



Ohio Information Security Conference '08

Security Considerations when implementing ERP systems

William Lovell
KPMG Advisory Services

Speaker Biography



- Manager in KPMG's Advisory Services practice in Columbus, OH.
- Focus on assessing the design and operating effectiveness of IT controls within both the infrastructure and application layers of the IT stack.



- Focus on security issues and considerations when implementing ERP systems to address:
 - Why think about this ahead of time?
 - How do you get to a high security level in your ERP?

WHY?

- Why think about ERP security before implementation begins?
 - Time and Budget
 - Compliance with regulations
 - Protection of sensitive information

- Time & Budget consequences
 - Companies spend millions when implementing an ERP
 - Improve workflow
 - Reduce costs
 - Security controls implemented at the end
 - These controls get glossed over
 - Project overruns and potentially create an “unstable foundation”

■ Compliance & Regulations

- ERPs are part of many types of audits
 - Federal/State Regulations
 - Corporate Internal Audit
 - Corporate Security
 - Subject Matter Professionals
- Included in audits for
 - SOX, HIPPA, Basel II, PCI, 21 CFR Part 11
 - Information Security Standards (COBIT, COSO, ITIL, IS27001)

■ Protection of Sensitive Information

- ERPs are abundant with sensitive information
 - Protect both legally and business-wise
- Challenge is identifying those who “need to know”
- Potential for real financial loss comes from insiders who abuse system privileges

How do you get there?

- How do you get to a high security level in your ERP?
 - Develop and document info security policies & procedures
 - Sets the stage for ERP security design
 - Develop a detailed design of a secure ERP environment
 - Authentication
 - Authorization
 - Administration
 - Infrastructure hardening
 - Monitoring
 - Training



■ Authentication

- ERP security starts with user-based controls
 - Unique ids
 - Strong passwords
 - Vendor ids – remove or disable
 - Shared ids – lowest access possible



■ Authorization

- Approval over who needs access
- Develop a matrix to identify segregation of duty issues
 - Administrators/super users should not have access to enter data

■ Administration

- Maintenance of users can be time consuming
- New business partners, departments or entry into new markets requires new or modified procedural rules
- System parameter settings



■ Infrastructure Hardening

- Secure the “backdoors” to your ERP
 - Databases, network, OS, interfaces
- Security risk assessments
 - Identify security threats the systems are exposed to
- Data encryption



■ Monitoring

- Audit trails & trace mechanisms
- Maintain audit logs
- Implement “Governance Risk and Compliance” tools
 - Approva
 - Virsa
 - Audit Vault



■ Training

- Highly important
- Raises the awareness of employees
- Minimize the rate of security related to mistakes/violations
- Maximizes employees reporting of security incidents

- Points discussed can be used for a checklist if evaluating ERP
- Considering ERP security up-front can save time and money
- Biggest challenges:
 - Identifying segregation of duties
 - Administration of users
 - Monitoring

Questions & Answers



Contact Information



William Lovell

KPMG LLP

Advisory Services

phone: 614-425-6112

email: williamlovell@kpmg.com

