Tackling SAP Security Audits

Tina Scuruchi
Compliance Consultant
Powercor

How to Connect with Me

E:Tinascuruchi@hotmail.com

M: +61 0405 451 198

Li: linkedin.com/in/tinascuruchi/

Tackling SAP Security Audits

Tips to Avoid the SAP Security

Mop and Bucket

Lets Get Started

Sound of Compliance

My First Audit

Where does one start with little or no experience?

- ❑ I had less than 6 months experience in my first SAP security role
- ❑ I had inherited more profiles than there were users x 3
- ❑ I had inherited Segregation of Duties risks
- ❑ Out of date documentation

Audit findings a plenty, including a recommendation to implement role based security across Financials and Materials Management modules

.

Profile Generator – the new tool for SAP Security

SAP was fairly new at this time and not much documentation available.

The Audit Interview

Questions, Questions and more Questions were asked by the Auditor's

It didn't take me long to work out that you should never volunteer any information that has not been requested

Silence is the key

- ❑ Keep answers short and to the point
- ❑ It is ok to ask questions
- ❑ It is ok to challenge the Audit Team especially when a risk is incorrectly stated
- ❑ If you don't know how to respond to a question, it is ok to say I will get back to you with the appropriate details

Audit Management Actions

Management Action Audit reports can be complex to interpret and implement

- ❑ Read through the full Audit report prior to actioning.

  The report may have a few offensive roles that may cause different risks.
  The risks is multiplied due roles that are incorrectly defined

- ❑ Draft up responses to Management Actions and discuss responses with the relevant stakeholder

- ❑ Ensure that the Agreed Action dates are set with enough time to complete

Agreed Management Action Items

Agreed Management Action Items can vary from excess access to profile parameter settings to privileged user accounts to locked transaction codes, etc.

- ❑ Group all like items. Objects require changing may impact more than a single action item
- ❑ Document findings for future reference > Policy / Standards document
- ❑ Not all Action Items are owned by SAP Security. Ensure discussions are had to officially hand over to the appropriate Team/s

Documentation

- ❑ Policy Document
  - ✓ Determine Segregation of Duties Risks
  - ✓ Create a Segregation of Duties Policy – seek assistance from your Finance Team (CFO)

- ❑ Standards Document
  - ✓ Document should include naming standards, provisioning rules, system rules, change management process, etc

Planning & Design

Management Engagement Re-Design

- ❑ Start with a proposal document, outlining reasons behind why a security review should be considered:

  - ✓ Difficult to maintain
  - ✓ Consider current risks noted by Audit findings
  - ✓ $savings if changes were made.

  Management may not approve any changes unless there is a viable cost savings benefit The value add must be quantifiable.

- ❑ Establish a Steering Committee Structure with Roles and Responsibilities

- ❑ Establish business Subject Matter Experts (SME's)

Design

Design

Workshop 1

- ❑ Hold SME workshops to identify security roles split per stream by transactional access requirements

Build

- ❑ Build roles with the transactional data only
- ❑ Design a Template to capture remaining requirements

Workshop 2

- ❑ Confirm transaction codes per stream
- ❑ Confirm Organisational data requirements
- ❑ Confirm the Business Rules

Design

Security Test Script

Stream	Robotics	**Business Role**	Robotics – Revenue Management
Name of Tester	Alex Graham	**Date Tested**	
SAP Role	Z_RPA_PM_ASSET_DEFECT	**Script ID**	
Roles Assigned	Z_RPA_PM_ASSET_DEFECT Z_CA_END_USER		
	Test Environment: TS3 010 User: R-PAD_MG1 Password: As per IIQ, Sailpoint	**Business Role Owner/s:**	Stuart McDonald
Author		**Team Lead / Approver**	
Name: Signature /Date :		Name: Signature /Date :	

Business Rules				
Business Rules	**B_USERSTAT**	**Technical Name**	**Allowable Y/N**	**Result Pass Fail N/A**
User Status	ACTVT = Create, Delete BERSL = Approver, Approval Required OBTYP = TASK STSMA = Tasks PC notif Tasks CR notif	B_USERSTAT Maintenance Notification		
Report Writer	ACTVT = Display, Save Extracts BRGRU = All	G_803J_GJB		
Table (ITGC) check	ACTVT = Display, Change DICBERCLS: ZCPM	S_TABU_DIS		
Customer Application Authorisations	ACTVT = Change, Display of Payment Cards Customer and Vendor MD = All	F_KNA1_AEN		
Customer Account Authorisation	ACTVT = Change BRGRU = All Auth Groups	F_KNA1_BED		

Security Test Script

OVERALL TEST OBJECTIVE / DESCRIPTION
The Robotics project is currently undergoing an upgrade. New accounts will be deployed using a consistent naming convention. The current SAP access requires to be further restricted. New roles are being defined to grant least privilege access. This script enables visibility of what transaction codes, authorisations and objects have been configured.

Transaction Code	**Transaction Text**	**Access Y/N**	**Transaction Entered**	**Result Pass Fail N/A**
i.e. VA01	***Create Sales Order***	***Y***	***Created new SO for Customer XYZ***	***Pass***
ZMAP	Maintenance Assessment Platform			
ZRES	RealEst – Real Estimating			

Authorisation Objects – Negative Testing required where Allowable is other than *				
Org Values	**Allowable**	**Access Y/N**	**Transaction Entered**	**Result Pass Fail N/A**
Org Values				
Maintenance planning plant	4* 8* 9*			
Controlling area	4500			
Notification Type	CA SC SL ZB ZF ZR ZS			
Maintenance Plant	4* 8* 9*			

Template can be used for Requirements Gathering / Test Script for UAT confirmation and approval

Page 2 of 5

Design

Design

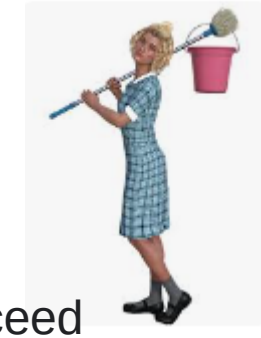
- ✓ Design a form / excel spreadsheet that covers the transactional access to add any new requirements to
- ✓ Establish naming convention rules, roles, authorisation objects, tables, etc
- ✓ Establish Organisational values per stream, and add information to the Design document
- ✓ Establish (if not previously completed) profile parameter rulesets

The key to above is documentation. Your documentation should include rulesets, naming standards, etc

If the rulesets are maintained, documented, and followed – audits will be simple

Ensure that you gain Management signoff off on all documentation where Policy and Standards apply

IT General Controls



IT Audit General Controls

- ❑ IT General controls and effective compliance must be well understood in order to succeed

- ❑ IT General Controls audits ensure that there is NO impact on the Company's Financials. The audit process includes main key areas as below:

  - ✓ User account maintenance
  - ✓ Password management
  - ✓ Change management
  - ✓ High privileged access
  - ✓ System Settings

IT General Controls

- Audit Management Items
  - Review last audit report with agreed Management Actions
  - Confirm if the Management Actions Items have been addressed
  - Address findings and implement a plan that mitigates future repeat findings?
  - Audit scripts - Follow the Change Management process. DO NOT install directly in Production
  - Always ensure that an ABAPer is engaged to review code
  - Review outputs of the Audit script tables, prior to submitting results to the Audit Team

- Analysis / Clean up
  - Ensure critical transactions are locked– eg Deleting Company Code
  - Schedule an SAP Security Optimisation Report and Review Findings
  - Did you know that there are Security transactions OY* and OP*?
    (Transaction Codes can be checked in SE93)
  - Confirm Company Password Policy
  - Confirm Profile Parameters are set in line with Company Security Policy

IT General Controls

System Checks

- ❑ Check elevated access across Production environments:
  - System Change Settings SCC4, SE06

Ensure settings are appropriately governed
Access should be restricted

Difference between SCC4, SE06?
SCC4 – Client specific objects
SE06 – Cross client objects

  - SM59 – Impacts from other systems, clients

IT General Controls

Getting Ready for Audits – Pre-Audit Planning

❑ Audit Management Items

- Review access to SA38/SE38
- Review access to SM30/31
- Review access to SE16/N
- Review SAP_ALL, SAP_NEW
- Ensure tables are executed via a customised transaction using appropriate authorisation group (&NC& auth group risk)
- Review access to Security transactions, PFCG, SU01, OY*, OP*
- Review SM59 access
- Ensure that no RFCs are available to log into Production environment without validating credentials
- Ensure Parameters are set in line with Company Security Policy

IT General Controls

Getting Ready for Audits – Pre-Audit Planning

- Audit Management Items - Review User Administration process
  - Can you easily find requests to confirm provisioning of access was appropriate?
  - Do you have Business Role Owner/s in place?
  - Confirm Super User accounts are locked accordingly
  - Confirm System/Comms not set to Dialog, if set either remediate or mitigate

IT General Controls

Getting Ready for Audits – Pre-Audit Planning

- ❑ Audit Management Items - Review User Administration process
  - Can you easily find requests to confirm provisioning of access was appropriate?
  - Do you have Business Role Owner/s in place?
  - Confirm System Super User accounts are locked accordingly
  - Confirm System/Comms not set to Dialog, if set either remediate or mitigate
  - Transactions no longer in use are de-activated via transport route or locked

Auditing - Documentation

- **Standard Operating Procedure Policy Document**
  - User Admin Process
  - Firefighter Process
  - Monthly Reporting
  - List of Locked Transactions
  - User Review Process
  - Anything process driven

Roles - Responsibility

Application Owner

- ❑ Manages Business Operations
- ❑ Manages Customer Relations
- ❑ Managers Application Team
- ❑ Ensures that IT Policy, Standards, Procedures are adhered

Data Application Owner

- ❑ is responsible for business data
- ❑ is the decision maker for all business changes
- ❑ is responsible for SoD's and mitigating controls

Business Role Owner

- ❑ Has responsibility assigned to a suite of security roles
- ❑ Approves all user admin changes in their area of responsibility
- ❑ Approves all security role changes requested
- ❑ Validates and approves the review of all accounts – Recommend 6 monthly

Segregation of Duties

This item should sit more with the business (CFO), however, for some reason these Rulesets are constantly requested during Audit Reviews.

- ❑ SoD Rulesets
  - ✓ Liaise with your Functional Consultant to identify the list of SoD risks
  - ✓ Map business risks to Roles
  - ✓ Analyse the ruleset against the role
  - ✓ Map single roles requiring mitigation or revoke
  - ✓ Discuss analysis with CFO or delegate
  - ✓ Ensure your Policy document is signed off by CFO and IT Management Team

- ❑ Policy Document
  - ✓ Should include:
    - ✓ Roles and Responsibilities
    - ✓ All rulesets
    - ✓ Process – Mitigation, Removal of Access, Temporary Access, Approvals, Reporting

Questions / Thoughts/ Anything Else