protiviti
Independent Risk Consulting

Application Control Effectiveness for SAP

December 2007

Meeting Objectives

protiviti
Independent Risk Consulting

- Application Control Effectiveness
  - Compliance at a glance
  - Trends and challenges
  - Technology issues
- Application Control Business Drivers
  - Key risks
  - Evolution of compliance technology
  - Key observations
  - Technology's role
- Automated Controls
  - Control optimization value proposition
  - End to end compliance
- Tool Overview
  - Issues
  - Success factors
- Questions

Application Control Effectiveness

protiviti
Independent Risk Consulting

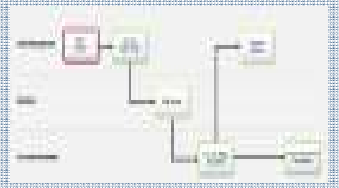
- Most companies are anxious for business unit managers to assume accountability for Sarbanes-Oxley compliance.
  - Yet, they also realize the biggest pain points in the compliance process — and the biggest opportunities for achieving savings and greater efficiency — lie not in better documentation, but in optimizing the control environment.
  - Which will lead to efficiencies in:
    - Control Testing…
    - Activity Monitoring…
    - Remediation and / or mitigation of issues…
- Companies are looking for an automated, process-driven environment to streamline security change management, improve the effectiveness of administrators, and prevent control and compliance issues from entering SAP environments
- Application control solutions enable organizations using SAP to streamline audits, reduce exposure to fraud, increase security administrator productivity, and reduce the cost of regulatory compliance

Compliance Process Flow At-a-Glance

protiviti
Independent Risk Consulting

Compliance Team & Business Process Owners

Define Control Environment



- Document entities, business processes, sub-processes, objectives, risks, controls, financial accounts
- Create hierarchies
- Define *manual* control test instructions
- Define *automated* control tests (Process Controls)

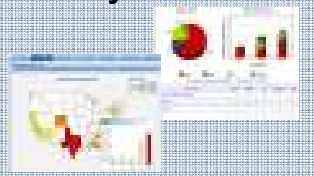
Control Testers & Internal Audit

Perform Control Activities

- Receive test instructions and perform control testing (people perform)
- Attach spreadsheet-based analyses and other evidence of controls operating effectively
- Automatically test process controls (system performs)

Managers & Business Process Owners

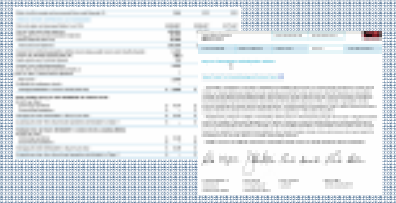
Identify & Resolve Violations from Manual & Automated Control Tests



- Monitor control activities and segregation of duties
- Identify violations
- Assign and approve remediation work

Executives & External Auditors

Report Financial Results



- Audit controls and financial accounts
- Attest to control effectiveness
- Report to regulatory agencies

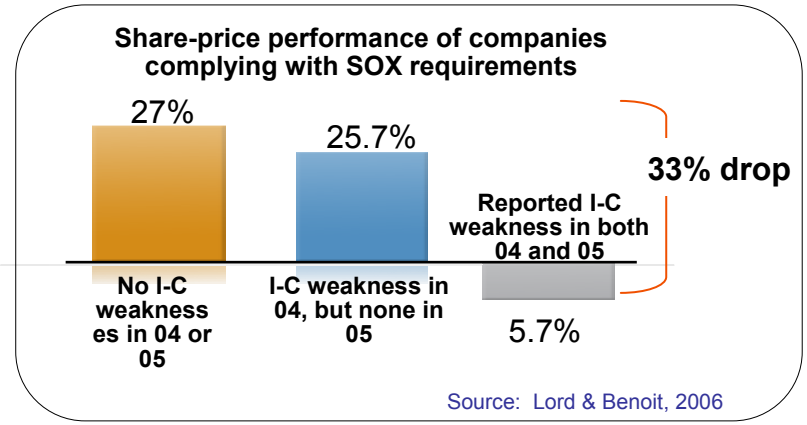
Trends and Challenges in Compliance

Increasing complexity, higher stakes, fewer resources

protiviti℠ Independent Risk Consulting

Increasing complexity of global compliance regulations

Higher stakes and proven impact on company bottom lines



Source: Lord & Benoit, 2006

Struggle to find qualified resources, compliant processes, and financial systems

Weakness	Companies Reporting	Percent Of Cos.
Personnel	166	41.5%
Taxes	132	33.0%
Financial Procedures *	106	26.5%
Documentation	67	16.8%
Revenue Recognition	58	14.5%
IT, Financial Systems	52	13.0%
Hedge Accounting	28	7.0%
Cash Flows	27	6.8%
Tone at Top	20	5.0%
Lease Accounting	18	4.5%
Vendor Contracts	14	3.5%

Source: Compliance Week, 2006

Growing imperative to achieve process-oriented improvements and automation

Year One

- **Comply at whatever cost**

Year Two

- **Focus on cost reduction and control rationalization**

Year Three and Beyond

- **Automate to reduce burden**

Source: AMR Research, 2006

Application Control Business Drivers

protiviti
Independent Risk Consulting

- **Sarbanes-Oxley Act (SOA) and Other External Pressures**
- **Cost Constraints**
- **Upgrades and Enhancements**
  - **Move to upgrade SAP 4.6 / 4.7 to ECC 5.0 or 6.0**
  - **Implementation of a continuous monitoring solution**
  - **Activation of configurable controls within SAP**
  - **SAP security changes**
  - **Interfaces and integration points**
- **Business Effectiveness**
  - **Reduction in audit and SOX compliance related fees**
  - **Reduced system maintenance costs**
  - **Lowered reporting costs**

Key Risks To Be Considered

protiviti
Independent Risk Consulting

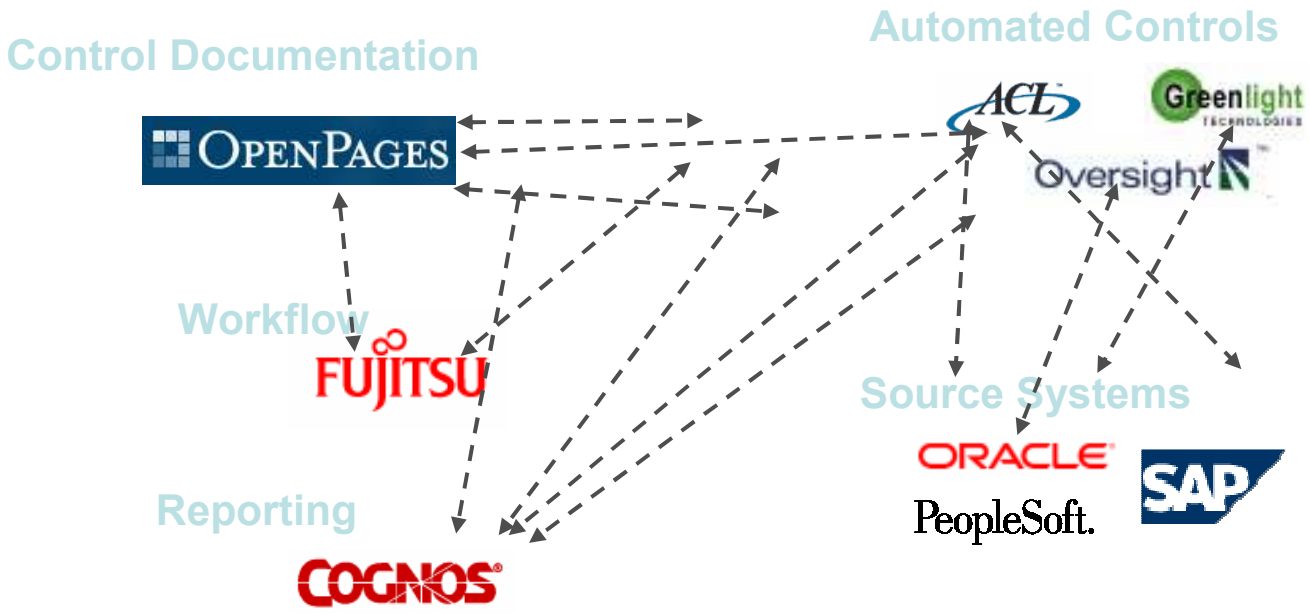
- **Customization & Configuration**
  - What are the SAP configuration options?
  - Does the current configuration really meet the business requirements?
  - Can SAP configuration be relied upon for SOX compliance?
  - How does system configuration impact the security solution?
- **Interfaces & Integration**
  - How many integration points are there?
  - What information is being passed between systems?
- **User Access Administration and Segregation of Duties**
  - How is user access and Segregation of Duties managed?
  - Is there a continuous monitoring solution in place?
    - If so, how is it integrated into compliance?
    - What is the process for the review and resolution of identified conflicts?
- **Different User Communities**
  - Do Business Owners and IT staff have different priorities?
  - Do the business owners understand the technology they are working with?
  - Is the IT organization looking for optimization opportunities?

Piece-meal Technology Creates Problems

Higher costs, incomplete visibility, integration issues

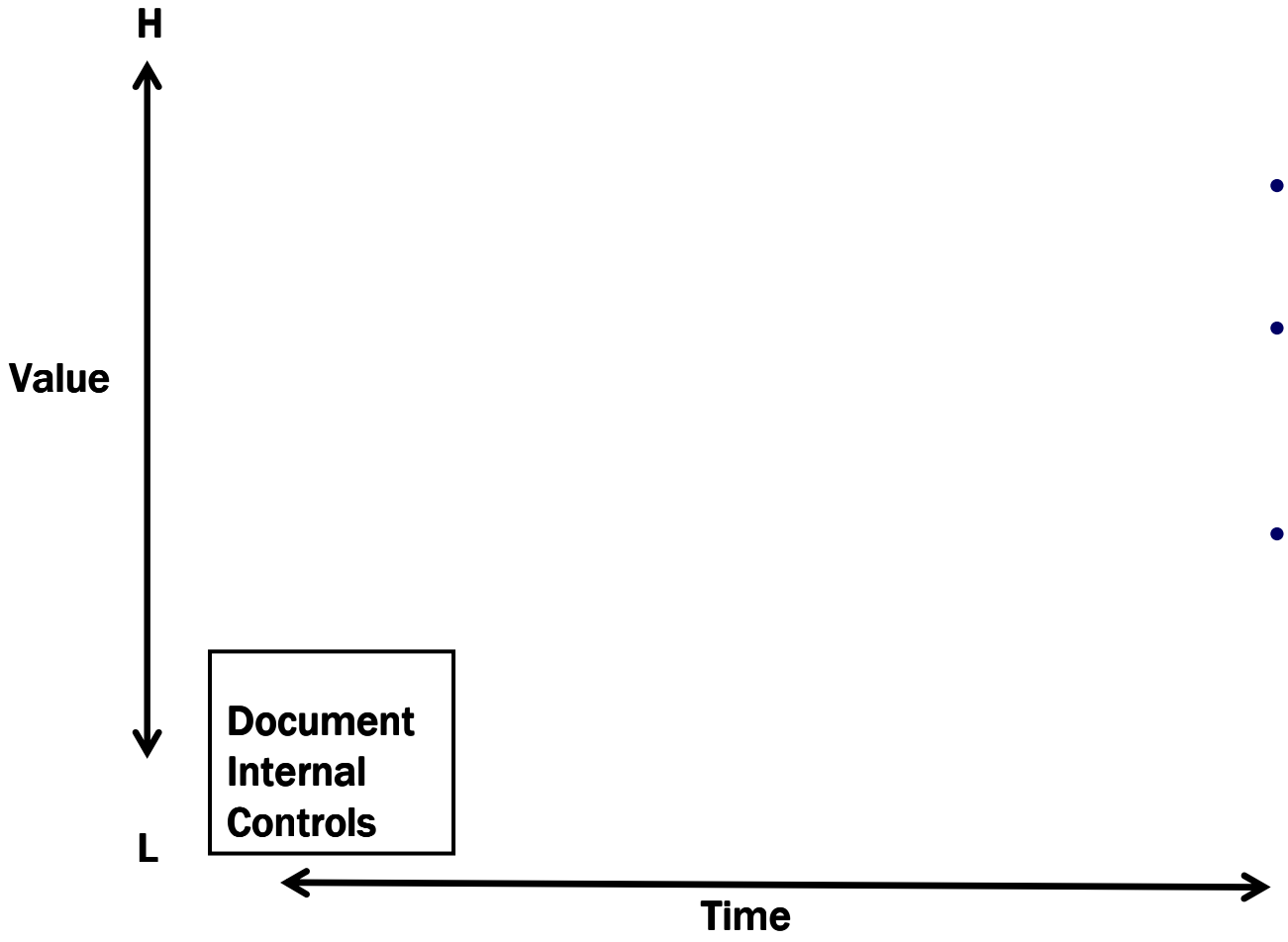
protiviti
Independent Risk Consulting

Complicated Compliance



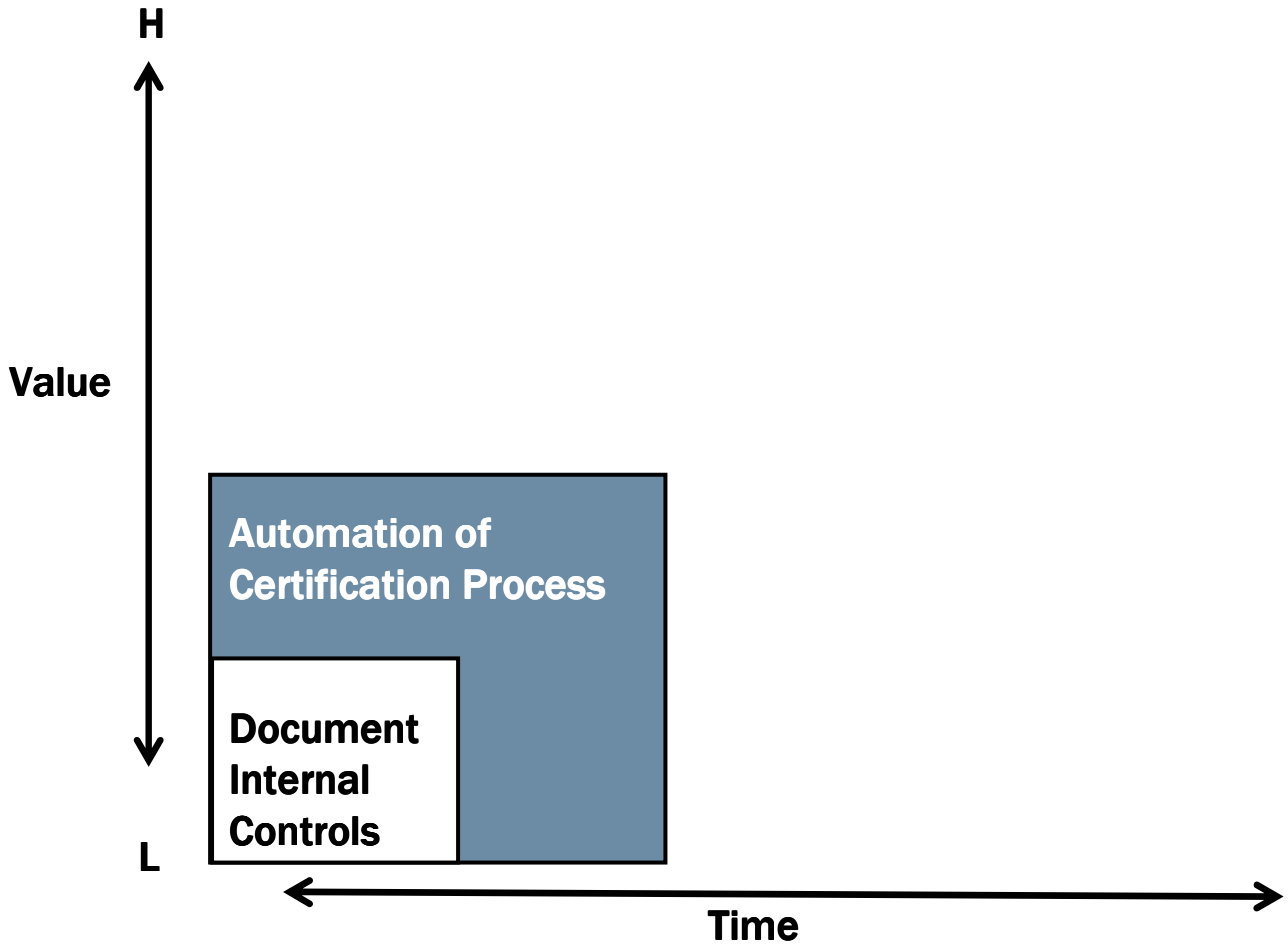
- **Many points of costly custom integration**
- **Lacks flexibility and auditability for evolving requirements**
- **Limited visibility – too many systems and hand-offs**

The Evolution of Compliance Technology



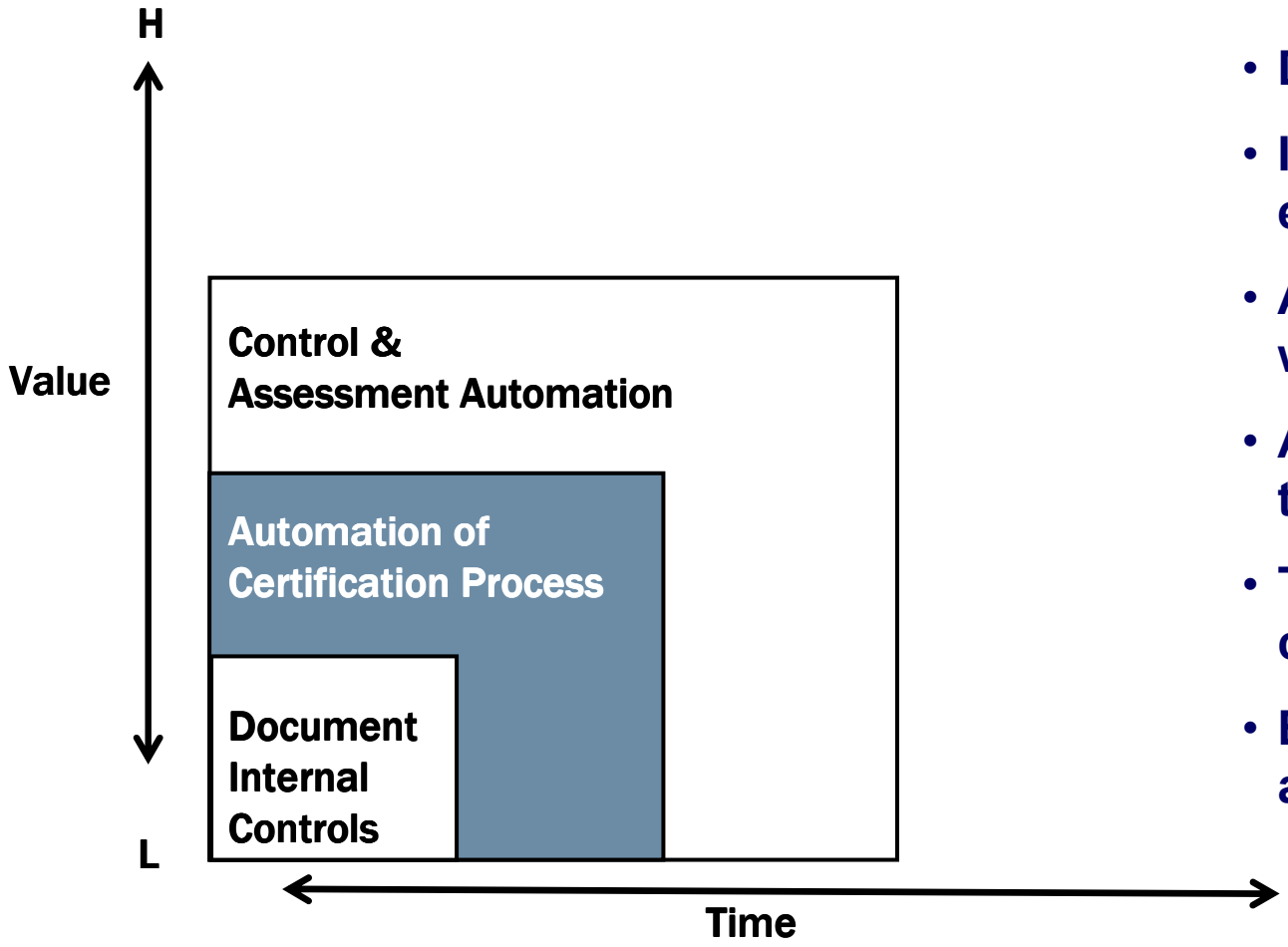
- **Enterprise content and document management**
- **Status updates and dashboards**
- **Multi-dimensional drill-down capability**
- **Archiving and rollback**

The Evolution of Compliance Technology



- Control Owner Updates
- 302 cascading certification
- Control self – assessment
- Routine risk assessment

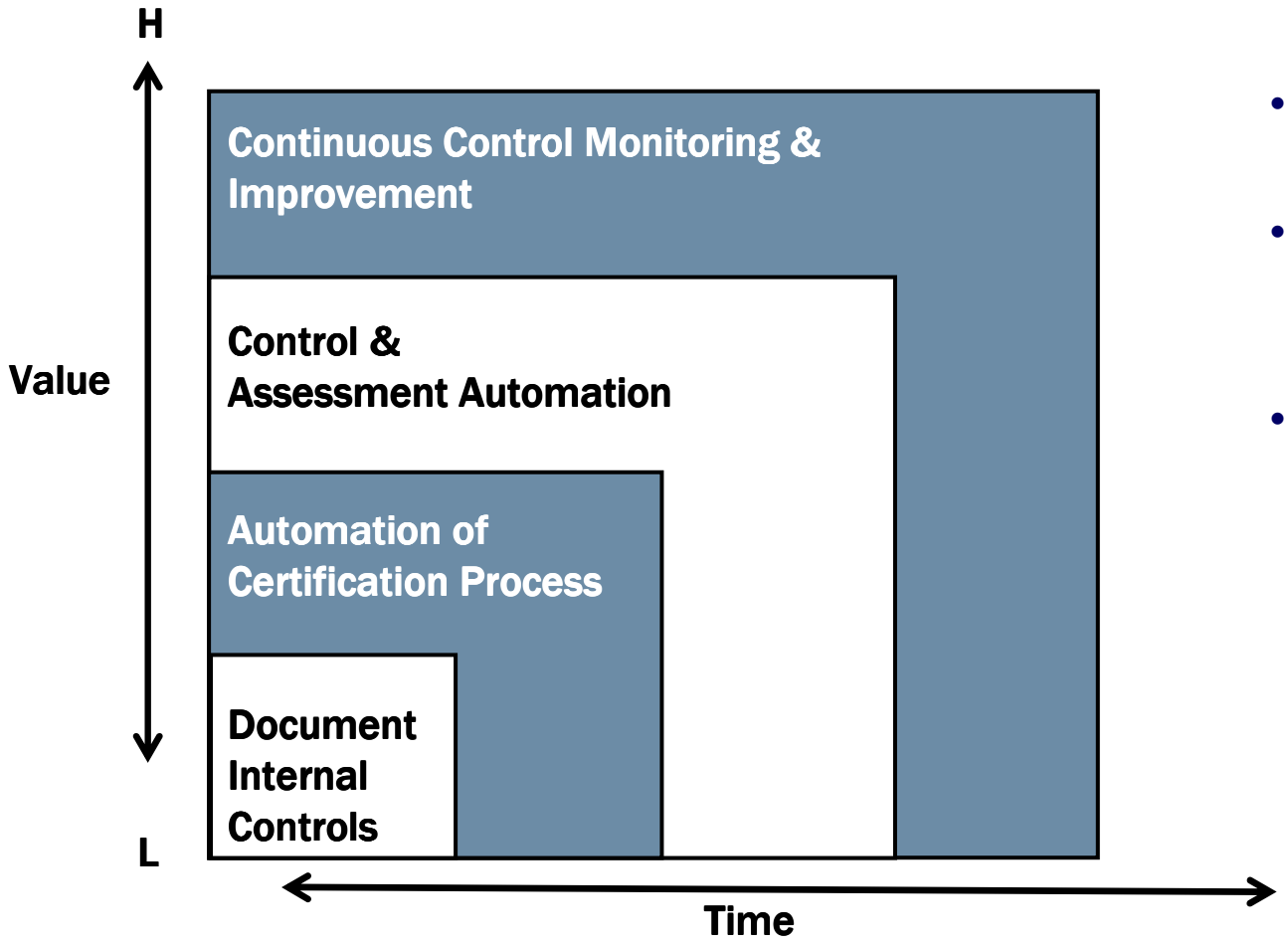
The Evolution of Compliance Technology



- Manual → Auto/System
- Detect → Prevent
- Improved system-enforced SOD
- Automation of access workflow and approval
- Analysis of system transactions
- Testing of process configurable controls
- Enhanced reporting and Analysis Tools

The Evolution of Compliance Technology

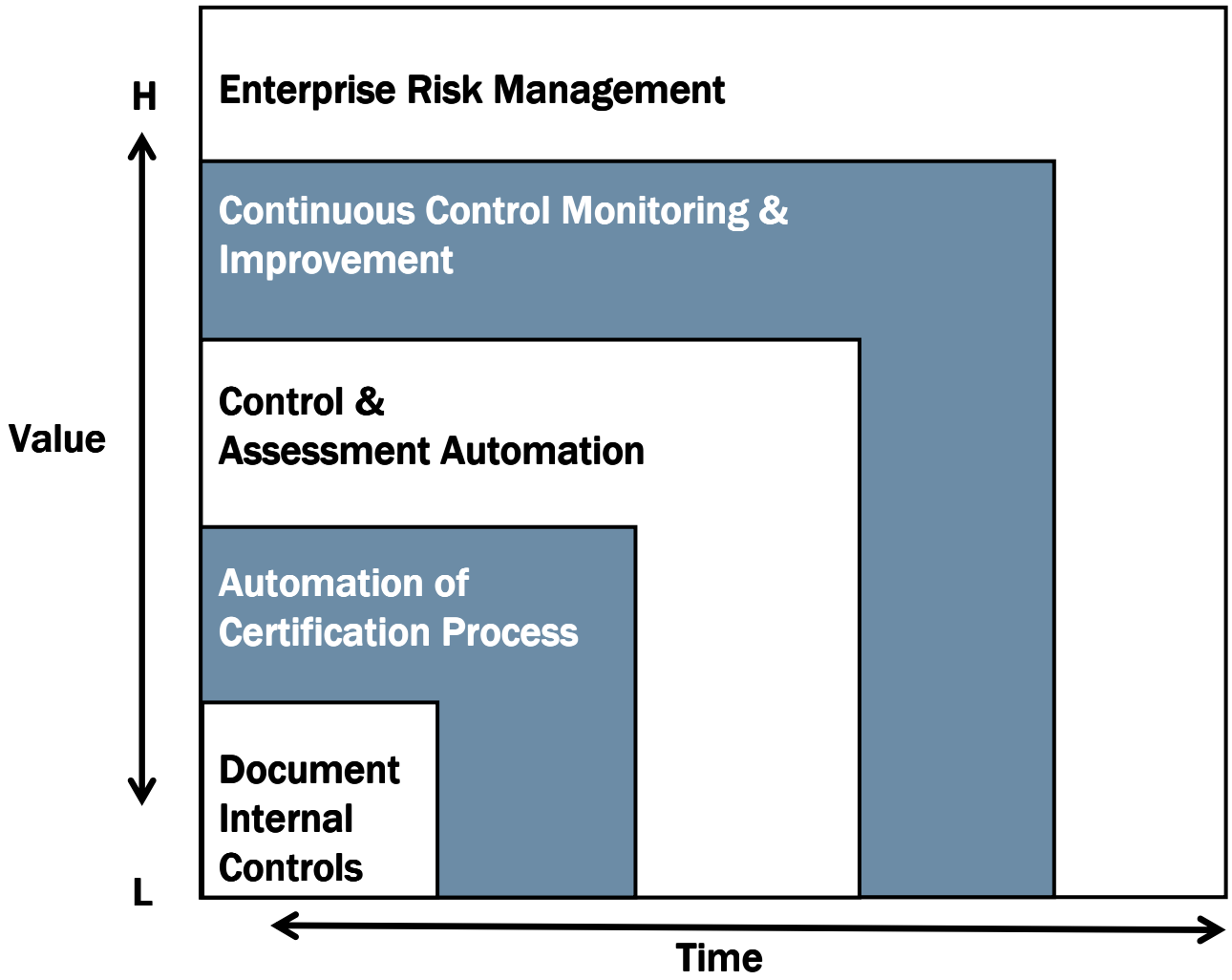
protiviti
Independent Risk Consulting



- **Preemptive SOD conflict analysis**
- **Real-time transaction exception monitoring**
- **Alerts to master data and process control changes**
- **Continuous system-wide monitoring**

The Evolution of Compliance Technology

protiviti
Independent Risk Consulting



- Integration of compliance frameworks, tools and data
- Portal access to personalized risk management information
- Proactive risk identification and evaluation

Key Observations

protiviti
Independent Risk Consulting

- **Prior year testing and conclusions may have been inaccurate** due to the inherent limitations of manual testing of sophisticated applications.
- External audit firms appear to be preparing for deployment of sophisticated application analysis tools as a part of **future audits/404 assessments**.
- Attain and Maintain processes *could* be used to **shift the focus** away from detailed application testing and onto the tools and rule sets used to monitor the applications.
- Analysis requires **detailed knowledge** of application, SOX compliance requirements, and unique business processes (e.g. business owner knowledge).

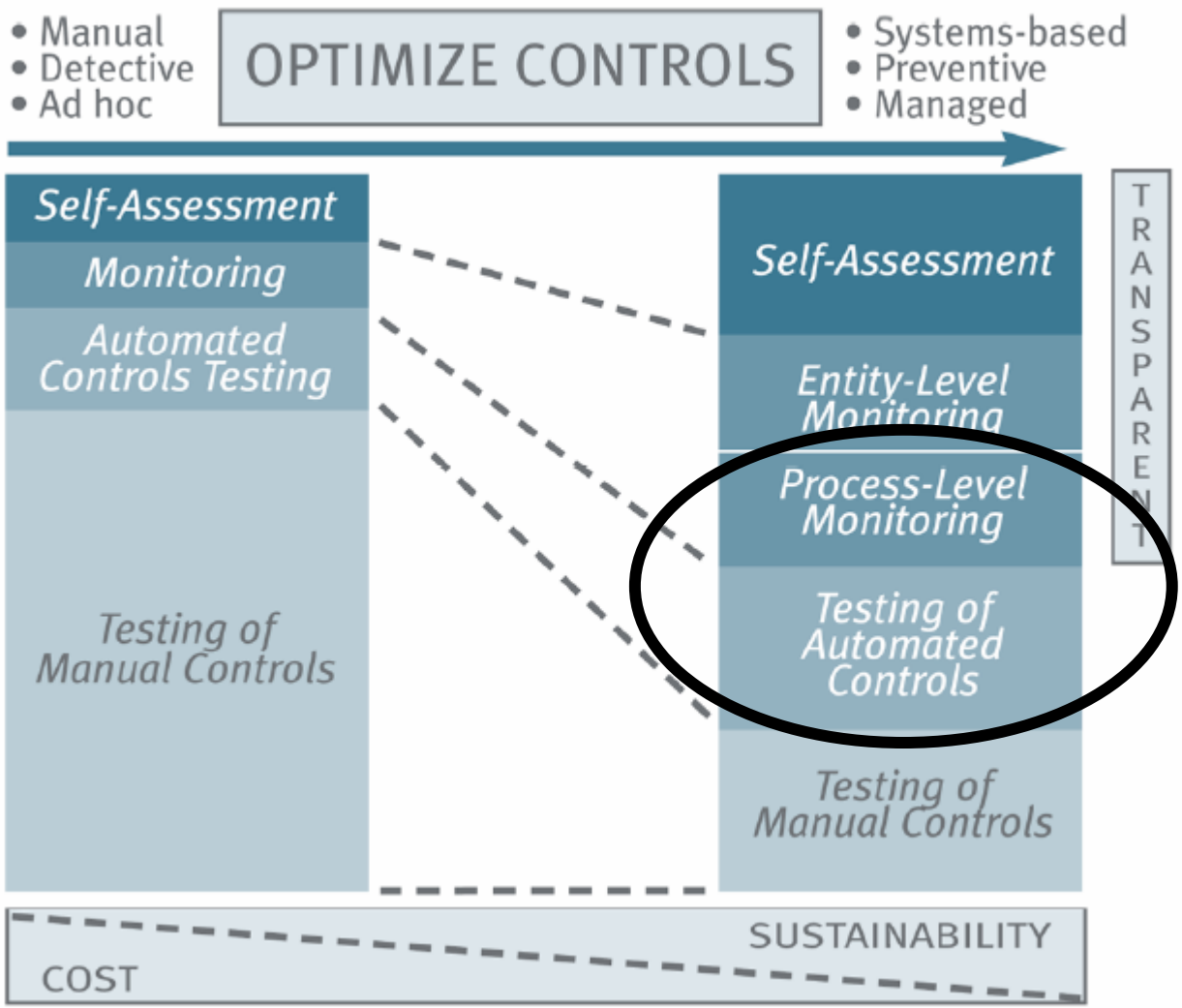
Application and Technology's Role

protiviti
Independent Risk Consulting

- The role of technology or automation in application control effectiveness can be broken down into two parallel tracks:
  - Automation of the internal control environment
  - Automation of the compliance process
- Sustainability, reduction in costs, and improved value to the organization require advances in **both**.
- Significant advances can be made for many companies through better leverage of already acquired applications and tools.

Key to Cost-Effectiveness: Balancing the Sources of Evidence

protiviti
Independent Risk Consulting



Automated Controls

protiviti
Independent Risk Consulting

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**

Control Optimization Value Proposition

protiviti
Independent Risk Consulting

By increasing reliance on automated controls in their ERP environment, companies will:

- **Decrease time spent conducting tedious manual controls**. Time saved through automation frees control owners to focus on more strategic matters.
- **Decrease time necessary to complete SOX management testing**. An automated control takes approximately 75% less time to test than a manual control.
  - How so? Manual controls require an inspection of each sample occurrence, often embedded in reams of paper, verses a one-time observation of a configuration setting. Also, remediation testing of a manual control requires additional sample time to accrue verses real-time resolution and retest of online controls. These savings can quickly add up.
- **Leverage enhancements to manage external audit fees**. The same principles for internal test savings apply to external test hours.
- **Increase the effectiveness of the internal control environment**. Automated controls decrease the opportunity for human error and manipulation. Real-time prevention also presents a much safer and efficient mechanism than downstream detection.
- **Decrease time performing detailed reviews**. If change management procedures are strong and user access is restricted, controls such as error checks and tolerances can reduce the need for detailed management monitoring.
- **Increase operating efficiency**. Taking advantage of certain functionality such as workflow can decrease transaction cycle times, while ensuring that necessary approvals are obtained consistently according to policy.

Control Optimization Value Proposition

protiviti
Independent Risk Consulting

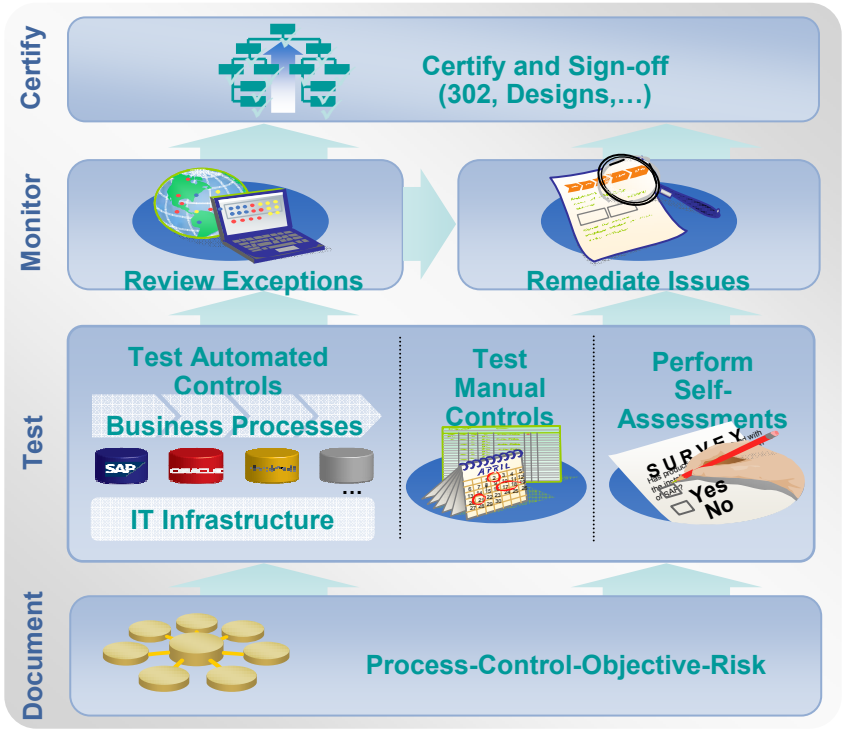
By addressing segregation of duty (SOD) and ERP security matters with methodical and sustainable solutions, your client will:

- **Limit the wildcard of segregation of duties as a potential for Material Weakness**. A number of the corporate 404 disclosures in 2004 dealt with poorly enforced segregation of duties. In addition, we have observed that in 2005, external auditors and audit committees are placing a much greater emphasis on incompatible duties and super-user access.
- **Certify with confidence**. The biggest challenge for companies who haven't initiated a study of this type is that certifiers don't know for sure that their information assets are properly protected.
- **Strengthen the program of fraud prevention and deterrence**. Traditional forensic analysis can be reduced and confidence increased if opportunities for manipulation and misappropriation are cut off at the source through good security.
- **Stream-line security maintenance**. Using sound architectures and new available tools, companies can increase the efficiency and effectiveness of profile management practices.

The Way Forward: End-to-End Compliance Process Management

protiviti
Independent Risk Consulting

Integrated Compliance



- **One system for end-to-end financial compliance process**
- **Flexible, configurable set-up with complete audit trails**
- **Enterprise-wide visibility into risks and controls**

How Optimized Is Your Control Environment?

protiviti
Independent Risk Consulting

Source: adapted from Carnegie Mellon University Capability Maturity Model

Tool Overview

protiviti
Independent Risk Consulting

- Many companies lean strongly to one solution or the other based on their biases and key requirements. Few companies run exhaustive selection processes.
- The features / functions of each are evolving quickly and it is important to separate the vendors "vision" from current reality.
- Vendors tend to sell their products as a rapidly implemented "silver bullet". They tend to gloss over the realities of configuring business rules, implementation, training, and planning for the remediation needs you may discover once the tool is operational.
- ERP Compliance tools assist management in:
  - Identifying and documenting controls related to sensitive SAP transactions and Segregation of Duties (SOD)
  - Manage control violations – redefine controls, remediate, or mitigate
- Tools such as Approva or Virsa would allow for streamlined operations by automating the environments (e.g. SAP and non-SAP) for continuous effectiveness by:
  - Preventing new violations from entering system
  - Ensuring proper change management and building an audit trail
  - Continuous monitoring of violations and exceptions
  - Sustain ongoing compliance
- The product would also leverage and improve business processes by building process efficiency improvements into the compliance process

Alliance Partner Tools - SAP

protiviti
Independent Risk Consulting

SAP GRC (Virsa)

- Access Control Suite
  - Compliance Calibrator
  - Access Enforcer
  - Role Expert
  - Firefighter
- Control Design and Documentation
- Process Controls
  - Procure to Pay
  - Order to Cash
  - Reconcile to Report
  - IT Controls

Approva (BizRights)

approva

- Application Control Suite
  - Authorizations
  - User Activity
  - Access Management
- Process Control Suite
  - Procure to Pay
  - Order to Cash
  - Financial Close
  - Payroll
- Platform
  - Adapters
  - SDK
  - Open Controls Framework

Common Issues During Implementation

protiviti
Independent Risk Consulting

Common Issues	Recommended Approach
• Implementing Approva or Virsa is not a technology project…	…Effective implementation requires Business Process Owner support to design, respond to exceptions, and build into on-going processes
• Rulebooks do not reflect business rules / controls…	…Understand business rules, information requirements before configuring Rulebooks
• Process infrastructure not defined or considered…	…Approva/Virsa implementation requires the definition of processes, procedures or guidelines to use, own and maintain the application
• Approva/Virsa not synchronized with SOX control and testing strategy…	…Understand SOX requirements prior to configuring the Rulebooks and link to SOX control objectives
• Key owners, potential users, Internal Audit and SOX Leaders not involved in design & implementation phases…	…Owners, users, internal audit and SOX leadership should be part of design & implementation activities to ensure best possible decisions are made for the entire company

Key Success Factors

protiviti
Independent Risk Consulting

- The goal should be that, upon go –live, **no exceptions** exist when considering compensating controls, and that existing change management and security administration processes are designed to keep it this way

- Attain ===> Maintain

- The presence of one or more of the following factors has been/can be the cause an implementation failure or reduction in ROI:

  - ✓ Lack of a long-term vision for the implementation and use of the product
  - ✓ All teams (e.g. SOX, IA, Business, IT) are not communicating or working effectively together
  - ✓ The underlying SAP change management and security administration processes are not effective, which should include approval of business rules
  - ✓ The profiles and access rights in SAP are not reviewed for propriety based upon business process owner needs and segregation of duties conflicts
  - ✓ The product itself is not configured correctly to ensure accurate identification of true issues vs. false positives.
  - ✓ Product configuration and rule sets are not customized to the specific needs of the business and risk profile of the company
  - ✓ Ownership of SAP security and the responsibility for managing the software and the results are given to those that do not understand SAP security or segregation of duties concepts.

Questions?

Bob Brett
Associate Director
Direct: 216.696.6094
E-mail: robert.brett@protiviti.com

Brian Smith
Associate Director
Direct: 216.696.6067
E-mail: brian.smith@protiviti.com