



O-ISC '07
Ohio Information Security Conference

How To Succeed With Identity Management

Juraj Siska

protiviti[®]
Independent Risk Consulting

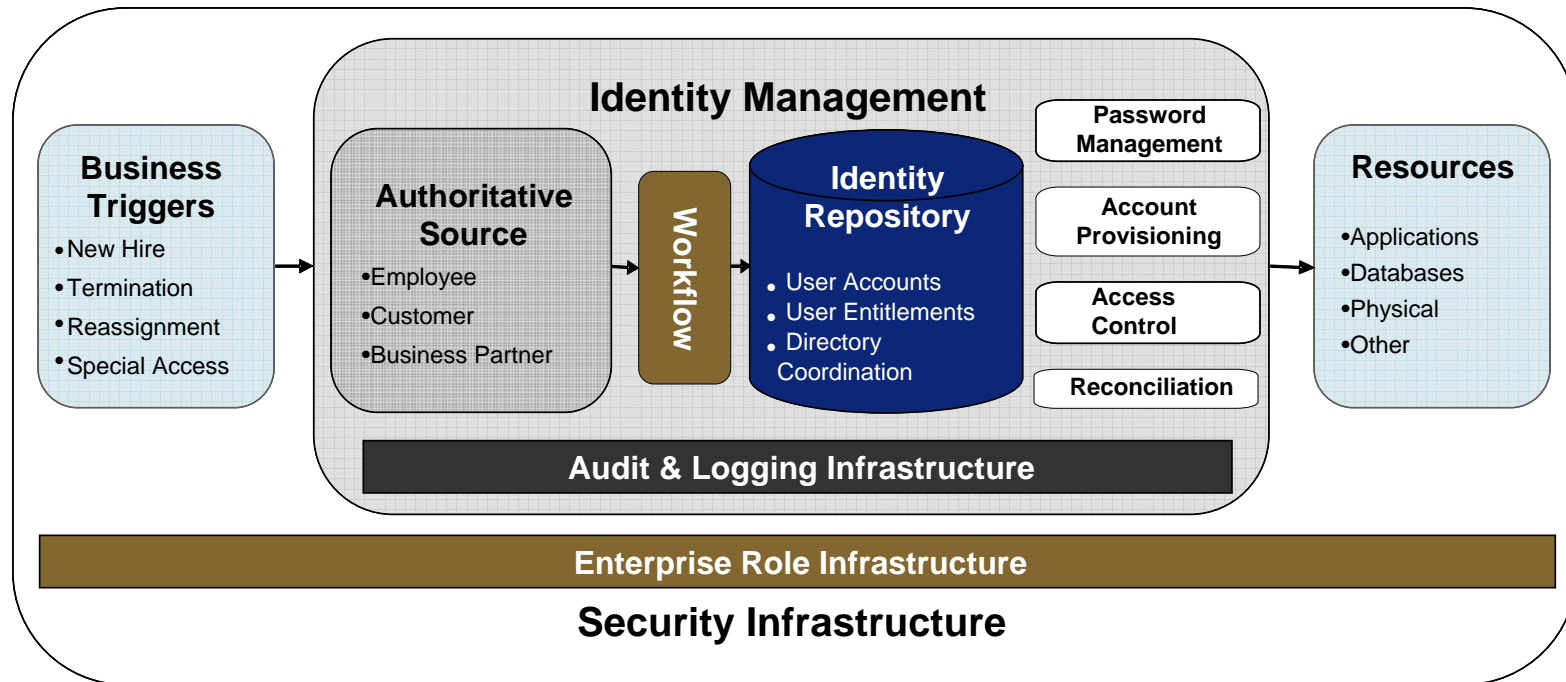
- Juraj Siska is an Associate Director in Protiviti's Technology Risk Consulting practice. Juraj has over 14 years of experience in identity management, enterprise architecture, strategy, design and technical leadership of computer systems. Proficient in using service and object oriented technologies, enterprise integration and application security. Primary business experience in the financial and insurance industries. Organizational skills in forming technology communities, shared services, promoting collaborative development, and information sharing. Management skills in software development, deployment, integration and quality assurance of enterprise wide technology systems. Vendor, contractor and outsourcing management skills. Creative and innovative thinker with exceptional analytical and decision making skills.

Agenda

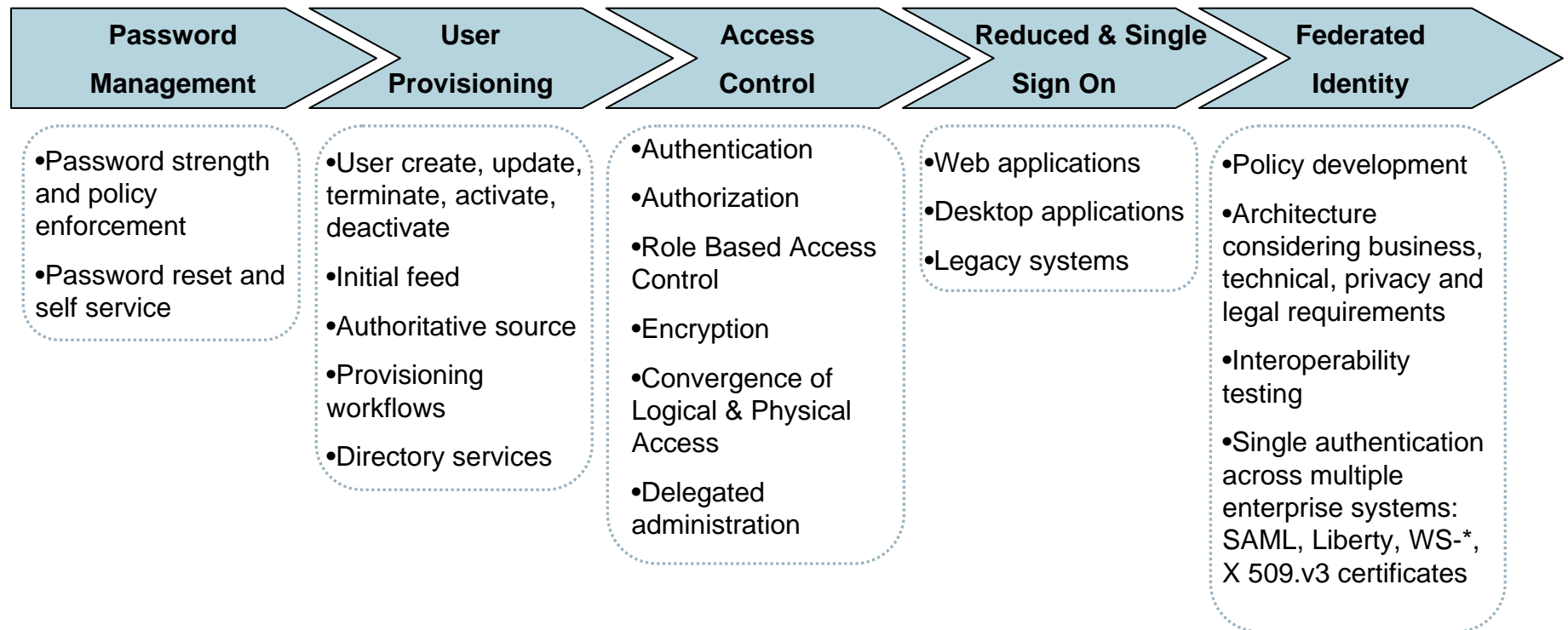
- IDM Main Components
- Sourcing IDM Risk
- Business Drivers
- Multi-factor authentication
- Five Factors of Success
- Case Study

IDM Main Components

Identity Management (IDM) facilitates and controls users' access to critical applications and resources. It promotes the notion of a holistic security environment which automates management of identities in a risk-balanced, business focused fashion.



Protiviti IDM Services



Sourcing IDM Risk

Strategy – Effective IDM roadmap, highlighting the current state and future benefits of an IDM solution and disadvantages of not implementing one. Get a buy in on the Strategy and make enough room for tactical, short term wins, without sacrificing the long term vision.

Technology – Efficient use of technology that fits the current and future (roadmap) requirements. Sufficient technical documentation that consists of architectural and design documentation might be a key from delivering a solution that will likely involve multiple in-house, local and off-shore vendor experts.

Processes – The new IDM system is likely to change existing IDM user management. Do you understand your current user management process? Do you understand the new processes and their impact? Even more importantly, does everybody else understand?

Organization – Are your C-levels in support of your IDM effort? Are they aware that you are doing it? If not, it's time to start talking before you roll out the perfect system ready to collect shelf dust. Do the key stakeholders understand and approve your new IDM processes? Are they excited? Don't forget that the word "enterprise" in the Enterprise IDM Implementation includes not only you but everybody else.

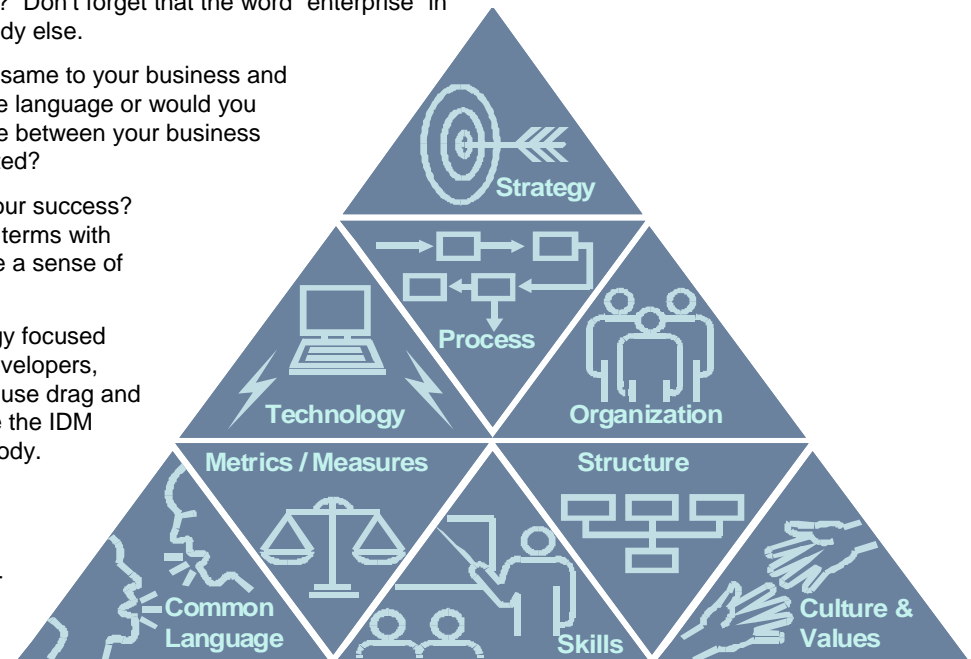
Common Language – Do terms like "user", "role", "access" mean the same to your business and technical users? Does HR and system administration share the same language or would you have to create a glossary of synonyms to bridge the continental divide between your business and technical managers. What can you tell them to make them excited?

Metrics and Measures – Can you be successful without measuring your success? Can you communicate your success to key stakeholders in their own terms with sufficient brevity? Are your measures meaningful enough to resonate a sense of urgency and the significance of your accomplishments?

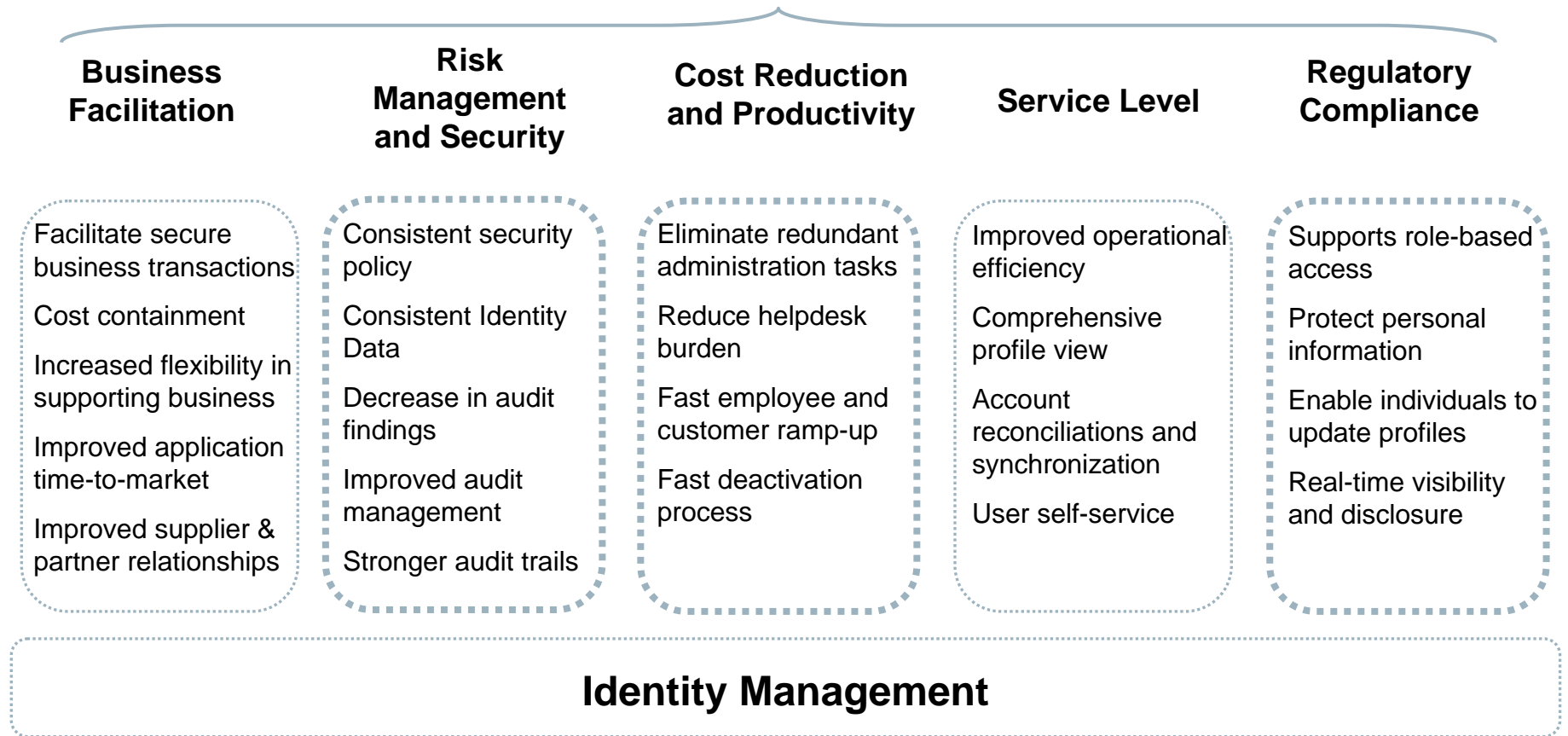
Skills – Wide variety of misconceptions around IDM skills. Technology focused companies tend to overestimate the value of architects and skilled developers, while non IT shops tend to think that IDM tools are packaged, easy to use drag and drop (MS-Visio like) tools and all that needs to be done is to convince the IDM repository owners that a centralized approach is a win-win for everybody.

Structure – Is current user account management structure conducive to the changes you are about to inflict on your enterprise? If not, will you have enough support to change it? Does an enterprise IDM solution mean that people will lose jobs or will they be able to do their existing jobs better? Make sure your metrics correspond to the generally accepted pre and post implementation organizational structure.

Culture and Values – Does this describe your organization? "We are independently minded free will entrepreneurs driven by business goals only and achieving them we will – even if we have to bend the rules". If this translates into numerous "emergency" super user requests, then your IDM development cycle is going to be longer and will require more convincing and communication.



Business Drivers





Key Business Measures

Business Facilitation

- Reduced vulnerabilities in customer facing systems
- Cost of securing new business applications
- Cost of managing business applications
- Reduced time to market
- Higher satisfaction survey score

Risk Management and Security

- Decreased amount of policy violations
- Decreased amount of audit findings
- Decreased number of ghost accounts
- Increased number of systems connected to an enterprise-wide IDM
- Consistent uid and password provisioning processes

Cost Reduction and Productivity

- Reduced number of administrators
- Reduced number of help desk calls
- Decreased time to provision user ids
- Reduced time to deactivate/terminate users

Service Level

- Reduced service calls
- Increased number of system ids tied to a person
- Reduced time to find this association
- Reduced time to synchronize repositories
- Increased number of self-service solutions

Regulatory Compliance

- Increased amount of RBAC systems
- Decreased likelihood of compromised personal information
- Shortened audit cycle
- Reduced time to provide audit visibility and disclosure

SOX Linkage to Identity Management



O-ISC '07
Ohio Information Security Conference

Mapping Selected CobiT Objectives to Identity Management

Key CobiT Objectives

	<i>Access Management</i>	<i>Role Based Access Control</i>	<i>Administration</i>	<i>Provisioning</i>	<i>Identity Repository</i>
DS5 Ensure Systems Security	✓	✓	✓	✓	✓
Management of Security Measures	✓		✓	✓	✓
Identification, Authentication and Access	✓	✓	✓	✓	
Security of Online Access To Data	✓	✓		✓	✓
User Account Management		✓	✓	✓	✓
Management Review of User Accounts	✓		✓	✓	✓
User Control of User Accounts		✓	✓		
Security Surveillance	✓			✓	
Central identification and Access Rights Mgt		✓		✓	✓
Violation and Security Activity Reports	✓			✓	✓
M2 Monitor the Processes	✓		✓	✓	

Multi-factor Authentication

Authentication Method	Security	Cost	Portability	Usability
Password, Passphrase	2	10	9	6
Virtual Keyboard	4	8	5	5
Grid Cards	5	9	8	5
One Time Password	10	4	4	5
Smart Card	8	4	4	4
Out of Band	6	3	7	6
Biometric	6	3	4	9
TAD*	8	4	10	10

*TAD – Transaction Anomaly Detection
 Scoring: 10 Best, 1 Worst

Safe	Affordable	Portable	Usable
------	------------	----------	--------

Five Factors of Success

Executive
Sponsorship

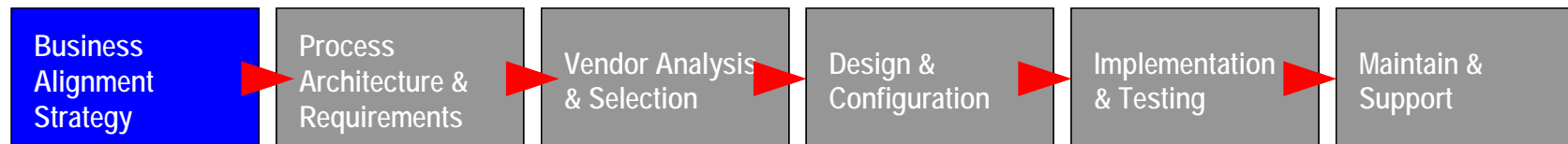
Enterprise-
wide
Socialization

Enterprise-
Level
Architecture

Effective
Project
Management

Execution
Excellence

Five Factors of Success
"Five Es"

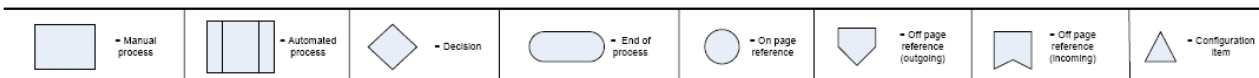
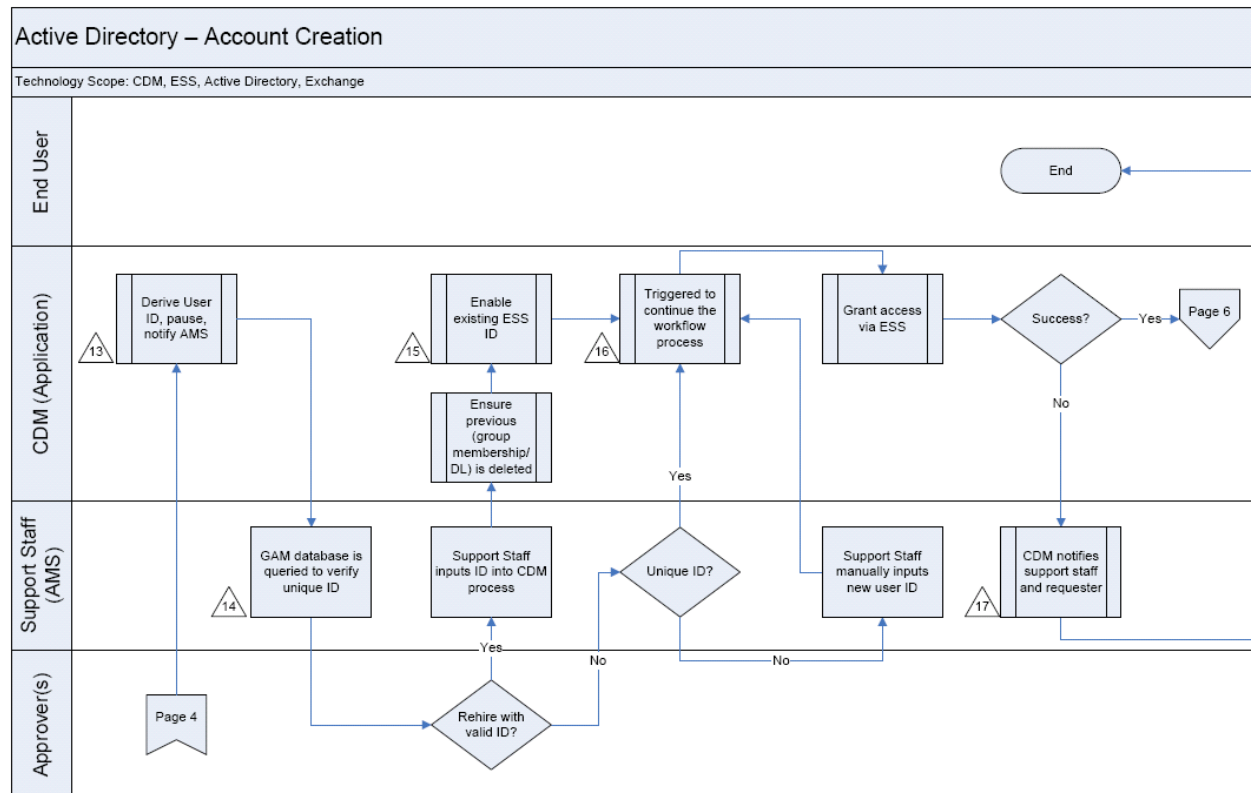
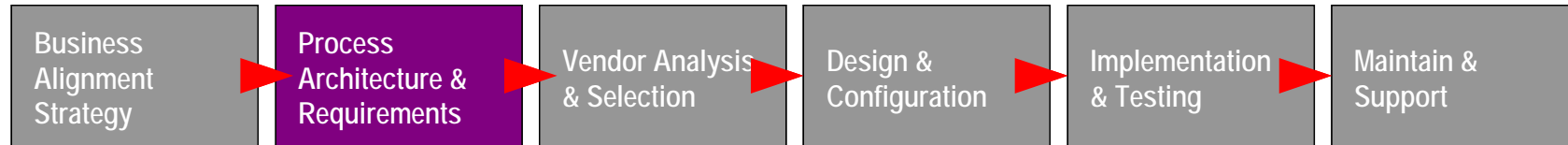


- Password management and automated user provisioning to the following repositories
 - AD 7000 users
 - 200 Unix servers
 - Exchange 7000 users, round robin mail server distribution
- Streamlining provisioning and user reconciliation between authoritative sources (PeopleSoft, MicroJ) and managed repositories

Robert Half International Case Study



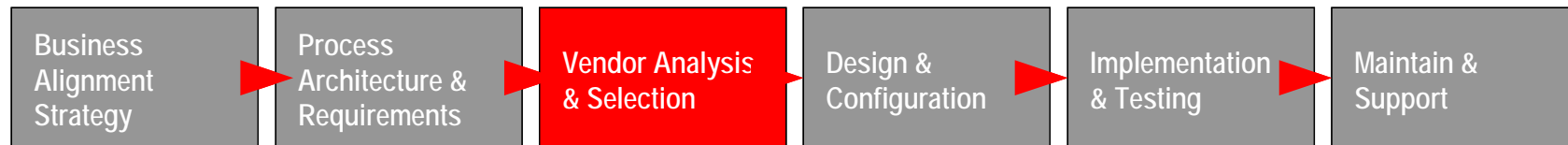
O-ISC '07
Ohio Information Security Conference



Robert Half International Case Study



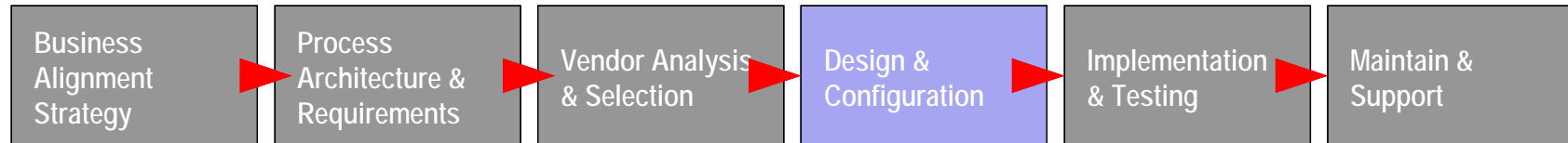
O-ISC '07
Ohio Information Security Conference



protiviti[™]
Independent Risk Consulting

Vendor Selection Tool

Infrastructure Category	Requirement	Solutoin 1	Solution 2	Weight Factor
Interface	Flexibility to add application and resources into the user interface as applications are added to the solution.	2.67	2.00	100%
Interface	Flexibility to add application and resources into the system interface as applications are added to the solution.	2.67	2.00	100%
Interface	For system administrators, provisioned activities should be searchable by request number, attributes, name, and date.	2.67	2.00	100%
Interface	At the user interface level, all denials must have comments added by the denier. Comments will be sent in the notifications of the denial.	2.00	2.00	100%
Interface	Has the flexibility to present resources with unique graphical icons and descriptions.	2.00	0.00	75%
Interface	A web-based GUI for system administration.	1.50	0.00	50%
Interface	A web-based GUI for configuration of business rules and workflow.	1.50	0.83	50%
Provisioning	Ability to run system compare between user stores and provision systems.	2.00	1.50	75%



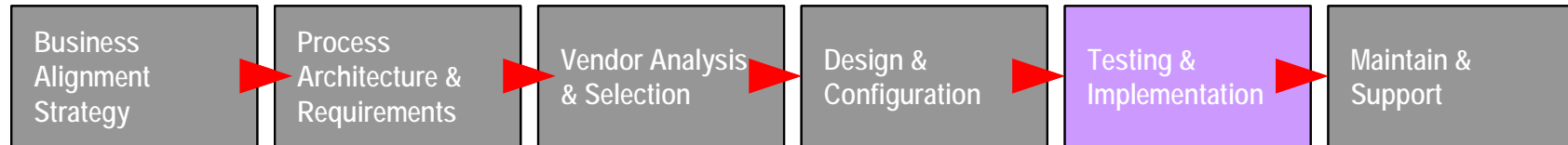
■ Architecture and code level design

- Logical
- Physical
- Configuration management

■ Authoritative source

■ Initial Feed and HR Synchronization

■ Reporting

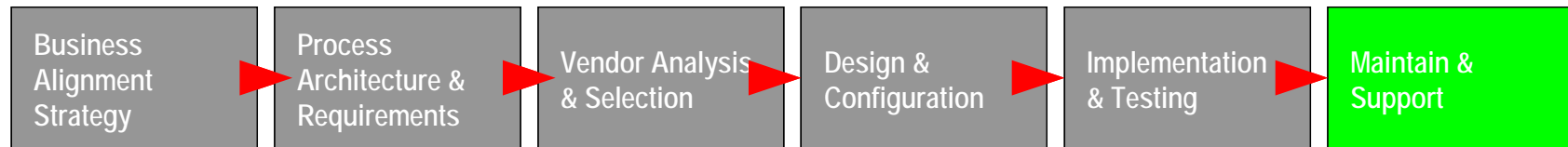


■ Implementation

- Your own staff
- Partner with experts
- Incorporate hand over tasks in the project plan (documentation, team work)

■ Testing

- Unit
- Integration
- Performance
- User Acceptance



- Deployment documentation
- Rollout plan
- Pilot phase
- Training and support

About Protiviti

Protiviti serves more than:

- 35% of all Fortune 100 companies
- 25% of all Fortune 500 companies
- 20% of all Fortune 1000 companies
- 1,200 clients around the world

We generate revenue at an annual rate of more than \$550 million.

Protiviti deploys nearly 2,900 professionals worldwide.

Protiviti fits strategically on the continuum of services provided by Robert Half International Inc., a \$6 billion NYSE company based in Menlo Park:



Recruiting



Specialized Staffing



Project Skills



Project Management



Our thought leadership in corporate governance, technology risk measurement, and internal audit is published globally.



Protiviti has more than 50 offices worldwide, including locations in London, Paris, Milan, Frankfurt, Tokyo, Melbourne, Sydney, Shanghai, Beijing, Hong Kong and Mexico City. Our international network of offices continues to grow...

PROTIVITI
*PROTIVITI ALLIANCE



Questions & Answers