Oracle Fusion Cloud Risk Management

Using Risk and Security Snapshot Report

26A

Oracle Fusion Cloud Risk Management
Using Risk and Security Snapshot Report

26A

G46429-01

Copyright © 2025, 2026, Oracle and/or its affiliates.

Author: David Christie

Contents

Get Help

There are a number of ways to learn more about your product and interact with Oracle and other users.

Get Help in the Applications

Some application pages have help icons to give you access to contextual help. If you don't see any help icons on your page, click your user image or name in the global header and select Show Help Icons. If the page has contextual help, help icons will appear.

Get Training

Increase your knowledge of Oracle Cloud by taking courses at *Oracle University*.

Join Our Community

Use *Cloud Customer Connect* to get information from industry experts at Oracle and in the partner community. You can join forums to connect with other customers, post questions, suggest *ideas* for product enhancements, and watch events.

Share Your Feedback

We welcome your feedback about Oracle Applications user assistance. If you need clarification, find an error, or just want to tell us what you found helpful, we'd like to hear from you.

You can email your feedback to *oracle_fusion_applications_help_ww_grp@oracle.com*.

Thanks for helping us improve our user assistance!

1 Introduction and Setup

Overview of Risk and Security Snapshot Report

Oracle Risk and Security Snapshot Report performs comprehensive analysis of risk in your business processes.

It's designed to be easy for you to use: First, select a "content pack," which is a set of Oracle-developed objects appropriate for analyzing risk in a specified business process. Next, select a time period. Then run an analysis job.

The analysis may involve a large amount of data, so the job typically runs for hours, up to a maximum of twenty-four. Upon completion, the analysis returns a report. It provides summary and detailed information about risk in the business process represented by the content pack you selected, over the period you specified.

Each content pack can perform two types of analysis:

- Access analysis identifies users with separation-of-duties conflicts: each user is assigned roles granting privileges that combine to create the potential for fraud or significant error. The analysis also identifies roles that provide sensitive access: each role on its own grants elevated access, and so can't be assigned without risk.
- Transaction analysis returns records of actual transactions in Oracle Cloud applications that display evidence of fraud, error, separation-of-duties violations, or other risk.

To perform these analyses, Risk and Security Snapshot Report uses objects called "algorithms." Each consists of filters that form a processing logic to select records exhibiting a risk. An access algorithm may, for example, filter for users who have the privileges both to create a payables invoice and approve payment on that invoice. For another example, a transaction algorithm may find occasions when individual users have completed both of those actions.

Each content pack is a set of algorithms developed by Oracle to implement best practices in risk management. Because the application uses algorithms created by Oracle, you don't have to wrestle with algorithm development or risk-logic definitions.

You can use Risk and Security Snapshot Report on its own, or to provide an initial "health check" for Advanced Controls, a more robust risk-management application. Advanced Controls enables you both to use Oracle-developed access and transaction algorithms, and to create your own; to deploy those algorithms as controls that provide continuous monitoring; and to track and resolve findings uncovered by those controls. As an implementation tool, Risk and Security Snapshot Report can identify key areas to focus on in each business process as you use Advanced Controls.

Set Up Risk and Security Snapshot Report

To use Risk and Security Snapshot Report, your organization must complete several setup procedures. Then your organization must create and assign a custom job role that contains a required privilege as well as a duty role that contains new elements called "permission groups."

The first setup procedure is to select a promotion code.

1. Click Navigator > My Enterprise > Enterprise.
2. In an Enterprise Information page, click the **Manage Promotion Codes** link.
3. In a Manage Promotion Codes page, click the **Enter Promotion Code** button.
4. In an Enter Promotion Code dialog, enter the value **GTG484673**. Then click Save and Close.

5. Click the **Done** button.

Next, opt in to Risk and Security Snapshot Report.

1. Click Navigator > My Enterprise > Offerings.
2. In the Offerings page, scroll to the Risk Management offering and select it.
3. Click the **Opt In Features** button.
4. In an Opt In: Risk Management page, select the **Enable** check box in the Recommendation Engine row.
5. Select the edit (pencil) icon in the Features column of the Recommendation Engine row.
6. In an Edit Features page, click the **Enable** check box for Security Checkup and Recommendations.
7. Click **Done** in the Edit Features page, and then **Done** again in the Opt In: Risk Management page.

Next, set a profile option that enables job roles to recognize permission groups (and the duty roles that contain them).

1. Click Navigator > My Enterprise > Setup and Maintenance.
2. Expand the Tasks panel tab and click Search.
3. In the Search Tasks field, enter **Manage Administrator Profile Values**. Click the Search icon.
4. In the list returned by the search, click the **Manage Administrator Profile Values** item.
5. The Search area of the Manage Administrator Profile Values page includes a Profile Option Code field. In it, enter **ORA_ASE_SAS_INTEGRATION_ENABLED**. Click the Search button.
6. A record of the ORA_ASE_SAS_INTEGRATION_ENABLED profile value appears. In the row for the Site profile level, select **Yes** in the Profile Value field.
7. Click **Save and Close**.

Next, create the custom job role that grants access to Risk and Security Snapshot Report, or edit an existing custom job role to provide that access, and assign the role to users. For the procedures to edit a custom job role and to create one from scratch, see two topics in the Securing Risk Management guide: *Create Risk Management Roles in the Security Console* and *Copy or Edit Risk Management Roles in the Security Console*. But add this information:

- In the Basic Information page, you assign a name and a code to your role, and select the **GRC - Job Roles** role category. (If you're editing a role, this is already done.) An **Enable Permission Groups** button then becomes active; click it. A dialog opens, showing the name of the role you're creating or editing. Click its **Enable Permission Groups** button.
- Use the Function Security Policies page (as instructed in the "Create Risk Management Roles" topic) to add the **Create and Manage Recommendation Engine Analyses** privilege. You may choose to search for it by its code, GTG_CREATE_AND_MANAGE_RECOMMENDATION_ENGINE_ANALYSES_PRIV.
- Don't select anything in the Permission Groups page.
- In the Role Hierarchy page, select the **Roles and Permission Groups** tab. In it, click **Add Role**. An **Add Role Membership** dialog opens. In it, search for and select **Security and Controls Snapshot Report**. This is the duty role that contains the permission groups your job role requires. You may choose to search for the duty role by its role code, ORA_DR_GTG_SECURITY_AND_CONTROLS_SNAPSHOT_REPORT_ DUTY.
- If you're editing a role, the Users page retains the role's user assignments. If you want to modify those assignments, or if you've created a new role and need to assign users to it, you must do so in the Users page.

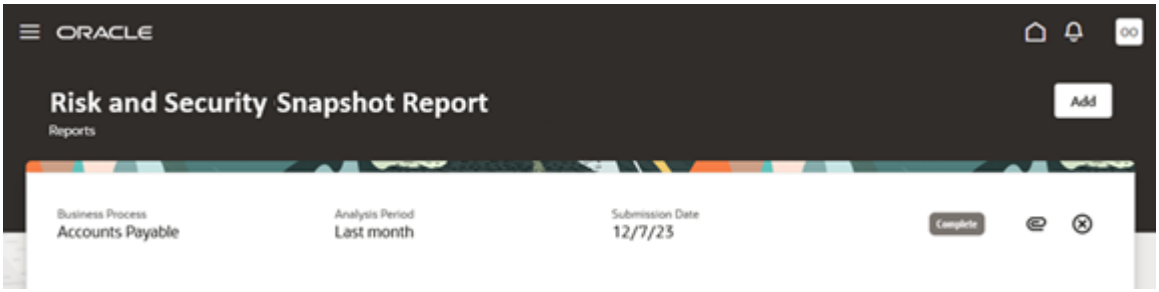
Finally, log off of Oracle Fusion Cloud Applications and log back in.

2 Manage Snapshot Reports

To Begin

To open the application, click the Risk and Security Snapshot Report icon in the Risk Management work area.

You land on a Risk and Security Snapshot Report page, which displays records of analyses that have been run. Each record identifies the business process that's been analyzed, the analysis period, when the job was submitted, and its status. (The page is empty if no analysis has yet been performed.)

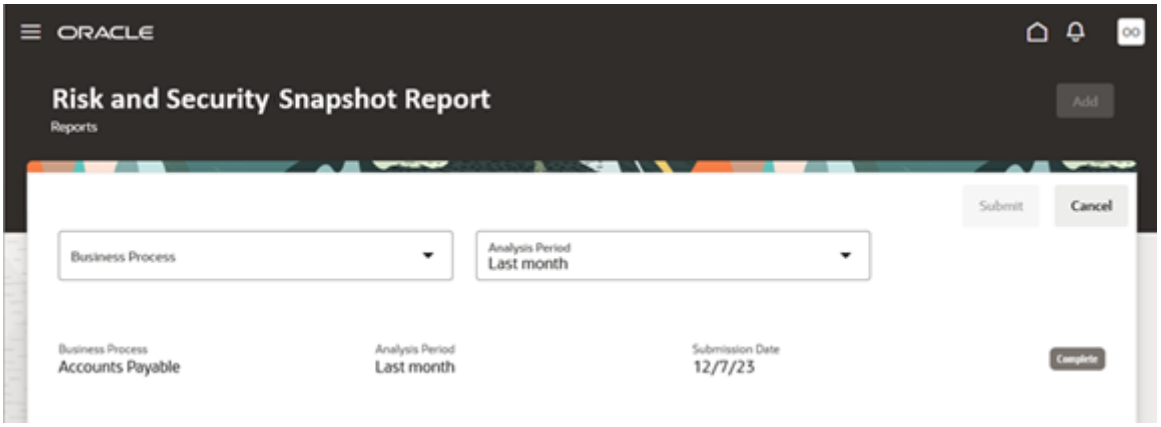


From this page you can run an analysis, check on the progress of an analysis that's running, or download the report generated by an analysis whose run is complete. You can also cancel an analysis job that's in progress, or delete a completed analysis.

Run an Analysis

To run an analysis:

1. Click the Add button in the Risk and Security Snapshot Report page. Two fields appear above the records of any analyses you've already run.



2. In the Business Process field, select the business process for which you want to evaluate risk: Accounts Payable, General Ledger, Order to Cash, or Human Capital Management. However, you can run only one analysis of each process at a time.
3. In the Analysis Period field, select the amount of time the analysis is to cover: the week, month, three months, or six months previous to the moment you submit the job. The previous month is the default.
4. Click the Submit button. A row for the analysis appears in the list of analyses.

As the job runs, its status advances from In Progress to either Complete or Job Has Errors. The job takes a while to run, so you're expected to close the Risk and Security Snapshot Report page while the job is running, and reopen it when the job is complete. Upon completion, you receive a notification. To view it, click the Notifications icon in the global header. It looks like a bell.

A job generates an error if it doesn't finish running within twenty-four hours. The solution would be to rerun the job with a shorter analysis period, so that the job would encompass a smaller volume of data.

Cancel an Analysis or Delete an Analysis Record

You can cancel a job while it's running, or delete the record of a job after it finishes running.

To cancel a job, click the Cancel button in the row for an analysis. The status for the job changes initially to Cancel Requested, and then to Job Canceled when the application completes the operation.

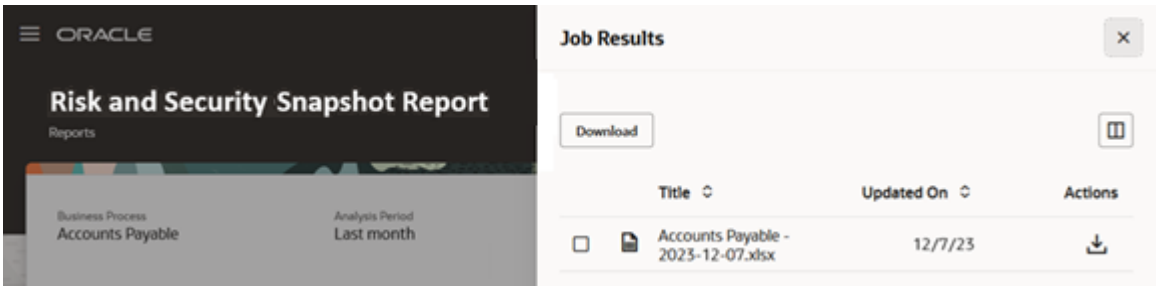
You can cancel a job only while it's running. But the Risk and Security Snapshot Report page refreshes only when you take some action, such as opening it. So if the page is already open when the job reaches completion, the Cancel button remains available even though it can no longer be used. If you click the Cancel button after a job is complete, however, the page simply refreshes: the Cancel button is removed and the job status is updated.

To delete the record of a completed job from the Risk and Security Snapshot Report page, click the Delete button in its row. Then respond to a confirmation message. When you delete the record of a job, the report associated with it is no longer available.

Download an Analysis Report

The record of each completed analysis job includes a Job Results icon (which looks like a paper clip). Click it to open a Job Results panel.

The panel displays the name of the report, which consists of the name of the business process and the date the analysis finished running. Click the Download icon in the Actions column. Or, select the report's check box and then click the Download button.



The report is an Excel workbook, in which four worksheets provide summary data, and other worksheets contain results of individual algorithms the analysis job has run.

3 Review Results of a Snapshot Report

Summary Worksheets

Four worksheets provide summaries of the overall analysis of access and transaction results. Click the following tabs to review them.

- Summary Table is the initial worksheet in every report. It provides an ID number and submission date for the analysis job, the name of the user who ran the analysis, the business process it examines, and the analysis period. It also provides distinct lists of all the access algorithms and all the transaction algorithms used in the analysis.

  Each row in each of the lists includes information about an algorithm the job has run, an "internal control" for which the algorithm detects issues, a risk that the control guards against, and a business process affected by the risk. For each of these elements, you'll see a name, a reference code, and a description. (A process name comprises three levels describing a focused effort within a larger process.) Each row also provides a summary of its algorithm's results.

  To ensure a meaningful set of results for investigation while also increasing the likelihood that the analysis job runs within twenty-four hours, the application applies limits to the analysis. The Summary Table reports the effects of these limits:

  - No algorithm can return more than 5,000 result records. An Algorithm Results Limited column reports whether the results for each algorithm are truncated because they've reached that limit, or are complete.
  - Before algorithms run, a synchronization job refreshes the data those algorithms analyze. Limits on the synch job may cause some algorithms to analyze incompletely synchronized data. An Algorithm Analysis Status column reports whether each algorithm has run against incompletely or fully synchronized data.
- Intrarole Access Risks is included if the analysis runs at least one access algorithm. It identifies roles that can't be assigned to any user without some risk, because each role contains access issues on its own. Each row shows the name of a role, the number and names of the algorithms it's violated, and the number of users assigned the role.
- User Access Risks is also included if the analysis runs at least one access algorithm. Each row gives the name of a user (and that user's position and manager), the number and names of the algorithms violated by that user's role assignments, and the number of unique paths that lead from a job role the user is assigned to another role or privilege involved in a conflict defined by the algorithm.
- Transaction Risk Summary is included if the analysis runs at least one transaction algorithm. Each row gives the name and a brief description of a transaction algorithm, the number of result records the algorithm has returned, and (if appropriate) the monetary value of the transactions that violate the algorithm.

Access Algorithm Results

In the worksheet that reports the results of an access algorithm, each row is a record of an access assignment to a user that the algorithm defines as risky. More often than not, a single access conflict involves assignments documented in more than one row. As you view results, you'll encounter some specialized terminology:

- An access point is any job role, duty role, or privilege. An access algorithm defines conflicts between access points. An Access Point column identifies the access point that's the focus of a result record, and an Access Point Type column indicates whether it's a privilege or a role.
- An Incident Information column reports the path to the access point that's the focus of the result record. (Paths to access points are defined by hierarchies established in your job and duty roles.)
- An access entitlement is a set of related access points. An algorithm may (and typically does) define conflicts between entitlements. If so, each access point in one entitlement conflicts with every access point in the other. An Access Entitlement Name column identifies the entitlement to which the Incident Information access point belongs.
- A Role column identifies the role that provides access to the Incident Information access point.
- User Name, First Name, and Last Name columns identify the user whose role assignments contain conflicts.

Often, an efficient way to review an access worksheet is to use it as the source of a pivot table, which can arrange data to emphasize what you want to see. Examples in the next two topics illustrate the use of pivot tables in access worksheets. Complete these preparatory steps before creating pivots from access-algorithm worksheets:

- Remove any rows above the column-header rows.
- Select all remaining rows: Click on the triangle icon in the upper left corner (between the letter A that labels the first column and the number 1 that labels the first row).

Access Examples: Intrarole Risk

To begin an intrarole-risk investigation, review the Intrarole Access Risks summary worksheet. It may contain records of analysis by two types of algorithm.

The first type detects sensitive access: A role may include individual privileges whose assignments are worthy of review because each provides broad access. These algorithms include the word "sensitive" in their names. For each of these algorithms that a role has violated, open the algorithm-result spreadsheet. In it, each record identifies a sensitive access point, the role that contains it, and a user assigned the role. You may remove the role from a user who doesn't need its sensitive access. More commonly, the user requires the sensitive access, but should be monitored.

The second intrarole-algorithm type detects occasions when a role on its own grants privileges that conflict with one another. The name of each of these algorithms consists of the names of two entitlements containing access points that would enable users to perform conflicting actions. For each algorithm that a role has violated, open the algorithm-result worksheet and create a pivot table based on these three values:

- Role: This identifies the role in which a conflict exits.
- Access Entitlement Name: Any role associated with two entitlements necessarily has an intrarole conflict. (The pivot table is likely to include records in which a role is associated with one entitlement. They apply to user-access-risk conflicts, so you can ignore them as you investigate intrarole conflicts.)

- Incident Information: These records identify paths to access points that conflict within the role. Each path belonging to one entitlement conflicts with every path belonging to the other entitlement.

For example, suppose the Intrarole Access Risks summary worksheet contains four rows that identify job roles with intrarole conflicts. One of them, Human Resource Manager, violates an algorithm called Manage Employee and Manage Payroll. The role is assigned to 25 people. This role is listed first in the following illustration.

Active Job Roles with Intra-Role Access Risk
Review and consider changing these job roles

Role Name	Number of Access Models Violated	List of Access Models Violated	Number of Users Assigned
Human Resource Manager	1	4051 Manage Employee and Manage Payroll	25
Custom AP Analyst Job Role	2	6390 Create Suppliers and Create Payables Invoices 6370 Create Suppliers and Approve Payables Invoices	24
Custom AP Analyst Job Role	3	9011 Merge Suppliers and Create Payables Invoices 9012 Merge Suppliers and Create Payments 9013 Merge Suppliers and Create Purchase Orders	17
Custom Supplier Manager Job Role	1	6410 Create Suppliers and Create Purchase Orders	6

Open the result worksheet for that algorithm (click on the tab labeled with its name), create the pivot table, and search on the role name. You'll find a set of records that looks like this:

Human Resource Manager
- **Manage Employee**
  - Human Resource Manager > Human Resource Specialist > Employee Hire > Hire Employee
  - Human Resource Manager > Human Resource Specialist > Employee Hire > Rehire Employee
  - Human Resource Manager > Human Resource Specialist > Manage Direct Report > Add Direct Report
  - Human Resource Manager > Human Resource Specialist > Manage Mass Updates Work Area
  - Human Resource Manager > Human Resource Specialist > Manage Work Terms and Assignment > Manage Work Terms and Assignment
- **Manage Payroll**
  - Human Resource Manager > Human Resource Specialist > Manage Payroll Relationship > Manage Payroll Relationship

In this example, the one path belonging to the Manage Payroll entitlement conflicts with each of the five paths belonging to the Manage Employee entitlement.

You might decide that the number of affected users is large enough that you should redesign the role to eliminate its conflicts. In this example, you might use the Security Console to remove the one access point that conflicts with all the others: Manage Payroll Relationship.

Or, suppose that the number of users had been smaller and that, having identified those users, you realize they require the conflicting access to do their jobs. You might choose to leave the role as it is, monitor those users regularly, and prevent the role from being assigned to users who don't need its conflicting access.

Then follow the same process to resolve conflicts in any remaining roles. (There are three in this example.) Use the Intrarole Access Risks summary worksheet to identify a suspect role and the algorithms it's violated. Open the worksheet for each algorithm, create the pivot table, and search for the role. Note, though, that if you've already created a pivot table for an algorithm as you cleaned up conflicts in another role, you can reuse that pivot table.

Access Example: User-Access Risk

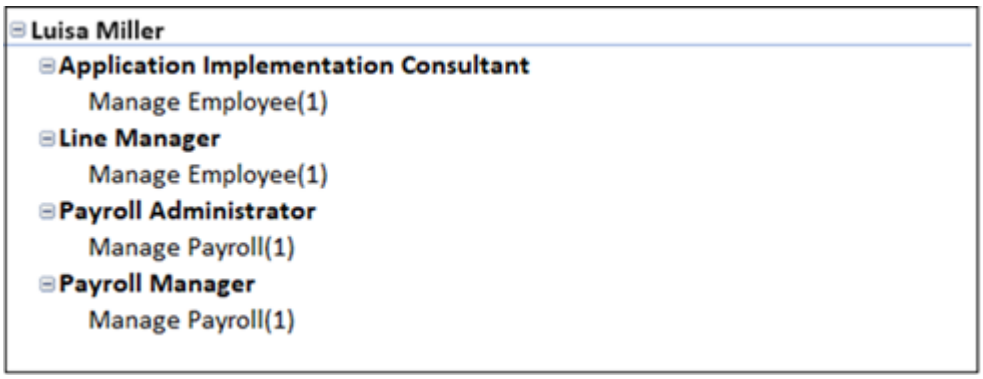
To begin investigating user-access risk, review the User Access Risks summary worksheet. For each user with role-assignment conflicts, identify the algorithms that define those conflicts. Open the worksheet for each algorithm, and create a pivot table based on these three values:

- User Name: This identifies a user assigned roles that combine to violate access algorithms.

- Role: This identifies the roles that potentially conflict.
- Access Entitlement Name: This names entitlements containing access points that in combination may violate access algorithms. Sometimes, a role may be associated with two entitlements, which indicates an intrarole conflict. To remove that "noise," it's recommended that you clean up intrarole conflicts before you investigate user-access conflicts. Then, each role in the pivot table for user-access risk typically lists a single entitlement. Conflicts exist between roles associated with one entitlement and roles associated with any other entitlements.

For example, suppose the User Access Risk summary worksheet contains a row stating that a user named Luisa Miller is assigned roles that violate the Manage Employee and Manage Payroll algorithm. (Once again, the algorithm name identifies two entitlements whose access points conflict.)

Open the result worksheet for that algorithm, create the pivot table, and search for the user name. You'll find a set of records that looks like this:



Each role associated with one entitlement conflicts with every role associated with the other entitlement. In this example, there are four conflicts: Application Implementation Consultant with Payroll Administrator, Application Implementation Consultant with Payroll Manager, Line Manager with Payroll Administrator, and Line Manager with Payroll Manager.

Your typical recourse is to rescind the user's access to one of the roles in each conflict. In this example, you would use the Security Console to remove either Application Implementation Consultant and Line Manager, or Payroll Administrator and Payroll Manager. Another option is to create customized versions of the two roles you would otherwise take away. Each custom role would remove a conflicting access point, but retain other access rights.

Transaction Algorithm Results

In the worksheet for a transaction algorithm, each row is the record of a transaction that violates the algorithm, although a single violation may encompass multiple rows. For example, an algorithm that detects duplicate invoices would return one row for each of the duplicated invoices.

Records may contain the following information:

- Most columns report values for attributes of business objects. A business object is a set of related fields in a business application subject to analysis by an algorithm. An attribute is one field in the set. However, every transaction algorithm is assigned its own result attributes, so the result worksheet for each algorithm contains a unique set of columns.

  The header for each of these columns concatenates the name of a business object with the name of one of its attributes, with a period as the delimiter. For example, "Supplier.Supplier Name" indicates the Supplier Name

attribute of the Supplier business object. In this example, the value reported for each record would be the name of a supplier.

- Attributes include key values, such as supplier number or invoice number, that you can use to search for records of suspect transactions in the applications in which they were created. These attributes are located in the first few columns of an algorithm-detail worksheet. They vary from algorithm to algorithm.
- Algorithms may use filters that divide records into groups. In each group, specified values are either equal or similar to one another. The records in each group constitute a set of transactions that may present an issue. For example, an algorithm may group invoice records by supplier, to determine whether invoice amounts for each supplier exceed a limit, or perhaps an average amount.

  When an algorithm creates groups, columns report the values that are equal or similar to one another. Their headings include the phrase "is the same" or "is xx percent similar" (in which xx is a number). They're among the last few columns in the worksheet. Also, each worksheet includes an algorithm description, which you're encouraged to read not only to understand what the algorithm sets out to find, but also to identify significant features such as grouping values.
- A transaction algorithm may incorporate "derived attributes." These are calculations performed by the algorithm. For example, the algorithm that groups invoice records by supplier may calculate the total value, or the average value, of invoices for each supplier. For each record in the group, a column reports the calculated value.

Some algorithms find transactions in each of which an individual user has acted in a way that violates sound separation-of-duties policy. Others find transactions that show signs of any sort of risk other than SOD risk. The type of an algorithm may influence how you review its results.

The name of each transaction algorithm begins with a five-digit code. You can use the first two digits of each code to distinguish the type of algorithm as well as the business process to which it applies:

Code Begins With	Algorithm Type
30	Non-SOD analysis in the Accounts Payable process
32	Non-SOD analysis in the General Ledger process
33	Non-SOD analysis in the Order to Cash process
40	SOD analysis in any of the Accounts Payable, General Ledger, or Order to Cash processes
50	SOD and non-SOD analysis in the Human Capital Management process

Transaction Example: SOD Risk

Algorithms may review transactions for separation-of-duties risk. Each specifies actions that may conflict, such as managing suppliers and creating payable invoices for those suppliers, and identifies users who have created or updated records of those actions.

In the result worksheet for one of these algorithms, each row is in itself a complete risk incident. For example, suppose the Transaction Risk Summary worksheet contains a row for an algorithm titled 40001: Supplier and Payables Invoices Created by the Same User. It indicates that algorithm violations exceed $100,000 and that the worksheet includes 56 result rows. For this type of algorithm, there are therefore 56 individual issues for you to investigate.

You open the result worksheet for the algorithm. Its description tells you that each row identifies users who have created both a payables invoice and a record of the corresponding supplier or supplier site. You might want to begin by sorting on the Payables Invoice.Amount column, so that you can start with the highest-value issue and descend from there.

You would then look for "Created By" columns. (Some SOD algorithms also include "Last Updated By" columns.) In this algorithm, the columns identify users who created supplier records, payables invoice records, and supplier-site location records. In the row for a particular supplier, you would discover the identity of an individual user who has created all three of these records, or two of the three. You could then investigate the related record numbers and follow up with that user to determine that the actions were legitimate.

	A	B	C	D	E	F	G	H
1	40001: Supplier and Payables Invoices Created by the Same User							
2								
3	Model Description	Identify payables invoices created for a specified time frame by the user who created the corresponding supplier or supplier site						
4	Last Run Date	11/10/23, 7:18:49 PM						
5								
6	Supplier.Supplier Name	Payables Invoice.Amount	Payables Invoice.Date	Payables Invoice.Invoice Currency	Payables Invoice.Number	Payables Invoice.Invoice Created By	Supplier.Created By	Supplier Site Location.Created By
7	Acme Hardware	20000.00	11/1/23 12:00 AM	CAD	Invoice5_NOVEMBER23	MWYLIE	MWYLIE	MWYLIE
8	Blue Star Limited	6700.00	11/3/23 12:00 AM	USD	Invoice17_Nov03_2023	JSMITH	JJONES	JSMITH
9	Blue Star Limited	6500.00	11/3/23 12:00 AM	USD	Invoice18_Nov03_2023	JSMITH	JJONES	JSMITH

Transaction Examples: General Risk

Algorithms may review transactions for risks other than separation of duties. Broadly, these algorithms come in two types.

For one type, each row in the result worksheet for an algorithm is by itself a complete risk incident. For example, suppose the Transaction Risk Summary worksheet contains a row for an algorithm titled 30003: Backdated Purchase Orders. It indicates that algorithm violations amount to more than $80,000 and that its worksheet includes 35 result rows. For this algorithm type, there are therefore 35 individual issues for you to investigate.

You open the result worksheet for the algorithm. Its description tells you that each row documents a purchase order created for a time period that comes after its payables invoice date. Each record provides a supplier name, purchase order number, creator of the purchase order, and other information you can use to investigate the issue. Your first step may be to sort on its Payables Invoices with Purchase Orders.Amount column; this enables you to focus on high-value issues first.

	A	B	C	D	E	F	G
1	30003: Backdated Purchase Orders						
2							
3	Model Description	Identify purchase orders created for a specified time frame and created after the payables invoice date					
4	Last Run Date	1/22/24, 7:18:52 PM					
5							
6	Payables Invoices with Purchase Orders.Supplier Name	Payables Invoices with Purchase Orders.Amount	Payables Invoices with Purchase Orders.Date	Payables Invoices with Purchase Orders.Invoice Currency	Purchase Order.Number	Purchase Order.Creation Date	Payables Invoices with Purchase Orders.Number
7	Insulation Supply Co.	12050.00	1/16/24 12:00 AM	USD	1005306	1/18/24 12:00 AM	ERS-10230-22003

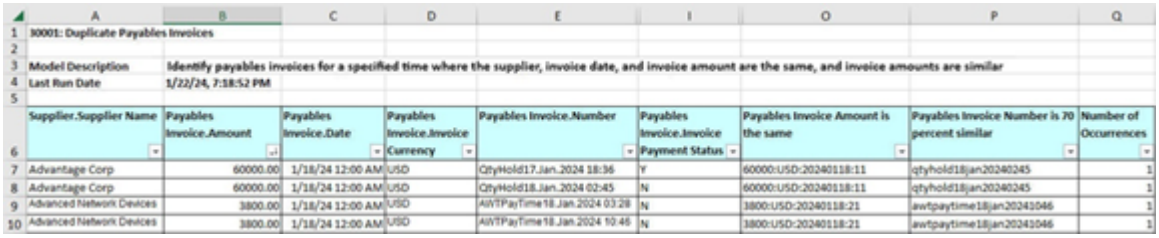
For the other type, result records in an algorithm form groups, each of which comprises a set of transactions that present an issue. As was already noted, in each group specified values are either equal or similar to one another. One aspect of reviewing the results of these algorithms is to isolate the records in each group so that you can compare them to identify risks.

For example, suppose the Transaction Risk Summary worksheet includes a row for an algorithm titled 30001: Duplicate Payables Invoices. It indicates that algorithm violations amount to more than $200,000, and that its worksheet includes

29 result records. (For a grouping algorithm, however, there's no direct correspondence between the number of result records and the number of issues to be investigated.)

You open the result worksheet for the algorithm. You discover that each row is the record of a payables invoice, and that these records form groups in each of which the supplier name, invoice date, and invoice amount are the same, and the invoice numbers are 70 percent similar.

Look for columns with headings that include the phrases "is the same" and "is xx percent similar" (in which xx is a number). These are the attributes that the algorithm uses to gather transactions into groups. The last of these performs the final step in defining groups; in this example, it's a column titled "Payables Invoice Number is 70 Percent Similar." You can filter on each distinct value in this column; in each case, the worksheet displays transactions that belong to one of the groups. An alternative might be to sort the worksheet on the Supplier.Supplier Name column so that you can easily compare the records for each supplier.



	A	B	C	D	E	I	O	P	Q
1	30001: Duplicate Payables Invoices								
2									
3	Model Description	Identify payables invoices for a specified time where the supplier, invoice date, and invoice amount are the same, and invoice amounts are similar							
4	Last Run Date	1/22/24, 7:18:52 PM							
5									
6	Supplier.Supplier Name	Payables Invoice.Amount	Payables Invoice.Date	Payables Invoice.Invoice Currency	Payables Invoice.Number	Payables Invoice.Invoice Payment Status	Payables Invoice Amount is the same	Payables Invoice Number is 70 percent similar	Number of Occurrences
7	Advantage Corp	60000.00	1/18/24 12:00 AM	USD	QtyHold17.Jan.2024 18:36	Y	60000:USD:20240118:11	qtyhold18jan20240245	1
8	Advantage Corp	60000.00	1/18/24 12:00 AM	USD	QtyHold18.Jan.2024 02:45	N	60000:USD:20240118:11	qtyhold18jan20240245	1
9	Advanced Network Devices	3800.00	1/18/24 12:00 AM	USD	AWTPayTime18.Jan.2024 03:28	N	3800:USD:20240118:21	awtpaytime18jan20241046	1
10	Advanced Network Devices	3800.00	1/18/24 12:00 AM	USD	AWTPayTime18.Jan.2024 10:46	N	3800:USD:20240118:21	awtpaytime18jan20241046	1

You may then cross-reference records in the group with payables records to determine whether any of the invoice records truly are duplicate, and if so, which. Finally, a Payables Invoice.Invoice Payment Status Indicator column indicates whether payment has been made for each record. You can cancel duplicates for which payments haven't been made. You would repeat this process for each distinct value in the column on which you're filtering.