SAP SECURITY – CLEARING THE CONFUSION AND TAKING A HOLISTIC APPROACH

WWW.MANTRANCONSULTING.COM

25 Mar 2011, ISACA Singapore
Let's clear the confusion!
Objectives

- Discuss various types of security controls in SAP
- Define framework for SAP security audits
- Discuss integration with IT and operational audits

This presentation does not cover individual SAP security controls and concepts in detail ....
And it is not a technical presentation on SAP security controls
SAP is a sensitive & critical system

- SAP is an ERP and a business application system
- Any security vulnerability may result in financial loss, business disruptions, misstatement of financial information, etc
- Unlike infrastructure security vulnerability, SAP security vulnerability may directly impact the business
- SAP is an integrated system – therefore, any errors may have a widespread impact
- One of the most important system in any organization
What is the impact on IT audit?

- It is important to secure SAP system
- To secure SAP, it is not sufficient to enforce controls inside SAP only
SAP is a part of IT infrastructure

User PC/ Laptop

Application Server 1

User PC/ Laptop

Application Server 2

The Cloud

Application Server 3

Database Server

© 2011 MANTRAN Consulting Pte. Ltd. All rights reserved.
What needs to be secured?

- Application – appropriate security controls need to be enforced in SAP
- Infrastructure – the supporting infrastructure needs to be secured as well
  - Network – routers, switches, firewalls
  - Server – application server and database server
    - Operating system
    - Database
  - PCs/ Laptops – presentation layer of the SAP system
What organizations review...

**SAP Audit/Review Scope**

- Authorizations: 70%
- SoD: 68%
- SAP security policies and procedures: 54%
- Configurable/automated business...: 38%
- BASIS controls: 24%
- Data migration: 16%
- Not performed: 14%
- Don't know/others: 8%

Source: MANTRAN SAP Security Practices Survey 2010
Security controls in SAP
Authorization controls

- Allow users in SAP to perform their work while securing transactions from unauthorized access
- It is a complex and scalable concept
  - Determines **WHAT** activity can be performed by a user as well as **WHERE** it can be performed
  - Enforced through a pseudo object oriented concept using authorization objects
  - Authorizations are assigned to Roles, which are then assigned to Users

Approximately 2,000 authorization objects control access to more than 100,000 transaction codes

© 2011 MANTRAN Consulting Pte. Ltd. All rights reserved.
Look for the holes …

- SAP checks user master record for required authorizations
- SAP provides information on which authorizations are required for each transaction codes

It is important to look for ‘disabled’ authorization checks!
Disabling authorization checks ...

- The Authorization Object check has been disabled for the Transaction Code using transaction SU24 (table USOBT_C and USOBX_C)

Don’t forget global deactivation of Authorization Objects through transaction AUTH_SWITCH_OBJECTS (profile parameter ‘auth/object_disabling_active’ should be set to Y for this to take effect!)
What should be reviewed?

- Access to critical/sensitive activities are controlled
- User access is appropriate (i.e., based on their roles and responsibilities)
- Roles are appropriate (i.e., authorizations within roles are as per the role definition)
Segregation of Duties (SoD)

- Ensures that no one individual has complete control over major phase of a process
- Key component of any effective internal controls environment
- Typically enforced through a combination of access control and mitigating controls
What should be reviewed?

- SoD framework has been defined
- Users do not have SoD conflicts
- Roles do not have SoD conflicts
- If SoD conflicts exists in users, there are appropriate mitigating controls
Beyond the basics …

- **Mitigating controls – do they work?**
  - It is important to check whether the mitigating controls work
  - Mitigating controls should be documented and tested regularly!
BASIS controls

- Refers to technical controls in SAP
  - Password controls
  - User administration
  - Privileged users
  - Auditing
  - Change controls
  - Batch job management
  - Direct access to data through tables
Go beyond the basics

- Client settings – direct changes should not be allowed on the production client

Don’t forget to check system settings!

And the table logging!
What should be reviewed?

- BASIS review
  - Policies and procedures
  - Technical settings in SAP
  - IT procedures related to SAP administration and maintenance
Business process controls

- Refers to automated (and IT dependent) controls available in SAP for various business processes such as purchasing, sales, financial reporting, inventory, HR, etc

- Broadly classified under following three categories:
  - Inherent controls
  - Configurable controls
  - Procedural controls
Business process controls

- **Inherent controls** — Enforced by default in SAP
  - Sales Order cannot be created with an invalid customer

- **Configurable controls** — ‘Switches’ that can be set by turning them on or off based on the business requirements
  - Configured through Implementation Guide (IMG)
  - Examples - tolerance limits for three way match, PO approval hierarchy

- **Procedural controls** — IT dependent controls (e.g., review of exception reports)
Do organizations use them?

Utilization of SAP automated controls

- Very confident: 13%
- Somewhat confident: 46%
- Not confident: 30%
- Don’t know/others: 11%

Source: MANTRAN SAP Security Practices Survey 2010
Some examples of such controls ...

PMIN condition for pricing

- PMIN is used: 16%
- PMIN is not required: 25%
- Not aware that SAP has PMIN: 35%
- Don't know: 24%

Source: MANTRAN SAP Security Practices Survey 2010
A few more examples ...

- Dual controls for customer and vendor masters
A few more examples ...

- Alternate payee
A few more examples ...

- Regular review of vendor reports such as RFKABLO0 (Changes to Vendors)

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Vendor</th>
<th>Changed By</th>
<th>Field Name</th>
<th>COC/PO/Org New value</th>
<th>Old value</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.01.2011</td>
<td>00:20:13</td>
<td>3900</td>
<td>BERNAD</td>
<td>Customer</td>
<td>390681</td>
<td></td>
</tr>
<tr>
<td>23.01.2011</td>
<td>00:20:13</td>
<td>3900</td>
<td>BERNAD</td>
<td>Returns vendor</td>
<td>3002 X</td>
<td></td>
</tr>
<tr>
<td>23.01.2011</td>
<td>00:20:13</td>
<td>3900</td>
<td>BERNAD</td>
<td>Shipping Cond.</td>
<td>3868 81</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>22:55:57</td>
<td>99993</td>
<td>BERNAD</td>
<td>Automatic P0</td>
<td>3002 X</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>21:06:59</td>
<td>99993</td>
<td>BERNAD</td>
<td>Ctrl Adr Adm</td>
<td>*** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>21:06:59</td>
<td>99993</td>
<td>BERNAD</td>
<td>Comp. code data</td>
<td>3006</td>
<td>*** Created ***</td>
</tr>
<tr>
<td>15.01.2011</td>
<td>21:06:59</td>
<td>99993</td>
<td>BERNAD</td>
<td>General data</td>
<td>*** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>21:06:59</td>
<td>99993</td>
<td>BERNAD</td>
<td>Partner functn</td>
<td>3868 *** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>21:06:59</td>
<td>99993</td>
<td>BERNAD</td>
<td>Purchasing data</td>
<td>3002 *** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>12:47:04</td>
<td>9</td>
<td>MARGNT1</td>
<td>Order currency</td>
<td>1868 USD</td>
<td>369</td>
</tr>
<tr>
<td>15.01.2011</td>
<td>11:21:31</td>
<td>99992</td>
<td>BERNAD</td>
<td>Ctrl Adr Adm</td>
<td>*** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>11:21:31</td>
<td>99992</td>
<td>BERNAD</td>
<td>Comp. code data</td>
<td>3006</td>
<td>*** Created ***</td>
</tr>
<tr>
<td>15.01.2011</td>
<td>11:21:31</td>
<td>99992</td>
<td>BERNAD</td>
<td>General data</td>
<td>*** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>11:21:31</td>
<td>99992</td>
<td>BERNAD</td>
<td>Partner functn</td>
<td>3002 *** Created ***</td>
<td></td>
</tr>
<tr>
<td>15.01.2011</td>
<td>11:21:31</td>
<td>99992</td>
<td>BERNAD</td>
<td>Purchasing data</td>
<td>3002 *** Created ***</td>
<td></td>
</tr>
</tbody>
</table>
What should be reviewed?

- Configuration settings
- Procedural controls
- Exception reports
Clearing the confusion

1. Business Process Review
2. Configuration Review
3. Blueprint Review
4. IT Automated Controls (ITAC) Review
5. IT Application Controls (ITAC) Review

1. BASIS Review
2. IT General Controls (ITGC) Review
3. Technical Review

1. Authorizations Review
2. Access Review
3. SoD review
4. Role Review
5. User Review
Security controls outside SAP

- It is equally important to enforce security controls in the underlying infrastructure components.
- SAP interacts with its underlying infrastructure components in unique ways.
- Therefore, it is important to consider controls related to these interactions at the infrastructure level.
Network controls are important

- SAP network security
  - Can users directly connect to the database through backend?
  - Is the data transmission over the network secure?
  - What network communication is allowed between user machines and application server?
  - What network communication is allowed between application server and database server?

- Apart from usual network security controls, consider SAP specific controls such as SAPRouter and SNC
SAP supports network security

- **SAPRouter**
  - SAPRouter is an SAP program that serves as an intermediate station (proxy) in a network connection between SAP systems or programs
  - Controls access to your network (application level gateway)
  - Useful extension to an existing firewall

- **Secure Network Communications**
  - SNC is used to secure SAP network connections
  - Provides reliable authentication as well as encryption of the data to be transferred
  - SAPRouter allows SNC connections to be set up
SAP server needs to be hardened

- Both application and database servers need to be hardened
- Consider SAP specific hardening requirements such as transport tools security, profile parameter file security and security audit logs security
SAP changes are controlled by OS

- Operating system level transport tools in SAP servers
  - Change and Transport System (CTS) is a set of tools to organize development projects in the ABAP Workbench and in customizing, and then transport the changes between the SAP systems and clients
  - It broadly consists of Change and Transport Organizer (CTO), Transport Management System (TMS) and some operating system level transport tools
SAP Change and Transport System

Transport Tools
(tp and R3trans)

CTO
Transport Organizer

Workbench Organizer

Customizing Organizer

TMS
Transport Management System

RFC

© 2011 MANTRAN Consulting Pte. Ltd. All rights reserved.
CTS depends on OS files

- There are two global configuration files – TP_DOMAIN_<SID>.PFL and TPPARAM that must include entries for each SAP systems taking part in transports.
  - ‘tp’ uses these files for making transports.
  - Stored in /usr/sap/trans or <DRIVE>/usr/sap/trans
  - Access rights should be configured so that all SAP systems within the transport group can access these files
Transport tools reside at OS level

- Imports can be performed using ‘tp’ program at the OS level by logging into the target system as user <SID>adm, going to /usr/sap/trans/bin directory and calling the program
SAP profiles are OS files

- Profile parameter files stored in SAP server
  - A profile in SAP is an operating system file containing parameters and configuration information of SAP instance.
  - The profile files are located under the directory `/usr/sap/<SID>/SYS/profile`.
  - This directory is shared by all application servers belonging to the same SAP system (i.e., SID).
  - Access to modify the profile files should be restricted.
Audit log is stored on server

- Security audit logs stored in SAP server
  - Rsau/local/file – define names and locations of the security audit log files
  - Access to the security audit log files and directories should be restricted
And vice versa .....

With appropriate access, OS level commands can be executed from within SAP!
Indicative SAP security framework ..
What does it mean for IT auditors?

- SAP audit covers both technical and functional areas
- Requires integration between IT and internal/operational auditors
- Within IT audit team, coordination between infrastructure and SAP auditors is important to ensure that important infrastructure controls are covered
- Excellent opportunity to understand business and align IT audit with business risks!
Integrated audit is not yet common

Source: MANTRAN SAP Security Practices Survey 2010
SAP review through its lifecycle

- SAP review may be performed at various stages of SAP lifecycle
- Accordingly, scope and coverage may vary

© 2011 MANTRAN Consulting Pte. Ltd. All rights reserved.
Conducted before SAP is implemented (i.e., before go-live) and may include

- Blueprint/configuration/business process controls review
- Authorizations and SoD review
- IT general controls/BASIS review
- Data migration/ conversion/cutover review
- Project management review
- Program development review
Pre-implementation review

- System may not exist or controls may not have been implemented
- It is often a document review based on documents such as
  - Business blueprints
  - Authorization design documents
  - Project plan, strategy and other project documents
  - Data migration plan, strategy and cutover plan
  - SAP technical design documents
  - UAT documents
Post-implementation review

- Usually conducted after system stabilization
- It usually includes the following areas
  - Configuration/ business process controls review
  - Authorizations and SoD review
  - IT general controls/ BASIS review
- Usually conducted by reviewing the system settings
Other areas

- There are new security concerns with use of various NetWeaver products
- Other SAP products such as CRM, SRM, SCM and SLM have their own security issues
Questions

Presented by
Barun Kumar
Director
Mantran Consulting Pte Ltd
+65 8118 9972

Email ID barunkumar@mantranconsulting.com
LinkedIn profile http://www.linkedin.com/in/barunkumar
My blogs http://www.mantranconsulting.blogspot.com/