ORACLE
AI World

ERP Security and Audit with AI

THR3691

Robert Singleton, CIA, CRMA, CDPSE, CGEIT, CRISC

Risk Solutions – Master Principal Solution Engineer

Oracle North America

October 15, 2025

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Forward-Looking statements

This presentation is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions, and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at https://oracle.com/investors/ All information in this presentation is current as of October 2025 and Oracle undertakes no duty to update any statement in light of new information or future events.

Some regulatory certifications or registrations to products or services referenced herein are held by Cerner Corporation. Cerner Corporation is a wholly owned subsidiary of Oracle. Cerner Corporation is an ONC-certified health IT developer and a registered medical device manufacturer in the United States and other jurisdictions worldwide.

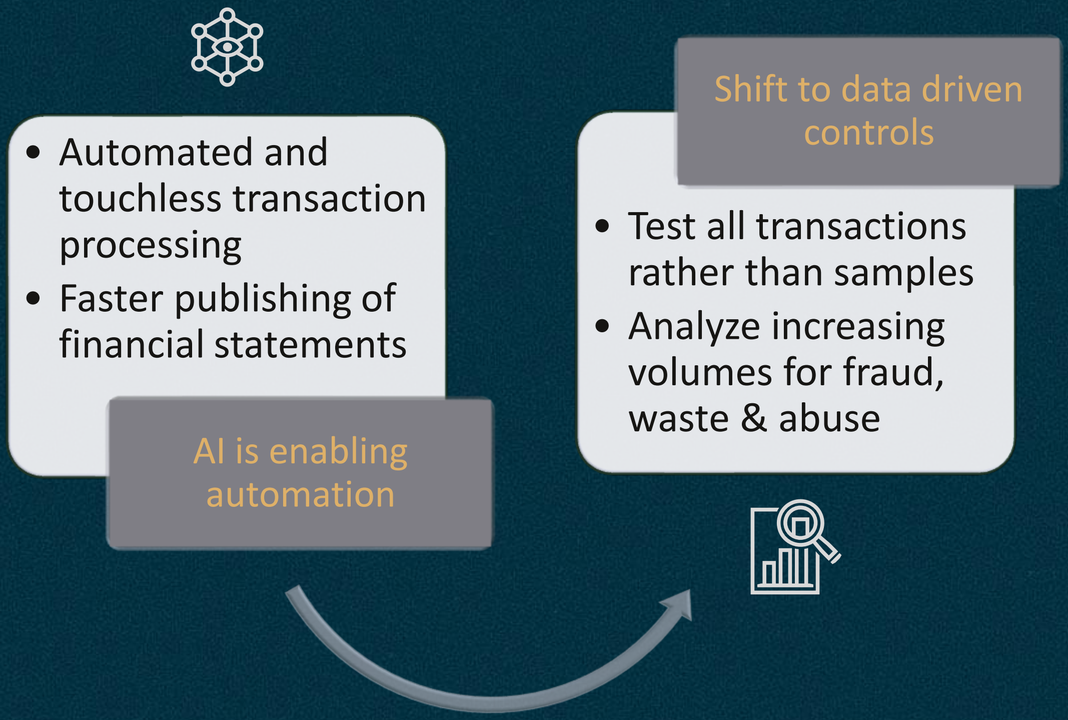
Robert Singleton

Master Principal Solution Engineer

Risk Solutions

The world around us is changing

Data driven controls are the new normal



- Automated and touchless transaction processing
- Faster publishing of financial statements

AI is enabling automation

Shift to data driven controls

- Test all transactions rather than samples
- Analyze increasing volumes for fraud, waste & abuse

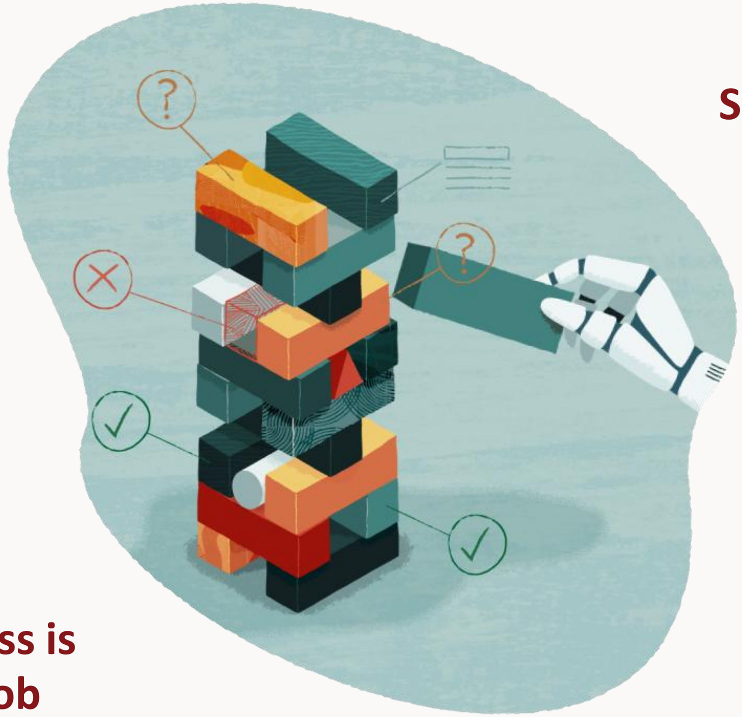
Risk Management and Compliance

An AI-driven risk management suite, embedded within Oracle Fusion Applications

Digitize Fusion controls

Automate audit trail notifications for setups & master data changes

Ensure employee access is appropriate for their job



Streamline Cybersecurity

Detect suspicious activity

Certify user access to sensitive data & privileges

Risk Management Features

1 Access Request Workflows

2 Access Certifications/Reviews

3 Automated Access & SOD Monitoring

4 Continuous Configuration & Transaction Monitoring

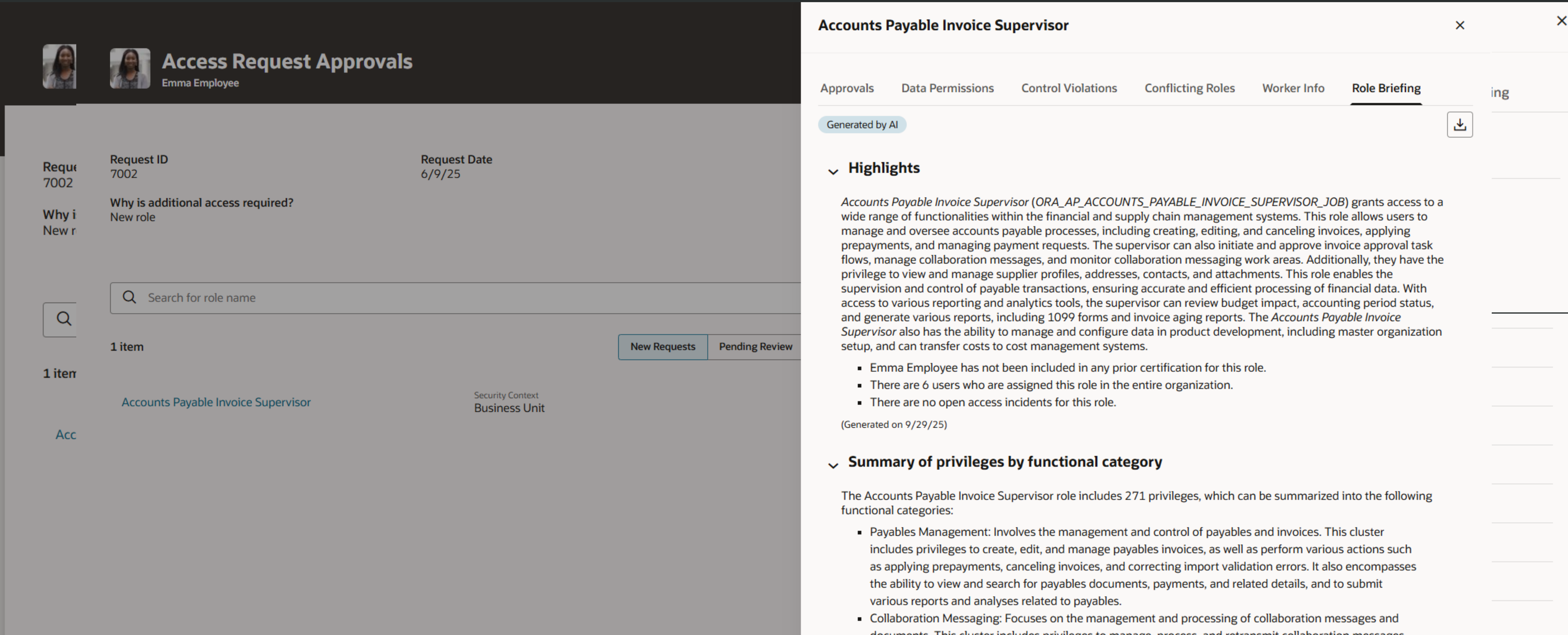
5 Superuser Activity Monitoring

6 Risk & Security Snapshot Report

Access Request Workflows

CHECK ACCESS REQUESTS for ACCESS VIOLATIONS

Enable self-service user access requests and help prevent SoD conflicts prior to provisioning access. Route access requests to business process owners for review, document exceptions, and grant access if approved.



Access Request Approvals
Emma Employee

Request ID
7002

Request Date
6/9/25

Why is additional access required?
New role

Search for role name

1 item

New Requests | Pending Review

Accounts Payable Invoice Supervisor

Security Context
Business Unit

Accounts Payable Invoice Supervisor

Approvals | Data Permissions | Control Violations | Conflicting Roles | Worker Info | Role Briefing

Generated by AI

Highlights

Accounts Payable Invoice Supervisor (*ORA_AP_ACCOUNTS_PAYABLE_INVOICE_SUPERVISOR_JOB*) grants access to a wide range of functionalities within the financial and supply chain management systems. This role allows users to manage and oversee accounts payable processes, including creating, editing, and canceling invoices, applying prepayments, and managing payment requests. The supervisor can also initiate and approve invoice approval task flows, manage collaboration messages, and monitor collaboration messaging work areas. Additionally, they have the privilege to view and manage supplier profiles, addresses, contacts, and attachments. This role enables the supervision and control of payable transactions, ensuring accurate and efficient processing of financial data. With access to various reporting and analytics tools, the supervisor can review budget impact, accounting period status, and generate various reports, including 1099 forms and invoice aging reports. The *Accounts Payable Invoice Supervisor* also has the ability to manage and configure data in product development, including master organization setup, and can transfer costs to cost management systems.

- Emma Employee has not been included in any prior certification for this role.
- There are 6 users who are assigned this role in the entire organization.
- There are no open access incidents for this role.

(Generated on 9/29/25)

Summary of privileges by functional category

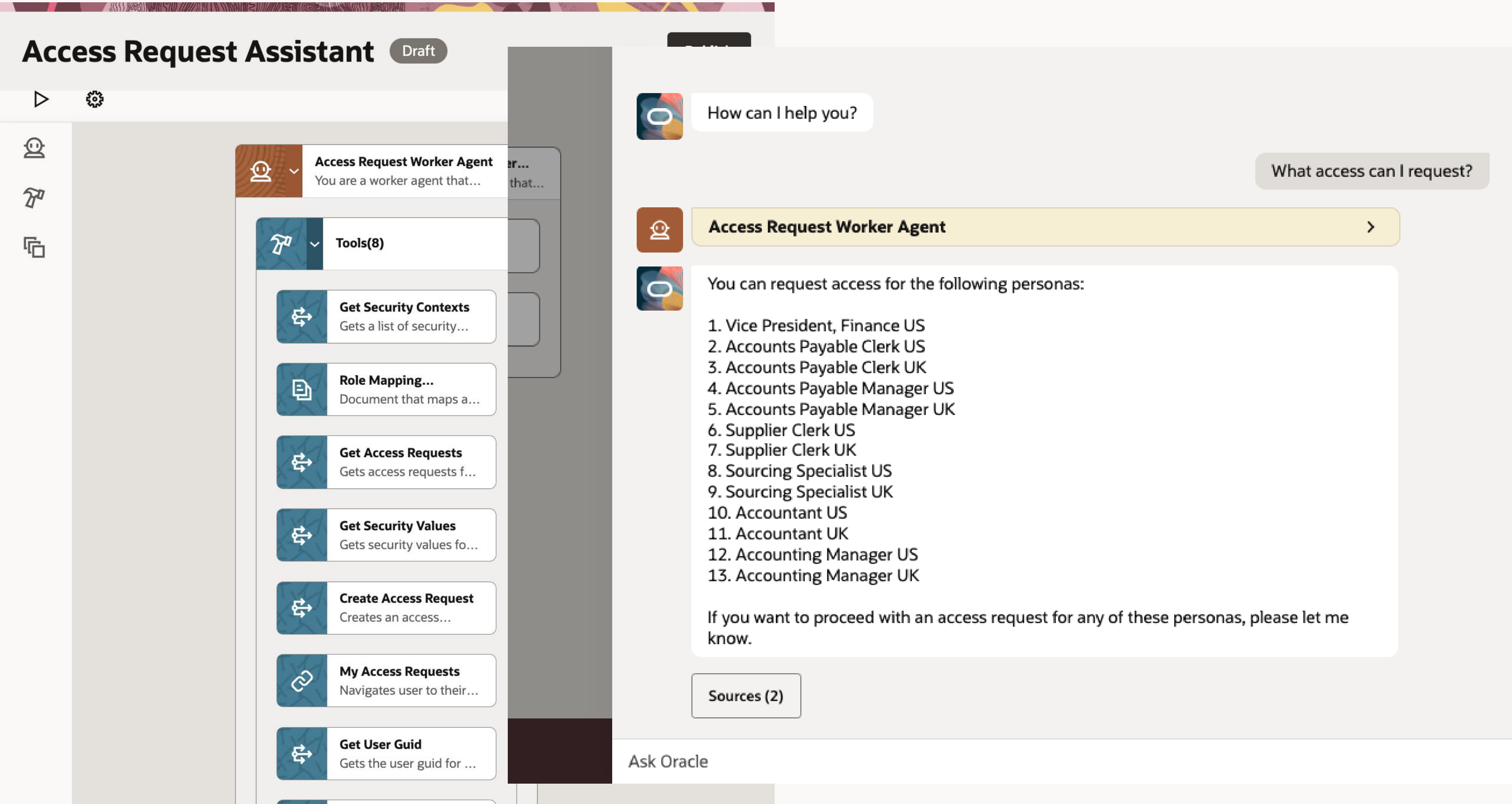
The Accounts Payable Invoice Supervisor role includes 271 privileges, which can be summarized into the following functional categories:

- Payables Management: Involves the management and control of payables and invoices. This cluster includes privileges to create, edit, and manage payables invoices, as well as perform various actions such as applying prepayments, canceling invoices, and correcting import validation errors. It also encompasses the ability to view and search for payables documents, payments, and related details, and to submit various reports and analyses related to payables.
- Collaboration Messaging: Focuses on the management and processing of collaboration messages and

Access Request – New Feature

Embedded AI: Access Request Assistant

25D - Simplifies access requests for Fusion ERP applications through chat



How can I help you?

What access can I request?

Access Request Worker Agent

You can request access for the following personas:

1. Vice President, Finance US
2. Accounts Payable Clerk US
3. Accounts Payable Clerk UK
4. Accounts Payable Manager US
5. Accounts Payable Manager UK
6. Supplier Clerk US
7. Supplier Clerk UK
8. Sourcing Specialist US
9. Sourcing Specialist UK
10. Accountant US
11. Accountant UK
12. Accounting Manager US
13. Accounting Manager UK

If you want to proceed with an access request for any of these personas, please let me know.

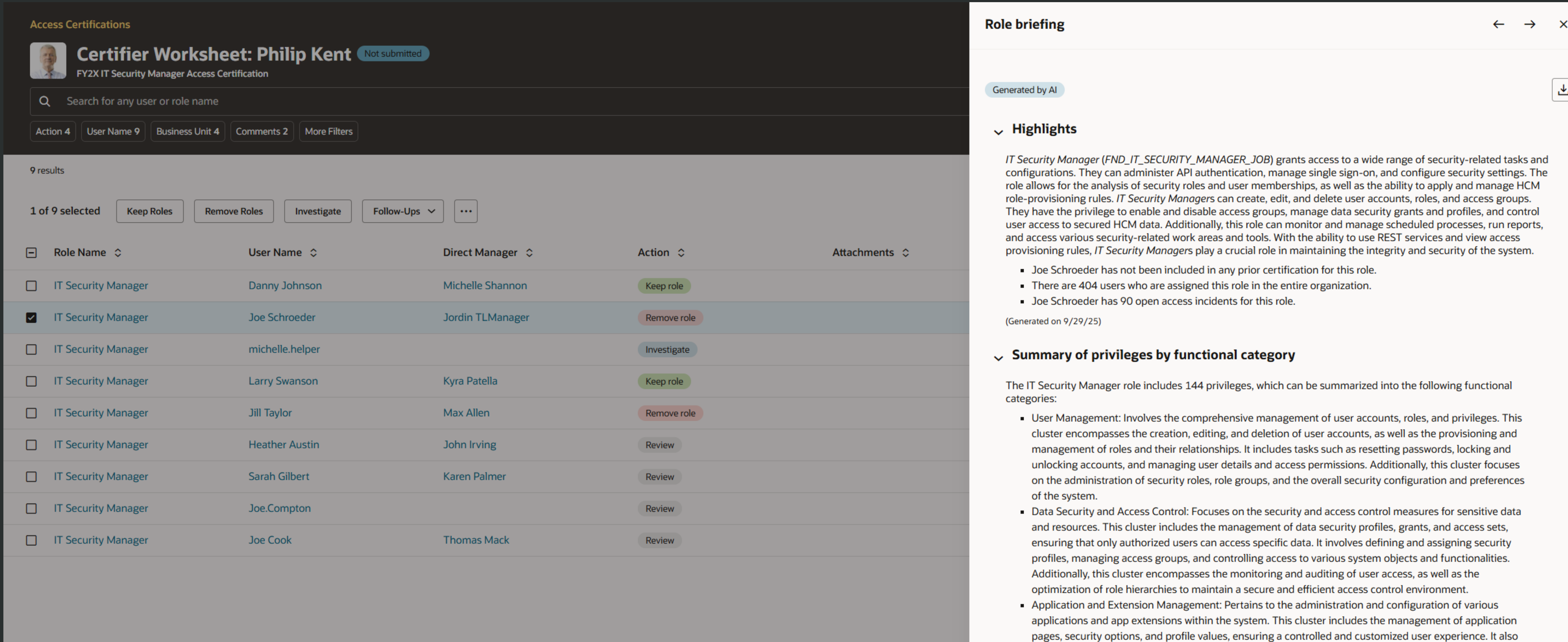
Access Certifications/Reviews

SENSITIVE ACCESS REVIEWS

Automate user access review workflows to ensure access is authorized by business process owners and meet audit and compliance requirements.

APPROVE, REMOVE OR INVESTIGATE HIGH RISK ACCESS

Scope out sensitive access by users and roles, track progress, provide attachments and comments, and either approve, remove or investigate access.



Access Certifications

Certifier Worksheet: Philip Kent Not submitted

FY2X IT Security Manager Access Certification

9 results

1 of 9 selected

☐	Role Name	User Name	Direct Manager	Action	Attachments
☐	IT Security Manager	Danny Johnson	Michelle Shannon	Keep role	
☑	IT Security Manager	Joe Schroeder	Jordin TLManager	Remove role	
☐	IT Security Manager	michelle.helper		Investigate	
☐	IT Security Manager	Larry Swanson	Kyra Patella	Keep role	
☐	IT Security Manager	Jill Taylor	Max Allen	Remove role	
☐	IT Security Manager	Heather Austin	John Irving	Review	
☐	IT Security Manager	Sarah Gilbert	Karen Palmer	Review	
☐	IT Security Manager	Joe.Compton		Review	
☐	IT Security Manager	Joe Cook	Thomas Mack	Review	

Role briefing

Generated by AI

Highlights

IT Security Manager (*FND_IT_SECURITY_MANAGER_JOB*) grants access to a wide range of security-related tasks and configurations. They can administer API authentication, manage single sign-on, and configure security settings. The role allows for the analysis of security roles and user memberships, as well as the ability to apply and manage HCM role-provisioning rules. *IT Security Managers* can create, edit, and delete user accounts, roles, and access groups. They have the privilege to enable and disable access groups, manage data security grants and profiles, and control user access to secured HCM data. Additionally, this role can monitor and manage scheduled processes, run reports, and access various security-related work areas and tools. With the ability to use REST services and view access provisioning rules, *IT Security Managers* play a crucial role in maintaining the integrity and security of the system.

- Joe Schroeder has not been included in any prior certification for this role.
- There are 404 users who are assigned this role in the entire organization.
- Joe Schroeder has 90 open access incidents for this role.

(Generated on 9/29/25)

Summary of privileges by functional category

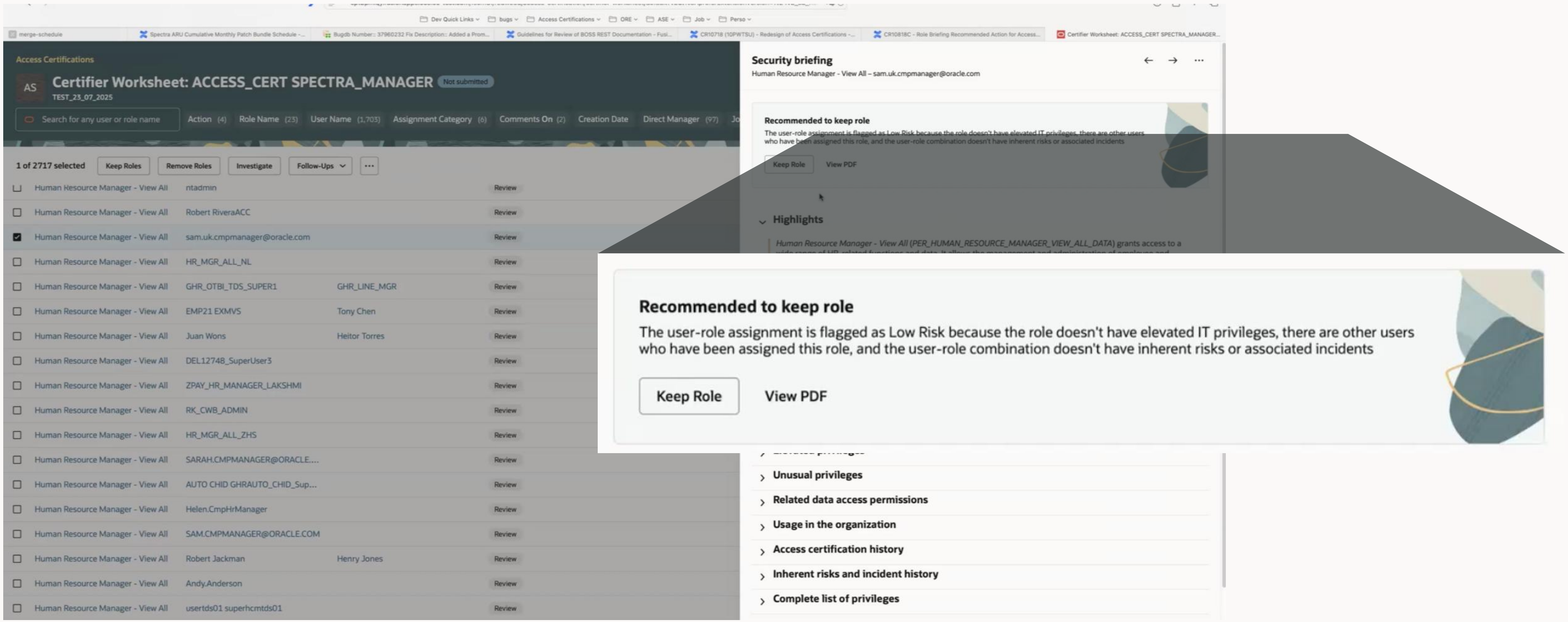
The IT Security Manager role includes 144 privileges, which can be summarized into the following functional categories:

- User Management: Involves the comprehensive management of user accounts, roles, and privileges. This cluster encompasses the creation, editing, and deletion of user accounts, as well as the provisioning and management of roles and their relationships. It includes tasks such as resetting passwords, locking and unlocking accounts, and managing user details and access permissions. Additionally, this cluster focuses on the administration of security roles, role groups, and the overall security configuration and preferences of the system.
- Data Security and Access Control: Focuses on the security and access control measures for sensitive data and resources. This cluster includes the management of data security profiles, grants, and access sets, ensuring that only authorized users can access specific data. It involves defining and assigning security profiles, managing access groups, and controlling access to various system objects and functionalities. Additionally, this cluster encompasses the monitoring and auditing of user access, as well as the optimization of role hierarchies to maintain a secure and efficient access control environment.
- Application and Extension Management: Pertains to the administration and configuration of various applications and app extensions within the system. This cluster includes the management of application pages, security options, and profile values, ensuring a controlled and customized user experience. It also

Access Certification/Review – New Feature

Embedded AI: Access Certification Advisor

26A - Recommendations help business users make fast, informed decisions while maintaining security



Dev Quick Links
bugs
Access Certifications
ORE
ASE
Job
Perso
merge-schedule
Spectra ARU Cumulative Monthly Patch Bundle Schedule -...
Bugdb Number:: 37960232 Fix Description:: Added a Prom...
Guidelines for Review of BOSS REST Documentation - Fusi...
CR10718 (10PWTSU) - Redesign of Access Certifications -...
CR10818C - Role Briefing Recommended Action for Access...
Certifier Worksheet: ACCESS_CERT SPECTRA_MANAGER...

Access Certifications

AS **Certifier Worksheet: ACCESS_CERT SPECTRA_MANAGER** Not submitted

TEST_23_07_2025

Search for any user or role name
Action (4)
Role Name (23)
User Name (1,703)
Assignment Category (6)
Comments On (2)
Creation Date
Direct Manager (97)
Jo

1 of 2717 selected

Keep Roles
Remove Roles
Investigate
Follow-Ups
...

☐	Human Resource Manager - View All	ntadmin		Review
☐	Human Resource Manager - View All	Robert RiveraACC		Review
☑	Human Resource Manager - View All	sam.uk.cmpmanager@oracle.com		Review
☐	Human Resource Manager - View All	HR_MGR_ALL_NL		Review
☐	Human Resource Manager - View All	GHR_OTBI_TDS_SUPER1	GHR_LINE_MGR	Review
☐	Human Resource Manager - View All	EMP21 EXMVS	Tony Chen	Review
☐	Human Resource Manager - View All	Juan Wons	Heitor Torres	Review
☐	Human Resource Manager - View All	DEL12748_SuperUser3		Review
☐	Human Resource Manager - View All	ZPAY_HR_MANAGER_LAKSHMI		Review
☐	Human Resource Manager - View All	RK_CWB_ADMIN		Review
☐	Human Resource Manager - View All	HR_MGR_ALL_ZHS		Review
☐	Human Resource Manager - View All	SARAH.CMPMANAGER@ORACLE....		Review
☐	Human Resource Manager - View All	AUTO CHID GHRAUTO_CHID_Sup...		Review
☐	Human Resource Manager - View All	Helen.CmpHrManager		Review
☐	Human Resource Manager - View All	SAM.CMPMANAGER@ORACLE.COM		Review
☐	Human Resource Manager - View All	Robert Jackman	Henry Jones	Review
☐	Human Resource Manager - View All	Andy.Anderson		Review
☐	Human Resource Manager - View All	usertds01 superhcmtds01		Review

Security briefing

Human Resource Manager - View All – sam.uk.cmpmanager@oracle.com

Recommended to keep role

The user-role assignment is flagged as Low Risk because the role doesn't have elevated IT privileges, there are other users who have been assigned this role, and the user-role combination doesn't have inherent risks or associated incidents

Highlights

Human Resource Manager - View All (PER_HUMAN_RESOURCE_MANAGER_VIEW_ALL_DATA) grants access to a

Recommended to keep role

The user-role assignment is flagged as Low Risk because the role doesn't have elevated IT privileges, there are other users who have been assigned this role, and the user-role combination doesn't have inherent risks or associated incidents

Keep Role

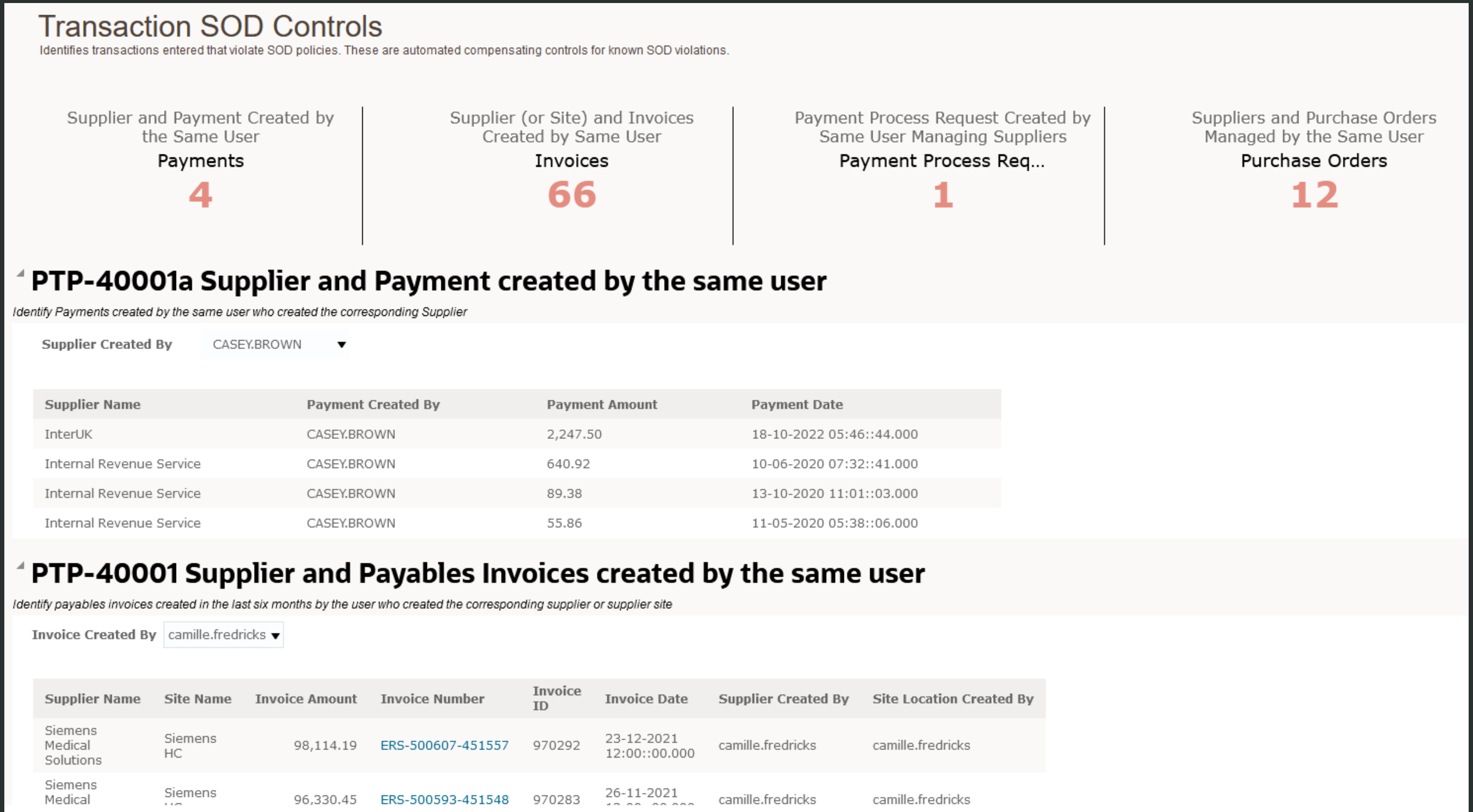
View PDF

- Unusual privileges
- Related data access permissions
- Usage in the organization
- Access certification history
- Inherent risks and incident history
- Complete list of privileges

Automated Access & SOD Monitoring

REPORT on SEPARATION of DUTIES CONFLICTS

Confidently generate SoD reports to address audit and compliance requirements while monitoring SoD Transactions at risk.



Transaction SOD Controls

Identifies transactions entered that violate SOD policies. These are automated compensating controls for known SOD violations.

Supplier and Payment Created by the Same User	Supplier (or Site) and Invoices Created by Same User	Payment Process Request Created by Same User Managing Suppliers	Suppliers and Purchase Orders Managed by the Same User
Payments	Invoices	Payment Process Req...	Purchase Orders
4	66	1	12

PTP-40001a Supplier and Payment created by the same user

Identify Payments created by the same user who created the corresponding Supplier

Supplier Created By CASEY.BROWN ▼

Supplier Name	Payment Created By	Payment Amount	Payment Date
InterUK	CASEY.BROWN	2,247.50	18-10-2022 05:46::44.000
Internal Revenue Service	CASEY.BROWN	640.92	10-06-2020 07:32::41.000
Internal Revenue Service	CASEY.BROWN	89.38	13-10-2020 11:01::03.000
Internal Revenue Service	CASEY.BROWN	55.86	11-05-2020 05:38::06.000

PTP-40001 Supplier and Payables Invoices created by the same user

Identify payables invoices created in the last six months by the user who created the corresponding supplier or supplier site

Invoice Created By camille.fredricks ▼

Supplier Name	Site Name	Invoice Amount	Invoice Number	Invoice ID	Invoice Date	Supplier Created By	Site Location Created By
Siemens Medical Solutions	Siemens HC	98,114.19	ERS-500607-451557	970292	23-12-2021 12:00::00.000	camille.fredricks	camille.fredricks
Siemens Medical	Siemens	96,330.45	ERS-500593-451548	970283	26-11-2021	camille.fredricks	camille.fredricks

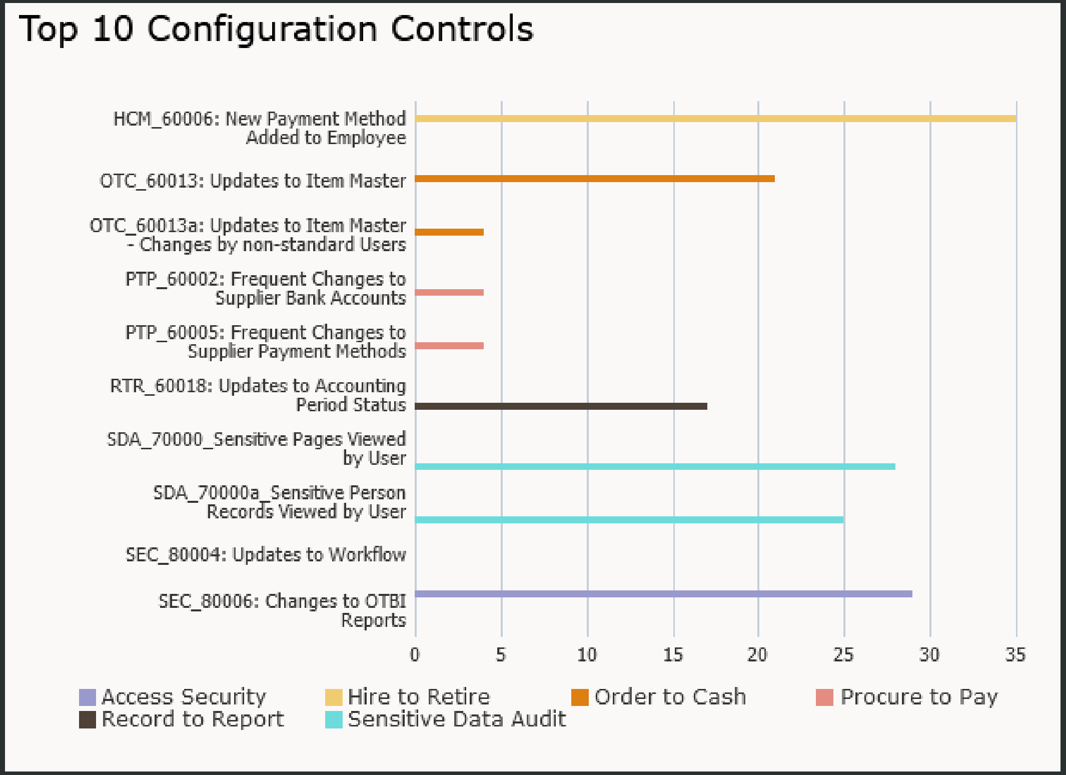
Continuous Configuration & Transaction Monitoring

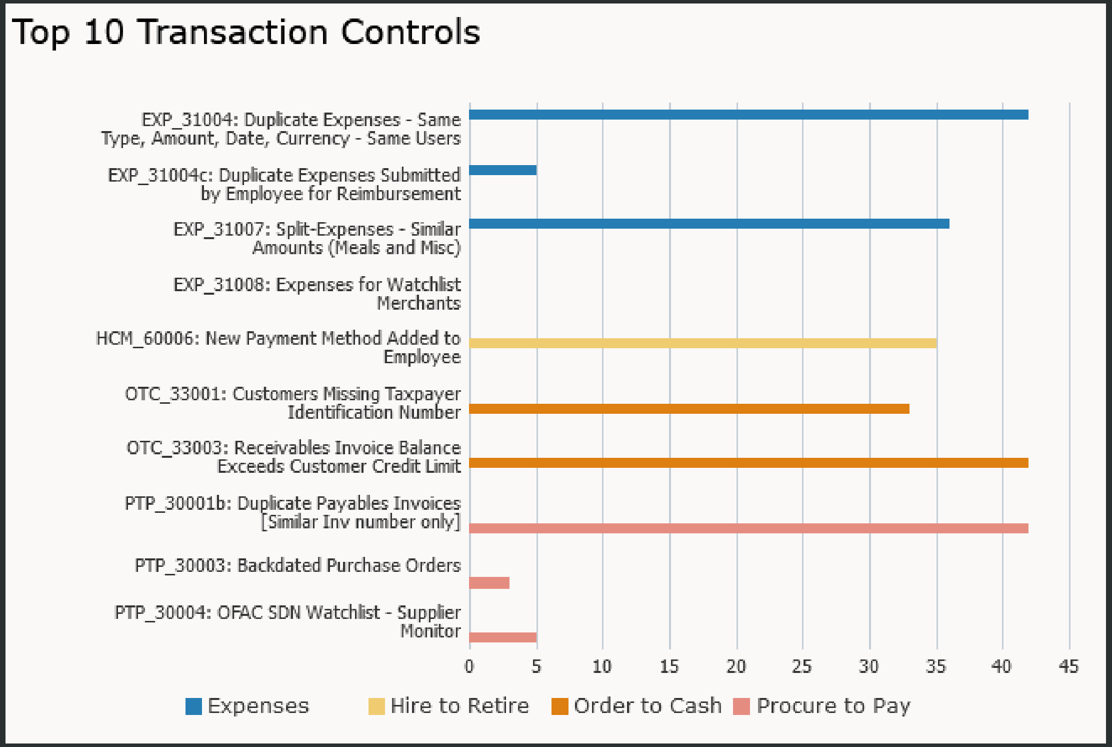
AUTHOR AUDIT RULES AND ALGORITHMS

Design automated auditing using integration with configuration data elements and visual editing and model results.

AUTOMATE TRANSACTION ANALYSIS

Continuously monitor financial transactions for process anomalies and policy violations.

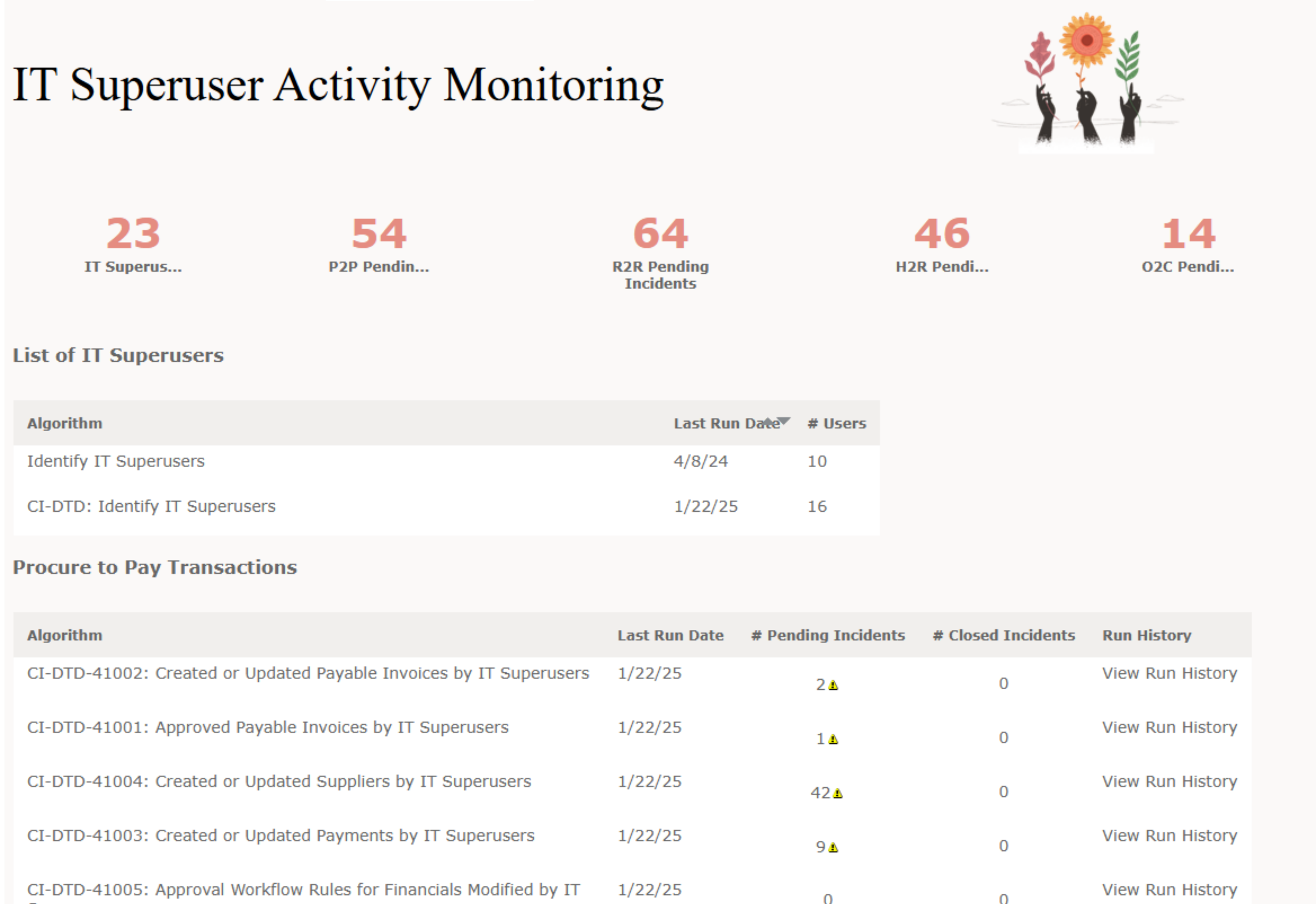




Superuser Activity Monitoring

MONITOR SUPERUSER ACCESS & TRANSACTIONS

Certain users (IT or Business) have broad, superuser access to facilitate manipulation of configurations, setups, and master data. Because of their deep functional and process knowledge, it makes sense to give these users broad access can be very powerful—provided safeguards are in place to monitor for unusual activity, such as error or misuse.



IT Superuser Activity Monitoring

23	54	64	46	14
IT Superus...	P2P Pendin...	R2R Pending Incidents	H2R Pendi...	O2C Pendi...

List of IT Superusers

Algorithm	Last Run Date	# Users
Identify IT Superusers	4/8/24	10
CI-DTD: Identify IT Superusers	1/22/25	16

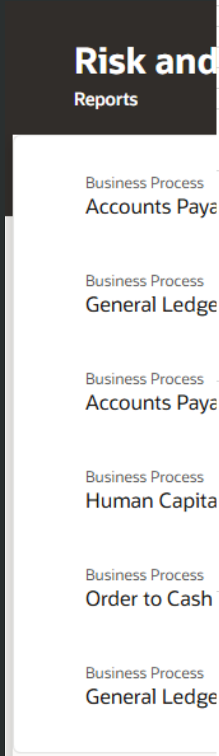
Procure to Pay Transactions

Algorithm	Last Run Date	# Pending Incidents	# Closed Incidents	Run History
CI-DTD-41002: Created or Updated Payable Invoices by IT Superusers	1/22/25	2 ⚠	0	View Run History
CI-DTD-41001: Approved Payable Invoices by IT Superusers	1/22/25	1 ⚠	0	View Run History
CI-DTD-41004: Created or Updated Suppliers by IT Superusers	1/22/25	42 ⚠	0	View Run History
CI-DTD-41003: Created or Updated Payments by IT Superusers	1/22/25	9 ⚠	0	View Run History
CI-DTD-41005: Approval Workflow Rules for Financials Modified by IT	1/22/25	0	0	View Run History

Risk & Security Snapshot Report

COMPREHENSIVE ANALYSIS of BUSINES PROCESS RISKS

Provides summary and detailed information about risk in the business process represented by the content pack you selected, over the period you specified.



Risk and
Reports

Business Process
Accounts Paya

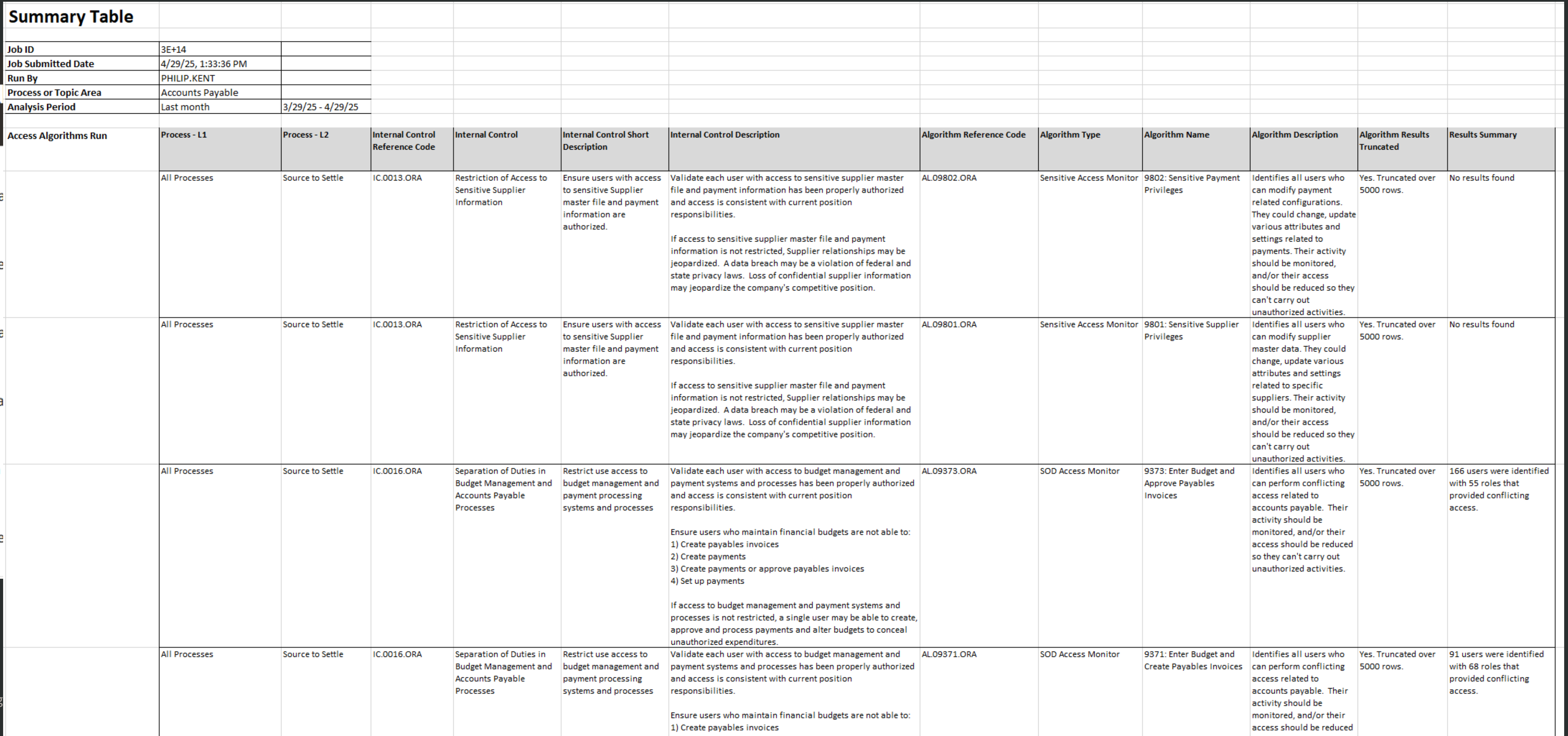
Business Process
General Ledge

Business Process
Accounts Paya

Business Process
Human Capita

Business Process
Order to Cash

Business Process
General Ledge



Summary Table

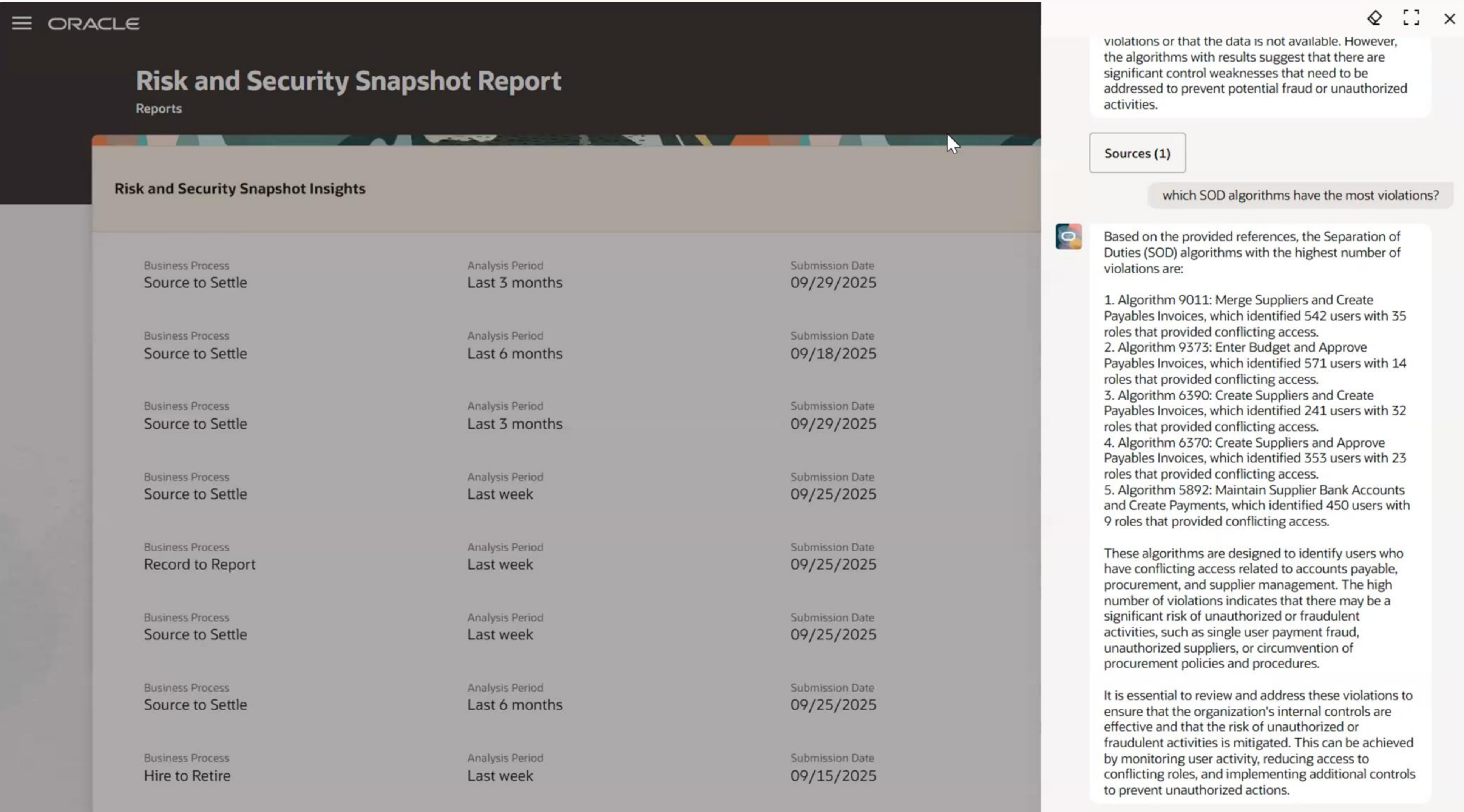
Job ID	3E+14	
Job Submitted Date	4/29/25, 1:33:36 PM	
Run By	PHILIP.KENT	
Process or Topic Area	Accounts Payable	
Analysis Period	Last month	3/29/25 - 4/29/25

Access Algorithms Run	Process - L1	Process - L2	Internal Control Reference Code	Internal Control	Internal Control Short Description	Internal Control Description	Algorithm Reference Code	Algorithm Type	Algorithm Name	Algorithm Description	Algorithm Results Truncated	Results Summary
	All Processes	Source to Settle	IC.0013.ORA	Restriction of Access to Sensitive Supplier Information	Ensure users with access to sensitive Supplier master file and payment information are authorized.	Validate each user with access to sensitive supplier master file and payment information has been properly authorized and access is consistent with current position responsibilities. If access to sensitive supplier master file and payment information is not restricted, Supplier relationships may be jeopardized. A data breach may be a violation of federal and state privacy laws. Loss of confidential supplier information may jeopardize the company's competitive position.	AL.09802.ORA	Sensitive Access Monitor	9802: Sensitive Payment Privileges	Identifies all users who can modify payment related configurations. They could change, update various attributes and settings related to payments. Their activity should be monitored, and/or their access should be reduced so they can't carry out unauthorized activities.	Yes. Truncated over 5000 rows.	No results found
	All Processes	Source to Settle	IC.0013.ORA	Restriction of Access to Sensitive Supplier Information	Ensure users with access to sensitive Supplier master file and payment information are authorized.	Validate each user with access to sensitive supplier master file and payment information has been properly authorized and access is consistent with current position responsibilities. If access to sensitive supplier master file and payment information is not restricted, Supplier relationships may be jeopardized. A data breach may be a violation of federal and state privacy laws. Loss of confidential supplier information may jeopardize the company's competitive position.	AL.09801.ORA	Sensitive Access Monitor	9801: Sensitive Supplier Privileges	Identifies all users who can modify supplier master data. They could change, update various attributes and settings related to specific suppliers. Their activity should be monitored, and/or their access should be reduced so they can't carry out unauthorized activities.	Yes. Truncated over 5000 rows.	No results found
	All Processes	Source to Settle	IC.0016.ORA	Separation of Duties in Budget Management and Accounts Payable Processes	Restrict use access to budget management and payment processing systems and processes	Validate each user with access to budget management and payment systems and processes has been properly authorized and access is consistent with current position responsibilities. Ensure users who maintain financial budgets are not able to: 1) Create payables invoices 2) Create payments 3) Create payments or approve payables invoices 4) Set up payments If access to budget management and payment systems and processes is not restricted, a single user may be able to create, approve and process payments and alter budgets to conceal unauthorized expenditures.	AL.09373.ORA	SOD Access Monitor	9373: Enter Budget and Approve Payables Invoices	Identifies all users who can perform conflicting access related to accounts payable. Their activity should be monitored, and/or their access should be reduced so they can't carry out unauthorized activities.	Yes. Truncated over 5000 rows.	166 users were identified with 55 roles that provided conflicting access.
	All Processes	Source to Settle	IC.0016.ORA	Separation of Duties in Budget Management and Accounts Payable Processes	Restrict use access to budget management and payment processing systems and processes	Validate each user with access to budget management and payment systems and processes has been properly authorized and access is consistent with current position responsibilities. Ensure users who maintain financial budgets are not able to: 1) Create payables invoices	AL.09371.ORA	SOD Access Monitor	9371: Enter Budget and Create Payables Invoices	Identifies all users who can perform conflicting access related to accounts payable. Their activity should be monitored, and/or their access should be reduced	Yes. Truncated over 5000 rows.	91 users were identified with 68 roles that provided conflicting access.

Risk & Security Snapshot Report – New Feature

Embedded AI: Risk & Security Snapshot – Assurance Advisor

25D – Using AI Agent Studio, configure a chatbot that summarizes risks within your business processes



Risk and Security Snapshot Report

Reports

Risk and Security Snapshot Insights

Business Process	Analysis Period	Submission Date
Source to Settle	Last 3 months	09/29/2025
Source to Settle	Last 6 months	09/18/2025
Source to Settle	Last 3 months	09/29/2025
Source to Settle	Last week	09/25/2025
Record to Report	Last week	09/25/2025
Source to Settle	Last week	09/25/2025
Source to Settle	Last 6 months	09/25/2025
Hire to Retire	Last week	09/15/2025

violations or that the data is not available. However, the algorithms with results suggest that there are significant control weaknesses that need to be addressed to prevent potential fraud or unauthorized activities.

Sources (1)

which SOD algorithms have the most violations?

Based on the provided references, the Separation of Duties (SOD) algorithms with the highest number of violations are:

1. Algorithm 9011: Merge Suppliers and Create Payables Invoices, which identified 542 users with 35 roles that provided conflicting access.
2. Algorithm 9373: Enter Budget and Approve Payables Invoices, which identified 571 users with 14 roles that provided conflicting access.
3. Algorithm 6390: Create Suppliers and Create Payables Invoices, which identified 241 users with 32 roles that provided conflicting access.
4. Algorithm 6370: Create Suppliers and Approve Payables Invoices, which identified 353 users with 23 roles that provided conflicting access.
5. Algorithm 5892: Maintain Supplier Bank Accounts and Create Payments, which identified 450 users with 9 roles that provided conflicting access.

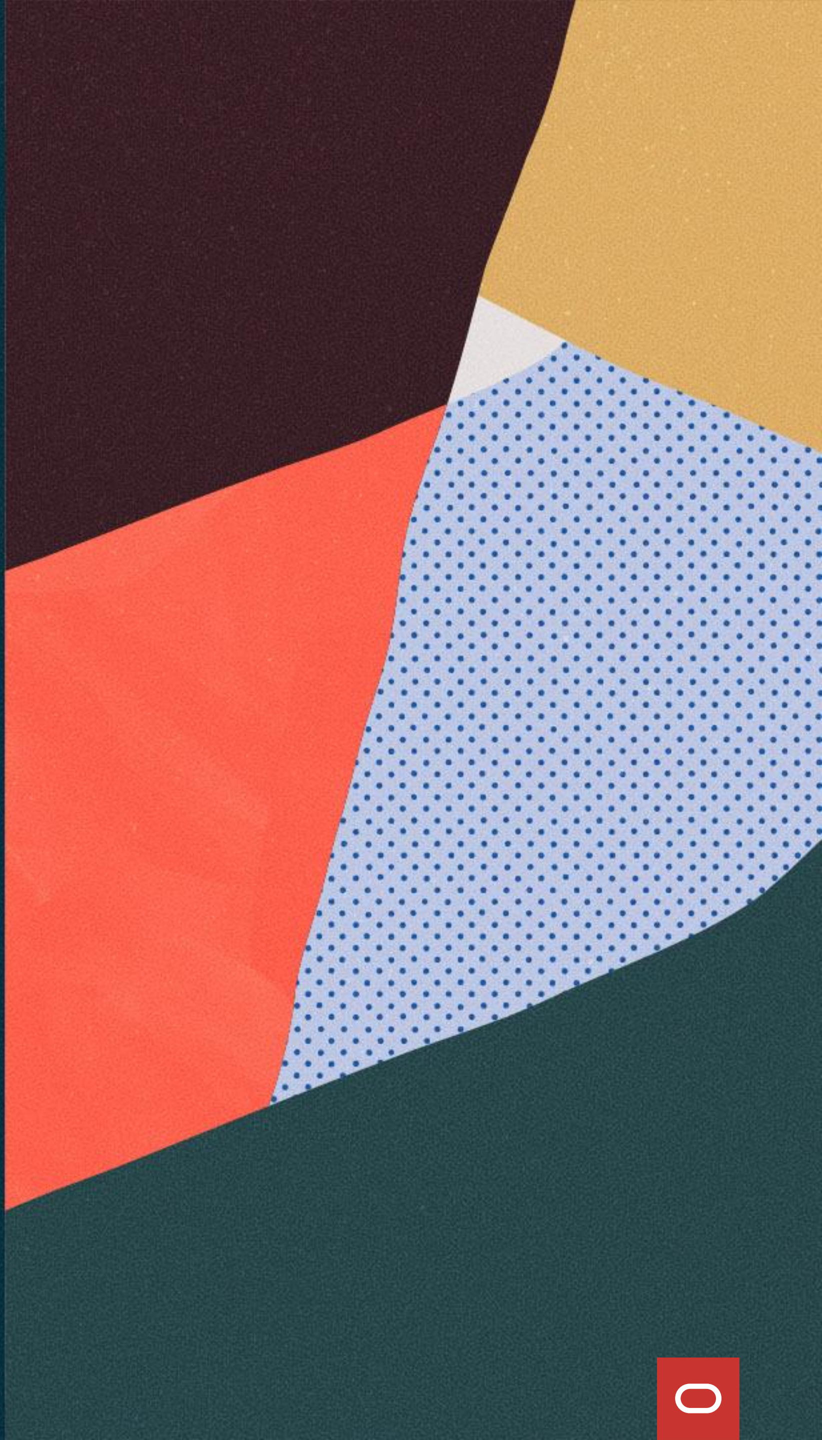
These algorithms are designed to identify users who have conflicting access related to accounts payable, procurement, and supplier management. The high number of violations indicates that there may be a significant risk of unauthorized or fraudulent activities, such as single user payment fraud, unauthorized suppliers, or circumvention of procurement policies and procedures.

It is essential to review and address these violations to ensure that the organization's internal controls are effective and that the risk of unauthorized or fraudulent activities is mitigated. This can be achieved by monitoring user activity, reducing access to conflicting roles, and implementing additional controls to prevent unauthorized actions.

Looking for more?

- Enhance Fusion Cybersecurity and Breach Detection with AI [PAN1328]
  - Hear from Meta & T-Mobile
    - **9:45 AM - 10:30 AM PDT**

- Risk Management Demo Hub @ APPS202
    - **Today until 6pm PDT**



Your feedback is important.

Scan this QR Code or use the Mobile App to share your thoughts on this session.

Thank you

Robert Singleton

https://www.oracle.com/erp/risk-management/

ORACLE