Secure.Compliant.Audit-ready authorisation concept for S/4

Are you really ready for S/4HANA Go-live?

Experience on how to tackle audit risks, compliance gaps and access issues from day one.

SAPSA Impuls Göteborg April 2026

DigitalTrust

WHO WE ARE


ERP
S/4HANA AI powered Migration
Business process optimization
SAP – Salesforce connector
MIGNOW
SAP
SAP Strategy and License Management
S/4 License conversions
SAP Strategy
License optimizations
License and contract reviews
M&A advisory
DigitalTrust
Data Ethics
SAP S/4 & ECC Authorizations
SAP Cybersecurity
SAP Compliance
Access & Identity Management
GDPR Management
Secure Logging
ONAPSIS
Compliance Now
Customer Platform Services
CIAM
SAP CDC and CDP
Customer Loyalty
Consent Management
BTP – Integration Suite & Event Mesh

WHO WE ARE

Troels Lindgård

E: Troels.Lindgaard@1digitaltrust.com

M: +45 5363 5787

WWW.1DIGITALTRUST.COM

Troels has worked with SAP Compliance since 2004. He has gained extensive experience as an SAP Compliance lead and project manager, having worked on some of the most complex SAP platforms.

Troels has been involved in all project phases, from estimation and planning—including requirements specification—through implementation, roll-out, and subsequent administration.

Troels began his career as an internal SAP Compliance consultant, giving him strong insight into how SAP Compliance should be designed and implemented to ensure efficient support after go-live. He has also worked as a solution architect and project manager within development and roll-out projects.

Many of Troels' projects have been carried out in close collaboration with SAP, where he has established a strong professional network.

Troels has been responsible for driving and ensuring the successful delivery of SAP Compliance projects, including ensuring that projects are delivered within the defined scope and aligned with the capabilities of SAP Compliance departments.

Customer cases

DigitalTrust

CUSTOMER CASES

AJVaccines

S/4 Greenfield implementation
+600 users

AAK

S/4 Brownfield implementation
+2000 users

TOYOTA

MATERIAL HANDLING

S/4 Greenfield implementation
+3000 users

Epiroc

S/4 Greenfield implementation
+2000 users

Audit risks, compliance gaps and access issues

DigitalTrust

AUDIT RISKS, COMPLIANCE GAPS AND ACCESS ISSUES

Excessive Authorizations and Security Risks

Roles are often too **generic** and **overly permissive**, granting broad access to transactions and Fiori apps beyond what most users need.

This **violates** the **principle of least privilege**, increasing the **risk** of **data breaches**, **fraud**, and **insider threats.**

Example: A role **might** allow both invoice creation and approval, creating a Segregation of Duties (SoD) conflict **AND** reports and display access.

Excessive use of standard roles

Regulatory frameworks like **SOX**, **GDPR**, **HIPAA require strict access controls** and **audit trails**.

Existing and Standard roles often **fail** these requirements because they:

- **Lack SoD** enforcement.
- **Contain excessive** access.

Result: Audit findings, and reputational damage, negative impact on stock prices.

Misalignment with S/4HANA Architecture

S/4HANA introduces:

- **Fiori-first approach** (apps replace many transactions).
- **Business Partner (BP)** model (merging vendor/customer data).
- **Embedded analytics** and **CDS views**.

Existing ECC roles were designed for ECC and do not reflect these changes fully, leading to:

- **Missing access for new apps.**
- **Redundant or obsolete authorizations**.
- **Operational disruptions during migration**.

Limited Flexibility and Poor Maintainability

Existing and Standard roles are **not tailored** to your new **business processes**.

They make it **hard to**:

- **Adapt** to **organizational changes.**
- **Implement custom workflows**.

SAP updates can **modify standard roles**, breaking existing access and requiring rework.

Increased Complexity and Cost

Using existing or standard roles often leads to:

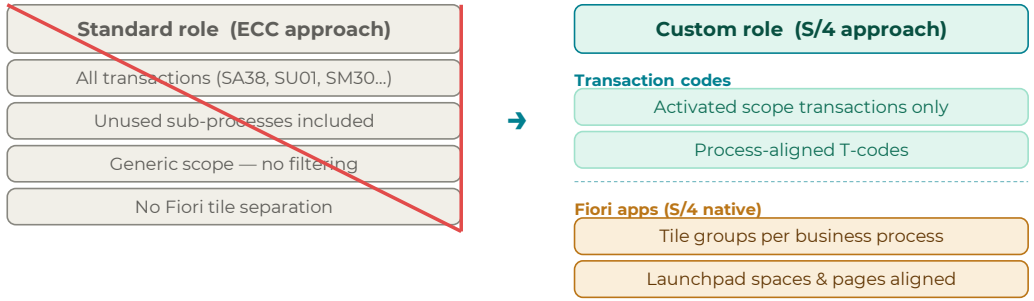
- **Over-licensing** (roles include apps that trigger higher license categories).
- **Higher operational costs** for audits and corrections.

Managing SoD conflicts in standard roles is cumbersome compared to custom role design.

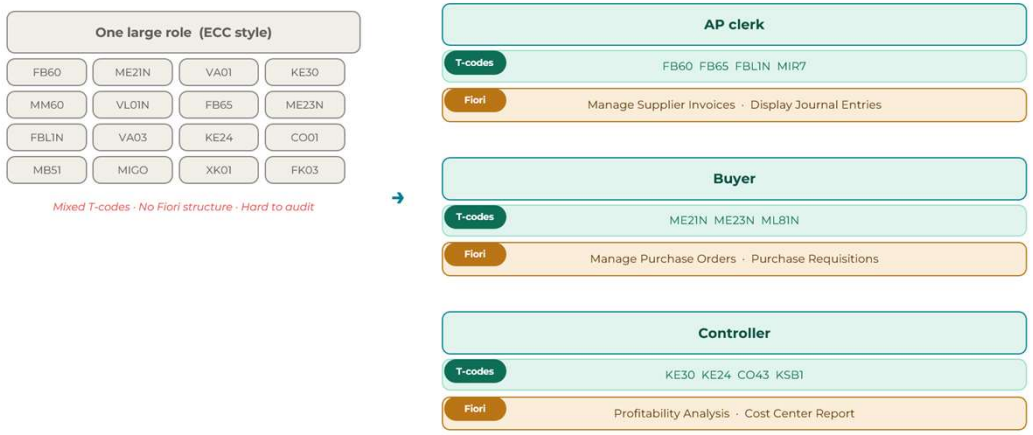
Analysis shows, that **95% of SAP standard roles** require a **higher per user license category**, than custom process fitted roles.

AUDIT RISKS, COMPLIANCE GAPS AND ACCESS ISSUES

Avoid using standard roles beyond the discovery phase. Instead, start **building custom roles early**, aligned with activated scope items, business processes, and defined sub-processes. Whether you "**lift-and-shift**" your authorization concept to S/4, or follow "**Fiori first**" principles, your role concept requires firm principles to support **SoD** and **FUE compliance.**

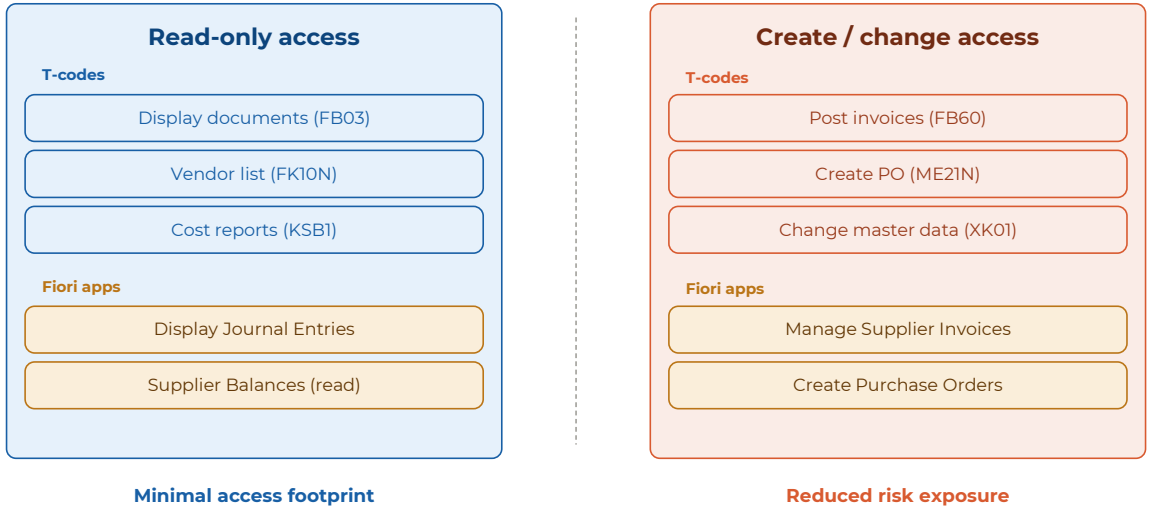


Design roles around **how users actually work**, grouping transaction codes and Fiori apps where they fit naturally, and **keep roles as small and focused as possible**.

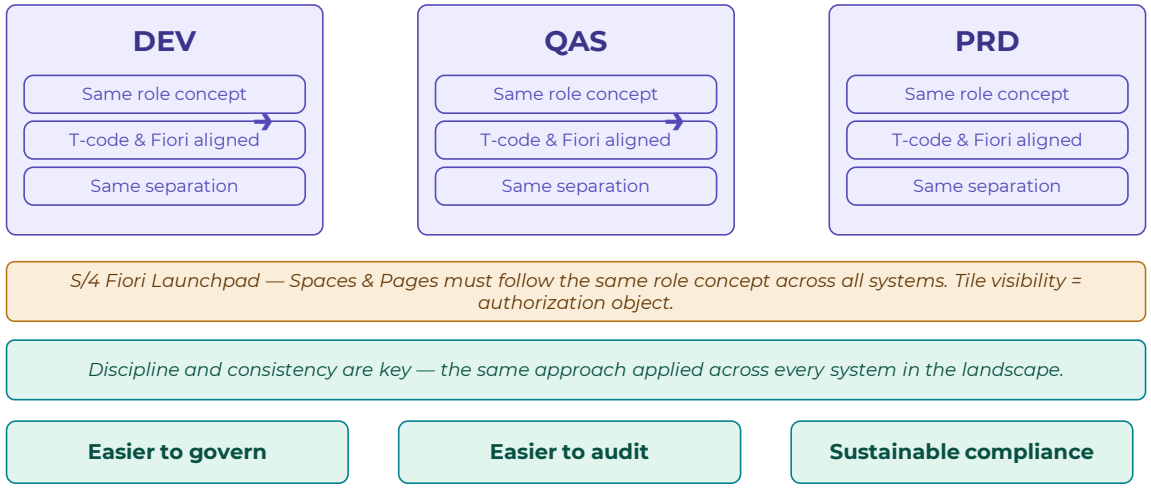


AUDIT RISKS, COMPLIANCE GAPS AND ACCESS ISSUES

Clearly **separate display, reporting, and analytical access from create and change permissions**. This **enables** a **minimal access footprint** for users who only require read-only or limited functionality, while reducing overall risk exposure.



Apply this approach consistently across the landscape, discipline and consistency are key. By doing so, you establish a role concept that is easier to govern, easier to audit, and ultimately results in manageable and sustainable compliance.



SAP Authorization Assessment

DigitalTrust

… Where do we start?

Do you know if your SAP environment is exposed by SoD risk?

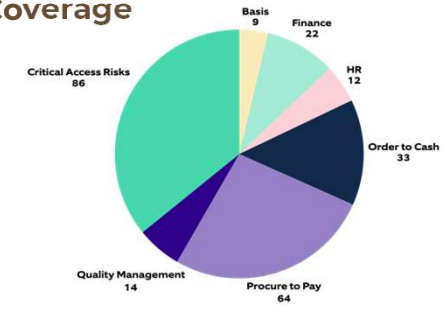
We begin every engagement by establishing a clear baseline. For organizations without an in-house SoD tool, we leverage **ComplianceNow AC** to perform a one-time, offline analysis. This quick and efficient assessment delivers:

- **Minimal time investment** for your team
- A **comprehensive overview** of Segregation of Duties (SoD) and critical access risks
- Actionable insights to determine whether these risks exist and require attention

This initial analysis provides clarity and confidence, helping you prioritize next steps effectively and with full transparency

ComplianceNow's risk library was developed as a proprietary asset of CN Access Control (the ComplianceNow SAP SoD tool). The primary aim of the risk library is to address common SAP risk areas, including SAP Security, SAP Basis, HR/Payroll, Finance, Procure to Pay, Order to Cash, and Quality Management — and is applicable across various industries. The risk library covers **154 SoD risks and 86 critical access risks**. The CN Risk Library is reviewed **annually by PwC** to ensure alignment with current best practices.

CN Risk Library Coverage



Output results

- Complete summary report of all SoD risks and Critical Access risks in the system by group.
- Detailed summary report detailing number of roles which each have risk.
- Details on individual risk – *only* first 5 in each group is shown.

Dependencies

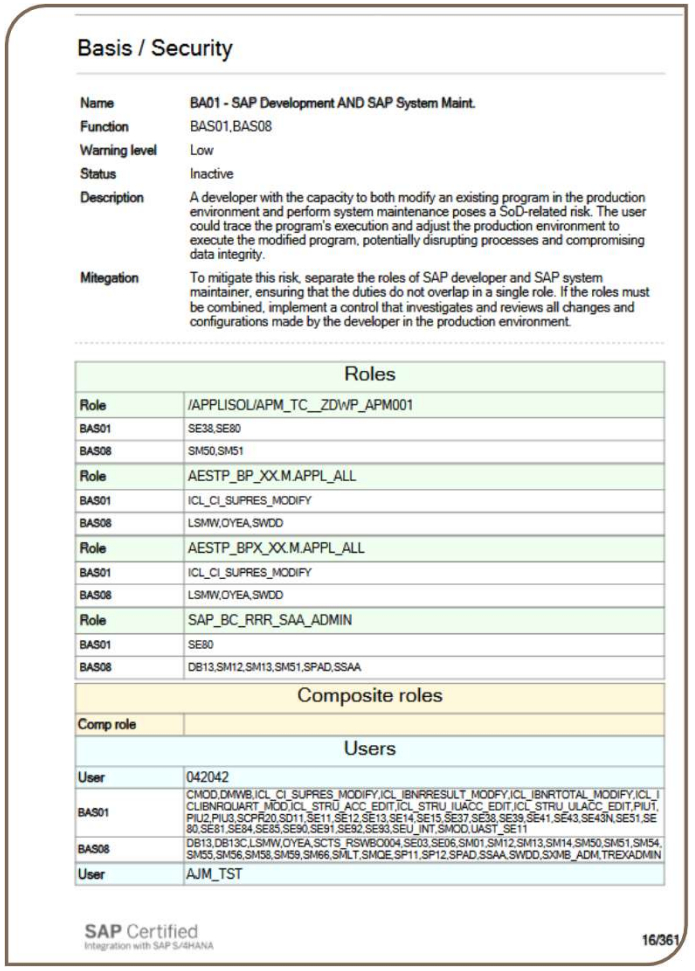
- Temporary offline license from Nagarro.
- An SAP user with specific user authorizations.
- The analysis runs directly from a client PC, with no SAP system installation needed.
- The analysis takes 10-30 minutes.

Has your organization debated whether it’s time to introduce tools into your SAP risk management strategy?

Strengthening Internal Decision-Making
Our offline analysis does more than provide data—it **empowers informed discussions within your organization**. By delivering **clear, fact-based insights**, it enables you to:

- **Assess the true scale of SoD and critical access risks**
- Determine whether these issues warrant **immediate attention and prioritization**

While the analysis itself does not initiate risk remediation, it serves as a **strategic enabler**. Running this assessment gives your team a **solid, evidence-backed foundation** for building a compelling business case to implement a robust SoD process. This foundation makes it **easy to communicate the urgency and value of action to stakeholders**, ensuring alignment and accelerating decision-making.



Basis / Security

Name	BA01 - SAP Development AND SAP System Maint.
Function	BAS01,BAS08
Warning level	Low
Status	Inactive
Description	A developer with the capacity to both modify an existing program in the production environment and perform system maintenance poses a SoD-related risk. The user could trace the program's execution and adjust the production environment to execute the modified program, potentially disrupting processes and compromising data integrity.
Mitegation	To mitigate this risk, separate the roles of SAP developer and SAP system maintainer, ensuring that the duties do not overlap in a single role. If the roles must be combined, implement a control that investigates and reviews all changes and configurations made by the developer in the production environment.

Roles	
Role	/APPLISOL/APM_TC__ZDWP_APM001
BAS01	SE38,SE80
BAS08	SM50,SM51
Role	AESTP_BP_XX.M.APPL_ALL
BAS01	ICL_CI_SUPRES_MODIFY
BAS08	LSMW,OYEA,SWDD
Role	AESTP_BPX_XX.M.APPL_ALL
BAS01	ICL_CI_SUPRES_MODIFY
BAS08	LSMW,OYEA,SWDD
Role	SAP_BC_RRR_SAA_ADMIN
BAS01	SE80
BAS08	DB13,SM12,SM13,SM51,SPAD,SSAA
Composite roles	
Comp role	
Users	
User	042042
BAS01	CMOD,DMWB,ICL_CI_SUPRES_MODIFY,ICL_IBNRRESULT_MODFY,ICL_IBNRTOTAL_MODIFY,ICL_ICLIBNRQUART_MOD,ICL_STRU_ACC_EDIT,ICL_STRU_IUACC_EDIT,ICL_STRU_ULACC_EDIT,PIUT,PIU2,PIU3,SCPR20,SD11,SE11,SE12,SE13,SE14,SE15,SE37,SE38,SE39,SE41,SE43,SE43N,SE51,SE80,SE81,SE84,SE85,SE90,SE91,SE92,SE93,SEU_INT,SMOD,UAST_SE11
BAS08	DB13,DB13C,LSMW,OYEA,SCTS_RSWBO004,SE03,SE06,SM01,SM12,SM13,SM14,SM50,SM51,SM54,SM55,SM56,SM58,SM59,SM66,SMLT,SMQE,SP11,SP12,SPAD,SSAA,SWDD,SXMB_ADM,TREXADMIN
User	AJM_TST

SAP Certified
Integration with SAP S/4HANA

16/361

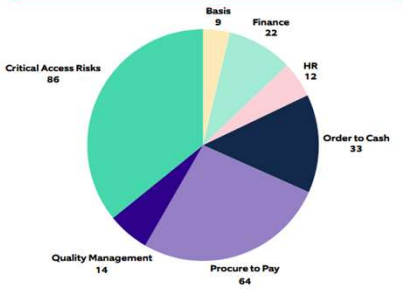
COMPLIANCENOW ACCESS CONTROL

What Risks Does The Analysis Check Against?

ComplianceNow's risk library was developed as a proprietary asset of CN Access Control (the ComplianceNow SAP SoD tool). The primary aim of the risk library is to address common SAP risk areas, including SAP Security, SAP Basis, HR/Payroll, Finance, Procure to Pay, Order to Cash, and Quality Management — and is applicable across various industries. The risk library covers **154 SoD risks and 86 critical access risks.**

The CN Risk Library is reviewed annually by PwC to ensure alignment with current best practices. Any findings or recommendations from the audit are incorporated into the ruleset as part of the continuous updates.

CN Risk Library Coverage



Output Results

- Complete summary report of all SoD risks and Critical Access risks in the system by group.
- Detailed summary report detailing amount of roles which have each risk.
- Details on individual risk – only first 5 in each group is shown.

Dependencies

- Temporary offline license from Nagarro.
- An SAP user with specific user authorizations.
- The analysis runs directly from a client PC, with no SAP system installation needed.
- The analysis takes 10-30 minutes.

- **Complete summary report of:**
  - **all SoD risks**
  - **Critical Access risks in the system by group.**
- **Detailed summary report detailing amount of roles which have each risk.**
- **Details on individual risk – only first 5 in each group is shown.**
- **The analysis is based on CN Risk Library is reviewed annually by PwC.**

ComplianceNow

One-Time System Compliance and authorization Assessment with ComplianceNow AC

Our one-time Compliance and authorization Assessment provides a clear, accurate view of your SAP system's compliance and authorization posture. Using the ComplianceNow platform, we perform a full analysis of your environment and deliver a concise, actionable report that highlights risks and recommendations.

A

What We Do

Run a comprehensive ComplianceNow analysis of your SAP system

Identify SoD and authorization risks

Analyze the findings to determine business impact and prioritize critical issues

B

What You Receive

Executive summary outlining overall system health

Detailed findings with severity ratings and affected components

Actionable recommendations for remediation and hardening

Review meeting to walk through the results and answer questions

C

Value for You

Immediate visibility into key security gaps

Expert guidance on how to reduce risk quickly

A clear roadmap for strengthening your SAP Compliance and Authorizations.

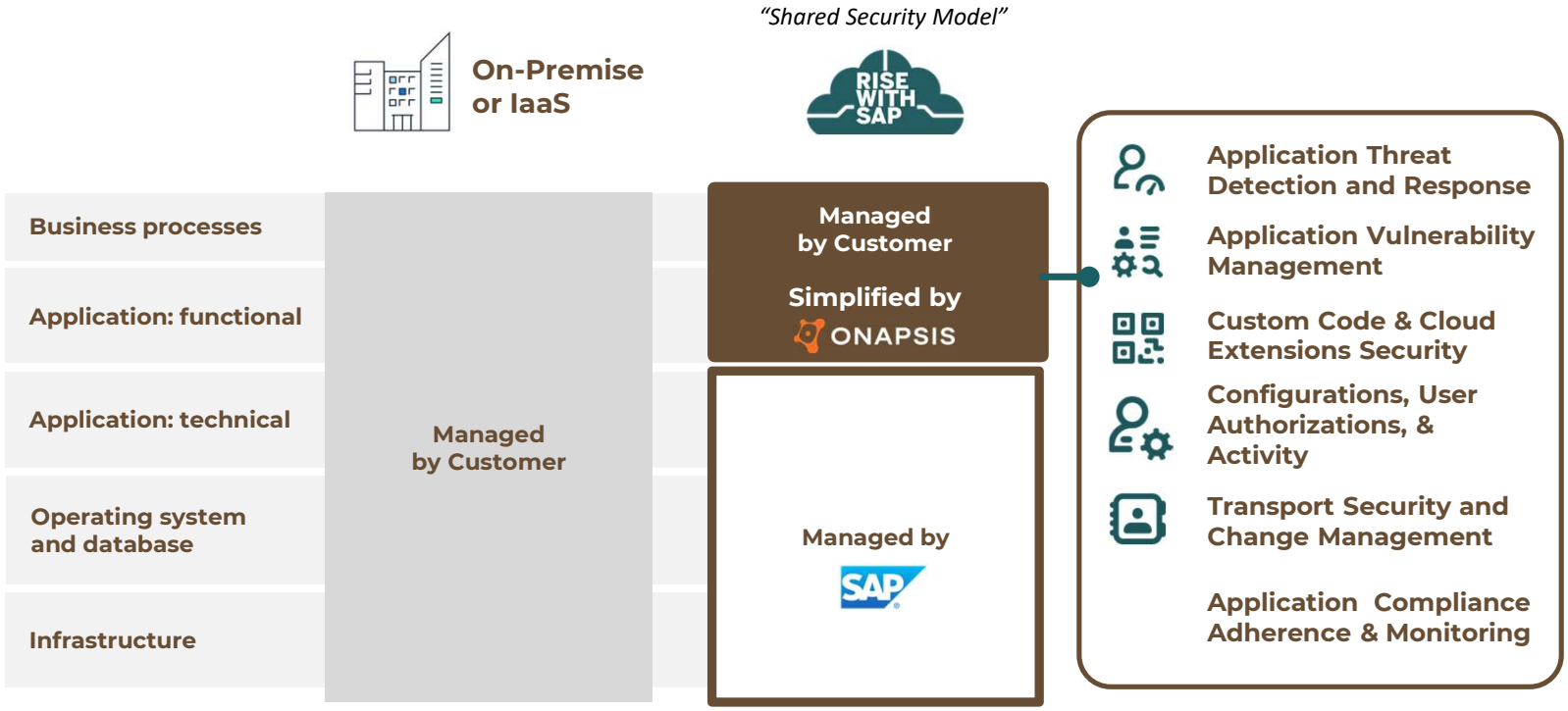
70.000 SEK

ComplianceNow

DigitalTrust

ONE MORE THING .... SAP CYBER SECURITY SHARED RESPONSIBILITY

What Do Clients Need to Consider Embarking On Transformation. SAP-Endorsed Solution for Cybersecurity - THEIR Shared Responsibilities.



"In the context of SAP RISE, the customer still keeps the ownership and responsibility to secure the application layer"

Roland Costea, Global Chief Security Officer for SAP Enterprise Cloud Services

Thank you

www.1digitaltrust.com

1DigitalTrust

FROM COMPLIANCE TO CONTROL: PRACTICAL TAKEAWAYS

Standard SAP roles are not go-live ready

- They are overly generic, violate least-privilege principles, and drive SoD, audit, security, and licensing risks when reused in S/4.

S/4HANA changes the authorization paradigm

- Fiori-first, Business Partner model, and embedded analytics require a redesigned role concept, not a technical ECC lift-and-shift.

Custom, process-aligned roles must be designed early

- Roles should be small, business-driven, aligned to activated scope items, and explicitly support SoD and FUE compliance from day one.

Separating read vs. create/change access is critical

- Consistent separation across DEV, QAS, and PRD reduces risk exposure, simplifies audits, and enables sustainable compliance.

Go-live readiness requires fact-based risk insight

- A one-time SAP authorization and SoD assessment provides a baseline, exposes hidden risks, and enables informed decisions before production start.

Contact us

We are always keen to talk SAP
... or wine

Thomas Bladh

E: thomas.bladh@1digitaltrust.com

M: +46 70-550 49 13

Troels Lindgård

E: Troels.Lindgaard@1digitaltrust.com

M: +45 5363 5787

AI IN SAP
Benchmark 2026

AI in SAP Benchmark 2026

Participate and benchmark your organization with SAP peers - And WIN !!!

IT Optimiser
Home of SAP specialists

DigitalTrust