



5 WAYS TO IMPROVE YOUR SECURITY POSTURE IN SAP HR

(OR HOW TO KEEP HUMAN RESOURCES/ TALENT MANAGEMENT/ PEOPLE OPERATIONS OR WHATEVER THEY'RE
CALLED, OFF YOUR BACK)

A N O R A N G E P A P E R

B Y

PUMPKIN CONSULTING

WHO ARE PUMPKIN CONSULTING?

Pumpkin began life back in 2004, way before IT security or cyber became cool.

We were amongst the pioneering generation that professionalized SAP security and helped shape it into what it is today which gives us a unique perspective on the full range of problems clients can encounter with SAP security.

What we do ultimately comes down to two things; managing the risk of running a key financial system like SAP and making sure security doesn't get in the way of you managing your business or perish the thought, stop the business from operating.

Our vast experience makes us the perfect partner for all technical implementation requirements, long term and day-to-day support and audit remediation works. Unashamed people pleasers, we're a friendly bunch, work with a smile on our faces and genuinely want and do the best thing for our clients.

ORANGE PAPER SUMMARY

OVERVIEW

This orange paper (we don't do white papers) provides some informal yet hopefully informative high-level guidance and more detailed neat tips and tricks to help towards optimal SAP Security administration and access management in SAP HR systems.

We've picked five of our favourite topics but the possibilities don't end there; contact us to see how we can help secure your SAP HR systems.

WHAT IS SAP HR?

Maybe if you're asking this question, this Pumpkin paper isn't the right one for you. We're talking specifically here about SAP HR Gui authorisations, contact us if you need help in Success Factors, we're good at that too!

CONTENTS

We'll explore five simple ways you can protect and improve your SAP HR security posture focusing on:

- 1.Context Sensitive authorisations.
- 2.integrating standard authorisations with structural authorisations.
- 3.INDX / SAP Memory.
- 4.HR data protection laws.
- 5.Beyond SAP HR.



DISCLAIMER: DO NOT PRINT THIS DOCUMENT, YOU DO NOT HAVE ENOUGH ORANGE INK.



PUTTING IT INTO
CONTEXT

TAKE ME THERE



A MEETING OF MINDS

TAKE ME THERE



MEMORY PROBLEMS

TAKE ME THERE



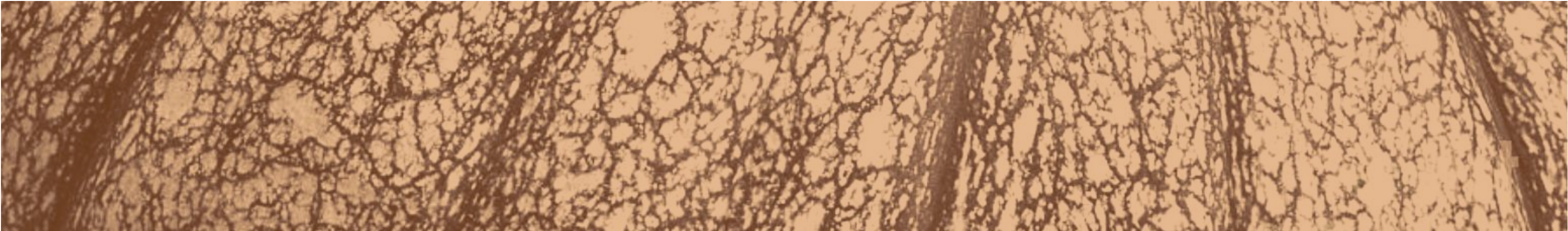
DATA PROTECTION

TAKE ME THERE



THINKING OUTSIDE THE
BOX

TAKE ME THERE



1. AS IN LIFE, CONTEXT IS KEY

Context is everything. The common problem in SAP HR also has a simple solution; don't be afraid of it. Most companies using SAP HR have had their fingers burnt by cross-pollination (or let's call it access-bleed which sounds a bit more gruesome) issues caused by different HR roles combining with each other enabling more access than desired. That doesn't mean you need to experience the same.

Like all problems where a user has too much access, it often requires an audit or review to find it, or an honest end-user (they do exist; we've met one). End-users are often less quick to report too much access, than they would be for too little, and who can blame them? We

had a client where an employee had written down the salary of the whole team gleaned from a SAP HR test system on a yellow post-it note that he kept in his wallet, only for it to fall out several years later. The code names he'd used for the employees were even more offensive than the fact he'd written down their salaries.

P_ORGIN versus P_ORGINCON

This issue happens because the standard HR personnel administration authorisation object controlling access to HR data via infotypes (e.g. 0008 for Basic pay), P_ORGIN, completely ignores how this interacts with the structural authorisations the user may have.

*If you are not already
using context
sensitive
authorisations, why
not?*



THE CLASSIC PROBLEM: A MANAGER WHO IS ALSO A TIME ADMIN

Let’s imagine we have a user, let’s call her Miss Manager.

- Miss Manager manages a team of 3 employees.
- The Manager role gives her access to view relevant HR data for that team of 3 via authorisation object P_ORGIN to important infotypes for her team, for example:
 - 00002 Personal data
 - 00008 Basic Pay

Here's an exciting screenshot from SAP showing you just that.

Manually	HR: Master Data	T-E901026300
Authorization level	M, R	AUTHC
Infotype	0002, 0008	INFTY
Personnel Area	TST1	PERSA
Employee Group	*	PERSG
Employee Subgroup	*	PERSK
Subtype	*	SUBTY
Organizational Key	TST1	VDSK1

- Miss Manager can see only her team due to Structural authorisations which contain an SAP standard function module showing her all the employees of the part of the org structure for which she holds chief position.
- In isolation, and in theory – Miss Managers access works perfectly.
- In practice, Miss Manager also performs a secondary role as Time Administrator for a department of 40 people. This role provides access to Time Admin related infotypes only:
 - 2001 Absences
 - 2002 Attendances

Manually	HR: Master Data	T-E901026301
Authorization level	M, R, S, W	AUTHC
Infotype	2001, 2002	INFTY
Personnel Area	TST1	PERSA
Employee Group	*	PERSG
Employee Subgroup	*	PERSK
Subtype	*	SUBTY
Organizational Key	TST1	VDSK1

This is where the problems start....



SAP HR standard auths set-up does not care about the users two hats, her two levels of access as a Manger and as a Time Administrator.

Instead, it combined the access

So, the Manager role provides access to Basic pay infotype 0008 (we could question a company structure where pay is so secret, but this is neither the time nor the place) from a role perspective, and the Time Admin structural authorisation provides access to 40 employees from an organizational / structural authorisation perspective.

Unsurprisingly, the user can now see basic pay details for all 40 people she should only manage time for, and frankly is appalled that Barbara earns more than her and will ask for a raise immediately.

SAP HR standard auths set-up does not care about the users two hats, her two levels of access as a Manager and as a Time Administrator.

Instead, it combined the access.

So, the Manager role provides access to Basic pay infotype 0008 (we could question a company structure where pay is so secret, but this is neither the time nor the place) from a role perspective, and the Time Admin structural authorisation provides access to 40 employees from an organizational / structural authorisation perspective.

Unsurprisingly, the user can now see basic pay details for all 40 people she should only manage time for, and frankly is appalled that Barbara earns more than her and will ask for a raise immediately.

Fortunately, the solution is simple.

SAP also offer an object called P_ORGINCON - HR: Master Data with Context

Context. Finally.

This object looks very similar to P_ORGIN but with one very crucial difference; we have a new field where we can specify the structural authorisation, and this now links the

Infotypes access to the Structural auth, meaning the people she can only view and change infotypes 2001, and 2002 for the people she is Time Admin for.

If Miss Manager tries to Display, 0008, basic pay for one of these users – she will receive, not just a guilty conscience, but also an authorisation error. The gap is closed.

		Manually		HR: Master Data with Context		T-E901025700	

2. PFCG AUTHORISATIONS, MEET STRUCTURAL AUTHORISATIONS

THE CHALLENGE

One of the biggest challenges we can face in SAP HR is how to marry your Personnel Administration restrictions with your Structural authorisations.

Not doing so can lead to quite a few headaches:



Dual Maintenance – Security administrators spend double the time restricting structural and standard authorisations



Manual tasks – Assigning Structural authorisations to users can be time consuming, and your SAP security people deserve to be doing more interesting work with their time on this earth.



Lack of symbiosis – An employee is added to a department, but the HR admin doesn't have access to the Personnel area of that employee. When the structure changes – the standard auths may need to change.



Problem solving complexity – Working out if the issue is structural or standard, can take a lot of time, especially when a lot of the errors kicked out in SU53 and auth trace may not relate to the issue at hand.

THE SOLUTION

Working with some very intelligent SAP HR experts and developers, at one of our happy customers, Pumpkin collaborated on a solution which we now recommend everywhere, and as the title suggests it involves bringing together your Structural auth design and your

The secret is in the Account Assignment field that all Position and Organizational Structures have in the SAP HR Org Structure.

We changed the process, so that all Positions and Departments had the relevant Personnel Area defined in this field.

*Your standard
role based
auths and
your structural
auths do not
need to be
strangers....*

2. PFCG AUTHORISATIONS, MEET STRUCTURAL AUTHORISATIONS

Your standard role based auths and your structural auths do not need to be strangers.....

THE CHALLENGE

One of the biggest challenges we can face in SAP HR is how to marry your Personnel Administration restrictions with your Structural authorisations.

Not doing so can lead to quite a few headaches:



Dual Maintenance – Security administrators spend double the time restricting structural and standard authorisations



Manual tasks – Assigning Structural authorisations to users can be time consuming, and your SAP security people deserve to be doing more interesting work with their time on this earth.



Lack of symbiosis – An employee is added to a department, but the HR admin doesn't have access to the Personnel area of that employee. When the structure changes – the standard auths may need to change.



Problem solving complexity – Working out if the issue is structural or standard, can take a lot of time, especially when a lot of the errors kicked out in SU53 and auth trace may not relate to the issue at hand.

THE SOLUTION

Working with some very intelligent SAP HR experts and developers, at one of our happy customers, Pumpkin collaborated on a solution which we now recommend everywhere, and as the title suggests it involves bringing together your Structural auth design and your

The secret is in the Account Assignment field that all Position and Organizational Structures have in the SAP HR Org Structure.

We changed the process, so that all Positions and Departments had the relevant Personnel Area defined in this field.



NOW WE HAVE A LINK BETWEEN

A

The roles which are restricted by,
you've guessed it;
Personnel Areas

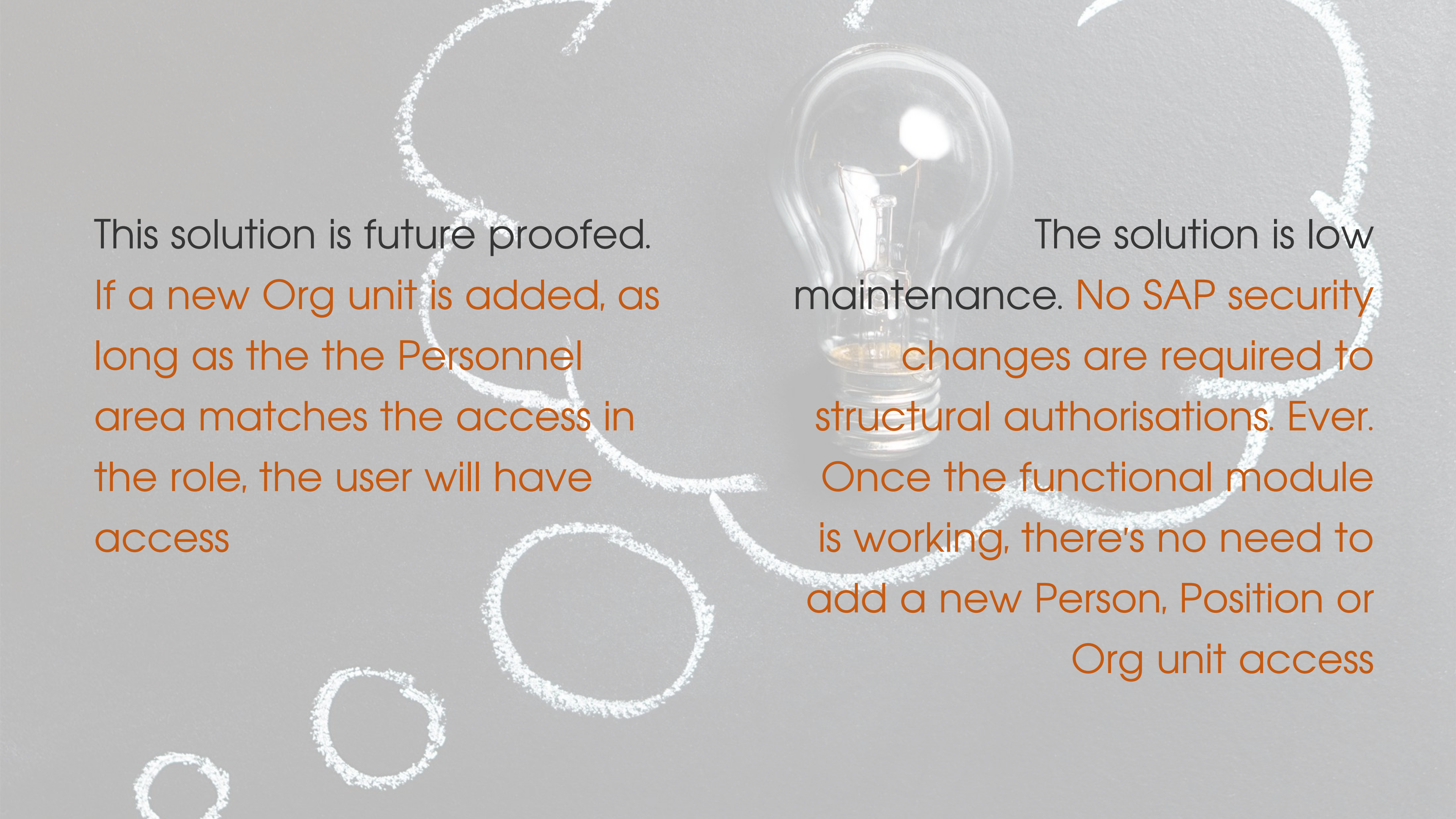
B

The Structural authorisations
relevant for those Personnel
Areas

To knit this all together, we created a Custom Object for this purpose, that includes the Personnel Area field. Our developer friends then created custom function modules for the structural authorisation that:

1 Searches for that object in the users roles, return personnel area's within the roles

2 Allow access to any Position or Org unit in the structure and the people beneath them, where the account assignment is the same as the Personnel Area the user has access to



This solution is future proofed.
If a new Org unit is added, as long as the the Personnel area matches the access in the role, the user will have access

The solution is low maintenance. No SAP security changes are required to structural authorisations. Ever. Once the functional module is working, there's no need to add a new Person, Position or Org unit access

A woman with long dark hair is lying down, her head resting on a white pillow. She is wearing a light-colored, long-sleeved shirt. Two rectangular cutouts of eyes are placed over her eyes. The background is a warm, orange-toned photograph of a woman lying down, with a pair of glasses visible on a surface in the lower right.

JUST
CHECKING IN
YOU'RE STILL
WITH US. WELL
DONE FOR
GETTING THIS
FAR. STAY
WITH US. THE
GOOD BITS
ARE STILL TO
COME

3. SAP MEMORY ISSUES: INDX

THE POISONED CHALICE THAT IS SAP MEMORY IN HR. PUMPKIN HAVE THE ANTIDOTE

HR Structural authorisations are resource hungry, and in the bad old days – running anything in SAP could take a long time to return the data you need.

SAP resolved this by creating an INDX entry in SAP Memory for a user's structural authorisations, so that data would be returned in a fraction of the time.

As the solution suggests, this was achieved by taking a snapshot of the authorisation access they had at that moment in time.

SO PROBLEM FIXED THEN, WHAT DO WE NEED PUMPKIN FOR?

Not really. In an organization, new hires or job moves happen all the time, and if there is one thing more annoying than waiting for a transaction to load, it is the transaction loading but then you don't have access to the new hire.

There is a standard job that refreshes the INDX entries – RHBAUS00.

The problem is this can take anywhere from 8 to 15 hours to run – the bigger the structure, the longer it takes.

So the one thing more annoying than waiting for a transaction or not having access, is being told by your friendly SAP Security expert to wait until the following morning for this mythical job to run at which point you will have the access.

THE HOLY GRAIL: RHBAUS00 FOR ALL!



So, a user can't see new changes to the structure until the RHBAUS00 job runs, and it takes hours to run for all users and only happens once a night. There must be a better way?

Sometimes the most elegant solutions are the most obvious, and this is a prime example of that, and you can have this one for free on us.

Our solution was simple, scroll to the next page for the big reveal.....

- 1

Create a user exit at logon for any user who logs into SAP HR
- 2


Upon logon, this triggers an execution of RHBAUS00 in the background unbeknownst to the user
- 3

As its only running for one user, it takes seconds/minutes not hours
- 4

By the time the user gets to the piece of work they want to do, the job has refreshed for them, and they have the access
- 5

In the worst case scenario, something changes whilst they are logged on, as our HR experts know, the user just needs to log out and back in to get the access
- 6

Mic drop

JobName	Spool	Job doc	Job CreatedB	Status
<input type="checkbox"/> RHBAUS00_BACKGRND				Finished
*Summary				

4. KEEPING ON TOP OF GLOBAL AND LOCAL HR DATA PROTECTION LAWS

You wouldn't support a finance system without understanding the financial risks so why try to secure a HR system without understanding data privacy?

Multinational Company? What's OK in one country may not be OK in another, consider regional and country based differences.

For example, did you know that in the United States, managers should not be able to view the personal data of their team?

The GDPR is a European data protection law that gives individuals more control over their personal information in the most basic interpretation. It's forced companies to reframe how they think about data privacy, making "privacy by design" paramount.

Are you focused on the data that matters? Don't spend time and effort restricting fields like first name, last name and email address which are most likely readily available in your organizations email system.

Target the high-stakes data.

What about your SAP support and technical team? Your BASIS experts, your developers, your functional experts, even your SAP security team. Is their access to personal HR data restricted in SAP?

And if not have they signed non-disclosure agreements?

5. THINKING OUTSIDE THE (HR) BOX

So, you're happy your SAP HR system is locked down. Now let's worry about when and how that data LEAVES your SAP HR system?

Pumpkin don't have a policy of scaremongering. We don't seek to win business by scaring our clients into hiring us. It just doesn't feel right. This, however, is something you do need to worry about, just a little bit. Otherwise, you risk undoing your hard work in your SAP HR system. Don't be afraid, we will hold your hand.

At Pumpkin we've seen this time and time again. A client will have a good robust SAP Security design within the SAP HR system itself. Access levels are appropriate and well managed; everybody is confident the data is secured. High-fives and back pats all around.

What has been given less thought is, where else is this data being used? We've had clients where the HR data is dropped into BW every night, with BW access levels being far too wide. We've also seen clients moving data into S/4 systems with the employees being created as Business Partners but no restriction on who can see these BP's.

A new trend made popular by a new desire for data analytics and

integration is HR data being extracted from SAP to be used for other reasons. This could be simply populating user details into an access management tool or dumping large swathes of data in a database for some future purpose.

NON PRODUCTION SYSTEMS: YOUR SAP HR DEVELOPMENT, TEST, TRAINING, SANDBOX SYSTEMS

- Is your Data scrambled? If not, do you restrict access exactly as you do in Production? *Thought not, if I was the type to want access to unauthorised HR data, I know where I'd be asking for access*

BW

- How confident are you that your HR data in BW is well protected?
- Do you have a solution for HR admins and Managers so that their access level is the same as in HR?
- What about the multitude of BW developers and administrators - can they see HR Data?

Including but not limited to:

- Do you know what employee data is available in your S/4 system?
- Do you have unique vendor / business partner authorization groups for employee?
- Are tables including personal information protected from people with table display access?
- Do you know which standard and bespoke transaction codes can display employee related info in S/4



OTHER NON-SAP INTERFACES

These days companies want to leverage the data held in SAP HR in other systems, often for perfectly risk free reasons (e.g. interfacing line managers into an IT help desk approval solution) but wherever this happens you need to think about

- What data is being extracted?
- Where does it end up?
- Who can access the data wherever it is stored?
- What if they try to extract other more sensitive data? Are interface ids restricted?



We hope you found some of these thoughts helpful. Our hope is that these informal, yet informative orange papers can provide some insight, tips and food for thought to point you in the right direction.

Of course, we would be lying if we didn't also want to blow our own trumpet and celebrate the Pumpkin way ultimately encouraging you to choose us to accompany you on your SAP authorisation improvement journey; we are a business after all.

Please do not hesitate to get in touch with us. We are as friendly as say we are or your money back.



About the author

Mark Stanley is Managing Director of Pumpkin Consulting and one of the pioneering generation of SAP security boffins. As we're sure you'll have noticed, he's very knowledgeable about and loves talking about SAP HR security so just don't sit next to him at a party.



[Follow Mark on LinkedIn](#)

CONTACT US

✉ support@pumpkinconsulting.com

☎ +44 (0)7917 518 690

📍 Pumpkin Consulting Ltd,
Cromford Creative
Cromford Mills, Mill Road,
Cromford,
DE4 3RQ
UNITED KINGDOM

www.pumpkinconsulting.com

PUMPKIN CONSULTING