Research Report | 2021

SAP Security Research Report 2021

Assessing the risk of using best practice roles in SAP S/4 HANA implementations

TURNKEY

www.turnkeyconsulting.com

Contents

SAP Security Report

01 Introduction

Despite the end of regular maintenance for SAP's ECC platform being pushed back to the end of 2027, a number of organisations have recognised the importance of migration - and the scale of the task at hand.

As such, many have already started to plan or implement their transition to S/4 HANA - around 50% of customers according to SAP's latest figures, released in 2019.

Because of the scale and complexity of the migration, many of the customers who have already made the switch, will have deployed the services of a systems integrator (SI) to support the process. Which for some, may have resulted in several areas of their deployment which need urgent security remediation.

E: info@turnkeyconsulting.com

TURNKEY

As a cloud-based system, S/4 HANA is a very different proposition to ECC, and along with the new SAP Fiori user interface opening up greater access, security has to be considered in a very different light. Despite the valuable implementation support offered by systems integrators, most are not security specialists and so they don't often have the specialist skills and expertise to ensure security is properly considered.

The biggest example of this, is how most SIs recommend the use of SAP's pre-defined 'Best Practice' roles. SAP has established around 170 of these roles that can be applied to individual users, each one giving access to a specific set of applications and authorisations. However, this 'cookie cutter' approach doesn't account for the fact that every business is different, and that applying these more general roles to users may give them more access or permissions than they should have.

Even though SAP themselves say these roles should be used as adaptable templates, many SIs implement them as they are. When this happens, proper segregation of duties (SoD) for individual users isn't put in place, and S/4 HANA is therefore implemented with inherent security risks unnecessarily - all of which will need to be remediated further down the line.

This report illustrates the scale of the problem, based on Turnkey analysis of these 'Best Practice' roles, we'll present data to help you identify potential areas for remediation within your own S/4 HANA estate.

TURNKEY

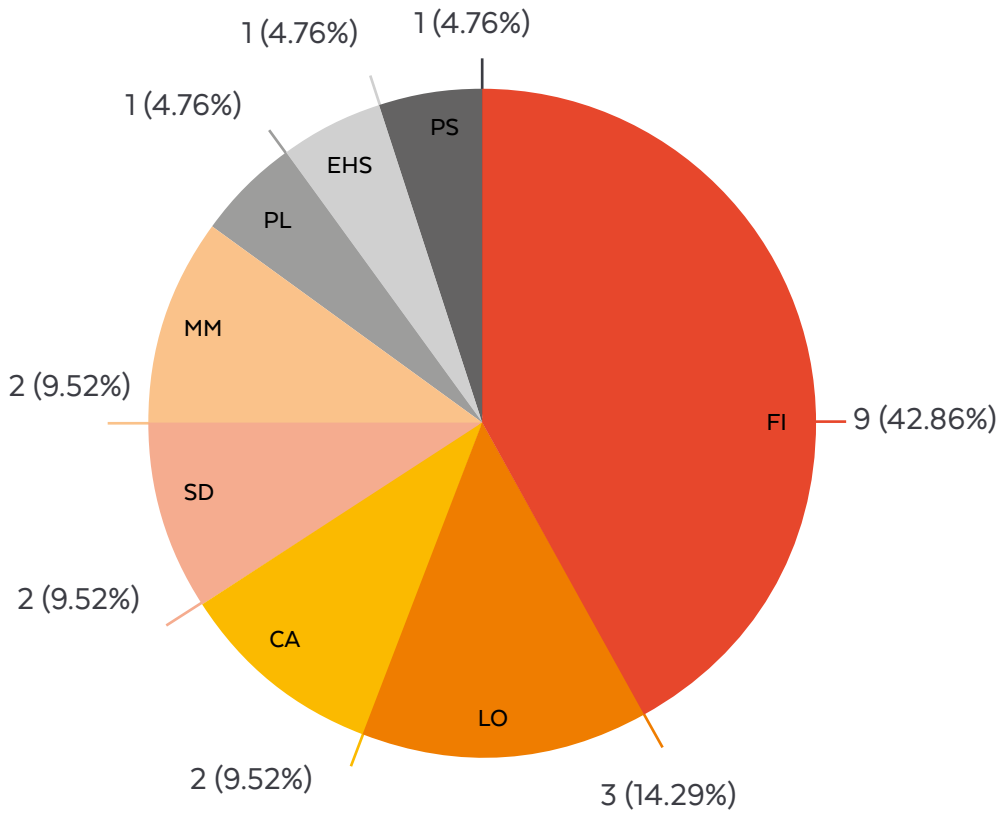
02

The data: where is the risk?

E: info@turnkeyconsulting.com

TURNKEY

Number of roles per process



"With SAP's focus on finance at the core of ERP, it isn't surprising to see that most roles focus on this area. If you've already transitioned to SAP S/4 HANA, start by looking into your finance roles, as this is the area most likely to contain SoD risks"

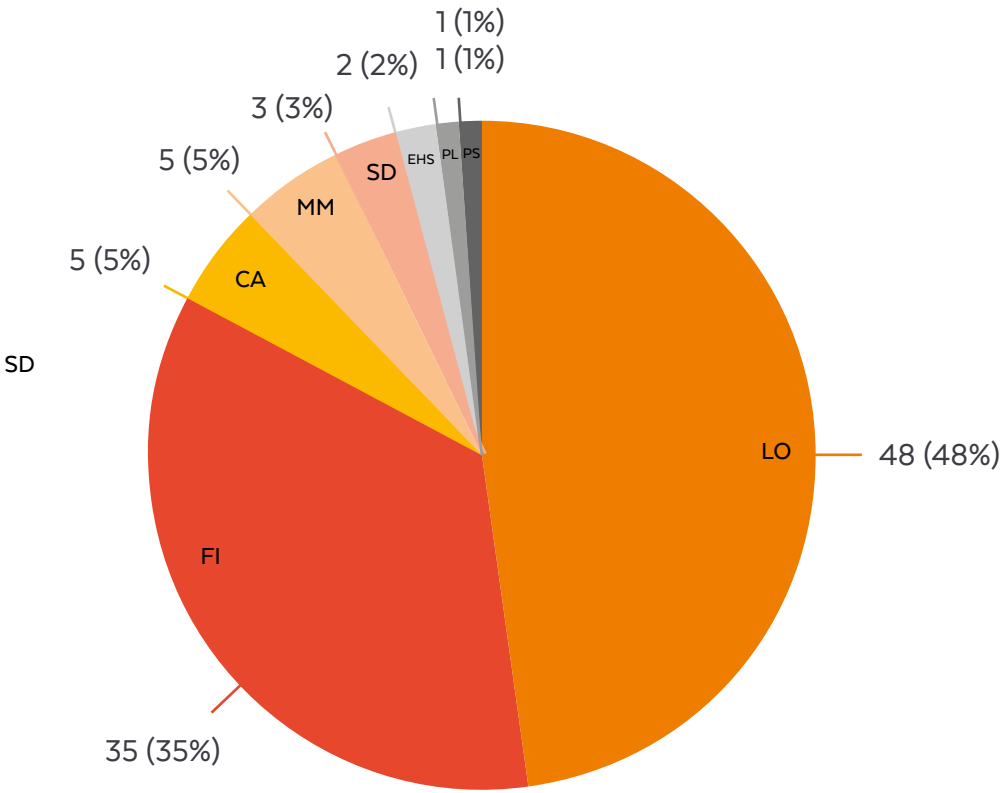
Commentary from Tom Venables, Practice Director, Cyber and Application Security, Turnkey.

Process	No of Roles
FI	9
LO	3
CA	2
SD	2
MM	2
PL	1
EHS	1
PS	1
Total	21

E: info@turnkeyconsulting.com

TURNKEY

Number of risks corresponding to all roles within a process



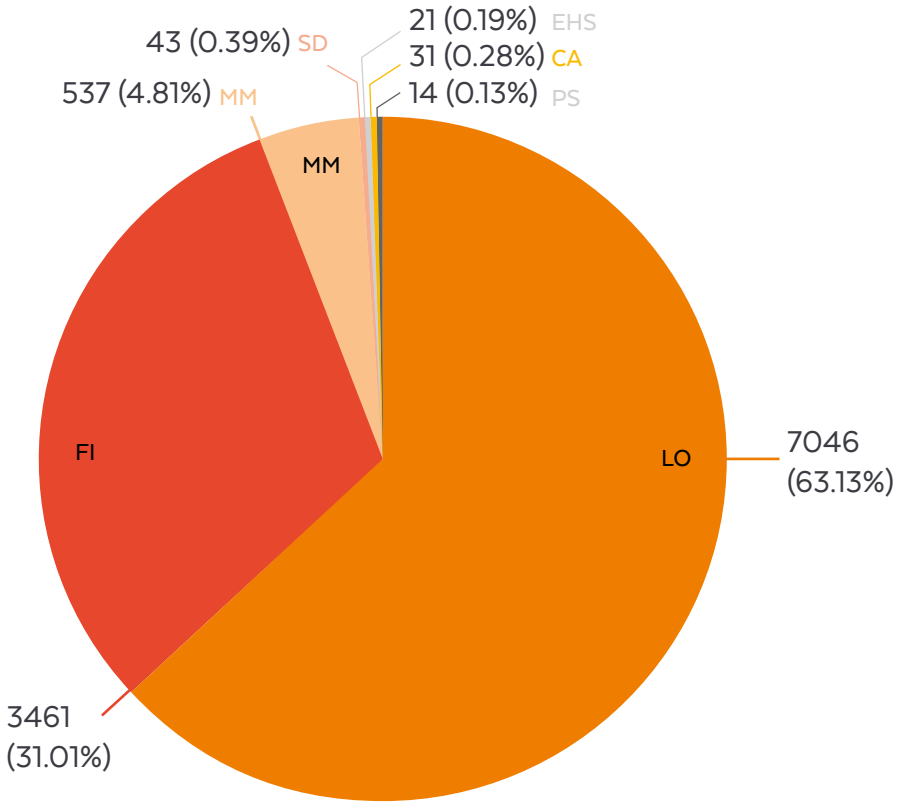
"The high number of risks for logistics despite its smaller number of roles should make it a focus of your review, alongside the finance function, which represents the second highest number of risks if not properly remediated"

Commentary from Tom Venables, Practice Director, Cyber and Application Security, Turnkey.

Process	No of Roles	No of Risks
FI	9	35
LO	3	48
CA	2	5
SD	2	3
MM	2	5
PL	1	1
EHS	1	2
PS	1	1
Total	21	100

TURNKEY

Number of violations corresponding to the roles within a process



"This finding demonstrates the effort required to remediate the risks within each role. While only one risk may be realised, the number of ways it can be executed are far greater. This means that wider roles bring with them a greater capability of a risk being realised. Again, this suggests that the finance and logistics functions are logical places to start when remediating the security of your S/4 HANA environment "

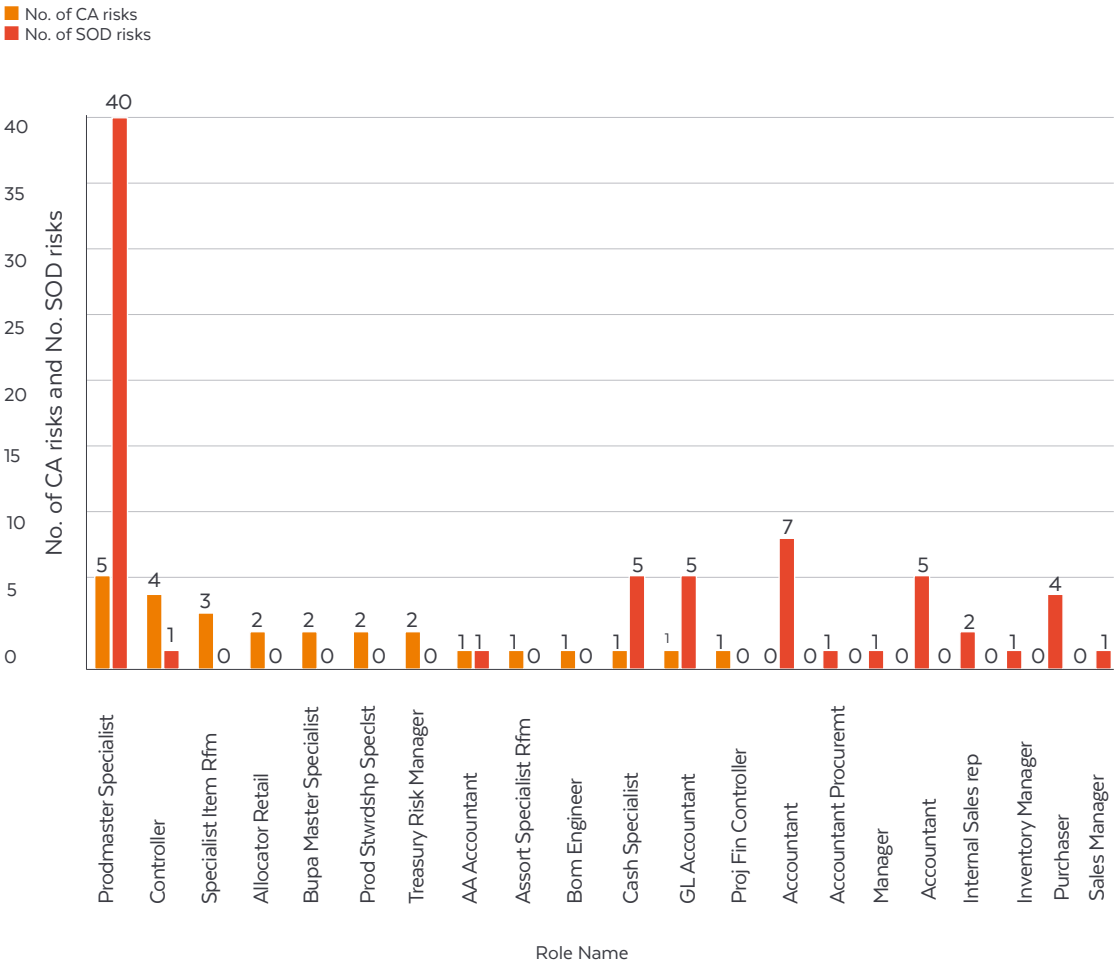
Commentary from Tom Venables, Practice Director, Cyber and Application Security, Turnkey.

Process	No of Roles	No of Risks	No of Violations
FI	9	35	3461
LO	3	48	7046
CA	2	5	31
SD	2	3	43
MM	2	5	537
PL	1	1	8
EHS	1	2	21
PS	1	1	14
Total	21	100	11161

E: info@turnkeyconsulting.com

TURNKEY

Roles broken down by risk type



“This graph demonstrates just how varied the risks can be between roles. Remediating the roles which present the greatest risk, is therefore going to have the biggest impact, helping you to secure your S/4 HANA environment in the shortest space of time”

Commentary from Tom Venables, Practice Director, Cyber and Application Security, Turnkey.

03

Summary - the risk of best practice roles

E: info@turnkeyconsulting.com

TURNKEY

It's clear that even just a few poorly-implemented roles can lead to large numbers of risks. Furthermore, relying solely on SAP's 'Best Practice' roles can lead to risks across an entire organisation, and the impact of these risks can be severe and far-reaching.

When roles are not segregated properly, the dangers to businesses include (but are not necessarily limited to):

- Legal: criminal investigations due to fraud, false accounting, or other compliance-related issues
- Financial: lost revenue through inefficiencies in operations, or through accounting and data errors
- Organisational: disruption to business processes that make it harder for employees and departments to be productive day-to-day
- Reputational: brand damage and negative publicity caused by any of the above becoming public knowledge

It should also be noted that as well as the risks to security, these generic roles also contribute to poorer user experiences. By being able to access a wider range of applications and authorisations, users may have to search through hundreds of choices to find those they need, adding to the complexity of using S/4 HANA efficiently.

As highlighted by the conflicts identified in this report, the solution to both of these issues is to separate roles much more thoroughly and ensure access is tied to business processes as much as possible. With the right levels of access put in place, the SoD risks within an S/4 HANA implementation can be vastly reduced.

TURNKEY

Four keys to a successful SAP S/4 HANA security migration

As this report has established, security is an absolutely vital consideration when implementing S/4 HANA. If a migration has been conducted without taking these four points into account, then now is the time to re-evaluate the potential risks and take action, partnering with an SAP security specialist if necessary:

1

Understand your ECC usage data: in brownfield migrations, analysing usage data of business processes not being fully redesigned is ideal for benchmarking ECC data, and being able to project usage in S/4 HANA.

2

Assess data and align to retained business processes: although transaction code changes in S/4 HANA make this a complex task, this data is vital in informing future process designs.

3

Analyse risk gaps and create mitigating controls: it's unlikely that every risk can be eliminated, even when roles are separated to the maximum level they can be without impairing operations. Controls should be put in place to mitigate the risks that remain, once they've been identified.

4

Evaluate the impact of SAP Fiori: security must also be considered in the context of Fiori, SAP's new primary user interface, when designing back-end roles. SAP's standard business roles are normally used by SIs and these don't offer the protection of a security-by-design approach.

E: info@turnkeyconsulting.com

About Turnkey

Turnkey have a proven track record with regards to security programmes. Our tried and tested methodology facilitates a robust approach within an accelerated timeframe, ensuring a successful outcome feeding into the implementation of solutions and the realisation of associated benefits.

Turnkey's substantial experience performing such engagements mean that common challenges associated with securing systems against risk have been identified and overcome, allowing us to work with you to define strategies which fit to your business and avoid regret costs associated with less integrated and methodical solutions.

Turnkey's global offices:
United Kingdom
United States
Australia
Germany
Malaysia
Singapore
France

Head Office:
Turnkey Consulting Ltd
58 Ayres Street
London
SE1 1EU

T: +44 (0)207 288 2578
E: info@turnkeyconsulting.com

Integrated Risk Management

Identity & Access Management

Cyber & Application Security

SAP Partner

www.turnkeyconsulting.com