Fees

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3	Total
B1	No. of consultants		6	2	2		
B2	Cost per day		\$1,000				
B3	Days		5				
B4	Weeks		26.00				
Bt	Professional services	B1*B2*B3*B4	\$780,000	\$260,000	\$260,000		\$1,300,000

Source: Forrester Research, Inc.

Internal Labor — Implementation

Internal resources for planning, solution design, and project management amount to three FTEs who earn average fully loaded annual compensation of \$150,000. Forrester assumes these staff would be 50% dedicated to this project for the initial six months of the project. The resulting total cost sums to \$225,000 (3 x \$150,000 x 50%).

Table 5: Internal Labor — Planning, Design, Project Management

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
C1	Number of internal staff		3			
C2	Fully loaded compensation		\$150,000			
C3	% dedicated		50%			

The Total Economic Impact™ Of Oracle Identity Manager

Ct	Internal labor — planning, design, project management	C1*C2*C3	\$225,000			
----	---	----------	-----------	--	--	--

Source: Forrester Research, Inc.

Internal Labor — Operations Support, Engineering, Administration

Once implementation is complete, internal resources will be required for ongoing support, upgrades and solution extensions, and administration. Based on interviews with OIM user organizations, Forrester assumes four, six and then eight FTEs earning average fully loaded compensation of \$125,000 would be dedicated 50% to identity and access management efforts around OIM. This produces an annual cost of \$500,000 (8 x \$125,000 x 50%) in Year 3.

Table 6: Internal Labor — Operations Support, Engineering, Administration

Ref.	Metric	Calc.	Initial	Year 1	Year 2	Year 3	Total
D1	Number of internal staff		0	4	6	8	
D2	Fully loaded compensation		\$125,000				
D3	%		50%				
Dt	Internal labor - operations support, engineering, administration	D1*D2*D3	-	\$250,000	\$375,000	\$500,000	\$1,125,000

Source: Forrester Research, Inc.

Hardware

Dedicated hardware is assumed for this implementation in order to provide server resources to house development, testing, and production environments. The cost of application and database servers, which provides platforms for three environments (development, testing/staging, and production), is assumed to amount to \$450,000.

Total Costs

Table 7 summarizes the costs expended by the composite company of implementing Oracle Identity Manager.

Table 7: Total Costs

Costs	Initial	Year 1	Year 2	Year 3	Total
Software license fees (internal users), incl. adapters	830,000				830,000
Annual maintenance		182,600	182,600	182,600	547,800
Professional services — implementation	780,000	260,000	260,000		1,300,000
Internal labor — planning, design, project management	225,000				225,000
Internal labor — operations support, engineering, administration		250,000	375,000	500,000	1,125,000
Hardware costs	450,000				450,000
Total	\$2,285,000	\$692,600	\$817,600	\$682,600	\$4,477,800

Source: Forrester Research, Inc.

Benefits

The OIM customers who were interviewed for this study described a range of hard and soft benefits that have accrued from their OIM implementations and the introduction of identity management processes. The most significant benefit described to Forrester was a major leap in the overall productivity for new employees and contractors when they do not have to wait for accounts to be provisioned or spend time asking where and from whom to request access to applications and databases. Other benefit categories that were revealed in interviews are reduction in help desk labor costs, incremental productivity for employees and external users with self-service for password resets, incremental productivity for attestation reviewers and application owners, avoided costs of audit remediations, software license cost reductions, and potential cost avoidance related to security breaches. Each of these categories of benefit is discussed below. Yet as the manager of Identity & Access at one customer organizations interviewed for this study explained, “The driver of this project was not so much cost savings as it was business enablement — eliminating impediments to the company’s growth.”

Increased User Productivity — New Hires Can Start Working Faster

Every company interviewed for this study described the productivity improvement that was gained from faster provisioning of accounts for new hires. OIM user organizations expressed improvements in the amount of time required for “on-boarding” new hires, citing gains by cutting the time — from days to minutes — to provide new hires with access to applications and data stores. OIM frequently serves as the single source of truth for HR purpose where previously these companies were burdened by siloed, disparate databases holding often-conflicting and incomplete identity and

The Total Economic Impact™ Of Oracle Identity Manager

access elements. Calculations of this benefit category are based on customers reporting that provisioning new employees takes minutes with OIM instead of three to five days required prior to OIM. For the composite company, which is experiencing 10 percent growth per year and 10 percent turnover, 8,000 employees and contractors must be on-boarded annually. Each earns an average fully loaded compensation of \$50 per hour. Each saves three days (3* 8 hours = 24 hours) with faster provisioning. Yet since new employees are not yet fully productive even with faster provisioning, Forrester discounts this amount by all but 20%. The resulting benefit amount is \$4.8 million per year, as show in Table 8 below.

Table 8: Increased Productivity: On-Boarding New Hires

Ref.	Metric	Calculation	Per period	Year 2	Year 3	Total
F1	Number of new users	10% growth, 10% turnover	8,000			
F2	Hourly rate per worker		\$50			
F3	Number of hours saved		24.0			
F4	Percent captured		20%			
Ft	Incremental productivity: on-boarding new hires	$F1 * F2 * F3 * F4$	\$1,920,000	\$1,920,000	\$1,920,000	\$5,760,000

Source: Forrester Research, Inc.

Reduction In Help Desk Labor Costs

When staff forget their passwords or have other difficulties accessing the applications and data they need, they call the help desk, unless, as with OIM, they have a self-service option. More employees are forgetting their passwords more often with the trend toward stronger passwords (longer, more complex passwords that need to be changed more frequently). One interviewee noted that his organization reduced their help desk ticket volume by 85%. For the composite company, Forrester assumes that the number of calls to the help desk is reduced by 80,000 calls per year (or two per worker per year) as requests for passwords, resets, etc., are shifted to the Web-based self-service portal. Eighty-thousand calls per year require 6.4 FTEs, as shown in Table 9 below.

Table 9: Help Desk Reps Available For Reassignment

Ref.	Metric	Calculation	Value
G1	Help desk calls converted to self-service		80,000
G2	Calls per week per help desk FTE	5 days*\$50/day	\$250
G3	Weeks		50
G4	Calls per FTE per year	$G2 * G3$	12,500

The Total Economic Impact™ Of Oracle Identity Manager

Gt	Help desk reps no longer required — shift to self-service	G1/G4	6.40
----	---	-------	------

Source: Forrester Research, Inc.

Each of the 6.4 help desk FTEs, each assumed to earn an average fully loaded compensation amount of \$60,000 per year, produces a savings of \$384,000 per year as those workers can be re-assigned to other responsibilities (such as generating compliance reports, etc.), or just over \$1.1 million over three years.

Table 10: Reduction In Help Desk Labor Costs

Ref.	Metric	Calc.	Per period	Year 2	Year 3	Total
H1	Number of FTEs		6.40			
H2	Fully loaded annual compensation		\$60,000			
Ht	Reduction in internal labor cost — help desk	H1*H2	\$384,000	\$384,000	\$384,000	\$1,152,000

Source: Forrester Research, Inc.

Incremental Productivity — Calls To Help Desk

When employees (and contractors, partners, customers) can reset their own passwords and update their own profiles without calling the help desk, they can avoid a hole in their workday and the resulting interruption and loss of work time. Assuming that each of the 40,000 workers at IMG would previously have had to call the help desk twice per year, each time resulting in a 30-minute delay, then the resulting productivity improvement is \$1.5 million per year. Forrester assumes that just 50% of the benefit would be captured; similar conservative factors are applied throughout this analysis for productivity improvement calculations.

Table 11: Incremental Productivity — Calls To Help Desk

Ref.	Metric	Calculation	Per period	Year 2	Year 3	Total
I1	Number of workers		40,000			
I2	Password resets per year/FTE		2.0			
I3	Number of hours saved		0.5			
I4	Fully loaded hourly compensation		\$50			
I5	Percent captured		50%			
It	Incremental productivity — password reset, calls to help	I1*I2*I3*I4*I5	\$1,000,000	\$1,000,000	\$1,000,000	\$3,000,000

The Total Economic Impact™ Of Oracle Identity Manager

	desk					
--	------	--	--	--	--	--

Source: Forrester Research, Inc.

Reduction In Administrative Labor Costs

OIM saves organizations administrative labor that was previously dedicated to a range of identity and access management tasks. This work is associated with recertification — manually answering questions about who has access to what, why, who authorized each permission, and removing expired or unexplained accounts. Additional manual work is usually eliminated in areas of new account requests among existing employees and contractors (e.g., move/add/change tasks) and audit support efforts. Forrester assumes that an organization can eliminate .80 FTEs for this work for every 5,000 users. For IMG, this calculates to 6.4 FTEs who earn \$100,000 salary plus benefits, for a total three-year amount of \$1.9 million.

Table 12: Labor Cost Savings — Administration

Ref.	Metric	Calculation	Per period	Year 2	Year 3	Total
J1	Number of FTEs	.80 FTE per 5,000 workers (.80*(40,000/5,000))	6.40			
J2	Fully loaded annual compensation		\$100,000			
Jt	Labor cost savings: Access re-certifications, new account requests, attestation, audit assistance	J1*J2	\$640,000	\$640,000	\$640,000	\$1,920,000

Source: Forrester Research, Inc.

Reduction In Labor Costs — Attestation Reviews

Attestation is the periodic process to re-certify that only appropriate individuals have accessed sensitive information. This requires a comprehensive audit trail of historical user privileges, including when, why, and through which systems information was accessed. Complying with regulatory audits and attestation requirements is expensive and time consuming, especially when the same manual processes must be repeated for every audit. Oracle Identity Manager automates the capture of historical user privilege profiles and automates the generation of attestation reports through an integrated workflow-based framework for management certification and automated execution of corrective actions. Manual tasks among first level managers and application owners throughout an organization can be minimized by automating audit processes and streamlining attestation. Forrester believes that approximately 3,000 staff (7.5% of this company's 40,000) have been involved in these kinds of activities prior to the OIM implementation. By automating these tasks, managers and application owners should save 8 hours per year (assuming two attestation runs per year) and assuming that 50% of this labor cost savings is captured and redirected toward productive work, then this benefit is worth \$600,000 per year or \$1.8 million over three years.

Table 13: Labor Cost Savings — Attestation Reviews

Ref.	Metric	Calculation	Year 1	Year 2	Year 3	Total
K1	Number of attestation reviewers, application owners		3,000			
K2	Hourly rate per worker		\$50			
K3	Number of hours saved per reviewer		8.0			
K4	Percent captured		50%			
Kt	Incremental productivity: attestation reviewers, application owners	$K1 \times K2 \times K3 \times K4$	\$600,000	\$600,000	\$600,000	\$1,800,000

Source: Forrester Research, Inc.

Audit Remediation Costs Avoided

Implementing OIM can be expected to reduce the number of audit findings that require remediation. With a centralized identity database, defined workflows, and automated processes, IMG will have fewer instances of practices running counter to security and access policies, and the resulting cost of fixing those problem areas in order to comply with auditors' requirements. Forrester believes an organization of this size will avoid approximately 25 such instances at an average cost to remediate of \$10,000 in labor. This results in an annual benefit of \$250,000.

Table 14: Audit Remediation Costs Avoided

Ref.	Metric	Calculation	Per period	Year 2	Year 3	Total
L1	No. of audit remediations		25			
L2	Cost per remediation		\$10,000			
Lt	Audit remediation costs avoided	$L1 \times L2$	\$250,000	\$250,000	\$250,000	\$750,000

Source: Forrester Research, Inc.

Software License Cost Savings

By identifying and eliminating orphan and rogue accounts, IMG will discover unused software licenses that can be re-allocated to active users or reported to the software vendor for credit or negotiating more accurate pricing and payment terms. Forrester assumes that only 30 of the applications at IMG fall within this recoverable license scenario and that an average of 200 unused licenses or seats can be recovered. At a conservative estimate of \$50 per user per application, this benefit amounts to \$300,000 per year.

Table 15: Software License Cost Savings

Ref.	Metric	Calculation	Per period	Year 2	Year 3	Total
M1	Number of applications		30			
M2	Number of unused licenses/seats per application		200			
M3	Cost per license (average)		\$50			
Mt	Software license cost savings — unused accounts	$M1 * M2 * M3$	\$300,000			
Mto	Total (original)		\$300,000	\$300,000	\$300,000	\$900,000

Source: Forrester Research, Inc.

Cost Avoidance — Security Breaches

Identifying orphan and rogue accounts and effectively terminating the accounts of departing workers reduces the risk of security breaches. Users of this study are familiar with news reports of monumental losses to companies suffering security breaches. Forrester’s calculation of the benefit or reducing this risk is conservative. Readers should note the potential for loss — and the inverse benefit of reducing such risk — is much greater than shown here. The calculation in Table 16 below indicates the cost of providing credit monitoring services to all employees, retirees, and affected others (assuming 75% of users take up the offer of these services) in the event of the discovery of a potential leak of personal data — a quantifiable, definite cost occurrence that serves as a proxy for cost estimation of security breaches. Forrester assumes OIM can help to avoid one breach every five years, and thus the untreated risk for any given year is 20%. The simple calculation below produces an annual benefit of \$675,000.

Table 16: Credit Monitoring Service Cost

Ref.	Metric	Calculation	Per Period	Year 2	Year 3	Total
N1	Active & retired users		100,000			
N2	% Redemptions		75.00%			
N3	Credit monitoring service cost per user		\$45.00			
N4	Reduced probability of breach		20.00%			
Nt	Potential cost avoidance - security breach	$N1 * N2 * N3 * N4$	\$675,000	\$675,000	\$675,000	\$2,025,000

Source: Forrester Research, Inc.

Total Benefits

Table 17 shows the total benefits that were quantifiable for this study.

Table 17: Total Benefits

Benefits	Year 1	Year 2	Year 3	Total
Incremental productivity: on-boarding new hires	1,920,000	1,920,000	1,920,000	5,760,000
Reduction in labor cost — help desk	384,000	384,000	384,000	1,152,000
Incremental productivity — password reset, calls to help desk	1,000,000	1,000,000	1,000,000	3,000,000
Labor cost savings: Access recertification, new account requests, attestation, audit assistance	640,000	640,000	640,000	1,920,000
Incremental productivity: attestation reviewers, application owners	600,000	600,000	600,000	1,800,000
Audit remediation costs avoided	250,000	250,000	250,000	750,000
Software license cost savings — unused accounts	300,000	300,000	300,000	900,000
Potential cost avoidance — security breach	675,000	675,000	675,000	2,025,000
Total	\$5,769,000	\$5,769,000	\$5,769,000	\$17,307,000

Source: Forrester Research, Inc.

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 still 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.

For the purpose of this analysis, Forrester risk-adjusts cost and benefit estimates to better reflect the level of uncertainty that exists for each estimate. 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 within the current environment. The risk-adjusted value is the mean of the distribution of those points.

For example, in the case of internal labor costs for design, development, and rollout on Table 5 above, the \$225,000 value used in this analysis can be considered the “most likely” or expected value. Labor costs vary based on the complexity and duration of the project, which can be difficult to assess before commencing. This variability represents a risk that can be captured as part of this study. Forrester uses a risk factor of 125% (3.75 FTEs) on the high end, 100% (3.0 FTEs) as the most likely, and also 100% of 3.0 FTEs on the low end. This has the effect of increasing the cost

The Total Economic Impact™ Of Oracle Identity Manager

estimate to take into account the fact that original cost estimates are more likely to be revised upward than downward. Forrester then creates a triangular distribution to reflect the range of expected costs, with 108% or 3.25 FTEs as the mean.

Other cost figures are not risk adjusted. License costs, for example, can be determined with a high degree of certainty (and contractually set) before a project is started. License and maintenance costs presented in this study are not risk adjusted for this reason.

On the benefits side, note the amount of internal labor that would be eliminated as a result of efficiencies affecting the help desk shown in Table 10 as an example. At the beginning of the deployment, IT and business decision-makers will not be completely certain about the number of full time associates that can be re-assigned. Forrester therefore assembled a range for this benefit category with 7.5 FTEs on the high end, the maximum benefit that would be envisaged, 6.4 FTEs as the most likely, and 5.0 FTEs on the very conservative low end. The mean, 6.3, is the risk-adjusted number, equivalent to \$378,000 in labor cost savings per year (compared to \$384,000 for the original estimate) when multiplied by the average annual fully loaded compensation rate of \$60,000.

The following tables show the values used to adjust for uncertainty in cost and benefit estimates. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Table 18: Risk Adjustment Factors — Costs

Ref.	Metric	Low	Most likely	High	Mean
Bt	Professional services	90%	100%	150%	113%
Ct	Internal labor — planning, design, project management	100%	100%	125%	108%
Dt	Internal labor — operations support, engineering, administration	100%	100%	125%	108%
Et	Hardware costs	85%	100%	125%	103%

Source: Forrester Research, Inc.

Table 19: Risk Adjustment Factors — Benefits

Ref.	Metric	Low	Most likely	High	Mean
Ft	Incremental productivity: on-boarding new hires	2 days	3 days	5 days	3.33 days
Ht	Reduction in internal labor cost — help desk	5.0 FTEs	6.4 FTEs	7.5 FTEs	6.3 FTEs
It	Incremental productivity — password reset calls to help desk eliminated	1.0 calls/yr/ FTE	2.0 calls/yr/ FTE	2.5 calls/yr/ FTE	1.83 calls/yr/ FTE

The Total Economic Impact™ Of Oracle Identity Manager

Jt	Labor cost savings: Access recertification, new account requests, attestation, audit assistance	4.0 FTEs	6.4 FTEs	8.0 FTEs	6.13 FTEs
Kt	Incremental productivity: attestation reviewers, application owners	4 hours saved/yr	8 hours saved/yr	10 hours saved/ yr	7.3 hours saved/yr
Lt	Audit remediation costs avoided	10 findings	25 findings	30 findings	21.67 findings
Mt	Software license cost savings — unused accounts	100 unused licenses	200 unused licenses	250 unused licenses	183 unused licenses
Nt	Potential cost avoidance — security breach	10% probability reduction	20% probability reduction	20% probability reduction	16.67% probability reduction

Source: Forrester Research, Inc.

Flexibility

Flexibility, as defined in Forrester's TEI methodology, is an investment in additional capacity or capability 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 specific future initiatives — but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement Oracle Identity Manager within a certain scope of activities and business areas and later discover additional value that can be realized by expanding usage. The flexibility component of TEI can capture that value, using the industry standard Black-Scholes option pricing model.

One example of flexibility is the ever-present prospect of an acquisition. If IMG were to acquire another company, the savings in time and labor would be significant because IMG would already have the foundation of Identity Manager to quickly integrate the identities of employees and contingent workers of the acquired company. One of the companies interviewed for this study explained the ease with which an acquisition was integrated, at least in terms of account provisioning and certain HR functions. “We saved a ton of time with the acquisition,” explained the director of technology services:

“In the past, if we acquired a company, we had to set up all these accounts. And IT was the bottleneck. We had to set up the email account, the network accounts, UNIX account, so on, and so forth. Well, after we implemented OIM, we acquired a company in Germany that had about 180 employees in it. And all that we had to do was enter their information once. We didn't have to create accounts, [or] do all the UNIX drives. We just did a validation. All of the information was there and created as soon as HR entered the new staff into our systems. So that saved probably five people's time for a week. And then just overall productivity — you're talking 180 people more productive in that week's period of time.”

Another company interviewed for this study, the US investment bank with 40,000 users, was subsequently acquired by another large financial services organization. Because both companies

were using OIM, their systems integration was very fast. The acquirer claimed that it took a total of two weeks to get all of the acquired company’s users onto the parent’s systems and vice versa.

Using the first example above, a relatively small acquisition, Forrester assumed that data entry, the cost of the option, amounts to two FTEs working for one day (8 hours) at an hourly rate of \$30. The value of faster on-boarding for new employees is equal to \$360,000 (180 x 5 days x \$400 per day), with a two-year horizon.

Table 20: Risk Adjustment Factors — Benefits

Ref.	Metric	Calculation	Value
P1	Asset value (benefit)	180 FTEs*5 days*\$400/day	\$360,000
P2	Cost to acquire	2 FTEs*8 hrs*\$30	\$480
P3	Expiration (years)		2.0
Pt	Flexibility	Black-Scholes option pricing model	\$359,548

Source: Forrester Research, Inc.

The flexibility component of TEI captures that value using either the financial industry standard Black-Scholes (http://en.wikipedia.org/wiki/Black-Scholes#The_model) or the binomial option pricing models. Forrester values the above flexibility option at more than \$359,000.

These are only three illustrations of flexibility options. The foundation or platform for more such options was created when Intercontinental Manufacturing Group implemented OIM, including these examples identified by customers as areas that represent business value that can be understood in terms of future flexibility options:

- OIM implementation prompting business users to simplify business processes, eliminate non-value add steps, etc.
- Include facility access badges within the scope of Oracle Identity Manager.
- Develop more efficient attestation processes.
- Extending IM to partners and customers and integration into SOA strategy.
- Expansion/federation to 10,000 partners and vendors.

The value of flexibility is unique to each organization, and the willingness to measure its value varies from company to company. Please note that the values calculated above exist in addition to risk-adjusted benefits described in this case study analysis; Forrester has not included the option value in the ROI calculations.

TEI Framework: Summary

Considering the financial framework constructed above, the results of the costs, benefits, risk, and flexibility sections using the representative numbers can be used to determine a return on investment, net present value, and payback period. Table 1 shows the consolidation of the numbers for the composite organization.

Tables 21 and 22 below show the risk-adjusted values, applying the risk adjustment method indicated in the Risks section and the values from Tables 18 and 19 to the numbers in Tables 7 and 17.

It is important to note that values used throughout the TEI Framework are based on in-depth interviews with four organizations and the resulting composite organization built by Forrester. 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 OIM.

Table 21: Total Costs — Risk Adjusted With Present Values

Costs	Initial	Year 1	Year 2	Year 3	Total	Present value
Software license fees incl. adapters	830,000				830,000	830,000
Annual maintenance		182,600	182,600	182,600	547,800	454,099
Professional services	884,000	294,667	294,667		1,473,333	1,395,405
Internal labor — planning, design, project management	243,000				243,000	243,000
Internal labor — operations support, engineering, administration		270,000	405,000	540,000	1,215,000	985,875
Hardware costs	465,000				465,000	465,000
Total	\$2,422,000	\$747,267	\$882,267	\$722,600	\$4,774,133	\$4,373,379

Source: Forrester Research, Inc.

Table 22: Total Benefits — Risk Adjusted With Present Values

Benefits	Year 1	Year 2	Year 3	Total	Present value
Incremental productivity: on-boarding new hires	1,973,333	1,973,333	1,973,333	5,920,000	4,907,388

The Total Economic Impact™ Of Oracle Identity Manager

Reduction in internal labor cost — help desk	378,000	378,000	378,000	1,134,000	940,030
Incremental productivity — password reset calls to help desk eliminated	916,667	916,667	916,667	2,750,000	2,279,614
Incremental productivity: attestation reviewers, application owners	550,000	550,000	550,000	1,650,000	1,367,769
Labor cost savings: Access recertification, new account requests, attestation, audit assistance	613,333	613,333	613,333	1,840,000	1,525,269
Audit remediation costs avoided	216,667	216,667	216,667	650,000	538,818
Software license cost savings — unused accounts	275,000	275,000	275,000	825,000	683,884
Potential cost avoidance — security breach	562,500	562,500	562,500	1,687,500	1,398,854
Total	\$5,485,500	\$5,485,500	\$5,485,500	\$16,456,500	\$13,641,627

Source: Forrester Research, Inc.

Study Conclusions

Forrester's interviews with Oracle Identity Manager customers yielded several important observations. Based on information collected in interviews with current OIM customers, Forrester found that organizations can realize benefits in the form of productivity improvements for new employees, incumbent staff, and those responsible for attestation. Benefits also include lower labor costs for help desk resources and access management administration. Forrester also found that OIM can reduce the number of negative audit findings that require remediation and reduce software license costs by pointing to unused accounts. And finally, the security improvements fostered by OIM have quantifiable value.

The financial analysis provided in this study illustrates a method for an organization to evaluate the value proposition of Oracle Identity Manager. Based on information collected in four in-depth customer interviews, Forrester calculated a three-year risk-adjusted ROI of 221% for the composite organization with a payback period of six months. All final estimates are risk-adjusted to incorporate potential uncertainty in the calculation of costs and benefits.

NOTE: If the estimates of productivity improvements are removed from the financial framework described in the study — to present the most conservative scenario — the ROI for the composite company is 16% with a payback period of 24 months.

Based on these findings, companies looking to implement OIM can see cost savings and productivity benefits. Using the TEI framework, many companies may find the potential for a compelling business case to make such an investment.

Table 1: Three-Year ROI, Risk-Adjusted

Summary financial results	Original estimate	Risk-adjusted
ROI	250%	212%
Payback period (months)	5.4	6.1
Total costs (PV)	(\$4,103,186)	(\$4,373,379)
Total benefits (PV)	\$14,346,649	\$13,641,627
Total (NPV)	\$10,243,463	\$9,268,247

Source: Forrester Research, Inc.

Appendix A: Composite Organization Description

In this TEI study, Forrester has created a composite organization to illustrate the quantifiable costs and benefits of implementing Oracle Identity Manager. The composite company is intended to represent an electronics design and manufacturing company, referred to in the study as Intercontinental Manufacturing Group (IMG), and is based on characteristics of the interviewed Oracle customers.

Organization Size And Dimensions

- Annual revenues of \$15 billion.
- Thirty-five thousand employees, 5,000 contractors, and 10,000 external vendors/partners. Turnover is 10% per year, and the user base is increasing 10% annually.
- Globally distributed IT infrastructure across four locations. Approximately 2,000 target resources and 10 major user repositories. These target resources include multiple instances of SAP for ERP, PeopleSoft for HR, Oracle e-Business Suite for financials and CRM, legacy ordering system deployed on RACF mainframe, an assortment of infrastructure technologies from a multitude of vendors such as Novell eDirectory, a few types of Unix servers, Microsoft Active Directory, Microsoft Exchange, BMC Remedy ARS, RSA SecurID, Oracle Weblogic Application Server, IBM Websphere Application Server, Oracle databases, SQL Server databases and others. Over half of the 2000 resources are custom homegrown applications, mostly built on Java but also including C and .NET applications. Twenty-four of these applications are Sarbanes Oxley (SOX) sensitive.

Identity Management Environment Prior To Investment

- No enterprisewide identity management products were employed prior to implementing OIM, with the exception of LDAP directories and Active Directory.
- Manual processes were used for provisioning, using application native tools and admin consoles. The help desk system was leveraged to accept provisioning requests and route tickets for manual provisioning.
- There were no HR event feeds from PeopleSoft or other identity repositories. Multiple legacy HR systems are in place from past acquisitions. HR events are exported to the help desk using a daily flat file dump. Only data on employees was stored in the HR system; contractor data were housed in a custom database.
- There were more than 10 different ways to request access to resources. Users had to figure out how to ask for application access or business functionality (entitlements) in applications.
- Quarterly sweeps of individual systems (although not all) were engaged to confirm current access information. No automated process existed to reconcile this information with HR information.
- No logs (past or current) were created of who has/had access to what and why. User access auditing and attestation processes are completely manual, distributed, and cumbersome.

Implementation

- Phase 1 of the implementation required six months starting in 2005 (Year 0 in the financial framework).
- Ten-thousand user groups / roles prior to OIM deployment were reduced to 3,000 roles after a role analysis before implementation.
- Simple role-based provisioning policy (similar to minimal standard, or 'birthright' provisioning), focuses on simple roles that apply to a large population of users. Roles like "employee," "contractor," "engineer," etc. The organization currently relies on these simple roles and policies to provision core systems used by all such as Active Directory, MS Exchange, etc.
- OIM became the aggregation point for user information across all HR and contractor databases. The HR systems send exports to OIM every 4 hours. The contractor database was eliminated and replaced by OIM.
- Eight core systems were provisioned in Phase 1: Active Directory, Exchange, Windows File Share, variety of Unix systems, Single Sign-On systems (from vendors like Oracle, CA, RSA), and three core business applications (ERP, etc.).
- Phase 2 and Phase 3 involved integrating additional systems, rolling out self-service capabilities, adding more roles and policies, performing periodic attestation of user access, and integrating the identity management framework with the SOA framework.
- Users no longer have to figure out where to go ask for access and permissions; request management has been centralized to OIM's self service feature.

Initial Reasons For Investment

Based on interviews with actual OIM customers, Forrester assumed that IMG identified the following business drivers for investing in OIM:

- Reduce risk and meet SOX compliance more easily.
- Reduce costs of manual provisioning and help desk resources.
- Terminate access when an employee leaves to eliminate security and information leaks associated with orphan and dormant accounts.
- Increase user productivity on Day 1 by ensuring new employees have immediate access to resources that they need to be productive and do their jobs.
- Reduce help desk call volume and improve user experience with self service (such as password reset) and single request portal.
- Centralize security administration provisioning processes so policy-compliant provisioning and approval workflows are executed, and one-stop for managers, system, and application administrators is available.

Benefits Realized/Achieved

- At least six help desk staff can be re-assigned due to reduced call volume resulting from automated provisioning and self-service password reset, lookup, etc.
- Reduced Windows account creation time from 5 days to minutes — now creating 12,000 accounts annually.
- Decreased new account requests from five to one per employee annually, through clearly defined roles.
- Reduced help desk calls for password reset requests via self-service capability; 80,000 requests now made annually through self service portal.
- Reduced business risk by facilitating regulatory and policy compliance.
- Cost avoidance of remediation audit findings.
- Increased productivity and better user experience from self-service of password resets, etc.
- Reduced time and effort required for auditing and regular attestation with identity data consolidation and process automation.
- Reduction of risk by eliminating ghost, dormant, and orphan accounts. Manual error or excessive access privileges due to lag in de-provisioning significantly minimized.
- Single source to look up all users and their current and past access privileges across all systems.

Appendix B: 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, costs, risks, and flexibility. For the purpose of this analysis, the impact of flexibility was not quantified.

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 to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit 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 in the forms 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 for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

Risk

Risk measures the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: the likelihood that the cost and benefit 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 benefit.

Flexibility

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify 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 already made. 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 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 C: 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.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project 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 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.

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 shown in Table 2 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

Ref.	Category	Calculation	Initial cost	Year 1	Year 2	Year 3	Total

Source: Forrester Research, Inc.

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 and solutions 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: Related Forrester Research

[Inquiry Spotlight: Identity And Access Management, Q4 2008](#), October 6, 2008.

[Best Practices: Enterprise Role Management](#), September 30, 2008.

[Privileged User Management Market Overview](#), June 30, 2008.

[Forrester TechRadar™: Identity And Access Management, Q2 2008](#), June 18, 2008.

[Topic Overview: Identity And Access Management](#), April 14, 2008.

[Identity-Management-As-A-Service](#), April 2, 2008.

[The Forrester Wave™: Identity And Access Management, Q1 2008](#), March 14, 2008.

[Understanding The Identity Management Market To Make Better Planning Decisions](#),
March 6, 2008.

[Identity Management Market Forecast: 2007 To 2014](#), February 6, 2008.

[Topic Overview: IT Security](#), December 5, 2007.

[The State Of Federation](#), September 27, 2007.

[User Account Provisioning For The Midmarket](#), August 20, 2007.