SOX Monday Morning Quarterback

and a Look Forward

Mark Nelson
Managing Director
Application Controls - Oracle Practice

protiviti® Independent Risk Consulting

Protiviti Overview

COLLABORATE08
Technology and Applications Forum for the Oracle Community

Who We Are

- Independent risk consulting and internal audit company
- More than 2,900 professionals
- 50 offices throughout the United States, Asia and Europe.
- 2006 annual revenues were $543 million.
- Our parent company, Robert Half International (RHI), is a $4 billion public company.

Business Risk

Technology Risk

Internal Audit

What We Do

Business Risk

Sarbanes-Oxley
Event-Related
Financial
Enterprise Risk Management
Operational
Treasury

Technology Risk

Application Controls Effectiveness
IT Strategy
Project Risk Management
Infrastructure
Business Continuity
Privacy & Security

Internal Audit

Co-Sourcing
Outsourcing
Internal Audit Transformation
Quality Assurance Reviews
Risk Assessment

protiviti®
Independent Risk Consulting

Common Themes

5 Lessons Learned

1. Deploy a top-down approach to focus on what's important

1 – Top Down Approach

Management Fraud:

- most often perpetrated at company level
- period end financial reporting
- not within upstream business process transactions.

Despite that most 404 work has been spent on process level controls

- Reduce number of key controls
- Management needs to place more emphasis on entity-level controls
- Utilize full knowledge of business process transactions

5 Lessons Learned

1. Deploy a top-down approach to focus on what's important
2. Consider qualitative and quantitative factors to implement a truly risk based approach

2 – Qualitative vs. Quantitative

2 – Qualitative vs. Quantitative

- The nature and significance of possible error or fraud that could occur in an account (otherwise known as “what can go wrong”);
- The susceptibility of an account to error or fraud; •
- The “robustness” versus “subjectiveness” of the processes for determining significant estimates;
- The nature and effect of related party transactions; and
- The testing experience and problem areas from prior years that may require attention during the current-year assessment.

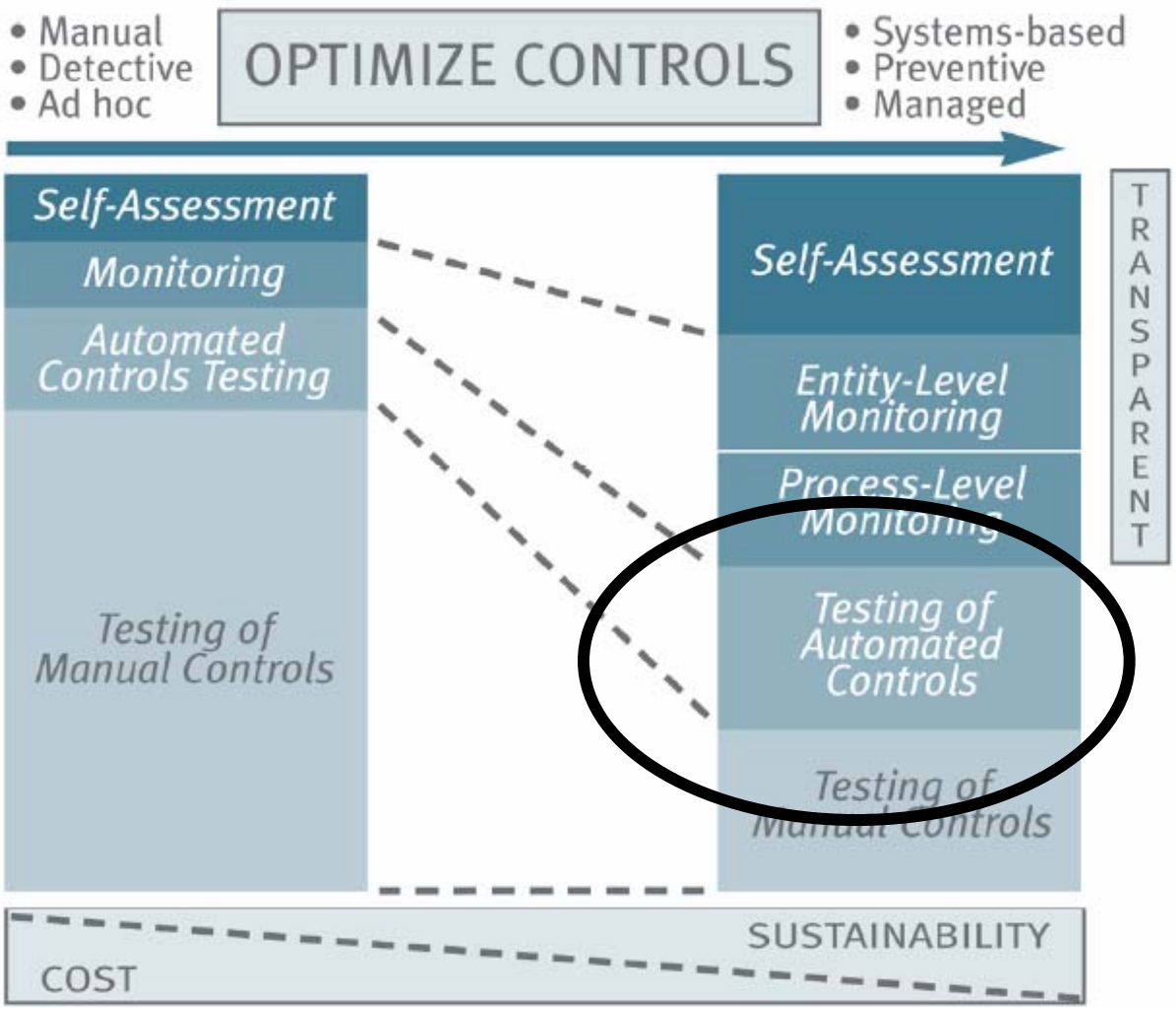
5 Lessons Learned

1. Deploy a top-down approach to focus on what's important
2. Consider qualitative and quantitative factors to implement a truly risk based approach
3. Optimize IT controls to increase the cost-effectiveness of the controls portfolio

3 – Optimize IT Controls

- IT Controls are less expensive to test
- Balance the mix of manual and IT controls
- Manual Controls – require inspection of documentation often embedded in reams of documentation
- Automated Controls – one time observation of system performance or ERP setting
  - Provided that it is designed, maintained secured effectively

Optimize Controls



5 Lessons Learned

1. Deploy a top-down approach to focus on what's important
2. Consider qualitative and quantitative factors to implement a truly risk based approach
3. Optimize IT controls to increase the cost-effectiveness of the controls portfolio
4. Improve operational effectiveness and efficiency of upstream financial reporting processes

4 – Improve Up Stream Processes

- Eliminating redundant activities, platforms and other nonessentials
- Simplifying and standardizing processes
- Centralizing common and similar activities
- Improving the mix of automated and manual controls
- Transforming inefficient “detect and correct” controls to preventive controls that "build in" versus "inspect in" quality.

Project to Process – Automated Controls

Optimize Automated Controls

Configured Controls

- Establish universe
- Assess existing controls
- Identify gaps & opportunities
- Implement control & process changes

(automated & manual)

Security/SOD

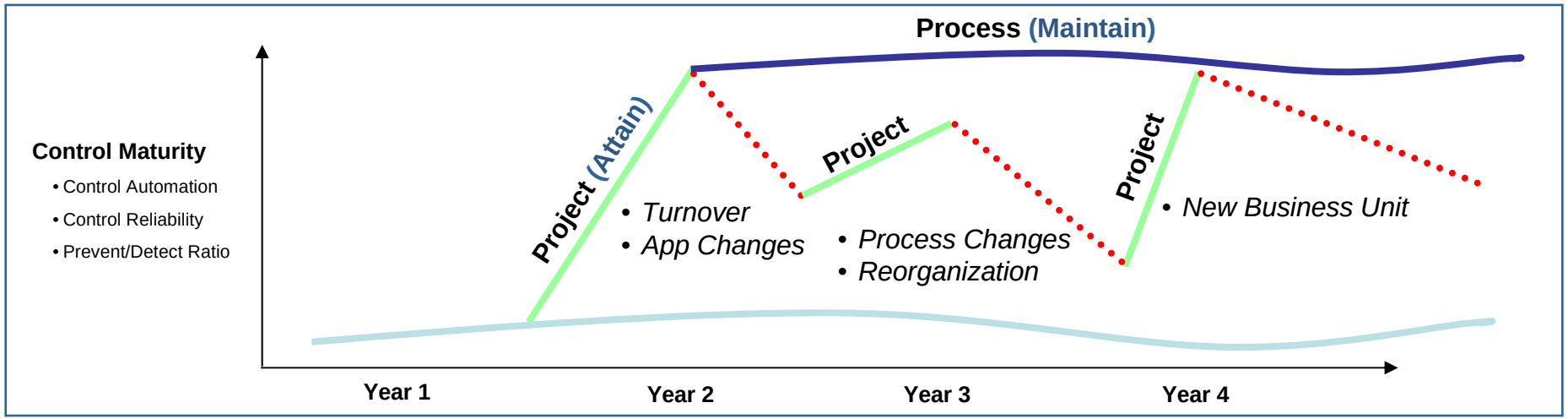
- Design/Acquire rule-sets
- Assess existing roles and assignments
- Identify potential gaps
- Investigate gaps and mitigation
- Redesign roles
- Clean up assignments

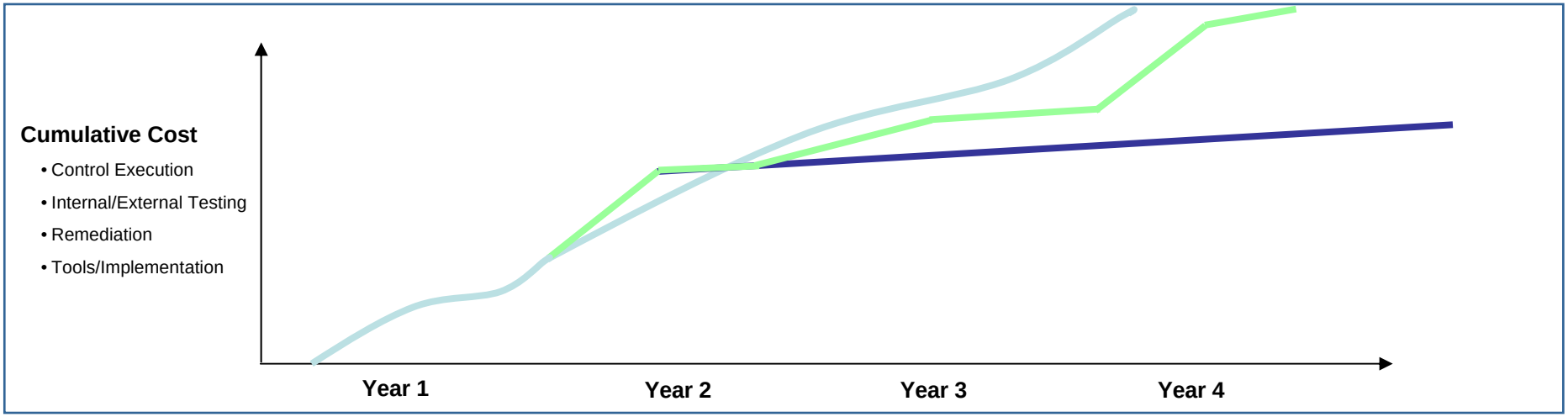
Continuous Monitoring & Automated Testing

- User setup request and approval
- SOD monitoring, analysis, mitigation documentation
- Configuration/setup change management
- Master data change management and monitoring
- Transaction monitoring
- Continuous or periodic independent audit / testing

Attain → **Maintain**

Attain and Maintain

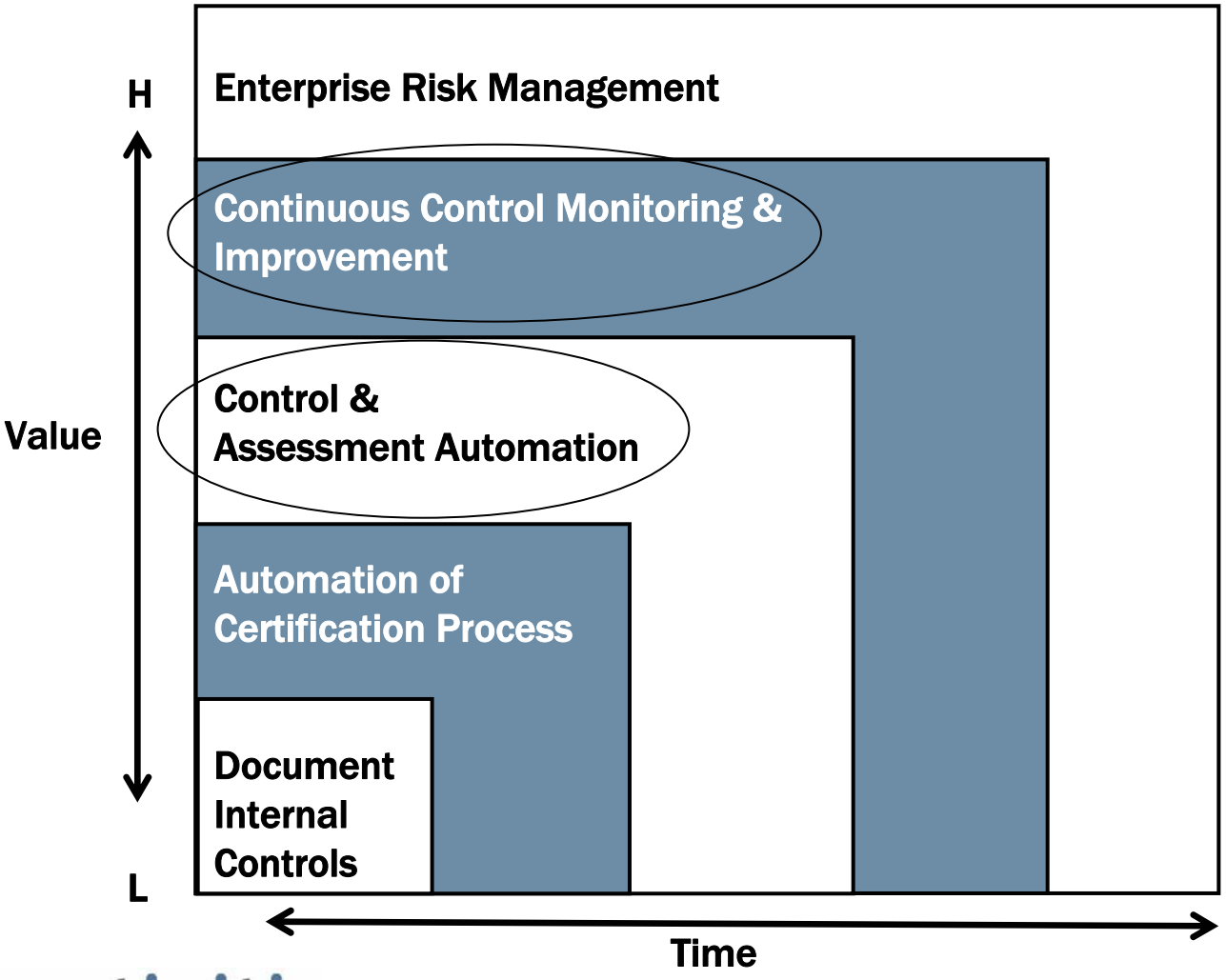




5 Lessons Learned

1. Deploy a top-down approach to focus on what's important
2. Consider qualitative and quantitative factors to implement a truly risk based approach
3. Optimize IT controls to increase the cost-effectiveness of the controls portfolio
4. Improve operational effectiveness and efficiency of upstream financial reporting processes
5. Don't wait for Washington to act

The Evolution of Compliance Technology



- Preemptive SOD conflict analysis
- Real-time transaction exception monitoring
- Master data and configuration change alerts

- Identify Systemic, Preventive controls
- Automated assessment of SOD
- Transaction analysis
- Configurable control testing

protiviti®
Independent Risk Consulting

protiviti®
Independent Risk Consulting

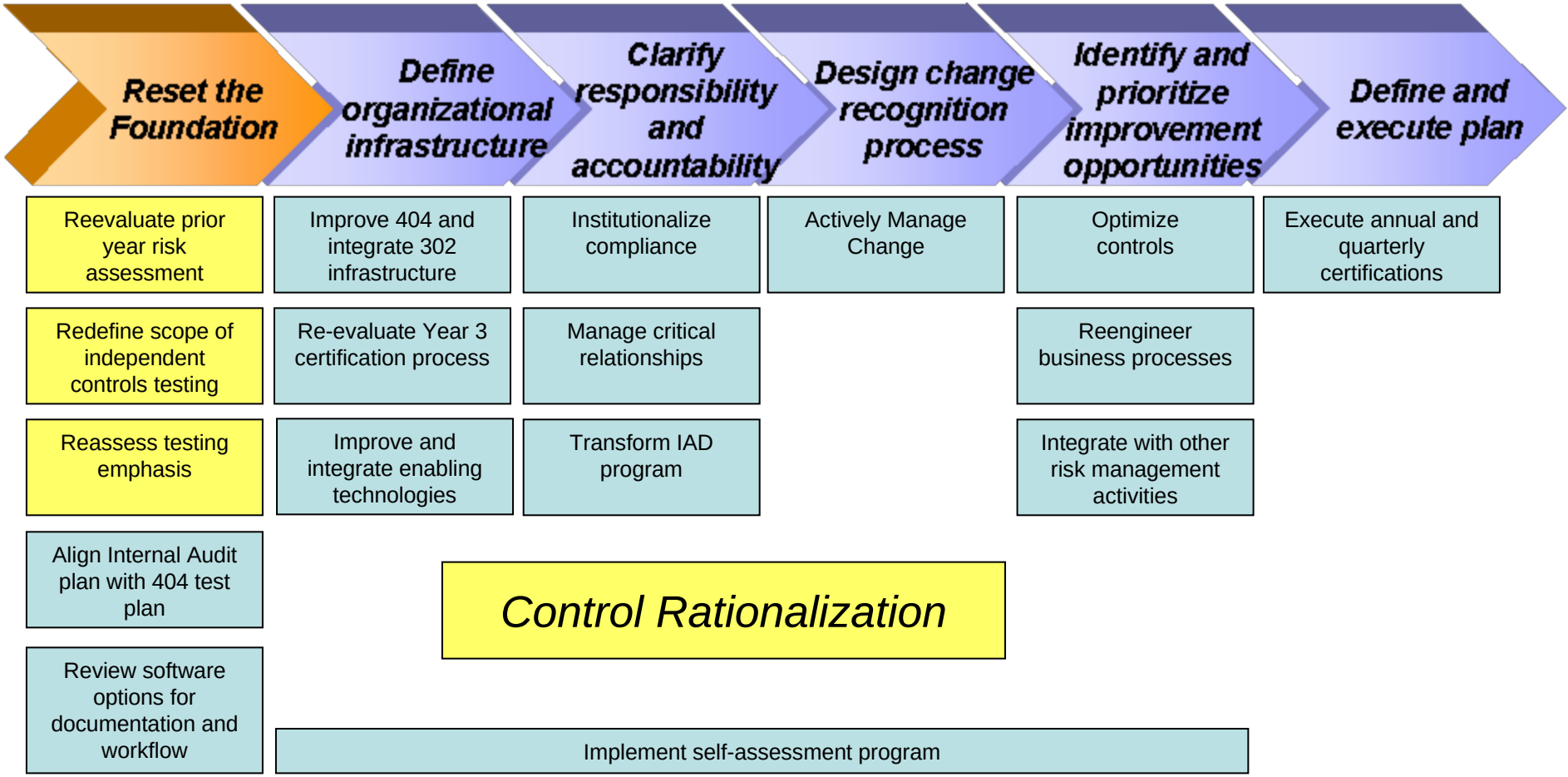
COLLABORATE08
Technology and Applications Forum for the Oracle Community

Project to Process

Business Risk | Technology Risk | Internal Audit

Our Suggested Approach to SOX Project to Process

Every Company starts in a different place but with the same objectives!



protiviti®
Independent Risk Consulting

Reduction of Processes by Location

Location	Before	After	% Reduction	Estimated Reduction by Hours
Midwestern Location 1 / Corporate	16	16	0%	0
Midwestern Location 2	11	11	0%	0
Additional Location	10	10	0%	0
European Location 1	11	10	9%	10
European Location 3	11	2	82%	240
European Location 2	11	6	45%	80
Asia Location	10	3	70%	120
TOTAL	**80**	**58**	**28%**	**450**

Estimated Time Savings from Project to Process

	Hours
Reduction from Scoping	450
Control Filtering & Optimization	500
Internal Audit Savings	1,450
Non Internal Audit Savings	3,500
Total Savings Hours	5,900
Total Dollar Savings ($150/hr)	$885,000

Q&A

Mark Nelson, Managing Director

Application Controls Effectiveness (ACE) – Oracle Practice

212-708-6333

mark.nelson@protiviti.com

www.protiviti.com