



One Identity Manager 9.3

Risk Assessment Administration Guide

Copyright 2025 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Risk Assessment Administration Guide
Updated - 06 January 2025, 10:22

For the most recent documents and product information, see [Online product documentation](#).

Contents

Risk assessment	5
One Identity Manager users for configuring risk assessment	6
Defining risk index functions	7
Calculating risk index functions	8
Default risk index functions	9
Risk index for user accounts	11
Risk index for system roles	12
Risk index for hierarchical roles and IT Shop structures	12
Risk index for compliance rules and rule violations	13
Risk index for identities	14
Defining risk index functions	15
General main data of risk index functions	16
Extended main data of risk index functions	18
Displaying the risk index function overview	19
Assigning source tables for risk index functions	19
Disabling risk index functions	20
Starting risk index calculations	20
Weighting and normalization	21
Mitigating controls	25
Defining mitigating controls	25
Creating and editing mitigating controls	27
Assigning mitigating controls to compliance rules	27
Assigning mitigating controls to attestation policies	28
Assigning mitigating controls to company policies	28
Assigning mitigating controls to SAP function definitions	29
Displaying mitigating controls overview	29
Calculating mitigation	30
Appendix: Risk index calculation example	31
About us	36
Contacting us	36

Technical support resources	36
Index	37

Risk assessment

Everyone with IT system authorization in a company represents a security risk for that company. For example, an identity with permission to edit financial data in SAP carries a higher risk than an identity with permission to edit their own main 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 identity that has this company resource assigned to it directly or indirectly. Company resources include target system entitlements (for example, Active Directory groups or SAP profiles), system roles, subscribable reports, software, and resources. In this way, all the people that represent 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 identity'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 identities' risk indexes. These include: the type of resource assignment (approved request in the IT Shop or direct assignment), attestations, exception approvals for rule violations, identity 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 modules are installed. You can also set up custom functions.

To use risk assessment functionality

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

If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

One Identity Manager users for configuring risk assessment

The following users are used for specifying risk indexes and editing risk index functions.

Table 1: Users

User	Tasks
Responsible for individual company resources	<p>The users are defined using different application roles for administrators and managers.</p> <p>Users with these application roles:</p> <ul style="list-style-type: none">• Specify company resource risk indexes for which you are responsible.
Compliance rules administrators	<p>Administrators must be assigned to the Identity & Access Governance Identity Audit Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Specify the risk indexes for compliance rules.• Specify mitigating controls.• Create and edit functions.
Administrators for attestation cases	<p>Administrators are assigned to the Identity & Access Governance Attestation Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Specify risk indexes for attestation policies.• Specify mitigating controls.• Create and edit functions.
Company policy administrators	<p>Administrators must be assigned to the Identity & Access Governance Company policies Administrators application role.</p> <p>Users with this application role:</p> <ul style="list-style-type: none">• Specify risk indexes for company policies.• Specify mitigating controls.• Create and edit functions.
Identity administrators	<p>Administrators must be assigned to the Identity Management Identities Administrators application role.</p> <p>Users with this application role:</p>

User	Tasks
	<ul style="list-style-type: none"> • Create and edit functions.
One Identity Manager administrators	<p>One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.</p> <p>One Identity Manager administrators:</p> <ul style="list-style-type: none"> • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required.

Defining risk index functions

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

The risk index can be entered for the following object types.

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

Object type	Application	Available in module
Target system entitlements, such as Active Directory groups or Google Workspace products and SKUs	Risk to the organization if the target system entitlement is assigned to a user account.	In the respective target system module
Software	Risk for the company if the account definition, software, or resource is assigned to an identity.	Software Management Module
Resources		always
Account definitions		Target System Base Module

Object type	Application	Available in module
Multi-request resources		always
Multi requestable/unsubscribable resources	Risk for the company if the resource is assigned to an IT Shop structure.	always
Assignment resources		always
Application roles	Risk for the company if an identity 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 policy.	Attestation Module
Subscribable reports	Risk for the company if an identity has subscribed to a report.	Report Subscription Module

To enter a risk index

1. In the Manager, open the object's main data form to enter a risk index.
2. Enter the desired value in the **Risk index** field.

The risk index must be given as a floating point number in the range **0.0...1.0**. This means:

- **0,0**: There is no risk
- **1,0**: There is an issue. A risk has been identified.

Calculating risk index functions

Based on the risk index history, resulting risk indexes are calculated for identities, user accounts, and hierarchical roles. 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
Identities	Calculated from the risk indexes of all associated user accounts, directly, and indirectly assigned software applications, resources, account definitions, and subscribable reports, membership in application roles, and rule violations.	always
User accounts, such as Active Directory user accounts or Google Workspace user accounts	Calculated from the risk indexes of all assigned target system entitlements.	In the respective target system module
Departments, locations, cost centers		always
Business roles	Calculated from the risk indexes of all assigned company resources.	Business Roles Module
System roles		System Roles Module
IT Shop structures		always
Rule violations	Determined by the risk index of the violated rule and the assigned mitigating control.	Compliance Rules Module

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 9
- [Defining risk index functions](#) on page 15

Default risk index functions

One Identity Manager provides a comprehensive collection of default risk index functions. These are used for calculating the risk index of all company resources assigned. These functions can be selected in the Manager in the **Risk Index Functions** category under **Assignments** filter.

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 the Manager in the **Risk index functions** category under the **Properties** filter.

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

- User accounts: Risk index (calculated) of all user accounts that are linked to an identity
- Company resources: Risk index (calculated) of all assigned company resources (such as, software, resources, subscribed reports)
- Rule violations: Risk index of violated rules taking into account mitigating controls
- Application roles: Risk index of all application roles with an identity as a member

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

NOTE: The default functions can be used to perform a risk assessment for most objects in One Identity Manager. This largely covers the standard requirements on this topic. The mode of calculation, weighting, and change values must be adjusted to suit your company's requirements.

Before running a risk assessment

- Check all default functions for relevance to your data situation.
- Disable all unnecessary functions.
- Adjust the calculation type, weighting, and change value in the enabled functions to suit your company.
- Define additional functions if required.

Detailed information about this topic

- [Risk index for user accounts](#) on page 11
- [Risk index for system roles](#) on page 12
- [Risk index for hierarchical roles and IT Shop structures](#) on page 12
- [Risk index for identities](#) on page 14
- [Risk index for compliance rules and rule violations](#) on page 13

Related topics

- [Disabling risk index functions](#) on page 20
- [General main data of risk index functions](#) on page 16
- [Weighting and normalization](#) on page 21
- [Defining risk index functions](#) on page 15

Risk index for user accounts

NOTE: This function is only available if the Target System Base Module and the target system module are installed.

First, the risk indexes of all system entitlements assigned to the user accounts are found in order to calculate user account risk indexes. To do this, functions are stored for the assignment tables, such as the **Active Directory user accounts: assignments to groups** or the **User accounts: assignments to system entitlements** table.

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

The highest value is determined from the risk indexes of these assignments for each user account (calculation type: **Maximum (weighted)**). To do this, functions are stored for the user account tables, such as the **Active Directory user accounts** or the **user accounts** table.

This value is reduced or increased by other factors.

- The user account is attested and approved
- The user account is not connected to an identity
- 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 highest value is determined for each SAP user account from these separate risks. 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 highest value is determined for each SharePoint user account from these separate risks. 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 identity
- The user account is a member of too many system entitlements
- The user account is disabled

Risk index for system roles

NOTE: This function is only available if the System Roles Module and the Attestation Module are installed.

First, the risk indexes of all company resources assigned to the system roles are found in order to calculate system role risk indexes. To do this, risk index functions are stored for the **System roles: assignments** table. 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.

The highest value is determined from the risk indexes of these assignments for each system role (calculation type: **Maximum (weighted)**). A function for the **System roles** table is stored for this purpose. 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: System roles can be given 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

NOTE: This function is only available if the Business Roles Module (for business role risk index) and the Attestation Module are installed.

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. To do this, functions are stored for the assignment tables, such as the **Roles and organizations: Roles and organizations: subscribable report assignments** or the **Roles and organizations: E-Business Suite entitlement assignments** table.

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 highest value is determined from the risk indexes of these assignments for each company resource (calculation type: **Maximum (weighted)**). 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 assigned a manager (UID_PersonHead).

NOTE: Roles and IT Shop structures can be given 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

NOTE: This function is only available if the Compliance Rules Module and the Attestation Module are installed.

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.

Using the **QER | CalculateRiskIndex | MitigatingControlsPerViolation** configuration parameter, you can control whether mitigating controls are assigned if an exception is granted to rule violations. 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 identity risk indexes are being calculated.

Table 4: Calculating compliance rule and rule violation risk indexes

Risk Index Function for	Configuration Parameter is	
	Not set	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.	
Identities with rule	The risk index corresponds to the calculated risk index of the	

Risk Index Function for	Configuration Parameter is	
	Not set	Enabled
violations (PersonInBaseTree. RiskIndexCalculated)	violated rule.	
Identities with approved rule violations (PersonInBaseTree. RiskIndexCalculated)	The risk index is reduced by a fixed amount if the rule violation was granted approval.	
Identities with attested rule violations (PersonInBaseTree. RiskIndexCalculated)	The risk index is reduced by a fixed amount if the rule violation was attested and granted approval.	
Identities 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. RiskIndexCalculated).	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 exception approval. If no mitigating controls are assigned, the reduced risk index corresponds to the calculated risk index of the rule violation (PersonInBaseTree. RiskIndexCalculated).
Identities (Person. RiskIndexCalculated)	The highest risk index of all the identity's rule violations is established. The calculation takes the reduced risk index of the rule violations in to account (PersonInBaseTree.RiskIndexReduced).	

Risk index for identities

NOTE: This function is only available if the Attestation Module is installed.

To calculate identity risk indexes, the risk indexes are found for all assigned company resources. To do this, functions are stored for the assignment tables, such as the **Resource assignments** table. The values also reduced by another factor.

- The assignment is attested and approved

In addition, the risk indexes of all identities in application roles and of rule violations are calculated (table **Identities: memberships in roles and organizations**). The membership risk index is reduced by another factor.

- The membership is attested and approved

The highest risk index is determined for each identity from the risk indexes of assignments, memberships, rule violations, and connected user accounts (calculation type: **Maximum (weighted)**).

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

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

NOTE: Identities 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 identity increases if:

- The identity is a manager or other identity
- The identity is deactivated but linked to enabled user accounts.


TIP: The default risk index functions **Business Roles and Organizations** on the **Identities: memberships in roles and organizations** table determines the risk indexes of all secondary memberships of identities 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 custom functions and edit certain properties of the default function.

To edit or create the functions for risk indexes

1. In the Manager, select the **Risk Index Functions** category.
2. In the navigation view, expand the **Risk index functions** node.
This shows all the tables with functions defined in them. These are tables with a RiskIndexCalculated column.
3. Select the table whose functions you want to edit and expand the menu item.
 - The **Assignments** filter groups all the risk index functions with assignments to the selected table (for example Active Directory user account membership in Active Directory groups).

- The **Properties** filter groups 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 then select the **Change main data** task.
- 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:
 - Deactivated
 - Calculation type
 - Weighting/change value
 - Calculate immediately
 7. Save the changes.

Related topics

- [General main data of risk index functions](#) on page 16
- [Assigning source tables for risk index functions](#) on page 19
- [Disabling risk index functions](#) on page 20

General main data of risk index functions

Enter the following information for a risk index function.

Table 5: Risk index function main data

Property	Description
Name	Name of the function as displayed in the One Identity Manager tools.
Description	Text field for additional explanation.
Deactivated	Specifies whether the function is taken into account in the overall calculation of risk indexes.
Calculation type	Method used to calculate the risk index. Permitted values are: <ul style="list-style-type: none"> • Maximum (weighted): The highest value from all relevant risk indexes is determined, weighted and used as the basis for further calculation. • Maximum (normalized): The highest value from all relevant risk indexes is calculated, weighted with the normalized

Property	Description
	<p>weighting factor and taken as basis for the next calculation.</p> <ul style="list-style-type: none"> • 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 the table column (target) is decreased 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. • Reduction: Used when calculating the reduced risk index for compliance rules, SAP functions, company policies, and attestation policies. You cannot add custom functions with this calculation type! <p>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.</p> <p>The following applies to all of a target column's risk index functions: Only combine risk index functions with the Maximum (weighted) and Average (weighted) calculation types or functions with the Maximum (normalized) and Average (normalized) calculation types!</p>

Weighting/change value	<p>The value by which to modify the risk index. There are three possible cases:</p> <ul style="list-style-type: none"> • Calculation types Maximum (weighted) and Average (weighted): Value used to weight the determined risk index in the overall calculation. • Calculation types Maximum (normalized) and Average (normalized): Value used to weight the determined risk index in the overall calculation. The value for this function is normalized to 1 beforehand. • Calculation types Decrement and Increment: Value by which the calculated risk index is decreased or increased in the overall calculation.
------------------------	---

Detailed information about this topic

- [Disabling risk index functions](#) on page 20
- [Weighting and normalization](#) on page 21

Extended main data of risk index functions

Enter the following information for a risk index function.

Table 6: Extended main data of a risk index 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 risk index calculations on page 20.
Query	Query in SQL syntax, which finds the risk index for each object in the target table.

The columns in the list below must be selected using the query.

- For maximum and average value calculation types:
 - 1st column: XObjectKey of the calculation object as ObjectKeyTarget
 - 2nd column: RiskIndex, RiskIndexReduced, or RiskIndexCalculated from one of the source tables as SourceValue
 - 3rd column: XObjectKey of the referenced object as ObjectKeySource, if RiskIndexCalculated or RiskIndexReduced is selected for the 2nd column
- For increment and decrement calculation types:
 - 1st column: XObjectKey of the calculation object as ObjectKeyTarget
 - 2nd column: 1.0 as SourceValue

Examples queries

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

```
select p.XObjectKey as ObjectKeyTarget, g.RiskIndexCalculated as
SourceValue, g.XObjectKey as ObjectKeySource
from Person p join ADSAccount g on p.UID_Person = g.UID_Person
```

Displaying the risk index function overview

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

To obtain an overview of a risk index function

1. In the Manager, select the **Risk Index Functions** category.
2. Navigate to **Risk index functions > <table> > <filter>** in the hierarchy.
3. Select the function in the result list.
4. Select **Function overview** category.

Assigning source tables for risk index functions

One Identity Manager obtains all the information necessary for calculating of 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. In the Manager, select the **Risk Index Functions** category.
2. Navigate to **Risk index functions > <table> > <filter>** in the hierarchy.
3. Select the function in the result list.
4. Select the **Assign source tables** task.
5. In the **Add assignments** pane, assign the tables that are required as source tables for the risk index function.

TIP: In the **Remove Assignments** pane you can remove tables that are not required.

To remove an assignment

- Select the table and double-click .
6. Save the changes.

Related topics

- [Starting risk index calculations](#) on page 20

Disabling risk index functions

One Identity Manager provides default risk index 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. In the Manager, select the **Risk Index Functions** category.
2. Navigate to **Risk index functions > <table> > <filter>** in the hierarchy.
3. Select a function in the result list and run the **Change main data** task.
4. Select the **General** tab.
5. Click **Disabled** category.
If this option is already set, you do not need to do this.
6. Save the changes.

Starting risk index calculations

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 run.

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 the **Calculate immediately** option 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
- The origin of an assignment has changed.
- The effectiveness of an assignment has changed.
- 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 run 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. The **Calculate risk index** schedule is provided to do this. This schedule is disabled, by default. Enable it to recalculate the risk indexes on a scheduled basis. Adjust the activation times to suit your company's requirements.

To enable the schedule for calculating risk indexes

1. In the Designer, select the **Base data > General > Schedules** category.
2. Select the **Calculate risk indexes** schedule in the List Editor.
3. Click **Enabled** in the edit view.
4. Save the changes.

Related topics

- [Assigning source tables for risk index functions](#) on page 19

Weighting and normalization

You can calculate the risk index for an object type using different methods.

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 to all of a target column's risk index functions: Only combine risk index functions with the **Maximum (weighted)** and **Average (weighted)** calculation types or functions with the **Maximum (normalized)** and **Average (normalized)** calculation types!

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 occur when the weighting is given with the value **1** in all the relevant functions.

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

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

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** within a calculation, because the range from **0** to **1** must be adhered to for the resulting risk 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 **Maximum (normalized)** or **Average (normalized)** calculation type.

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
- G1 = 0.3
- G1 = 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 factor: 0.6
Structural profile weighting factor: 0.8
SAP function weighting factor: 0.7
- By method 4: Maximum (normalized)
SAP group weighting factor: 0.6
Structural profile weighting factor: 0.8
SAP function weighting factor: 0.7

Table 7: 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	$1 * 0.4 = 0.4$	$0.6 * 0.4 = 0.24$	$(0.6 / (0.6 + 0.8 + 0.7)) * 0.4 = 0.11428$

Calculation	Method 1	Method 3	Method 4
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

Mitigating controls

Effective permissions of identities, 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 identities through the IT Shop, a rule check can be integrated into the request's approval process. 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.

Defining mitigating controls

Mitigating controls can be defined in One Identity Manager functions.

Table 8: 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 Module

Function	Object type	Application	Available in 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 the Designer, set the **QER | CalculateRiskIndex** configuration parameter and compile the database.

If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

Use SAP to assign mitigating controls to compliance rules, Manager functions or company policies.


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*.

Detailed information about this topic

- [Creating and editing mitigating controls](#) on page 27
- [Displaying mitigating controls overview](#) on page 29
- [Assigning mitigating controls to compliance rules](#) on page 27
- [Assigning mitigating controls to attestation policies](#) on page 28
- [Assigning mitigating controls to company policies](#) on page 28
- [Assigning mitigating controls to SAP function definitions](#) on page 29

Creating and editing mitigating controls

To create or edit mitigating controls

1. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select a mitigating control in the result list and run the **Change main data** task.
- OR -
Click  in the result list.
3. Edit the mitigating control main data.
4. Save the changes.

Enter the following main data of mitigating controls.

Table 9: General main data of 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.

Assigning mitigating controls to compliance rules

NOTE: This function is only available if the Compliance Rules Module is installed.

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. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign rules** task.
4. In the **Add assignments** pane, assign the compliance rules.

TIP: In the **Remove assignments** pane, you can remove assigned compliance rules.

To remove an assignment

- Select the compliance rule and double-click .

5. Save the changes.

Assigning mitigating controls to attestation policies

NOTE: This function is only available if the Attestation Module is installed.

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

To assign attestation policies to mitigating controls

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

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 mitigating controls to company policies

NOTE: This function is only available if the Company Policies Module is installed.

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. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign company policies** task.

In the **Add assignments** pane, assign company policies.

TIP: In the **Remove assignments** pane, you can remove company policies.

To remove an assignment

- Select the company policy and double-click ✓.
4. Save the changes.

Assigning mitigating controls to SAP function definitions

NOTE: This function is only available if the SAP R/3 Compliance Add-on Module is installed.

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. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign function definitions** task.

In the **Add assignments** pane, assign the function definitions.

TIP: In the **Remove assignments** pane, you can remove function definitions assignments.

To remove an assignment

- Select the mitigating control and double-click ✓.
4. Save the changes.

Displaying mitigating controls overview

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

To obtain an overview of a mitigating control

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

Calculating mitigation

The reduction in significance 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 **QER | CalculateRiskIndex | MitigatingControlsPerViolation** configuration parameter.

Table 10: Effect of configuration parameters on calculating mitigation

Configuration parameters	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. This calculates the reduced risk index of identities with rule violations and takes into account mitigating controls that were assigned to a rule violation during an exception approval.

$$\text{Risk index (reduced)} = \text{Risk index} - \text{sum significance reductions}$$

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 13

Risk index calculation example

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

Jo User1 is:

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

The "Personnel" department is assigned

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

The following also applies

- Jo User1 has requested three software applications through the IT Shop. The requests were approved; the software assigned.
- The JOU user account (SAP R/3) was created through an account definition.
- The JOU user account is a direct member of the SAPG2 SAP group .
- The JOU user account is assigned directly to the SAPSP structural profile.
- Jo User1 is team lead of a work group and therefore manager of 10 staff members.
- Identity are attested regularly.

The following risk indexes are calculated for the company resources:

Company Resource	Risk index
KRSAP	0.0
SAPG1	0.7
SAPG2	0.2
SAPSP	0.5

Company Resource	Risk index
Software 1	0.1
Software 2	0.2
Software 3	0.3

One Identity Manager uses the default risk index functions to calculate risk indexes for the following objects:

Table	From the object's risk indexes
Identities	All assigned objects
Software assignments	Software applications
Account definition assignments	Account definitions
SAP user accounts	SAP groups, structural profiles
Roles and organizations	Software (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 **SAP user accounts: group assignments** table.
The table contains two entries for the JOU user account. The risk indexes correspond to the risk indexes of the assigned SAPG1 and SAPG2 SAP groups. As the SAP group is assigned to SAPG1 by inheritance, the risk index of this SAP group is decremented.
2. Determine risk indexes of the **SAP user accounts: assignments to structural profiles** table.
The table contains one entry for the JOU user account. The risk index corresponds to the risk index of the assigned structural profile SAPSP.
3. Calculate the risk index of the **SAP user accounts** table.
The table contains one entry for the JOU user account. The risk index is calculated from the risk indexes determined in steps 1 and 2.
4. Find the risk index of the **Software assignments** table.
The table contains three entries for Jo User1 for the three assigned software applications. The risk indexes correspond to the risk indexes of the software applications.

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

The table contains one entry for Jo User1. The risk index corresponds to the risk index of the assigned account definition KRSAP.

6. Calculate the risk index of the **Identities** table.

The table contains one entry for Jo User1. The risk index is calculated from the risk indexes found in steps 3, 4, and 5. The calculated risk index is increased because Jo User1 is the manager of other identities. The calculated risk index is reduced because the last attestation case for Jo User1 was approved.

Table 11: Risk index calculation results

#	Object	Calculated risk index	+/-	Resulting risk index	Comment
1	JOU: SAPG1	0,7	-0,05	0,65	Decrement, because inherited
	USERC: SAPG2	0,2		0,2	Directly assigned
2	JOU: SAPSP	0,5		0,5	Directly assigned
3	JOU	0,65		0,65	Maximum value from steps 1 and 2
		0,5			
4	Jo User1: Software 1	0,1		0,1	
	Jo User1: Software 2	0,2		0,2	
	Jo User1: Software 3	0,3		0,3	
5	Jo User1: KRSAP	0,0		0,0	
6	Jo User1	0,65		0,65	Maximum value from steps 3, 4, and 5
		0,3			
		0.0			
			+0,2	0,85	Incremented, as Jo User1 manages other identities
	-0,33	0,52	Decrement, as attestation is approved		

Legend: # - step, +/- - increment/decrement

7. Find the risk index of the **Roles and organizations: software assignments** table.
The table contains one entry each for the requested software applications. The risk indexes correspond to the risk indexes of the software applications.
8. Calculate the risk index of the **Roles and organizations** table.
The table contains one entry each for the requested software applications. The risk indexes are calculated from those determined in step 7.
9. Find risk index or the table **Roles and organizations: account definition assignments**.
The table contains one entry for the "Personnel" department. The risk index corresponds to the risk index of the assigned account definition KRSAP.
10. Find the risk index of the **Roles and organizations: SAP group assignments** table.
The table contains one entry for the "Personnel" department. The risk index corresponds to the risk index of the assigned SAP group SAPG1.
11. Calculate the risk index of the **Roles and organizations** table.
The table contains one entry each for the "Personnel" department. The risk index is calculated from the risk indexes determined in steps 9 and 10. Since no manager is assigned to the department, the calculated risk index is incremented.
12. Find the risk index of the **Identities: memberships in roles and organizations** table. The table contains three entries for Jo User1 because they are a member of the 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 Jo User1 is not a secondary member of this department.

Table 12: Risk index calculation results

#	Object	Calculated risk index	+/-	Resulting risk index	Comment
7	Product node 1: Software 1	0,1		0,1	
	Product node 2: Software 2	0,2		0,2	
	Product node 3: Software 3	0,2		0,3	
8	Product node 1	0,1		0,1	

#	Object	Calculated risk index	+/-	Resulting risk index	Comment
	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 steps 9 and 10
		0,5			
		0,5	+0,05	0,55	Increment, as the department has no manager
12	Jo User1: Product node 1	0,1		0,1	
	Jo User1: Product node 2	0,2		0,2	
	Jo User1: Product node 3	0,3		0,3	

Legend: # - step, +/- - increment/decrement

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 and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

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

A

- application role
 - administrators 6
 - Identity and Access Governance
 - attestation
 - administrators 6
 - company policy
 - administrators 6
 - Identity Audit
 - administrators 6
 - Identity Management
 - identity
 - administrators 6

M

- mitigating control 25
 - assign attestation policy 28
 - assign company policy 28
 - assigned object type 25
 - attestation policy 25
 - company policy 25
 - compliance rule 25
 - log 27
 - overview 29
 - SAP function 25
 - significance reduction 27

R

- risk assessment 5
 - administrators 6
 - user 6

- risk index 5
 - average 16, 18, 21
 - calculate 9, 20-21, 30
 - example 31
 - exclude object type 20
 - calculate immediately 18
 - calculation procedure 20
 - calculation type 16
 - change amount 16
 - decrement 9, 16, 18
 - increment 9, 16, 18
 - log 7
 - maximum 16, 18, 21
 - object type with risk index 7
 - object types with a calculated risk index 8
 - reduced
 - calculate 30
 - reduction 16
 - risk index function
 - assign source table 19
 - deactivate 16, 20
 - default risk index function 9
 - define 15
 - for roles 12
 - for system roles 12
 - for user accounts 11
 - overview 19
 - table column (target) 18
 - target column 18

start calculation
 after data change 20
 scheduled 21
weighting 16, 21

S

significance reduction 27