One Identity Manager 8.1.1

Risk Assessment Administration Guide

One Identity Manager Risk Assessment Administration Guide
Updated - August 2019
Version - 8.1.1

Contents

Risk assessment **5**
One Identity Manager user for configuring risk assessment 5
Defining risk index functions 7
Calculating risk index functions 9
Default risk index functions 11
Risk index for user accounts 12
Risk index for system roles 14
Risk index for hierarchical roles and IT Shop structures 14
Risk index for compliance rules and rule violations 15
Risk index for employees 17
Defining risk index functions 18
General master data for a risk index function 19
Extended master data for a risk index function 20
Additional tasks for risk index functions 21
Disabling risk index functions 22
Starting a calculation 23
Weighting and normalization 24
Mitigating controls **27**
Mitigating controls define 27
master data for a mitigating control 28
Additional tasks for a mitigating control 29
Mitigating controls overview 29
Assigning compliance rules 29
Assigning attestation policies 30
Assigning company policies 30
SAPAssigning function definitions 31
Calculating mitigation 31
Appendix: Example of a risk index calculation **33**
About us **39**
Contacting us 39

Technical support resources 39

Index **40**

1

Risk assessment

Everyone with IT system authorization in a company represents a security risk for that company. For example, an employee with permission to edit financial data in SAP carries a higher risk than an employee with permission to edit their own personal data. To quantify the risk, you can enter a risk value for every company resource in One Identity Manager. A risk index is calculated from this value for every employee who is assigned this company resource, directly or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, applications and resources. In this way, all employees representing a particular risk to the company can be found.

Rules in the context of Identity Audit can also be given a risk index. Each rule violation can increase the security risk. Therefore, these risk indexes are also included in the employee's risk calculation. You can define appropriate countermeasures through mitigating controls, and store them with the compliance rules.

Other factors can influence the calculation of employee risk indexes. These include: the type of resource assignment (approved request in the IT Shop or direct assignment), attestations, exception approvals for rule violations, employee responsibilities, and defined weightings. Furthermore, the risk index can be calculated for all business roles, organizations, and system roles that have company resources assigned to them. The user account risk index is calculated based on the system entitlements assigned.

One Identity Manager provides default functions for the risk index calculations described in the following. These are available if the respective module is installed. You can also can set up custom functions.

To use risk assessment functionality

- Set "QER\CalculateRiskIndex" in Designer and compile the database.

One Identity Manager user for configuring risk assessment

The following users are connected with specifying risk indexes and editing risk index functions.

Table 1: User

User	Task
Employee responsible for individual company resources	The users are defined using different application roles for administrators and managers. Users with these application roles: • Specify company resource risk indexes for which you are responsible.
Compliance rules administrators	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Administrators**. Users with this application role: • Specify the risk indexes for compliance rules. • Specify mitigating controls. • Create and edit functions.
Administrators for attestation cases	Administrators are assigned to **Identity & Access Governance | Attestation | Administrators**. Users with this application role: • Specify risk indexes for attestation policies. • Specify mitigating controls. • Create and edit functions.
Company policy administrators	Administrators must be assigned to the application role **Identity & Access Governance | Company policies | Administrators**. Users with this application role: • Specify risk indexes for company policies. • Specify mitigating controls. • Create and edit functions.
Employee administrators	Administrators must be assigned to **Identity Management | Employees | Administrators**. Users with this application role: • Create and edit functions.
One Identity Manager administrators	• Create customized permissions groups for application roles for role-based login to administration tools in Designer as required. • Create system users and permissions groups for non-role-based login to administration tools in Designer as

User	Task
	required. • Enable or disable additional configuration parameters in Designer as required. • Create custom processes in Designer as required. • Create and configures schedules as required. • Create and configure password policies as required.

Defining risk index functions

A risk index can be entered in One Identity Manager for the following objects types.

NOTE: Object types are defined in the One Identity Manager modules and are not available until the modules are installed.

Table 2: Risk index for objects in the One Identity Manager

Object type	Application	Available in Module
Active Directory groups		Active Directory Module
SAP groups, SAP roles, SAP profiles,		SAP R/3 User Management Module
Structural profiles		SAP R/3 Structural Profiles Add-on Module
BI analysis authorizations	Risk for the company if target system entitlements are granted.	SAP R/3 Analysis Authorizations Add-on Module
LDAP groups		LDAP Module
IBM Notes groups		IBM Notes Module
SharePoint groups, SharePoint roles		SharePoint Module
E-Business Suite permissions		Oracle E-Business Suite Module

Object type	Application	Available in Module
Azure Active Directory groups		Azure Active Directory Module
G Suite groups		G Suite Module
G Suite products and SKUs		G Suite Module
UNIX groups		Unix Based Target Systems Module
Cloud Groups		Cloud Systems Management Module
PAM user groups		Privileged Account Governance Module
System entitlements in the Unified Namespace		Target System Base Module
Applications	Risk for the company if the account definition, application or resource is assigned to an employee.	Application Management Module
Resources		always
Account definitions		Target System Base Module
Multi-request resources	Risk for the company if the resource is assigned to an IT Shop structure.	always
Multi-requestable/un-subscribable resources		always
Assignment resources		always
Application roles	Risk for the company if an employee is a member of this application role.	always
Compliance rules	Risk for the company if a rule is violated.	Compliance Rules Module
SAP functions	Risk for the company if SAP user accounts match the SAP function.	SAP R/3 Compliance Add-on Module
Company policies	Risk for the company if a company policy is violated.	Company Policies Module
Attestation policies	Risk for the company if an attestation procedure denies approval for an	Attestation Module

Object type	Application	Available in Module
	attestation policy.	
Subscribable reports	Risk for the company if an employee has subscribed to a report.	Report Subscription Module

To enter a risk index

1. Open the master data form for the object for which you want to enter the risk index.
2. Enter the desired value in **Risk index**.

   The risk index is specified as a floating point number in the range 0.0 ... ... 1.0. This means:

   - 0.0: no risk
   - 1.0: problem; risk involved

Calculating risk index functions

One Identity Manager calculates the resulting risk indexes for employees, user accounts, and hierarchical roles based on the risk indexes already stored. All direct and indirectly assigned objects are taken into account.

The risk index is calculated for the following object types.

Table 3: Object types with a calculated risk index

Object type	Calculation	Available in Module
Employees	Calculated from the risk indexes of all associated user accounts, directly, and indirectly assigned applications, resources, account definitions, and subscribable reports, membership in application roles, and rule violations.	always
Active Directory user accounts	Calculated from the risk indexes of all assigned target system entitlements.	Active Directory Module
SAP user accounts		SAP R/3 User Management Module
BI user accounts		SAP R/3 Analysis Authorizations

Object type	Calculation	Available in Module
		Add-on Module
LDAP user accounts		LDAP Module
IBM Notes user accounts		IBM Notes Module
SharePoint user accounts		SharePoint Module
E-Business Suite user accounts		Oracle E-Business Suite Module
Azure Active Directory user accounts		Azure Active Directory Module
G Suite user accounts		G Suite Module
UNIX user accounts		Unix Based Target Systems Module
Cloud User Accounts		Cloud Systems Management Module
PAM User accounts		Privileged Account Governance Module
User accounts		Target System Base Module
Departments, locations, cost centers	Calculated from the risk indexes of all assigned company resources.	always
Business roles		Business Roles Module
System roles		System Roles

Object type	Calculation	Available in Module
		Module
IT Shop structures		always
Rule violations	Determined by the risk index of the violated rule and the assigned mitigating control.	Compliance Rules Module

NOTE: If you work with the Data Governance Edition, you can also specify and calculate risk indexes for data under governance. These are included in the employee's risk index calculation. For more information, see the Data Governance User Guide.

One Identity Manager supplies default functions for the risk indexes with risk functions defined for the objects types listed here. Certain properties of default functions can be edited in One Identity Manager. Furthermore, you can make custom functions.

Related topics

- Default risk index functions on page 11
- Defining risk index functions on page 18

Default risk index functions

The One Identity Manager supplies a comprehensive collection of default functions. These are necessary for calculating the risk index of all company resources assigned. These functions can be selected in **Risk index functions** under **Assignment**.

Additional factors, like the type of assignment or attestation, influence how the risk index is calculated. There is separate function stored for each factor additionally affecting a calculated risk index. These functions can be selected in **Risk index functions** under **Properties**.

The following object type risk indexes are determined to calculate the risk index of employees:

- User accounts

  Risk index (calculated) of all user accounts connected to an employee
- Company resources

  Risk index (calculated) of all company resources assigned (for example, applications, resources, subscribable reports)
- Rule violations

  Risk index of violated rule taking mitigating controls into accounts

- Application roles

  Risk index of all application roles in which the employee is member

Risk index calculation for the different object types is described in more detail in the following sections.

NOTE: The default functions allow a complete risk assessment for all objects in One Identity Manager. The mode of calculation, weighting and change values must be adjusted to suit you company's requirements.

Before running a risk assessment

- Check all default functions for relevance to your data situation.
- Disable all unnecessary functions.
- Modify the calculation type, weighting, and change value to meet your requirements.
- Define custom functions if required.

Detailed information about this topic

- Risk index for user accounts on page 12
- Risk index for system roles on page 14
- Risk index for hierarchical roles and IT Shop structures on page 14
- Risk index for employees on page 17
- Risk index for compliance rules and rule violations on page 15

Related topics

- Disabling risk index functions on page 22
- General master data for a risk index function on page 19
- Weighting and normalization on page 24
- Defining risk index functions on page 18

Risk index for user accounts

Installed modules:	Target System Base Module
	Active Directory Module
	Azure Active Directory Module
	Oracle E-Business Suite Module
	LDAP Module
	IBM Notes Module
	SAP R/3 User Management Module

SAP R/3 Analysis Authorizations Add-on Module

SharePoint Module

G Suite Module

Cloud Systems Management Module

Unix Based Target Systems Module

Privileged Account Governance Module

Attestation Module

First, the risk indexes of all system entitlements assigned to the user accounts are found in order to calculate user account risk indexes. There are functions stored for the assignments tables to do this (for example "Active Directory user accounts: assignments to groups", "User accounts: assignments to system entitlements"). The risk factor of these assignments depends on other factors. Each of these factors reduces the risk index found.

- Assignment through inheritance (without IT Shop requests)
- Assignment through an approved IT Shop request
- The assignment is attested and approved

One Identity Manager determines the highest value from the assignment risk indexes (calculation type: "Maximum (weighted)") for each user account. There are functions stored for the user account tables to do this (for example: "Active Directory user account", "User accounts"). This value is reduced or increased by other factors.

- The user account is attested and approved
- The user account is not connected to an employee
- The user account is disabled
- The user account is member of too many system entitlements

The risk index of SAP user accounts is calculated from different individual risks.

- Highest risk index of the assigned SAP groups
- Highest risk index of the assigned structural profiles
- Highest risk index (reduced) of the SAP functions matching an SAP user account

The One Identity Manager finds the highest value of these individual risks for each SAP user account. This value is decreased or increased by given factors if the conditions are fulfilled.

The risk index of SharePoint user accounts is calculated from different individual risks.

- Highest risk index of the assigned SharePoint groups
- Highest risk index of the assigned SharePoint roles

The One Identity Manager finds the highest value of these individual risks for each SharePoint user account. This value is decreased or increased by given factors if the conditions are fulfilled.

NOTE: User accounts can obtain a calculated index even if there are no risk indexes stored with the system entitlements. In this case, the risk index is calculated from the additional factors which increase the risk index. The risk index of a user account increases if:

- The user account is not linked to an employee
- The user account is a member of too many system entitlements
- The user account is disabled

Risk index for system roles

Installed modules:	System Roles Module
	Attestation Module

First, the risk indexes of all company resources assigned to the system roles are found in order to calculate system role risk indexes. There are functions stored for the assignments tables to do this ("System roles"). The system role risk index is made up of the risk indexes of the assigned objects. There is a separate function stored for each assignable object type.

One Identity Manager determines the highest value from the assignment risk indexes (calculation type: "Maximum") for each system role. There are functions stored for the "system role" table to do this. This value is reduced or increased by other factors.

- The system role is attested and approved
- The system role is not assigned to a manager

NOTE: Employees can obtain a calculated index even if there are no risk indexes stored with the company resources. In this case, the risk index is calculated from the additional factors which increase the risk index. The risk index of a user account increases if no manager is assigned.

Risk index for hierarchical roles and IT Shop structures

Installed modules:	Business Roles Module (for business role risk indexes)
	Attestation Module

First, the risk indexes of all assigned company resources are established in order to calculate risk indexes for business roles, departments, locations, cost centers, and IT Shop structures. There are functions stored for the assignments tables to do this (for example "Roles and organizations: Subscribable report assignments", "Roles and organizations: E-

Business Suite responsibility assignments"). The risk factor of these assignments depends on other factors. Each of these factors reduces the risk index found.

- Assignment through an approved IT Shop request
- The assignment is attested and approved

The One Identity Manager determines the highest value from the assignment risk indexes (calculation type: "Maximum (weighted)") for each company resource. This value is reduced or increased by other factors.

- The rule or IT Shop structure is attested and approved.
- The role or IT Shop structure is not a assigned a manager (`UID_PersonHead`).

NOTE: Roles and IT Shop structures can obtain a calculated index even if there are no risk indexes stored with the company resources. In this case, the risk index is calculated from the additional factors which increase the risk index. The risk index of a role or IT Shop structure increases if no manager is assigned to the role or IT Shop structure.

Risk index for compliance rules and rule violations

Installed modules:	Compliance Rules Module
	Attestation Module

Table 4: Configuration Parameters for Calculating Risk Indexes of Rule Violations

Configuration parameter	Effect when set
QER\CalculateRiskIndex\MitigatingControlsPerViolation	This configuration parameter controls calculation of risk indexes for rule violations. If the parameter is set, exception approvers can assign mitigating controls to rule violations. The risk index calculation only takes these mitigating controls into account. If the parameter is disabled, risk index calculation take mitigating control assigned to compliance rules into account.

Risk indexes can be applied to compliance rules to evaluate the risk of rule violations. Each rule can be assigned mitigating controls that are implemented the moment the rule is violated. If a rule violation is approved, the rule violation's exception approver can assign a specified mitigating control. Mitigating control reduce the compliance rule's risk index.

Use "QER\CalculateRiskIndex\MitigatingControlsPerViolation" control whether mitigating controls are assigned to rule violations in the case of exception approval. If this configuration parameter is set, only mitigating controls assigned to rule violations are taken into account when calculating risk indexes. The configuration parameters is disabled by default.

The risk index of violated rules is taken into account when employee risk indexes are being calculated.

Table 5: Calculating compliance rule and rule violation risk indexes

Risk Index Function for	Configuration Parameter is	
	Disabled	**Enabled**
Compliance rules (`ComplianceRule.RiskIndexReduced`)	The reduced risk index is calculated from the compliance rule risk index and the significance reductions of all assigned mitigating controls.	The risk index is not reduced. The reduced risk index corresponds, therefore, to the stored compliance rule's risk index.
Violated rules (`BaseTree.RiskIndexCalculated`)	The risk index corresponds to the reduced risk index of the violated rule.	
Employees with rule violations (`PersonInBaseTree.RiskIndexCalculated`)	The risk index corresponds to the calculated risk index of the violated rule.	
Employees with approved rule violations (`PersonInBaseTree.RiskIndexCalculated`)	The risk index is reduced by a fixed amount if the rule violation was granted approval.	
Employees with attested rule violations (`PersonInBaseTree.RiskIndexCalculated`)	The risk index is reduced by a fixed amount if the rule violation was attested and granted approval.	
Employees with approved rule violations and assigned mitigating controls (`PersonInBaseTree.RiskIndexReduced`)	The risk index is not reduced further. Therefore, the reduced risk index corresponds to the risk index of the rule violation (`PersonInBaseTree.`	The reduced risk index is calculated from the risk index of the rule violation (`PersonInBaseTree.RiskIndexCalculated`) and the significance reduction of the mitigating controls assigned on

Risk Index Function for	Configuration Parameter is	
	Disabled	**Enabled**
	RiskIndexCalculated)	exception approval. If no mitigating controls are assigned, the reduced risk index corresponds to the calculated risk index of the rule violation (PersonInBaseTree. RiskIndexCalculated)
Employees (Person. RiskIndexCalculated)	The highest risk index of all the employee's rule violations is established. The calculation takes the reduced risk index of the rule violations in to account (PersonInBaseTree.RiskIndexReduced).	

Risk index for employees

Installed modules: Attestation Module

To calculate employee risk indexes, the risk indexes are found for all assigned company resources. To do this, there are functions stored with the assignment tables to do this (for example, "Resource assignments"). The values also reduced by another factor.

- The assignment is attested and approved

The risk indexes for all employee memberships in application roles and for rule violations are found (table "Employees: membership in roles and organizations"). The membership risk index is reduced by another factor.

- The membership is attested and approved

One Identity Manager determines the highest risk index per object type from assignment, rule violations, and connected user account risk indexes (calculation type: "Maximum (weighted)") for each employee.

An employee risk index results from the highest risk index of the calculated single values. This value is reduced or increased by other factors.

- The employee is attested and approved
- The employee is a manager or other employee
- The employee is disabled and linked to an enabled user account

NOTE: Employees can obtain a calculated index even if there are no risk indexes stored with the company resources. In this case, the risk index is calculated from the additional factors which increase the risk index. The risk index of an employee increases if:

- The employee is a manager or other employee
- The employee is disabled and linked to an enabled user account

TIP:"Business roles and organizations" in the "Employees: memberships in roles and organizations" table finds the risk indexes for all secondary employee memberships in hierarchical roles and IT Shop structures. In the process, the risk indexes are determined for secondary membership in business roles, departments, locations, cost centers, and IT Shop structures. You can use risk indexes from these memberships for custom calculation or evaluation. Implement your own functions or processes to do this.

Defining risk index functions

You can define company specific functions and edit certain properties of the default function.

To edit risk index functions

1. Select **Risk index functions**.
2. In the navigation view, expand the **Risk index functions** node.

   All tables with functions defined in them are shown in the navigation view. These are tables including a `RiskIndexCalculated` column.
3. Select the table whose risk index functions you want to edit and expand the node.

   The **Assignments** and **Properties** filters are displayed.

   All the functions with assignments to the selected table are collected under **Assignments** (for example, Active Directory user account membership in Active Directory groups).

   The **Properties** filter groups together all risk index functions that further increase or decrease the calculated risk indexes.
4. Select a filter.
5. Select the password policy in the result list and select **Change master data** in the task view.

   - OR -

   To create a new risk index function, click in the result list .
6. Fill out the function data.

   You can customize the following properties for default functions:

   - Disabled
   - Calculation type
   - Weighting/change value
   - Calculate immediately
7. Save the changes.

Related topics

- General master data for a risk index function on page 19
- Assigning source tables on page 22
- Disabling risk index functions on page 22

General master data for a risk index function

Enter the following information for a risk index function.

Table 6: Risk index function master data

Property	Description
Name	Name of the function as displayed in the One Identity Manager tools.
Description	Spare text box for additional explanation.
Deactivated	Specifies whether risk index functions are taken into account in the total calculation of risk indexes.
Calculation type	Method with which to calculate the risk index. Permitted values are:

Maximum (weighted)	The highest value from all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.
Maximum (normalized)	The highest value from all relevant risk indexes is calculated, weighted with the normalized weighting factor and taken as basis for the next calculation.
Increment	The risk index of Table column (target) is incremented by a fixed value. This value is specified in **Weighting/Change value**.
Decrement	The risk index of Table column (target) is decremented by a fixed value. This value is specified in **Weighting/Change value**.
Average (weighted)	The average of all relevant risk indexes is calculated, weighted and taken as basis for the next calculation.
Average (normalized)	The average of all relevant risk indexes is calculated with the normalized weighting factor and taken as basis for the next calculation.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>Reduction
Used when calculating the reduced risk index for rules, SAP functions, company policies and attestation policies. You cannot add custom functions with this calculation type!

NOTE: If calculation types for both weighting and normalization are implemented in risk index functions for one and the same target column, the risk index calculation does not determine a reasonable value.
The following applies for all risk index functions of one target column: Only combine functions with the calculation type "Maximum (weighted)" and "Average (weighted)" or the functions with calculation types "Maximum (normalized)" and "Average (normalized)".</td></tr>
<tr><td>Weighting/change value</td><td>The value by which to modify the risk index. There are three possible cases:
<table><tr><th>Calculation type</th><th>Weighting/change value</th></tr><tr><td>Maximum (weighted) and average (weighted)</td><td>Value by which the risk index is weighted in the total calculation.</td></tr><tr><td>Maximum (normalized) and average (normalized)</td><td>Value by which the risk index is weighted in the total calculation. The value for this calculation is normalized to 1 beforehand.</td></tr><tr><td>Increment and decrement</td><td>Value by which the risk index is incremented or decremented in the total calculation.</td></tr></table></td></tr>
</table>

Detailed information about this topic

- Disabling risk index functions on page 22
- Weighting and normalization on page 24

Extended master data for a risk index function

Enter the following information for a risk index function.

Table 7: Extended Master Data for a Function

Property	Description
Table column (target)	Table column to be calculated.
Calculate immediately	Specifies whether the calculation can be immediately run asynchronously triggered through the DBQueue Processor. If this option is set, the risk index is calculated immediately. For more information, see Starting a calculation on page 23.
Query	Query in SQL syntax, which finds the risk index for each object in the target table.

The following columns must be selected through the query:

For the Calculation Type	1. column	2. column
Maximum and average values	XObjectKey of the object to calculate as ObjectKeyTarget	RiskIndex, RiskIndexReduced or RiskIndexCalculated from one of the source tables as SourceValue
Increment and decrement		1.0 as SourceValue

Query example

```
select a.XObjectkey as ObjectKeyTarget, b.RiskIndex as SourceValue from
BaseTreeHasADSGroup a
join ADSGroup b on a.UID_ADSGroup = b.UID_ADSGroup
```

Additional tasks for risk index functions

After you have entered the master data, you can run the following tasks.

Risk index function overview

You can see the most important information about a function on the overview form.

To obtain an overview of a risk index function

1. Select **Risk index functions**.
2. In the navigation view, select **Risk index functions | <Table> | <Filter>**.

3. Select the function in the result list.
4. Select **Function overview**.

Assigning source tables

One Identity Manager Obtains all the necessary information for calculating a risk index from the source tables. Specify tables here that cause the risk index to be recalculated when changes are made to the table's data. Source tables are mainly all tables containing risk indexes.

Once an object is added or deleted in a source table or a risk index is changed, a calculation task for risk index calculation is queued in the DBQueue Processor.

To assign a function to a source table

1. Select **Risk index functions**.
2. In the navigation view, select **Risk index functions | <Table> | <Filter>**.
3. Select the function in the result list.
4. Select **Assign source tables**.
5. Double-click on the icon next to the table you want to assign as source table for risk index calculation in **Add assignments**.

   - OR -

   In **Remove assignments**, remove the tables that are not required.
6. Save the changes.

Related topics

- Starting a calculation on page 23

Disabling risk index functions

One Identity Manager provides default functions for all assignable company resources. Not all functions are required, it depends on your custom configuration of One Identity Manager. In order to exclude irrelevant functions from the risk index calculation, you can disable these functions. This means, the calculation procedures effected are reset.

To disable functions

1. Select the category **Risk Index Functions**.
2. Open **Risk index functions | <table> | <filter>** in navigation view.
3. Select a function in the result list and run **Change master data**.
4. Select the **General** tab.

5. Click **Disabled**.

   If this option is already set, you do not need to do this.
6. Save the changes.

Starting a calculation

The risk index calculation is started by the following events:

- A function was changed.
- Objects in the source table have changed.
- A scheduled calculation task is being executed.

Risk index function was modified

The moment a function changes, a calculation procedure for the effected table column (target) is set up. There is exactly one procedure set up for each table column (target), which bundles all enabled functions for the table column. Then the risk indexes are calculated.

Data change in a source table

Once data in the source tables changes, the risk indexes are recalculated. To do this, a calculation task is queued in the DBQueue Processor. If **Calculate immediately** is set for a function, the risk indexes effected are calculated immediately. In this case, the calculation is not DBQueue Processor controlled.

The following changes to the source tables trigger recalculation

- Objects are added or deleted
- Risk indexes were changed
- Risk indexes were calculated

All other changes do not cause automatic recalculation of risk indexes. You can use a process plan task to calculate risk indexes so that changes made to them can take effect. This is required, for example, in order to take into account approval of attestation cases in calculated risk indexes. Functions that are not assigned to a source table are also only taken into account when scheduled recalculation is run.

Scheduled calculation task is executed for the DBQueue Processor

To ensure that calculated risk indexes are continually update, taking all functions into account, you can configure a scheduled calculation task to calculate risk indexes. One Identity Manager provides the "Calculate risk index" schedule to do this. This schedule is disabled, by default. Enable it to recalculate the risk indexes on a scheduled basis. Adjust the execution times to suit your company’s requirements.

To enable the schedule for calculating risk indexes

1. Open the Designer.
2. Select **Base Data | General | Schedules**.
3. Select "Calculate risk indexes" in the List Editor.
4. Check the box in the **Enabled** column.
5. Save the changes.

Related topics

- Assigning source tables on page 22

Weighting and normalization

You can calculate the risk index for an object type in different ways.

1. Highest risk index of all assigned company resources
2. Average of all assigned company resource risk indexes
3. Highest weighted risk index of all assigned company resources
4. Sum of all normalized to 1 and weighted assigned company resource risk indexes

In the default functions, the risk indexes are calculated by the first method.

NOTE: If calculation types for both weighting and normalization are implemented in risk index functions for one and the same target column, the risk index calculation does not determine a reasonable value.

The following applies for all risk index functions of one target column: Only combine functions with the calculation type "Maximum (weighted)" and "Average (weighted)" or the functions with calculation types "Maximum (normalized)" and "Average (normalized)".

Weighting

In the calculation using method 3, the maximum and average values are determined of the risk index of all assigned company resources of an object type. This value is weighted with the given weighting. The highest weighted risk index is the calculated risk index.

Calculations using methods 1.and 2. arise when the weighting in all relevant functions, is given with the value 1.

To calculate risk indexes using methods 1, 2, or 3

- Select the calculation type "Maximum (weighted)" or "Average (weighted)".

Normalization

In the calculations using method 4, the maximum and average values of the risk index for all assigned company resources of an object type are determined. This value is weighted. The sum of all weighted risk indexes of this object type is the calculated risk index.

The sum of the weightings must be exactly 1 with a calculation, because the range from zero to 1 must be adhered to for the resulting index. That is why, the weightings of all enabled functions for the same target column are normalized to 1. The risk index found is weighted with this normalized value. The normalized weighting is calculated from the weighting divided by the sum of all relevant weighted values. This results in the following formula for calculating the risk index:

$$\Sigma\left(\frac{\text{Risk index function weighting}}{\text{Sum of weightings of all enabled functions for the same target column}} * \text{Risk index}\right)$$

To calculate risk indexes using method 4

- Select the calculation type "Maximum (normalized)" or "Average (normalized)".

The weighting is only relevant if there is more than one function for a target column because the result of normalization is exactly 1. In this case, calculations using method 4 return the same result as calculating with method 1. The difference between weighting and normalization is only relevant if more than one function is enabled for a target column. This is made clear in the following example.

Example

Calculate the risk index for SAP user accounts from risk indexes of assigned SAP groups and structural profiles, and from SAP function risk indexes that match with the user accounts. Three SAP groups (G1, G2, G3) and two structural profiles (P1, P2) are assigned to a user account. The user account matches one SAP function (FS) exactly.

Risk Indexes

- G1 = 0.2
- G2 = 0.3
- G3 = 0.4
- P1 = 0.6
- P2 = 0.7
- SF = 0.5

Calculation type

- By method 1: maximum (weighted), weighting = 1
- By method 3: maximum (weighted)

  SAP group weighting: 0.6

  Structural profile weighting: 0.8

SAP function weighting: 0.7

- By method 4: maximum (normalized)

  SAP group weighting: 0.6

  Structural profile weighting: 0.8

  SAP function weighting: 0.7

Table 8: Risk index calculation results

Calculation	Method 1	Method 3	Method 4
Highest risk index of all assigned SAP groups	0.4	0.4	0.4
Weighting/Normalization	1 * 0.4 = 0.4	0.6 * 0.4 = 0.24	(0.6 / (0.6 + 0.8 + 0.7)) * 0.4 = 0.11428
Highest risk index of all assigned structural profiles	0.7	0.7	0.7
Weighting/Normalization	1 * 0.7 = 0.7	0.8 * 0.7 = 0.56	(0.8 / (0.6 + 0.8 + 0.7)) * 0.7 = 0.26667
Highest risk index of all matching SAP functions	0.5	0.5	0.5
Weighting/Normalization	1 * 0.5 = 0.5	0.7 * 0.5 = 0.35	(0.7 / (0.6 + 0.8 + 0.7)) * 0.5 = 0.16667
Highest weighted value/sum normalized value (= resulting user account risk index)	0.7	0.56	0.54762

2

Mitigating controls

Effective permissions of employees, roles or user accounts are checked in the context of Identity Audit on the basis of regulatory requirements. Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to compliance rules, SAP functions, attestation policies and company policies. These risk indexes provide information about the risk involved for the company if this particular rule, SAP function or policy is violated. Once the risks have been identified and evaluated, mitigating controls can be implemented.

Mitigating controls are independent on One Identity Manager's functionality. They are not monitored through One Identity Manager.

An example of a mitigating control is the assignment of system entitlements only through authorized requests in the IT Shop. If system entitlements are issued to the employee through the IT Shop, a rule check can be integrated into the request's approval procedure. System entitlements that would lead to a rule violation are therefore assigned not at all or only after gaining exception approval. The risk that rules are violated is thus reduced.

Mitigating controls define

Mitigating controls can be defined in One Identity Manager functions.

Table 9: Object types with mitigating controls

Function	Object type	Application	Available in Module
Compliance	Compliance rules	Reduces the risk connection with violating rules.	Compliance Rules Module
	Rule violations	Reduces the risk connected with the exception approval of a concrete rule violation.	
	SAP functions	Reduces the risk of SAP user accounts matching SAP functions.	SAP R/3 Compliance Add-on

Function	Object type	Application	Available in Module
			Module
Attestation	Attestation policies	Reduces the risk connected with denied attestation cases.	Attestation Module
	Attestation Cases	Reduces the risk connected with the denial of a concrete attestation case.	
Company policies	Company policies	Reduces the risk connection with violating policies.	Company Policies Module
	Policy Violations	Reduces the risk connected with the exception approval of a concrete policy violation.	

To edit mitigating controls

- In Designer, set the configuration parameter **QER | CalculateRiskIndex** and compile the database.

Use Manager to assign mitigating controls to compliance rules, SAP functions or company policies. For more information, see Additional tasks for a mitigating control on page 29.

You can assign mitigating controls directly to a specific rule violation when editing exception approval for rule violations in the Web Portal. You can assign mitigating controls direct to a specific attestation case during attestation in the Web Portal. You can assign mitigating controls directly to a specific rule violation when editing exception approval for policy violations in the Web Portal. For more information, see the One Identity Manager Web Portal User Guide.

master data for a mitigating control

To edit mitigating controls

1. In Manager, select **Risk index functions | Mitigating controls**.
2. Select a mitigating control in the result list and run **Change master data**.

   - OR -

   Click in the result list.
3. Edit the mitigating control master data.
4. Save the changes.

Enter the following master data for mitigating controls.

Table 10: General master data for a mitigating control

Property	Description
Measure	Unique identifier for the mitigating control.
Significance reduction	When the mitigating control is implemented, this value is used to reduce the risk of denied attestation cases. Enter a number between 0 and 1.
Description	Detailed description of the mitigating control.
Functional area	Functional area in which the mitigating control may be applied.
Department	Department in which the mitigating control may be applied.

Additional tasks for a mitigating control

After you have entered the master data, you can run the following tasks.

Mitigating controls overview

You can see the most important information about a mitigating control on the overview form.

To obtain an overview of a mitigating control

1. In Manager, select **Risk index functions | Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select **Mitigating control overview**.

Assigning compliance rules

Installed modules: Compliance Rules Module

Use this task to specify for which compliance rules a mitigating control is valid. You can only assign original rules on the assignment form.

To assign compliance rules to mitigating controls

1. Select **Risk index functions | Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select **Assign rules**.

4. In **Add assignments**, double-click the rules you want to assign.

   - OR -

   In **Remove assignments**, double-click the rules whose assignment is to be deleted.
5. Save the changes.

Assigning attestation policies

Installed modules: Attestation Module

Use this task to specify for which attestation policies the mitigating control is valid.

To assign attestation policies to mitigating controls

1. In Manager, select **Risk index functions | Mitigating control**.
2. Select the mitigating control in the result list.
3. Select **Assign attestation polices** in the task view.

   Assign the attestation policies in **Add assignments**.

   TIP: In **Remove assignments**, you can remove the assignment of attestation policies.

   To remove an assignment

   - Select the approval policy and double-click .
4. Save the changes.

Assigning company policies

Installed modules: Company Policies Module

Use this task to specify for which company policies the mitigating control is valid. You can only assign company policy working copies on the assignment form.

To assign company policies to mitigating controls

1. Select **Risk index functions** | **Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select **Assign company policies**.
4. In **Add assignments**, double-click the company policies you want to assign.

   - OR -

   In **Remove assignments**, double-click the company policies whose assignment is to be deleted.

5. Save the changes.

SAPAssigning function definitions

Installed modules: SAP R/3 Compliance Add-on Module

Use this task to specify the function definitions for which a mitigating control is valid. You can only assign function definitions that are enabled on the assignment form.

To assign SAP function definitions to mitigating controls

1. Select **Risk index functions | Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select **Assign function definitions**.
4. In **Add assignments**, double-click the function definitions you want to assign.

   - OR -

   In **Remove assignments**, double-click the function definitions whose assignment is to be deleted.
5. Save the changes.

Calculating mitigation

Table 11: Configuration Parameters for Calculating Risk Indexes of Rule Violations

Configuration parameter	Effect when set
QER\CalculateRiskIndex\MitigatingControlsPerViolation	This configuration parameter controls calculation of risk indexes for rule violations. If the parameter is set, exception approvers can assign mitigating controls to rule violations. The risk index calculation only takes these mitigating controls into account. If the parameter is disabled, risk index calculation take mitigating control assigned to compliance rules into account.

The significance reduction of a mitigating control supplies the value by which the risk index of a compliance rule, SAP function, attestation policy or company policy is reduced when

the control is implemented. One Identity Manager calculates a reduced risk index based on the risk index and the significance reduction. One Identity Manager supplies default functions for calculating reduced risk indexes. These functions cannot be edited with One Identity Manager tools.

The reduced risk index is calculated from the SAP function, attestation policy or company policy and the significance reduced sum of all assigned mitigating controls.

Calculating mitigation for rule violations depends on the configuration parameter "QER\CalculateRiskIndex\MitigatingControlsPerViolation".

Table 12: Effect of the Configuration Parameter "QER\CalculateRiskIndex\MitigatingControlsPerViolation" on Calculating Mitigation

Configuration parameter	Effect
Deactivated	The compliance rule's reduced risk index is calculated. This takes mitigating controls into account that are assigned to a compliance rule.
Enabled	The compliance rule's risk index is not reduced. The reduced risk index corresponds, therefore, to the compliance rule's risk index. The reduced risk index of employees with rule violations is calculated. This takes mitigating controls into account that were assigned to a rule violation during exception approval.

```
Risk index (reduced) = Risk index - sum significance reductions
```

If the significance reduction sum is greater than the risk index, the reduced risk index is set to **0**.

Related topics

- Risk index for compliance rules and rule violations on page 15

Appendix: Example of a risk index calculation

Risk index calculation is explained here using an employee with SAP system authorizations and assigned applications. The employee is a manager.

Clara Harris is:

- External employee
- Primary membership in the department "Personal"
- Customer in IT Shop "Software"

The department "Personnel" is assigned

- An account definition "KRSAP" for the SAP client "SAPClient"
- An SAP group "SAPG1"

The following also applies

- Clara Harris has requested three applications through the IT Shop. The requests were approved; the applications assigned.
- The user account "CLARAH" (SAP R/3) was created through an account definition.
- The user account "CLARAH" is a direct member of the SAP group "SAPG2".
- The user account "CLARAH" is assigned directly to the structural profile "SAPSP".
- Clara Harris is team lead of a work group and therefore manager of 10 staff members.
- Employee are attested regularly.

The following risk indexes are calculated for the company resources:

Company Resource	Risk index
KRSAP	0.0
SAPG1	0.7

Company Resource	Risk index
SAPG2	0.2
SAPSP	0.5
Application 1	0.1
Application 2	0.2
Application 3	0.3

One Identity Manager calculates the risk indexes for the following object types using the default functions:

Table	From the Object's Risk Indexes
Employees	All assigned objects
Application assignments	Applications
Account definition assignments	Account definitions
SAP user accounts	SAP groups, structural profiles
Roles and organizations	Applications (for the product nodes of the three applications) SAP groups (for department R) Account definitions (for the department R)

The calculation type is "Maximum (weighted)". The weighting is "1".

Calculation Sequence

1. Determine risk indexes of the table "SAP user accounts: group assignments".

   The table contains two entries for user account CLARAH. The risk indexes correspond to the risk indexes of the assigned SAP groups SAPG1 and SAPG2. The risk index of this SAP group is reduced because the SAP group SAPG1 is assigned through inheritance.
2. Determine risk indexes of the table "SAP user accounts: assignments to structural profiles".

   The table contains one entry for the user account CLARAH. The risk index corresponds to the risk index of the assigned structural profile SAPSP.
3. Calculate the risk index of the table "SAP user accounts ".

   The table contains one entry for the user account CLARAH. The risk index is calculated from the risk indexes determined in steps 1 and 2.

4. Find the risk index for the table "Application assignments".

   The table contain three entries for Clara Harris for the three assigned applications. The risk indexes correspond to the application risk indexes.

5. Find the risk index of the table "Account definitions assignments".

   The table contains one entry for Ines Franz. The risk indexes corresponds to the risk index of the assigned account definition KRSAP.

6. Calculate the risk index of the table "Employees".

   The table contains an entry for Clara Harris. The risk index is calculated from the risk indexes found in steps 3, 4, and 5. The calculated risk index is increased because Clara Harris is the manager of other employees. The calculated risk index is reduced because the last attestation case for Clara Harris was approved.

Table 13: Risk index calculation results

#	Object	Determined risk index	+/-	Resulting risk index	Comment
1	CLARAH: SAPG1	0.7	-0.05	0.65	Decrement because inherited by
	CLARAH: SAPG2	0.2		0.2	Directly assigned
2	CLARAH: SAPSP	0.5		0.5	Directly assigned
3	CLARAH	0.65		0.65	Maximum value from step 1 and 2
		0.5			
4	Clara Harris: Application 1	0.1		0.1	
	Clara Harris: Application 2	0.2		0.2	
	Clara Harris: Application 3	0.3		0.3	
5	Clara Harris: KRSAP	0.0		0.0	

#	Object	Determined risk index	+/-	Resulting risk index	Comment
6	Clara Harris	0.65		0.65	Maximum value from step 3, 4, and 5
		0.3			
		0.0			
			+0.2	0.85	Increment because Clara Harris manages other employees
			-0.33	0.52	Decrement because the attestation is approved

Key: # – step, +/- – increment/decrement

7. Determine the risk index of the table "Roles and organizations: application assignments".

   This table contains one entry for each requested application. The risk indexes correspond to the application risk indexes.

8. Calculate the risk index of the table "Roles and organizations".

   This table contains one entry for each product node of the three applications. The risk indexes are calculated from the risk indexes found in step 4.

9. Find risk index or the table "Roles and organizations: account definition assignments".

   This table contains one entry for the department "Personnel". The risk indexes corresponds to the risk index of the assigned account definition KRSAP.

10. Determine the risk index of the table "Roles and organizations: SAP groups assignments".

    This table contains one entry for the department "Personnel". The risk index corresponds to the risk index of the assigned SAP group SAPG1.

11. Calculate the risk index of the table "Roles and organizations".

    This table contains one entry for the department "Personnel". The risk index is calculated from the risk indexes determined in steps 9 and 10. The calculated risk index is increased because the department does not have a manager.

12. Determine the risk index of the table "Employees: memberships in roles and organizations".

    The table contain three entries for Clara Harris because she is member of three product nodes. The risk indexes are taken from those calculated in step 8. The table does not contain any entries for the department R because Clara Harris is not a secondary member of this department.

Table 14: Risk index calculation results

#	Object	Determined risk index	+/-	Resulting risk index	Comment
7	Product node 1: Application 1	0.1		0.1	
	Product node 2: Application 2	0.2		0.2	
	Product node 3: Application 3	0.3		0.3	
8	Product node 1	0.1		0.1	
	Product node 2	0.2		0.2	
	Product node 3	0.3		0.3	
9	Personnel: KRSAP	0.0		0.0	
10	Personnel: SAPG1	0.5		0.5	
11	Personnel	0.0		0.5	Maximum value from step 9 and 10
		0.5			
		0.5	+0.05	0.55	Increment because the department has no manager
12	Clara Harris: Product node 1	0.1		0.1	
	Clara Harris: Product	0.2		0.2	

#	Object	Determined risk index	+/-	Resulting risk index	Comment
	node 2				
	Clara Harris: Product node 3	0.3		0.3	

Key: # – step, +/- – increment/decrement

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

A

application role
- administrators 5
- Identity and Access Governance
  - attestation
    - administrators 5
  - company policies
    - administrators 5
  - Identity Audit
    - administrators 5
- Identity Management
  - employees
    - administrators 5

M

mitigating control 27
- assign attestation policy 30
- assign company policy 30
- assign compliance rule 29
- assign SAP function 31
- assigned object types 27
- attestation policy 27
- company policy 27
- compliance rule 27
- enter 28
- overview 29
- SAP function 27
- significance reduction 28

R

risik index
- risk index function
  - target column 20

risk assessment 5
- administrators 5
- user 5

risk index 5
- average 19-20, 24
- calculate 11, 23-24, 31
  - example 33
  - exclude object types 22
- calculate immediately 20
- calculation procedure 23
- calculation type 19
- change amount 19
- decrement 11, 19-20
- enter 7
- increment 11, 19-20
- maximum 19-20, 24
- object types with calculated risk index 9
- object types with risk index 7
- reduced
  - calculate 31
- reduction 19
- risk index function
  - assign source table 22
  - default risk index function 11
  - define 18

disable 19, 22
for employees 17
for roles 14
for system roles 14
for user accounts 12
overview 21
table column (target) 20
start calculation
after data change 23
scheduled 23
weighting 19, 24

S

significance reduction 28