WHITE PAPER

ENSURING DATA SECURITY, CONFIDENTIALITY, AND PRIVACY FOR ERP TRANSFORMATIONS

NEXTLABS

Infosys®
Navigate your next

Introduction

Fluctuating economic times have heightened the digital agenda for many organizations as they pivot to adjust to new market realities. Modernizing one's ERP system and capitalizing on intelligent automation capabilities can help harness the necessary agility and data insights to compete in today's increasingly challenging business environment.

While working toward becoming an intelligent enterprise, many organizations are consolidating their ERP systems as they are modernizing. In doing so, it allows them to unlock the benefits of digital transformation, such as increased efficiency, greater business agility, and creating new value for employees, customers, and shareholders.

However, digital transformation requires a new mindset, allowing enterprises to reimagine business processes. One area that's receives less attention but is critical to the success of ERP transformations is ensuring data security, confidentiality, and privacy for sensitive information involved in the digital transformations. Explore in this white paper how enterprises can factor in data security when embarking on their ERP transformation.

Common Challenges for ERP Transformation

Enterprise Resource Planning (ERP) systems are often seen as the backbone of an intelligent enterprise, as they can accelerate innovation, data delivery, and business intelligence. However, ERP transformations can raise many challenges as it affects business processes across the entire organization, replacing longstanding manual processes with ones that are more efficient and automated. In order to realize the benefits of an ERP transformation, it's critical that the data of these processes remain secure. Some of the common challenges enterprises face when ensuring data privacy and confidentiality in ERP transformations are:

Data Privacy and Compliance:

With the proliferation of data privacy regulations, such as GDPR, CCPA, SOX, or industry-specific standards like CMMC, ITAR, EAR, GLBA, HIPAA, organizations face increasing pressure to protect sensitive data and comply with stringent requirements.

Single Global Instance:

With the consolidation of data into a single instance, it's critical to ensure need-to-know access so only authorized users can access data they are entitled to.

Insider Threats and Data Leakage:

Organizations face the risk of insider threats, where employees or authorized individuals may misuse or leak sensitive data.

Data Governance and Data Management Complexity:

As organizations accumulate vast amounts of data from multiple sources, data governance and management become increasingly challenging.

Collaboration and Data Sharing Requirements:

Organizations often need to collaborate with external partners, suppliers, or customers, requiring controlled data sharing.

Taking a Closer Look

When taking a closer look at the areas that are that are being overhauled as part of an ERP transformation, one will see that there are many cross-functional business areas that need to be considered when ensuring the security of these processes. Some of these cross-functional business areas include:

Security Challenges Encountered in

Procure to Pay

- Protect sensitive vendor information
- Safeguard material/transfer pricing data
- Segregate access in cases of divestiture

Plan to Produce

- Safeguard sensitive bill of material (BOM) information
- Protect business-critical drawings and designs

Record to Report

- Protect sensitive pricing information
- Segregate access in case of divestitures
- Fine-grained access restriction based on cost/profit center

Procure to Pay

This process cuts across multiple functional areas like procurement, warehouse management and financial accounting (accounts payable) and is one of the most common business processes which undergoes transformation. The process starts with a purchase requisition or purchase order and goes on through goods receipt, invoicing and payment. There are different variations of this process depending on the type of organization or type of good / services procured. The whole process might not be running through one application and often involves multiple applications e.g. one for procurement activities and the other for accounting / payments.

Protecting sensitive vendor information, material pricing / transfer pricing information, segregating access in cases of divestures are some of the data security related challenges that are commonly observed in this process.

Plan to Produce

This process cuts across multiple functional areas like demand forecasting, supply planning and production. It starts with analysis of historical sales data to carry out demand forecasting which leads to planning for the resources required to produce the necessary goods. This planning exercise provides input to the procurement team to procure the required materials in line with the plan. Once the demand and supply plans are in place, production scheduling is carried out to produce goods. This process again might not be running through one application and often involves multiple applications e.g. one for demand / supply planning and other for production.

Protecting sensitive material bill of material information, drawings / designs are some of the data security related challenges that are commonly observed in this process.

Record to Report

This process is limited to the functional area of financial accounting where the objective is to produce complete and accurate financial statements for the company. The process starts with recording of transactions either automatically through the other processes (e.g. procure to pay / order to cash) or through manual entry (e.g. manual journal entries). Transactions recorded are then reconciled periodically and later presented in the form of financial statements adhering to different regulatory reporting requirements. The whole process is often run in the same application, but sometimes different applications are used for recording, reconciliation, and reporting.

Protecting sensitive pricing information, segregating access in cases of divestures, applying fine-grained access restrictions based on cost center / profit center are some of the data security related challenges that are commonly observed in this process.

Introducing a Solution

ERP transformations often consist of data consolidation, which offers benefits such as simplification, unified business processes, cut costs, and better data quality due to easy analysis from a single pane of glass. These benefits also allow for quicker and better decision making, which improves execution.

To unlock the benefits from consolidation, enterprises need a way to dynamically segregate information when consolidated into one source to ensure in real-time the security, confidentiality, and privacy of data when being accessed.

By using logical data segregation and obfuscation, enterprises can separate data based on specific criteria, such as sensitivity, access requirements, or functional requirements. It involves implementing measures to control access, visibility, and security of data based on its classification, user roles, or other relevant factors.

Strategy to Enable Data Security, Confidentiality, & Privacy for ERP Transformations

When enterprises consolidate data for ERP transformation, it also introduces the need to automate access controls to ensure the security, confidentiality, and privacy of data. To achieve this, enterprises need to utilize a policy platform that incorporates attribute-based policies, dynamic authorization, and zero trust principles to aid in access decision making. Said platform needs to be combined with an enforcement approach that uses logical data segregation and obfuscation to enhance data management, security, and privacy. There are several techniques and strategies enterprises can employ to logically segregate data. The specific technique an enterprise selects will depend on the nature of the data and organizational requirements. The following are some commonly used techniques for logical data segregation and obfuscation:

Data Segmentation:

Enables data to be segregated logically by dividing data into smaller, and more manageable partitions based on specific criteria. It can be divided logically based on attributes or characteristics such as data type, sensitivity level, departmental boundaries, geolocation, or access patterns. This segmentation helps enforce data separation and allows for more granular access controls, allowing only need-to-know access when data is consolidated.

Data Masking:

Allows for data to be segregated by replacing sensitive data with fictitious but realistic values using techniques such as nulling out, encryption or substitution. This technique allows organizations to protect sensitive data while still preserving the format and structure required for analysis or application testing. Data masking helps maintain data privacy and security while allowing access to non-sensitive or anonymized data.

Data Filtering:

Another technique to logically segregate data is data filtering. It works by applying filters to data sets to control access and visibility based on specific criteria. Data filtering can be implemented at the application and data access layer, ensuring that users can only access data they are authorized to. Approaches to filter data include: row-level filtering, column-level filtering, attribute-based filtering, time-based filtering, location-based filtering, and custom filtering rules.

Access Control:

Using attribute-based access control (ABAC), companies can ensure that users are only able to access the data they are authorized to see. With the implementation of ABAC, data access is restricted by policy that is based on identity, role, user attributes, and metadata. This enhances logical data segregation by enabling least privilege access based on dynamic and context-aware access control policies to ensure that only authorized individuals or systems can access specific datasets.

Digital Rights Management (DRM):

This technique works by applying rights protection to selected files based on policy, ensuring persistent protection of sensitive information at rest, in transit, and throughout its lifecycle. DRM helps prevent unauthorized access even if the data is compromised or misdirected. It also employs policy-based authorization with strong encryption algorithms and secure key management practices to ensure the integrity and confidentiality of the data.

By implementing effective data segregation practices based on zero trust principles, organizations can achieve efficient data management and safeguard their consolidated ERP data, all while maintaining trust with stakeholders, and reducing the potential negative consequences associated with data breaches or non-compliance.

Case in Point: Enhancing Security for Plan to Produce Transformation

To get a better picture of how enterprises can use different techniques to implement data security, confidentiality, and compliance for ERP transformation, let’s take a closer look at 2 use cases of the PL2PR (Plan to Produce) value stream as it is one of the most common business processes that undergoes transformation and consolidation.

Use Case-1: Enable Export Control Compliance with Dynamic Data Masking & Filtering

Bill of Material (BOM) is one of the key data objects in Plan to Produce. Protecting sensitive BOMs or BOM components within the BOM explosion is critical as many enterprises need to comply with export control regulations such as US and Swiss Export Control. These requirements can be addressed using dynamic data filtering, which enables sensitive BOM or BOM components are not disclosed to unauthorized users.

Below find the security dimensions and user permissions for Use Case 1:

Security Dimension: *US Export Control - ITAR*

User ID	User’s Security	Expected Behavior
DEMOUSER_01	US Citizen	Can access BOM and all components within BOM
DEMOUSER_02	Non-US Person / Entity with ITAR license	Can access BOM and all components within BOM
DEMOUSER_03	Non-US Person without ITAR license	Can access BOM but ITAR components filtered out

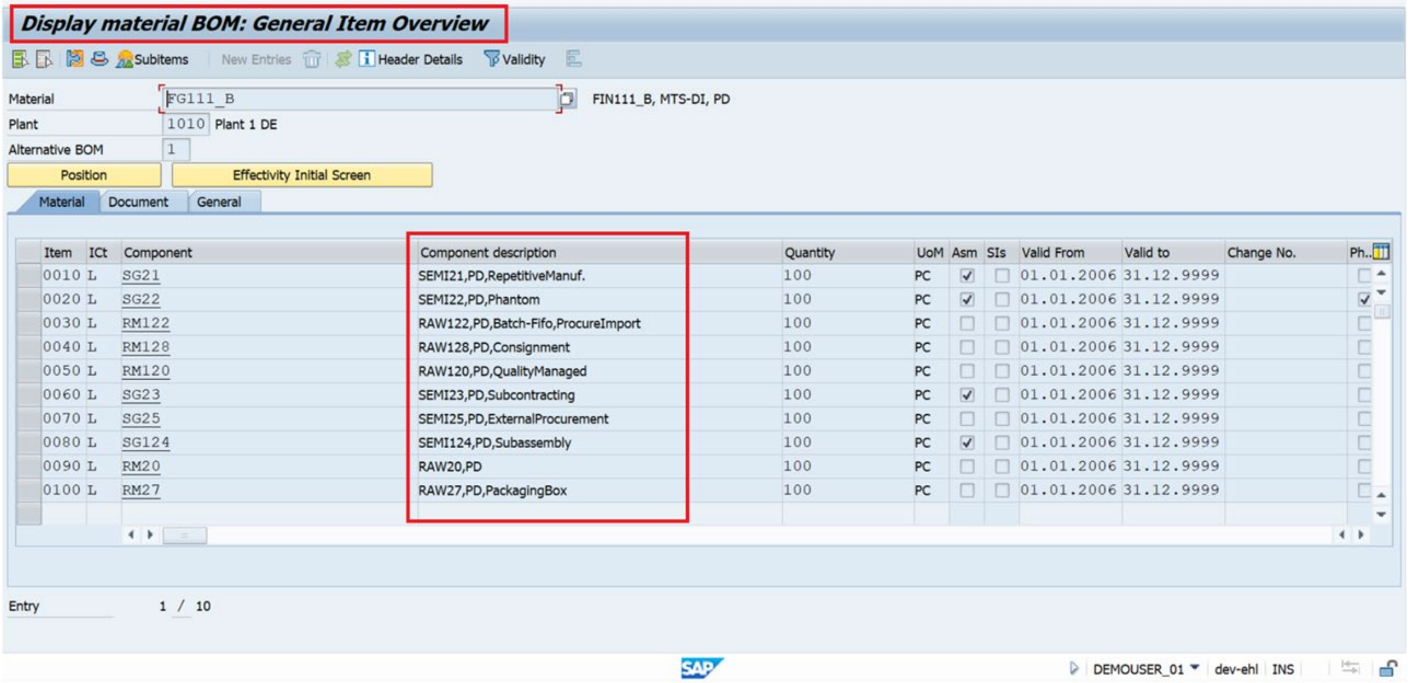
Additionally, dynamic data masking can be used for more granular field-level controls. Instead of completely segregating out the sensitive BOM component, the sensitive field(s) are masked with values such as “********.”

Security Dimension: *US Export Control - ITAR*

User ID	User’s Security	Expected Behavior
DEMOUSER_01	US Citizen	Can access BOM and all components within BOM
DEMOUSER_02	Non-US Person / Entity with ITAR license	Can access BOM and all components within BOM
DEMOUSER_03	Non-US Person without ITAR license	Can access BOM and its components but material/component description, long texts are masked as ********

DEMOUSER_01: US Citizen

Since DEMOUSER_01 is a US citizen, they can access the BOM and all components within BOM. There will be no segregation or masking applied to their view.



Display material BOM: General Item Overview

Material	FG111_B	FIN111_B, MTS-DI, PD
Plant	1010	Plant 1 DE
Alternative BOM	1	

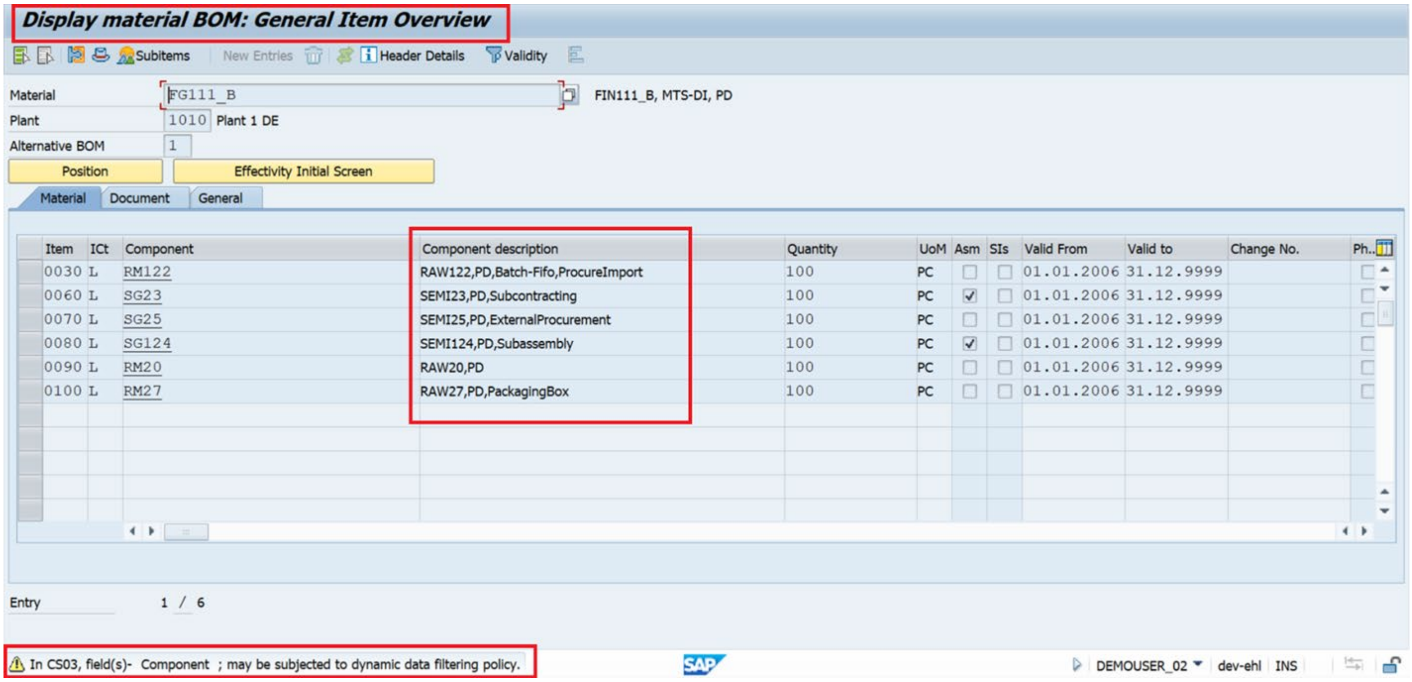
Item	ICt	Component	Component description	Quantity	UoM	Asm	SIs	Valid From	Valid to	Change No.	Ph..
0010	L	SG21	SEMI21,PD,RepetitiveManuf.	100	PC	☑	□	01.01.2006	31.12.9999		□
0020	L	SG22	SEMI22,PD,Phantom	100	PC	☑	□	01.01.2006	31.12.9999		☑
0030	L	RM122	RAW122,PD,Batch-Fifo,ProcureImport	100	PC	□	□	01.01.2006	31.12.9999		□
0040	L	RM128	RAW128,PD,Consignment	100	PC	□	□	01.01.2006	31.12.9999		□
0050	L	RM120	RAW120,PD,QualityManaged	100	PC	□	□	01.01.2006	31.12.9999		□
0060	L	SG23	SEMI23,PD,Subcontracting	100	PC	☑	□	01.01.2006	31.12.9999		□
0070	L	SG25	SEMI25,PD,ExternalProcurement	100	PC	□	□	01.01.2006	31.12.9999		□
0080	L	SG124	SEMI124,PD,Subassembly	100	PC	☑	□	01.01.2006	31.12.9999		□
0090	L	RM20	RAW20,PD	100	PC	□	□	01.01.2006	31.12.9999		□
0100	L	RM27	RAW27,PD,PackagingBox	100	PC	□	□	01.01.2006	31.12.9999		□

Entry 1 / 10

DEMOUSER_01 dev-ehl INS

DEMOUSER_02: Non-US Person with ITAR License

On the other hand, DEMOUSER_02 is a non-US person but they have an ITAR license. Due to this, they can also access the BOM and most of the components within the BOM. The components DEMOUSER_02 are not entitled to view, have been filtered with the use of attribute-based policy and dynamic data segregation.



Display material BOM: General Item Overview

Material	FG111_B	FIN111_B, MTS-DI, PD
Plant	1010	Plant 1 DE
Alternative BOM	1	

Item	ICt	Component	Component description	Quantity	UoM	Asm	SIs	Valid From	Valid to	Change No.	Ph..
0030	L	RM122	RAW122,PD,Batch-Fifo,ProcureImport	100	PC	□	□	01.01.2006	31.12.9999		□
0060	L	SG23	SEMI23,PD,Subcontracting	100	PC	☑	□	01.01.2006	31.12.9999		□
0070	L	SG25	SEMI25,PD,ExternalProcurement	100	PC	□	□	01.01.2006	31.12.9999		□
0080	L	SG124	SEMI124,PD,Subassembly	100	PC	☑	□	01.01.2006	31.12.9999		□
0090	L	RM20	RAW20,PD	100	PC	□	□	01.01.2006	31.12.9999		□
0100	L	RM27	RAW27,PD,PackagingBox	100	PC	□	□	01.01.2006	31.12.9999		□

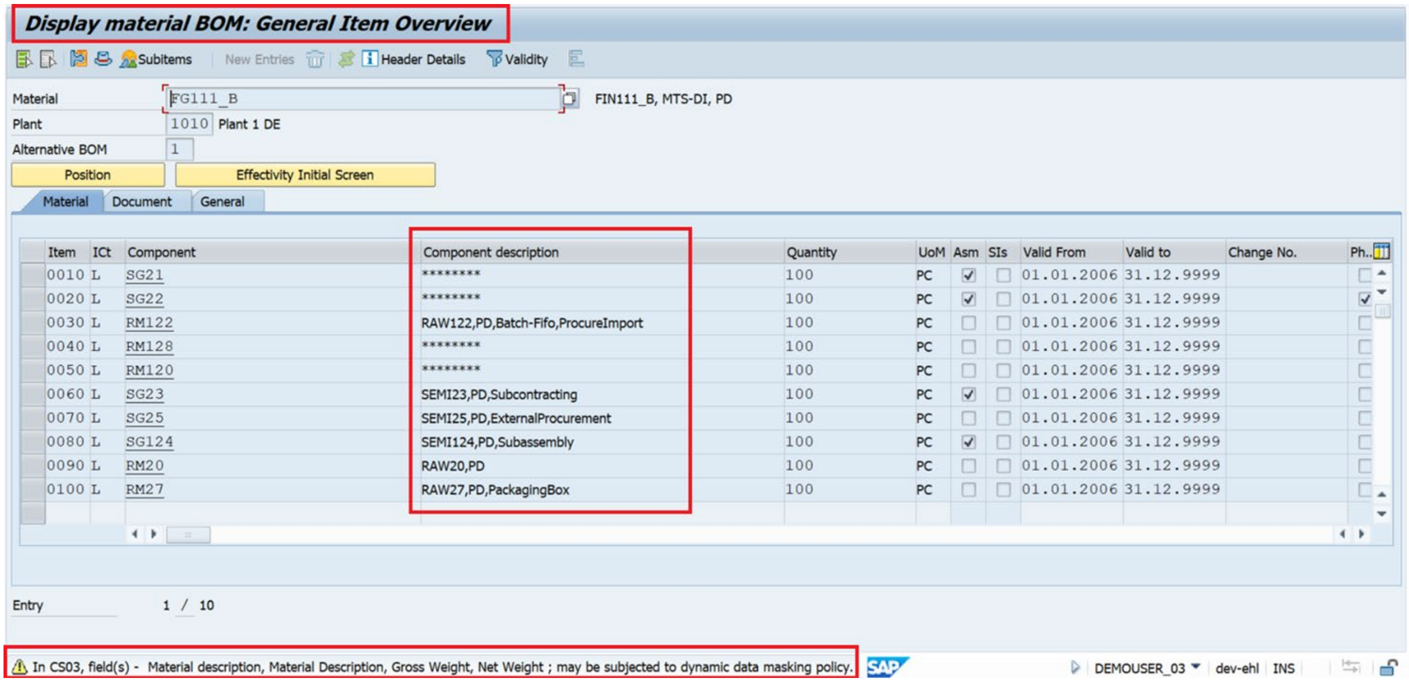
Entry 1 / 6

⚠ In CS03, field(s)- Component ; may be subjected to dynamic data filtering policy.

DEMOUSER_02 dev-ehl INS

DEMOUSER_03: Non-US Person without ITAR License

In contrast, DEMOUSER_03 is a non-US person who does not have an ITAR license. Due to this, they can access the BOM, but ITAR components are filtered out and the component descriptions are masked with "********."



Display material BOM: General Item Overview

Material FG111_B FIN111_B, MTS-DI, PD

Plant 1010 Plant 1 DE

Alternative BOM 1

Item	ICt	Component	Component description	Quantity	UoM	Asm	SIs	Valid From	Valid to	Change No.	Ph..
0010	L	SG21	********	100	PC	☑	□	01.01.2006	31.12.9999		□
0020	L	SG22	********	100	PC	☑	□	01.01.2006	31.12.9999		☑
0030	L	RM122	RAW122,PD,Batch-Fifo,ProcureImport	100	PC	□	□	01.01.2006	31.12.9999		□
0040	L	RM128	********	100	PC	□	□	01.01.2006	31.12.9999		□
0050	L	RM120	********	100	PC	□	□	01.01.2006	31.12.9999		□
0060	L	SG23	SEMI23,PD,Subcontracting	100	PC	☑	□	01.01.2006	31.12.9999		□
0070	L	SG25	SEMI25,PD,ExternalProcurement	100	PC	□	□	01.01.2006	31.12.9999		□
0080	L	SG124	SEMI124,PD,Subassembly	100	PC	☑	□	01.01.2006	31.12.9999		□
0090	L	RM20	RAW20,PD	100	PC	□	□	01.01.2006	31.12.9999		□
0100	L	RM27	RAW27,PD,PackagingBox	100	PC	□	□	01.01.2006	31.12.9999		□

Entry 1 / 10

⚠ In CS03, field(s) - Material description, Material Description, Gross Weight, Net Weight ; may be subjected to dynamic data masking policy.

Use Case-2: Controlling Access for Sarbanes-Oxley Act (SOX) and Segregation of Duties (SoD)

Access Controls on key financial transactions is very important both from compliance point of view such as Sarbanes-Oxley Act (SOX) and SoD (Segregation of Duties) to reduce risk and fraud. Using real time attributes of user, ABAC policies can be applied to enforce dynamic and context-aware access controls not only to view datasets but also to post transactions.

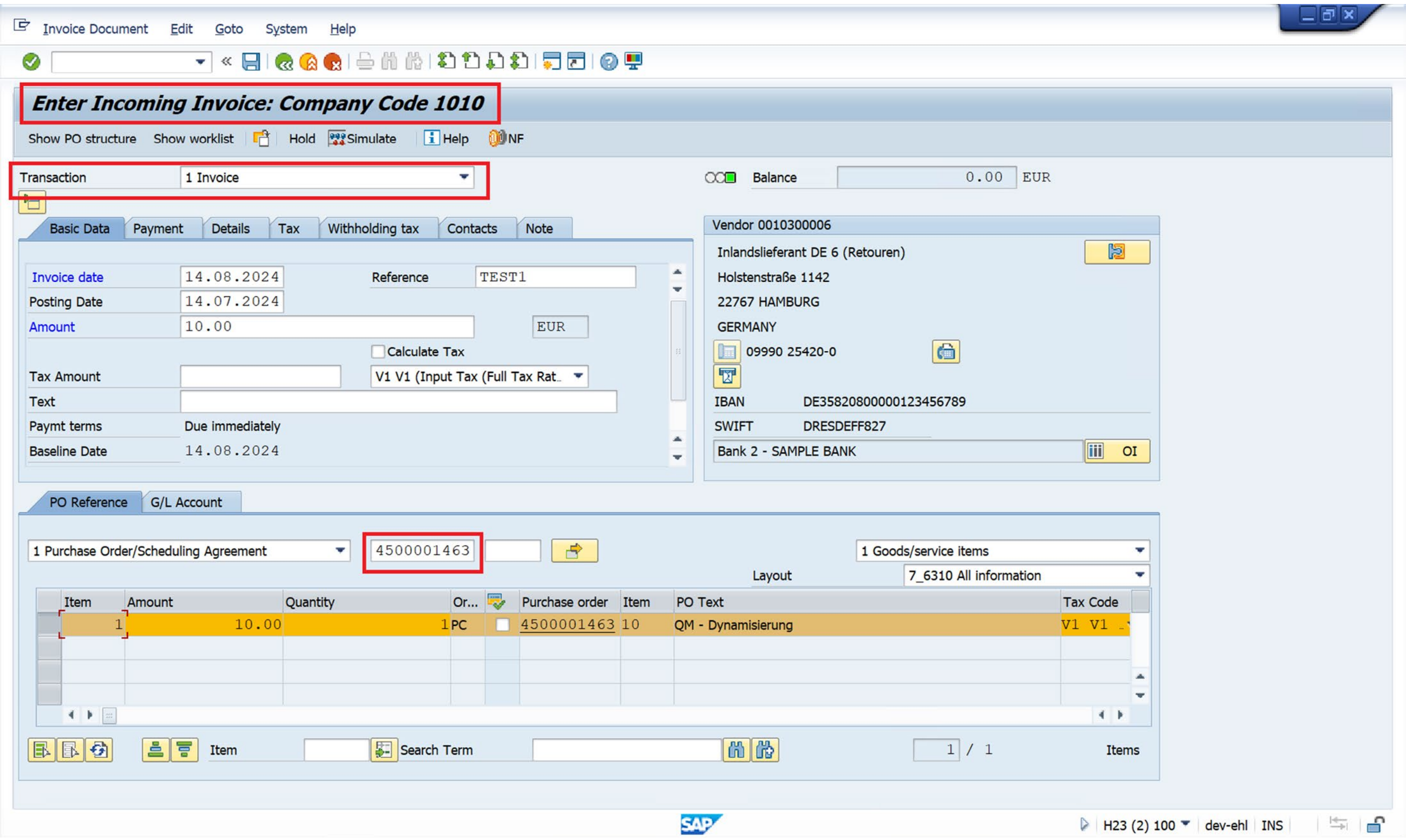
As an example, in Accounts Payable SSC (Shared Service Center), AP clerks (designated by role) with MoD (Ministry of Defense) clearance attribute can only process MOD vendor invoices. All other AP clerks who are not authorized for MOD vendor invoices, should not be allowed to post these financial transactions.

Security Dimension: *MOD (Ministry of Defense) clearance*

User ID	User's Security	Expected Behavior
H23 (2) 100	AP Clerk with MoD Clearance	Can post financial transactions for MoD vendors
H23 (3) 100	AP Clerk without MoD Clearance	Can't post financial transactions for MoD vendors

User H23 (2) 100: AP Clerk with MoD Clearance

Since user H23 (2) 100 is an AP Clerk with MoD clearance, they can post financial transactions for the MoD vendors. See below as they have full permissions and are able to create document "no. 51000001155."



Enter Incoming Invoice: Company Code 1010

Transaction: 1 Invoice

Balance: 0.00 EUR

Invoice date	14.08.2024
Reference	TEST1
Posting Date	14.07.2024
Amount	10.00 EUR
Calculate Tax	□
Tax Amount	
Tax code	V1 V1 (Input Tax (Full Tax Rat..
Text	
Paymt terms	Due immediately
Baseline Date	14.08.2024

Vendor 0010300006
Inlandslieferant DE 6 (Retouren)
Holstenstraße 1142
22767 HAMBURG
GERMANY
09990 25420-0
IBAN DE35820800000123456789
SWIFT DRESDEFF827
Bank 2 - SAMPLE BANK
OI

1 Purchase Order/Scheduling Agreement: 4500001463

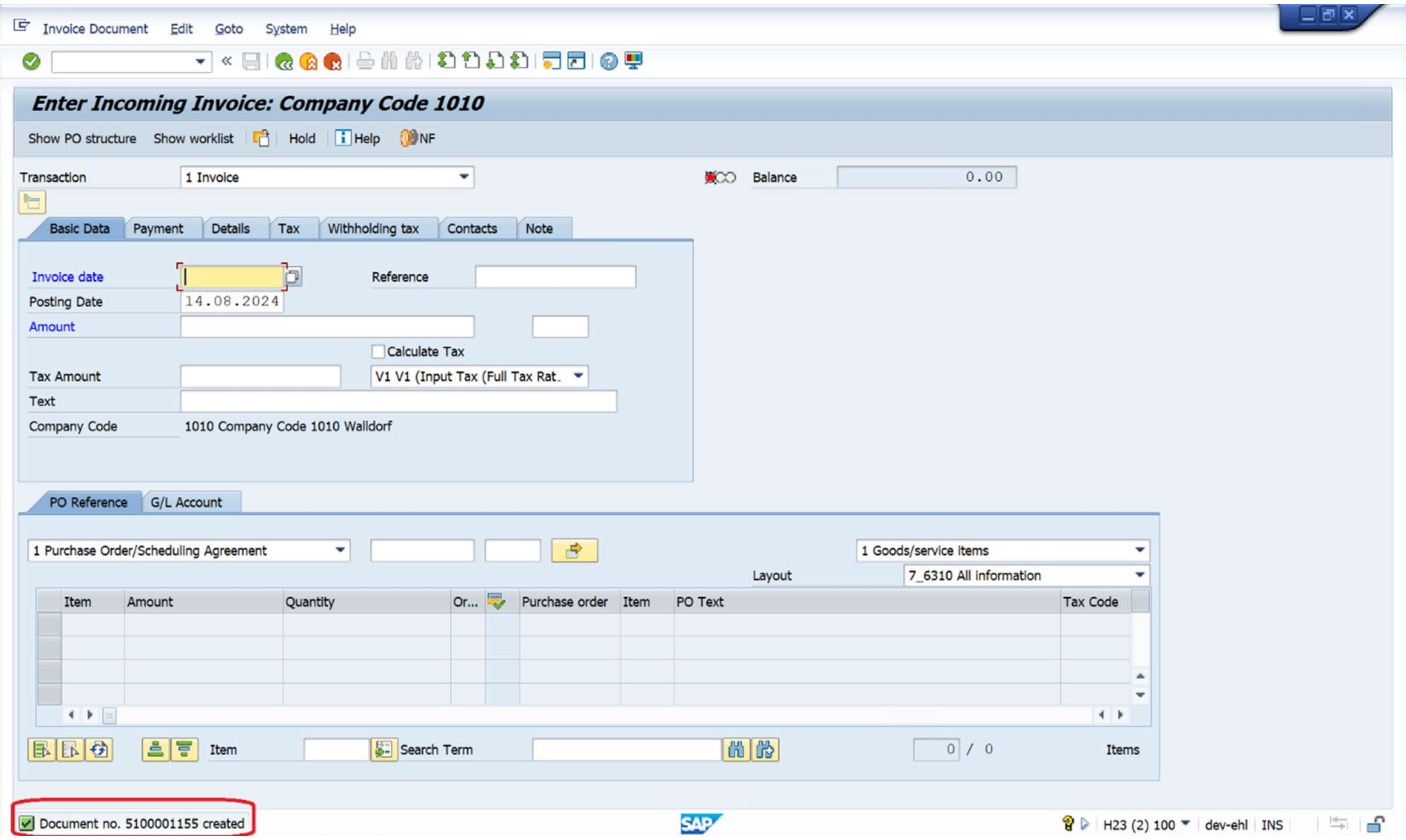
1 Goods/service items

Layout: 7_6310 All information

Item	Amount	Quantity	Or...		Purchase order	Item	PO Text	Tax Code
1	10.00	1	PC	□	4500001463	10	QM - Dynamisierung	V1 V1 ..

1 / 1 Items

H23 (2) 100 | dev-ehl | INS



Enter Incoming Invoice: Company Code 1010

Transaction: 1 Invoice

Balance: 0.00

Invoice date	
Reference	
Posting Date	14.08.2024
Amount	
Calculate Tax	□
Tax Amount	
Tax code	V1 V1 (Input Tax (Full Tax Rat..
Text	
Company Code	1010 Company Code 1010 Walldorf

1 Purchase Order/Scheduling Agreement

1 Goods/service items

Layout: 7_6310 All information

Item	Amount	Quantity	Or...		Purchase order	Item	PO Text	Tax Code

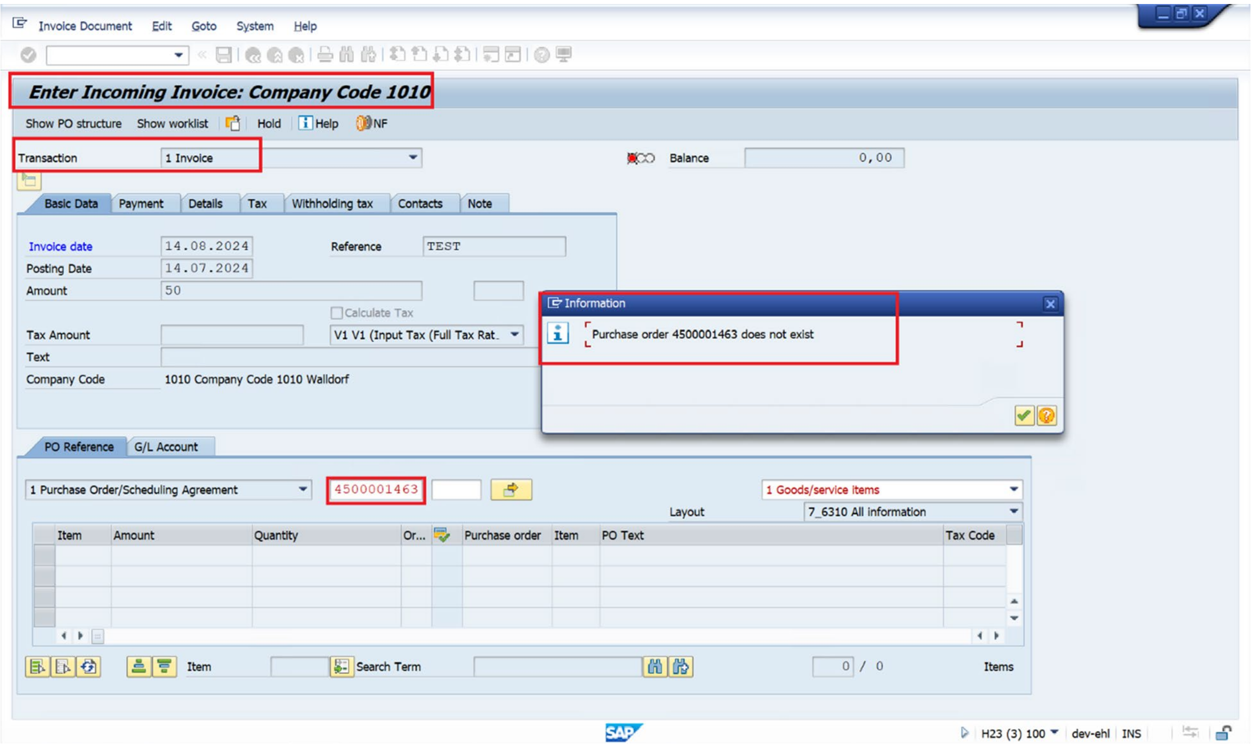
0 / 0 Items

☑ Document no. 5100001155 created

H23 (2) 100 | dev-ehl | INS

User: H23 (3) 100: AP Clerk without MoD Clearance

In contrast, user H23 (3) 100 is an AP Clerk who doesn't have MoD clearance. Due to this, they cannot post financial transactions for MoD vendors. See below as they attempt to post invoice nr. 4500001463 and are prevented from doing so.



Enter Incoming Invoice: Company Code 1010

Transaction: 1 Invoice

Balance: 0,00

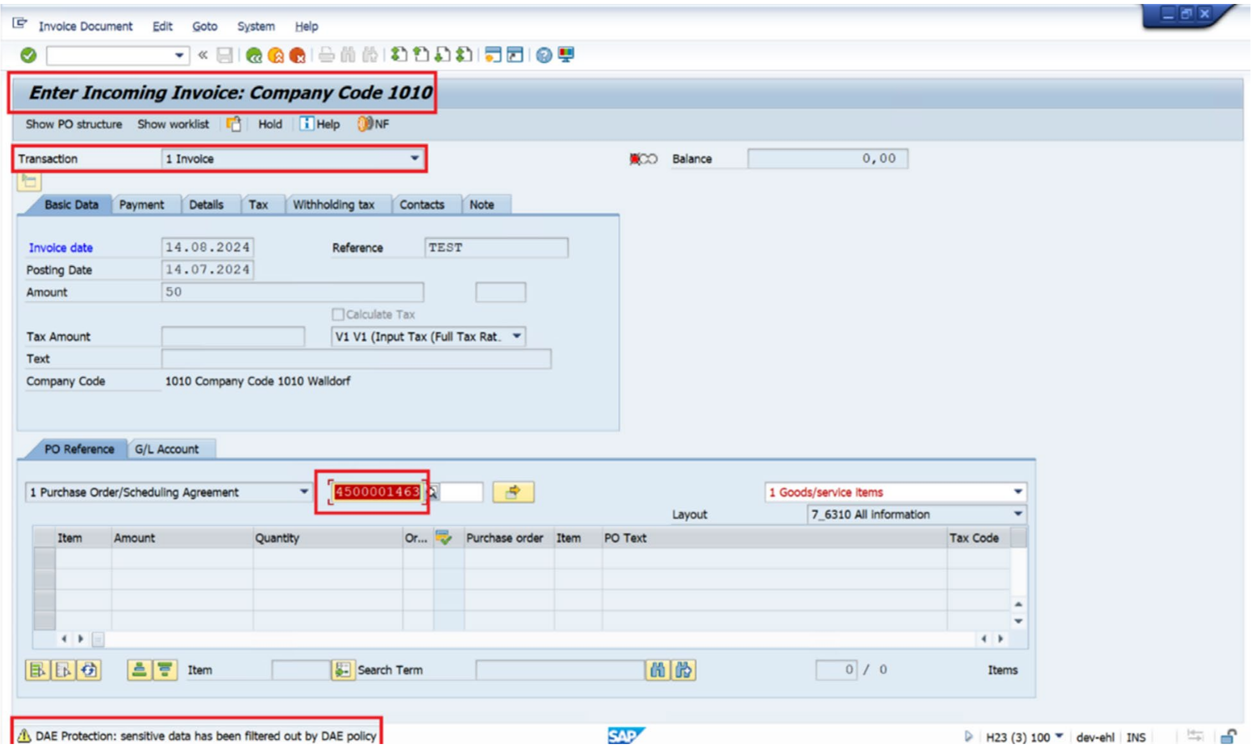
Invoice date: 14.08.2024
Reference: TEST
Posting Date: 14.07.2024
Amount: 50
□ Calculate Tax
Tax Amount:
V1 V1 (Input Tax (Full Tax Rat.
Text:
Company Code: 1010 Company Code 1010 Walldorf

Information
Purchase order 4500001463 does not exist

1 Purchase Order/Scheduling Agreement: 4500001463
1 Goods/service items
Layout: 7_6310 All information

0 / 0 Items

H23 (3) 100 | dev-ehl | INS



Enter Incoming Invoice: Company Code 1010

Transaction: 1 Invoice

Balance: 0,00

Invoice date: 14.08.2024
Reference: TEST
Posting Date: 14.07.2024
Amount: 50
□ Calculate Tax
Tax Amount:
V1 V1 (Input Tax (Full Tax Rat.
Text:
Company Code: 1010 Company Code 1010 Walldorf

1 Purchase Order/Scheduling Agreement: 4500001463
1 Goods/service items
Layout: 7_6310 All information

0 / 0 Items

DAE Protection: sensitive data has been filtered out by DAE policy

H23 (3) 100 | dev-ehl | INS

As exemplified by these two use cases in the PL2PR value stream, the previously described strategy using logical data segregation and obfuscation can be used to address a variety of security and compliance needs to protect ERP data and ensure confidentiality and privacy of sensitive data.

Additionally, the same strategy can also be applied to other value streams such as procure to pay, record to report, order to cash, source to pay, etc. In doing so, it aids in keeping the value stream secure during ERP transformation and in day-to-day operations.

Takeaways

While ERP systems are often seen as the backbone of an intelligent enterprise, when undertaking an ERP transformation and consolidating systems, organizations often face many challenges when it comes to ensuring data privacy and confidentiality.

To address these challenges in key ERP processes, enterprises need to logically segregate data to be able to control access, visibility, and security of data. This can be achieved by combining a zero trust policy platform that incorporates attribute-based policies and dynamic authorization, with an enforcement approach that uses logical data segregation (via data segmentation, masking, filtering, access control, or DRM).

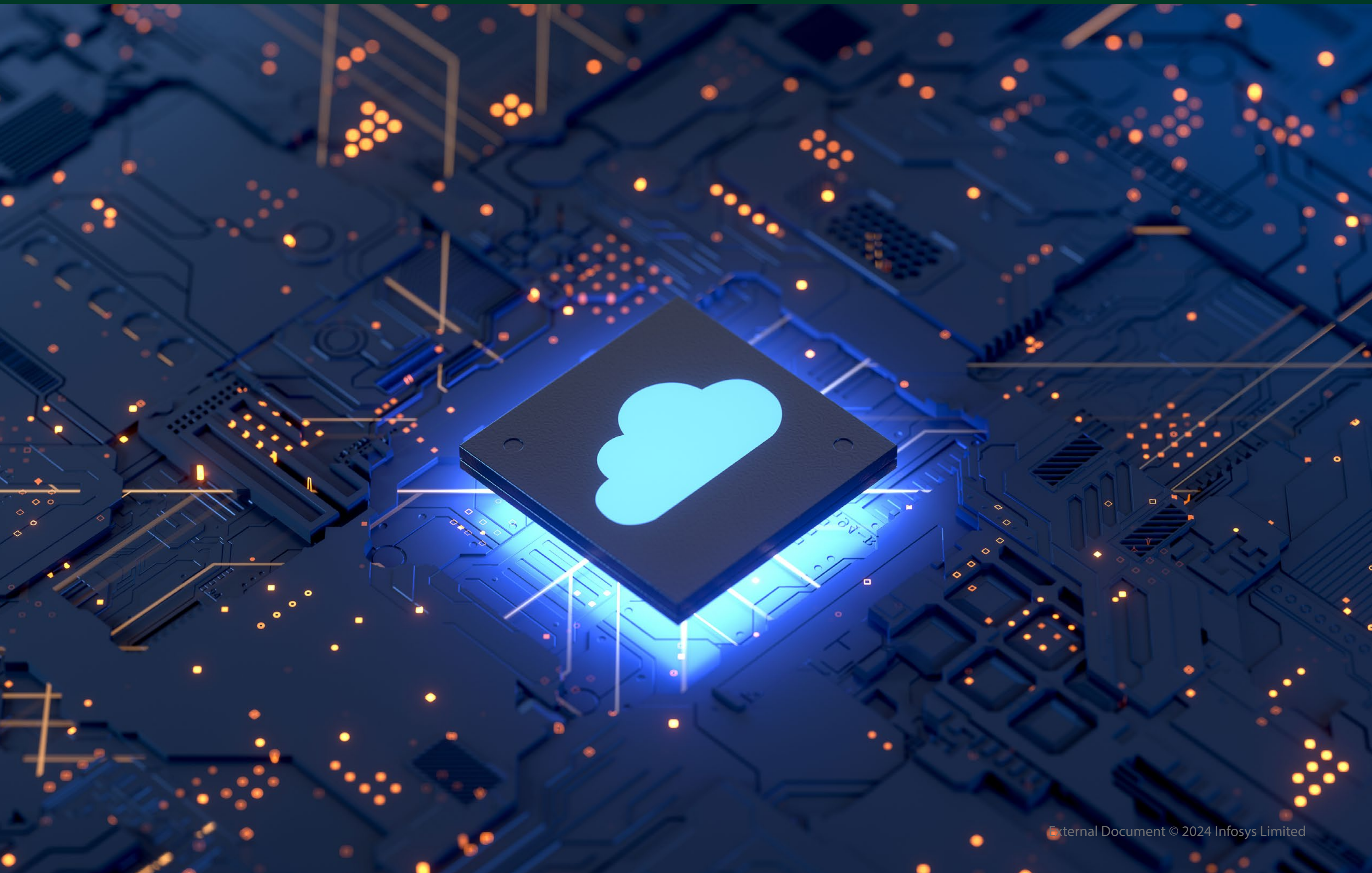
By implementing effective logical data segregation practices based on zero trust principles, organizations can achieve efficient data management and safeguard their consolidated ERP data, all while maintaining trust with stakeholders, and enabling data confidentiality and privacy.

References

- Infosys | Define your ERP transformation objectives and keep them time-bound
- NextLabs | Protect ERP data & improve compliance with dynamic authorization and zero trust compliance
- NextLabs | Why should you care about logical data segregation?

Resources

- NextLabs |Implement data segregation with zero trust
- NextLabs | Proactive protection with zero trust data-centric security
- NextLabs | Fortify data protection: Insights from 4 industry leaders



About Authors

Nitin

is an Associate Partner at Infosys Consulting with 21+ years' experience in delivering and managing Enterprise Risk Management & Compliance engagements. During this time, he has led compliance projects across companies in different verticals and has interactions with CXO level stakeholders to define and implement Enterprise-wide Security and GRC strategies. Nitin is also member of Technology Advisory Board of NextLabs Inc.

Krishna Mohan

is a Director at NextLabs, with 20+ years of experience in IT Systems and Solution architecture with expertise on cyber security. With his thought leadership and breakthrough innovation, Krishna played a key role in NextLabs Zero-Trust Data Centric Security, especially for ERP and PLM Systems.

Zola Lamprecht

is the Head of Marketing at NextLabs, with experience in digital marketing, SEO, advertising, rich media, and project management. During her time at NextLabs, she has introduced a variety of new initiatives and led many projects with customers and partners to increase thought leadership and share insights from their Zero Trust Data Security implementations.

For more information, contact askus@infosys.com

Infosys®
Navigate your next