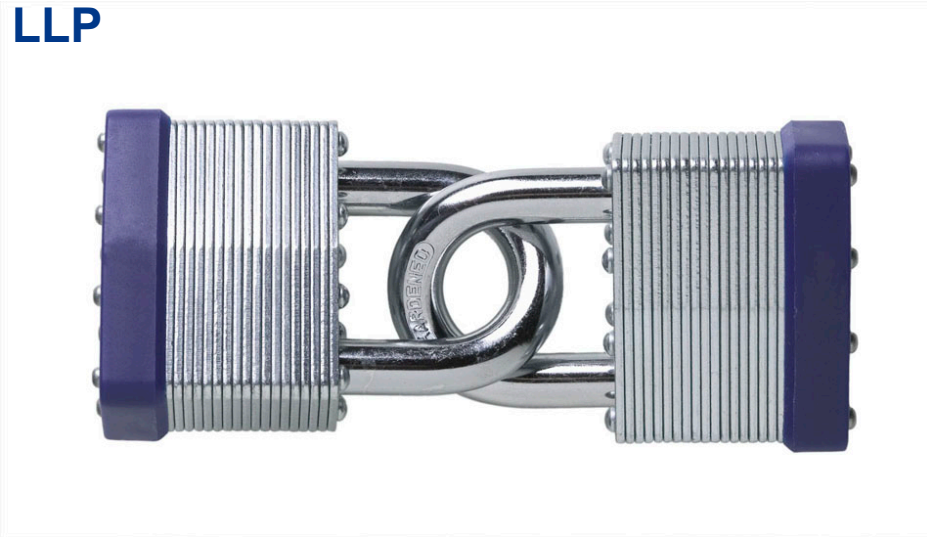




# Implementing Security, Privacy and Controls Using Modern ERP-Based Tax Systems

**Richard Rudnicki, Deloitte & Touche LLP**  
**Rita Scoggins, Deloitte Consulting LLP**



# Introduction

## **Richard J. Rudnicki, Senior Manager, Security & Privacy Deloitte & Touche LLP**

Richard has 12 years of IT related experience focused on implementing and assessing application security and business process controls for a variety of clients specializing in the Health Sciences & Government Industry. In addition to client experience, Richard has developed technical security and controls content published in an ISACA book on Oracle (PeopleSoft) auditing and has facilitated several SAP security and controls training classes.

## **Rita C. Scoggins PMP, Senior Manager, SAP Package Technologies Deloitte Consulting LLP**

Rita has 14 years of experience performing functional lead roles during large and complex ERP implementations primarily in State Government, Tax and Revenue agencies. She has designed and implemented solutions for tax return processing for multiple types of taxes, case management and contact centers and has over 10 successful tax related go-lives across projects at the State of Florida and State of Michigan.

### **Our Tax and Revenue professionals focus on:**

- \* Market-leading COTS integrated tax solutions
- \* Emerging and innovative technical solutions including SOA
- \* Business process assessment and improvement
- \* Broad strategies for increasing collections
- \* Organizational performance improvement
- \* Improving the accuracy and security of taxpayer data
- \* Program management and quality control
- \* Improving revenue performance in challenging economic times

# Agenda

- ERP-based Integrated Tax Systems – Benefits
- Security, privacy and controls considerations
- Risk-based approach to address multi-layered requirements
- Hot security and privacy topics
  - 24/7 secured taxpayer access
  - Data protection
  - Data labeling and monitoring
  - Segregation of duties and privileged access restrictions
- Key controls for integrated tax systems
- ERP enablers to build required controls
- Questions?

## ERP-Based Integrated Tax Systems – Benefits

- Less costly to implement because the majority of the system already exists
- Less complex to implement with fewer moving parts to coordinate as integration is inherently built in the software design
- Provide documentation and training materials as a starting point
- Less delivery risk because the solutions are demonstrated in other similar organizations
- SOA-enablement out of the box, requiring fewer resources to implement
- Allow for early prototyping for users to see the entire solution, provide feedback and input, and prepare for implementation earlier in a project. Achieving a good understanding of the entire system early reduces user anxiety over the unknown
- Provide flexibility through a business rules engines and other configuration
- Provide “plug and play” for many third party products
- Works with multiple operating systems, database management systems and hardware platforms
- Provide an upgrade program for new functionality and technology enhancements to extend the life of the system

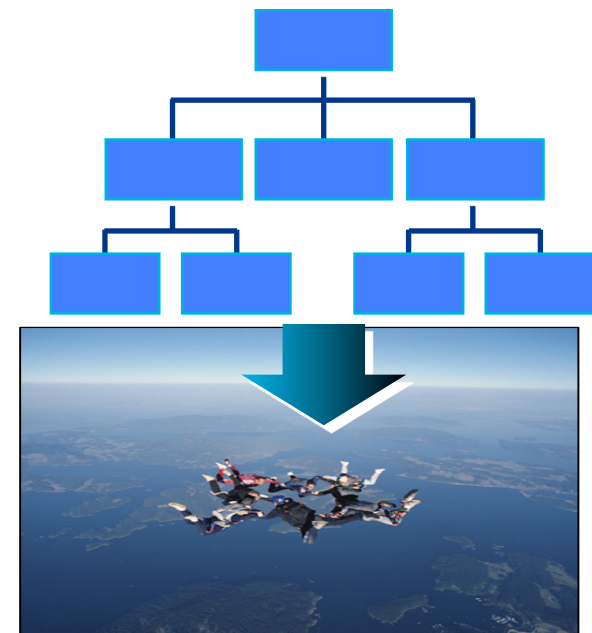
# Security, Privacy and Controls Considerations

The shift from vertical functional processes to end-to-end, ERP web-enabled processes will have a profound impact on the internal control structure. An integration of data and expansion of access points also affects security and privacy requirements:

**Points of control** — from multiple validations of data or transaction a single validation at the point of creation

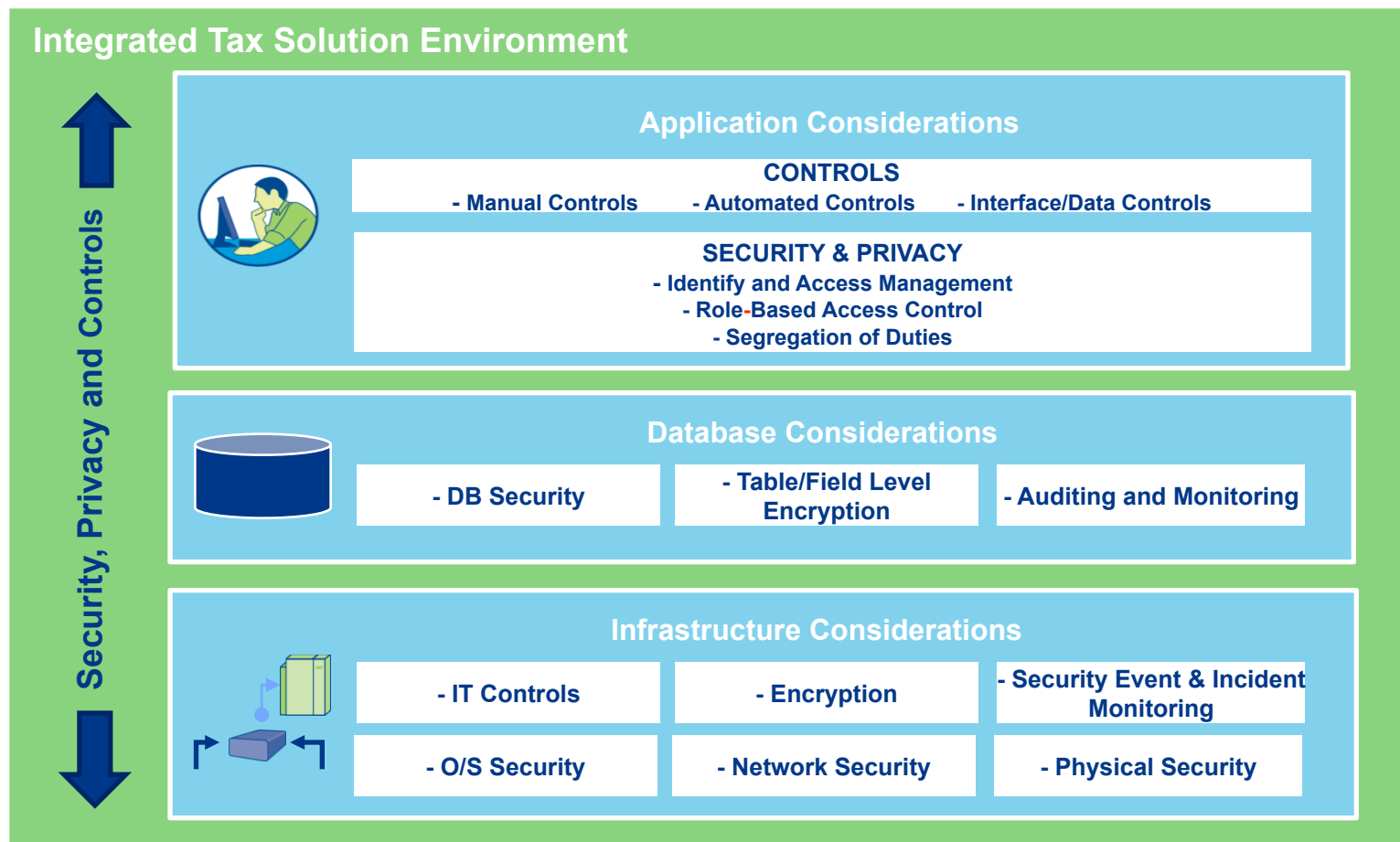
**Integration of data** — data previously stored and secured across many disparate systems is stored in a common database accessible through one integrated system

**Additional access points** — with web based functionality and a push for open government, user self service access is being increasingly deployed by many states

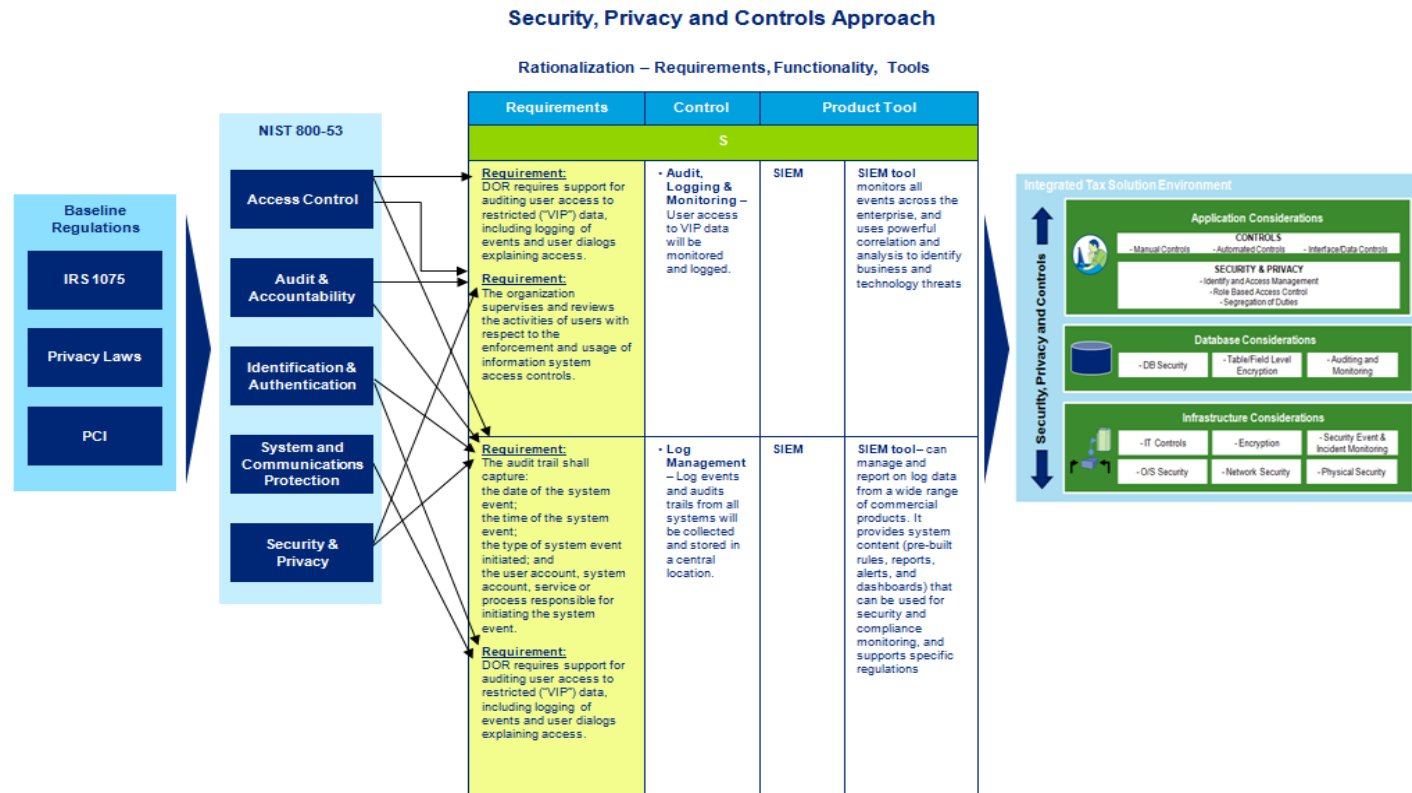


# Security, Privacy and Controls Considerations

Security, Privacy and Controls considerations should be addressed using a multi-layered approach



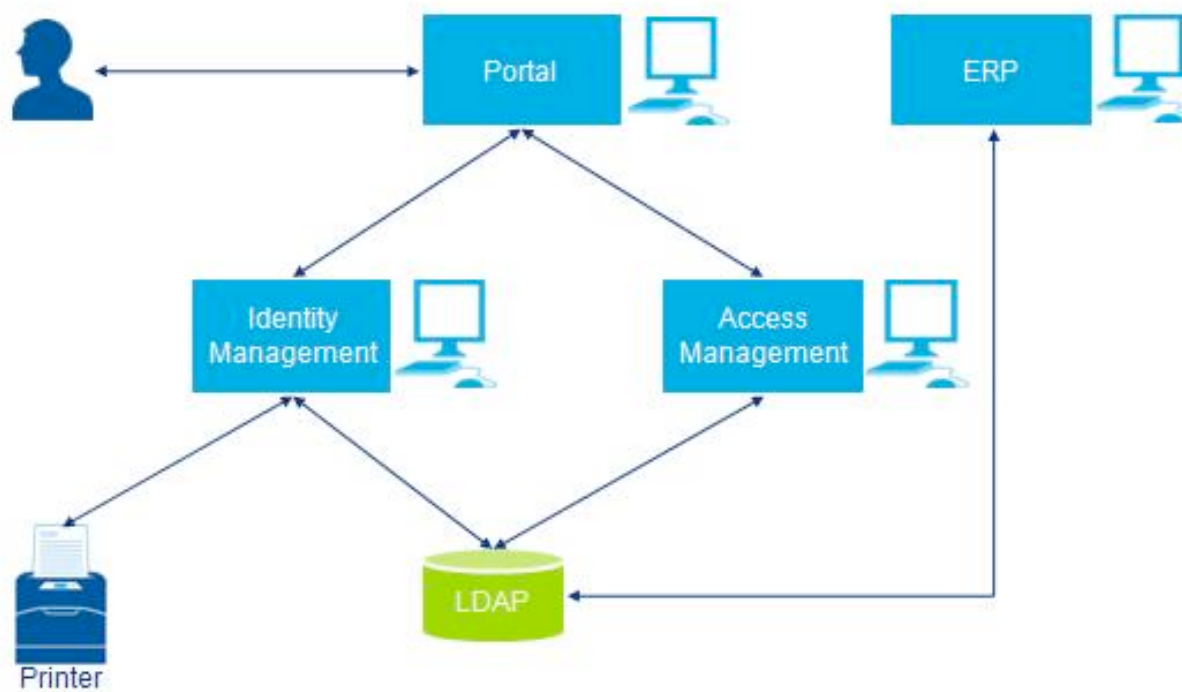
# Risk-Based and Rationalized Approach to Address Multi-Layered Requirements



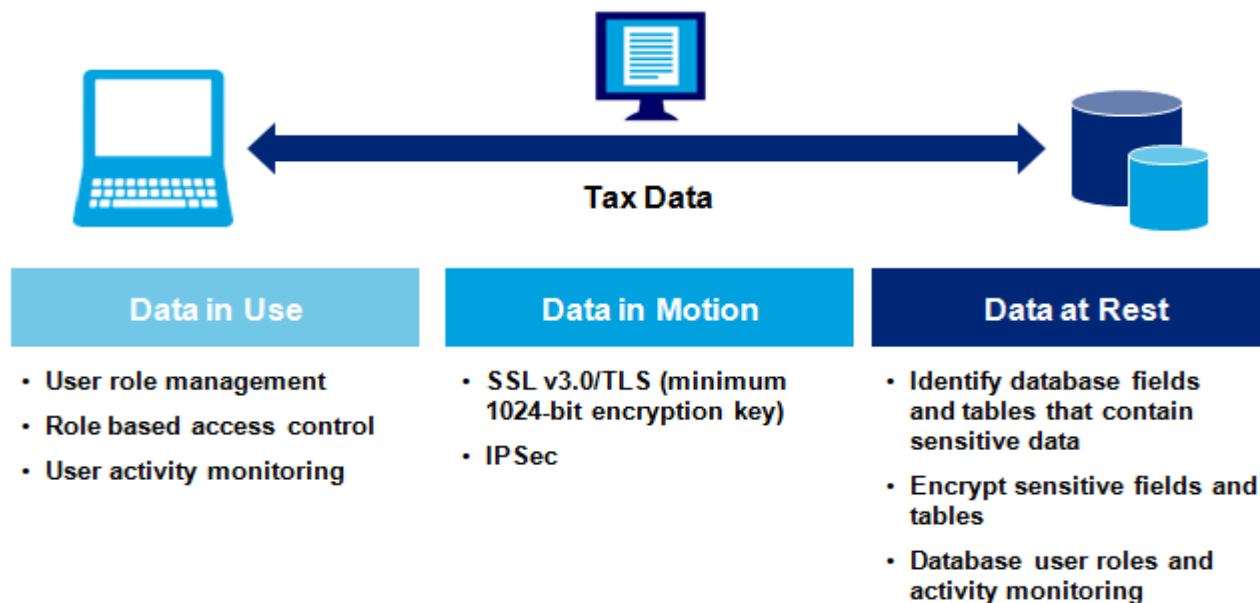
- Security, Privacy and Control efforts must appropriately address compliance requirements
- Government is expected to do more with less resources
- Solutions must fit within budgets and be sustainable
- Risks and compliance requirements must be understood and should be rationalized and prioritized

## Hot Topic: 24/7 Secured Access for Taxpayers

- Provide self-service infrastructure for 24/7 self-registration and taxpayer account maintenance
- Appropriately restrict/grant access to taxpayer data online
- Log requests to access top-level accounts and communicate to corresponding taxpayers

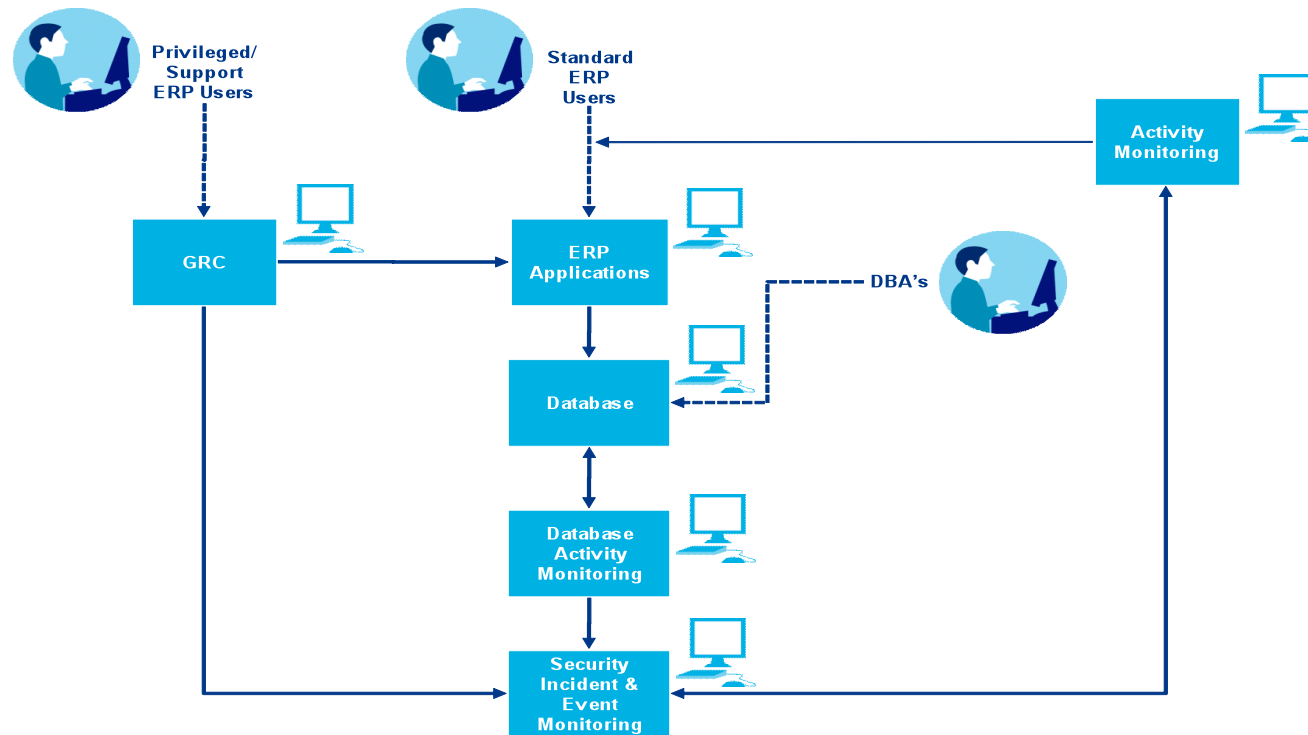


## Hot Topic: Data Protection



- Develop an understanding of entry and exit points for high risk data (i.e., PII, High Profile Taxpayer Records, Federal Tax Information, etc.) and its flow through the ERP system and across to other applications. Specific security and privacy requirements exist across the following:
  - **Data at Rest** — Secure access to data stores and encrypt high risk data
  - **Data in Motion** — Secure data transferred over the network/interfaces
  - **Data in Use** — Apply role-based access controls to enforce need-to-know/need-to-use principles. Monitor user interactions with high risk data

# Hot Topic: Data Labeling and Access Monitoring



- Develop an inventory of access points to high risk data
- Apply labels where required
- Monitor access (Consider supplementing ERP delivered audit functionality with leading COTS products to monitor view activity)
- Develop reports and procedures to review logs in order to investigate inappropriate access to high-risk data

# Hot Topic: Segregation of Duties and Privileged Access Restrictions

- An integrated system creates the need for segregation of duties which must be identified, enforced through appropriate access assignment and monitored

- ERPs provide functionality, and COTS (GRC) tools provide segregation of duties requirements

## Illustrative Sample Segregation of Duties Matrix

			FINANCE / ACCOUNTING					SECURITY ADMINISTRATION		
			FI MASTER DATA	BANK / CHECK RECONCILIATION	POST GL JOURNAL ENTRY	PARK GL JOURNAL ENTRY	OPEN & CLOSE ACCOUNTING PERI	USER CREATE	ROLE/PROFILE ASSIGN	ROLE DEVELOPMENT
Process	Function	ID	FI01	FI02	FI03	FI04	FI05	BS01	BS02	BS03
FINANCE / ACCOUNTING	GL MASTER DATA MAINTENANCE	FI01								
	BANK / CHECK RECONCILIATION	FI02								
	POST GL JOURNAL ENTRY	FI03	F011							
	PARK GL JOURNAL ENTRY	FI04			F012					
	OPEN & CLOSE ACCOUNTING PERIOD	FI05	F013		F014					
SECURITY ADMINISTRATION	USER CREATE	BS01	B137	B138	B139	B140	B141			
	ROLE/PROFILE ASSIGN	BS02	B020	B021	B022	B023	B024	B001		
	ROLE DEVELOPMENT	BS03	B049	B050	B051	B052	B053			

# Enforcing Segregation of Duties and Privileged Access Restrictions

- Privileged access to functionality and data must be identified, tightly restricted and monitored

## Privileged Access Roles

Firefight ID	FF ID Controller	Status	Description	FF ID Used By	Message	Log on user
FIREFIGHT01	PMINKLER	●●●	PERFORM BASIC ACTIVITIES - ASGIG	SJONES	Message	Log on
FIREFIGHT02	SPETERS	●●●	TO PERFORM MATERIAL MANAGEM...		Message	Log on

## Document Why Needed

MIRSA Firefighting Administration Tool

Please enter the reason for using this FirefightID

Reason:

Please enter the actions that you anticipate to perform.

Activity:

## Audit Log

FirefightID	Firefighter	Session Date	Session Time	Reason	
Date	Time	Server Name	Transaction	Report Name	Report Title
TCode	Time	Table	Field Text	Old value	New Value
FIREFIGHT01	SJONES	04.11.2004	10:03:12	TO CREATE USERID FOR TOM HEMMER AND ASSIGN TH	
04.11.2004	10:03:12	pluto_v03_00		MainMenu	
04.11.2004	10:03:17	pluto_v03_00	SUB1	SAPR000	User Maintenance
04.11.2004	10:04:24	pluto_v03_00	PFC6	SAPLPRGH_TREE	Role Maintenance
FIREFIGHT02	SJONES	04.11.2004	10:07:18	TO CREATE MATERIAL MATRESS SPRING	
04.11.2004	10:07:18	pluto_v03_00		MainMenu	
04.11.2004	10:07:23	pluto_v03_00	MM01	SAPR001	Create Material &
10:09:52	0900000000000002		DMAKT		New record Created.
10:09:52	0900000000000002		DMAKM		New record Created.
10:09:52	0900000000000002		NARA		New record Created.
FIREFIGHT03	MCARTER	04.11.2004	10:14:49	CREATING A G/L ACCOUNT	
04.11.2004	10:14:49	pluto_v03_00		MainMenu	
04.11.2004	10:14:55	pluto_v03_00	FSM1	SAPR02H	Create Sample Account

## Key Controls for Integrated Tax Systems

- With the implementation of an ERP-based tax solution, it will be important to design and implement controls which manage risks and meet control objectives related to:
  - **Financial Reporting** — Controls which determine the accuracy, completeness and reliability of financial information
  - **Operational Efficiency and Effectiveness** — Controls which determine business objectives are met (e.g., customer service, operations, etc.)
  - **Regulatory Compliance** — Controls which facilitate compliance with applicable laws and regulations (e.g., IRS 1075 Guidelines, etc.)

## Key Controls for Integrated Tax Systems

- The following are examples of common controls for ERP-based Integrated Tax Systems:
  - Ability to define error and exception conditions and associated severity level via configurable controls
  - Ability to provide statistics on items in suspense and on exception-based work lists and indicate the number of items that are suspended or work listed by error type and also indicate whether that error type can be overridden or not
  - Ability to specify which errors should be overridden and automatically reprocess items in suspense or on exception work lists to release those returns with only error/exception conditions
  - Online process monitoring reporting that shows backlog, throughput, arrival and resolution rates, by tax, return type, work list, and work list reason
  - The ability to establish user defined tolerances (by dollar amount or percentage) as appropriate across relevant exception identification criteria.

# ERP Enablers to Build Required Controls

- ERPs have features and functions which can enable an effective and efficient internal control structure. A key objective is to leverage ERP automated controls including:
  - **Authorization checks**
  - **Data entry validation**
  - **Number ranges**
  - **Automatic postings**
  - **Tolerance levels**
  - **Document blocking**
  - **Document types**
  - **Posting keys**
  - **Reference documents**
  - **Sample documents**
  - **Control accounts**
  - **Match codes**
  - **Logging of changes**
  - **Archiving documents**
  - **Balance verification**
  - **Supervisory release**
- During implementation, business processes must be analyzed and controls designed and configured using these and other enablers
- These control types would be part of the design, documentation and implementation of controls

## Questions?

Name	Title	Contact Information
Richard J. Rudnicki	Senior Manager, Security & Privacy, Health Sciences & Government, Deloitte & Touche LLP	<a href="mailto:rrudnicki@deloitte.com">rrudnicki@deloitte.com</a> Suite 900 600 Renaissance Center Detroit, MI, 48243-1704 U.S.A Direct: +1 313 396 2519 Main: +1 313 396 3000 Fax: +1 313 566 9444
Rita C. Scoggins	Senior Manager, Enterprise Applications, Public Sector, Deloitte Consulting LLP	<a href="mailto:rscoggins@deloitte.com">rscoggins@deloitte.com</a> Suite 1500 191 Peachtree Street, NE Atlanta, GA 30303-1924 USA Direct: +1 404 631 2447 Main: +1 404 631 2000 Fax: +1 404 890 9630



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

#### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2010 Deloitte Development LLC. All rights reserved.