- Profile/Template Permission Descriptions -

FOR RISKMAN VERSION 19.02

Last reviewed December 2019

CONTENTS

Introduction 3
General Permissions 3
Basic Permissions 3
My Details 5
Reporting Permissions 7
Management Permissions 10
Administrative Permissions 10
Register Permissions 14
Basic Permissions 14
Reporting Permissions 17
Analyser Permissions (Incident Register only) 19
Management Permissions 20
Administrative Permissions 22
Attach Document Permissions 23
Journal Permissions 24

INTRODUCTION

There are two kinds of permissions in RiskMan; the permissions which are specific to each particular register in your system, and the generic, universal permissions which are not related to one particular register in your system ("General" permissions).

The General permissions in the system will be first explained, and then the permissions for a register will be explained; keeping in mind that, in certain circumstances, there are some permissions which only appear for particular registers. Any such permissions will be obviously denoted in this guide.

If you examine a user profile and a user template, you will note that all of the permissions exist in both entities. You should refrain from giving an individual user any 'extra' permissions on their individual user profile, because the next time you apply the template permissions for that user's template, the extra permissions you gave that user will be overwritten.

GENERAL PERMISSIONS

Basic Permissions

Can "Bookmark" entries

Allows the user to assign a bookmark to a record, in order to easily locate it at a later date. These bookmarked records can be located and opened from the menu *My Workspace > Reminders & Alerts* under the Bookmarked items tab, or from the Bookmarked Records panel on the home page.

Can view Reminders

Allows the user to view the "Reminders" page accessed from the *My Workspace > Reminders & Alerts* menu option, containing a list of records based on the following:

- **Active Ownership**: (If Sequential Distribution Lists is turned on) Records that have been assigned to the user from a Distribution list where the user is the active owner
- **Distribution Lists**: (if Concurrent Distribution Lists is turned on - most common option) Records that have been assigned to the user via a Distribution list that have not yet been viewed
- **Bookmarked Items**: Records from any Register the user has flagged as bookmarked

- **Allocated Actions**: Actions that have been allocated to the user from a Risk in the Risk Register that have not been responded to

Allocated Journal Actions: Journals from Records from any Register that have been allocated to the user but have not been actioned i.e. the user's outstanding actions list.

Can use the "Contact Riskman" (developers) link on the Help menu

Allows the **RiskMan Support** and **What's New** menu options to be displayed under the **Help** menu.

- The RiskMan Support option provides a user with the ability to direct questions, bug reports, general enquiries, and suggestions to RiskMan Support staff at RiskMan International Pty Ltd. An email is automatically triggered with the details of the request and who it came from. A member of the RiskMan support team will respond to your request.
- The What's New menu option allows users to view RiskMan News and updates, download RiskMan User Guides & What's New Features documents.

Can edit own Line Managers

Allows the user to change the manager(s) they report to, either via *My Workspace > Edit My Managers* or when they are saving a new Register item.

Can bypass manager selection

If this permission is enabled, users will not have to select a manager to report to.

If this permission is not enabled, users will be required to select a manager they report to. If they do not have a selected manager, then every time they log onto RiskMan, the **Assign Your Managers** page will open for the user to select a manager.

Can not be the target of a Distribution List on item entry

If this permission is enabled, then the user will not be available for selection from a record's Distribution list, if a user elects to create a distribution list immediately after they have saved a record item. They will, however, be able to select that user in the Distribution list from any record or from any record list page.

Can Not be selected as their Manager by a user

When enabled, this permission will prevent the user from being selected as a manager from:

- The My Workspace > Edit My Managers page, or
- When a user clicks on the Click here to change the manager you report to button after saving a record, or
- When a user is presented with the Assign Your Managers page when logging onto RiskMan

However, for those users with permission to the *Manager/Staff > Edit Staff* page, these users will be available to select.

Can see personal email log on menu

Enables the menu option *My Workspace > My Email Log*, which lists all emails sent to that user.

Refer to the RiskMan Email Log Guide for more details

My Details

My Details relates to what a user can modify in regards to their User Profile from the *My Workspace > My Details* page

The “My Details” permissions will only be visible if the following setting is turned on under the *Administration > Configuration > Global Settings*

- Users | User Control | 120) Allow users to edit their own personal details

Can change own password

User can change their password

Note:

This permission should not be turned on if only network logins are used in your system

Note:

To enable users to change their password, the following Global Setting also needs to be turned on: Users | User Control | 80) Allow users to change their own password (RiskMan 'Standard' accounts only.)

Can modify own sites (if enabled in Global Settings)

User can change their own Organisation/Site restrictions

Note:

It is recommended that this option be turned off, however if you wish to allow this permission to be visible then the following Global Setting needs to be turned on - Users | User Control | 110) Allow users to edit their own Site. *(Not Recommended)*

Note:

If a user does change their Organisation/Site restriction, it will ONLY affect the user's entry/update restrictions (NOT the user's reporting restrictions)

Can change display name

User can change their display name eg. first name and/or surname.

Note:

A user cannot change their username. If their username needs to be changed, delete their current user profile and create a new one (care should be taken as it may affect manager/staff relations and alerts, and the user will not have access to their previous notifications/actvitities/items).

Note:

If network logins are used, and the users' display names are controlled by your network logins, it is recommended that this permission not be enabled.

Can change contact number

User can change their contact phone number

Can change mobile number

User can change their mobile phone number (which is used if SMS notifications are set up in your system)

Can change email address

User can change their email address

Note:

*This permission should **not** be turned on if network logins are used*

Can change alternate email address

User can provide an alternate email address. This email address can be used in alerts.

Note:

Contact RiskMan Support if a user's alternate email address is to be used in an alert

Can change own position

User can change their position within the organisation from a drop down list

Reporting Permissions

Can view Indicators

When enabled, the **Indicators** menu option is displayed under the **Reports** menu option. Indicators are customised reports that are set up for individual organisations. They provide users with a high-level statistical snapshot of the information in their domain.

Note:

A user still needs to be granted permission to an indicator set. If the user does not have permission to view any indicator sets, and this permission is enabled, the user can still access the indicators page, but they cannot do anything.

Can Create Indicator Set

If checked, an **"Add Set"** option will display on the Indicators page to allow the user to create a new Indicator Set. Once the Indicator set has been created, to be able to create the indicators that appear under that set, the user will need the Administrative Permission: **"Can manage All Indicator Set".** *Refer to the "Creating Indicators Guide" for more information on how to create Indicators Sets and Indicators within these sets*

Note:

__If required,__ contact RiskMan Support - support@riskman.net.au, if you need assistance with setting up an Indicator or would like to commission RiskMan to create your Indicators

Can Access InfoCentre

When enabled, allows the user to access the InfoCentre. The InfoCentre is an interactive dashboard reporting tool, which shows the information that the user considers important and relevant to them.

Please refer to the InfoCentre Guide for more information.

Can Edit Standard InfoCentre Datasources

Allows a user to create and edit datasources using the Datasource Builder.

Can Edit Advanced InfoCentre Datasources

Allows a user to create and edit datasources using Advanced mode.

Can Generate Workbook Reports

When enabled, allows the user to access Workbook Reports. Workbook Reports are completely bespoke, highly formatted Excel spreadsheets written for the requirements of an organisation.

Note

A user still needs to be granted permission to workbook report. If the user does not have permission to view any workbook reports, and this permission is enabled, the user can still access the Workbook Reports page, but they cannot do anything.

Can Share Workbook Reports

When enabled, allows the user to modify the sharing properties of any Workbook Report to which they have been granted permission.

Can Add Report from Library

Allows you to see the Report Library when you navigate to Reports > My Reports.

Can Edit Library Reports

You will be able to edit the report comments within the Library if enabled.

Can Delete Library Reports

You will be able to delete the report comments within the Library if enabled.

Note:

Report library permissions above will be removed once you migrate to the use of version 2 reports

Can access Reports V2

This allows you to see the menu option Analysis > Reports.

Is Reports Library V2 Administrator

This allows you to:

- See all folders in the Report Library
- Modify the sharing permissions of all folders in the Report Library
- Delete any report, provided you have at least the Read/Write permission for the folder that contains the report you wish to delete

Can view Reports Library V2

Allows you to see the Report Library when you navigate to Analysis > Reports.

Can share MyReports V2

Allows you to share folders you have created in your My Reports

Can see "Identifying" fields in reports

Allows a user to see the content of fields marked as identifiable when they run reports. This effectively allows you to setup a privileged group of users who can see identifiable information in reports, whereas other users cannot.

Management Permissions

Can view Manager/Staff relationships

Allows the user to view the Manager/Staff relationships hierarchy accessed from the menu option *Administration* > *Manager/Staff* > *Staff Hierarchy*. Refer the “RiskMan Managing-Staff Relations Guide” for more details.

Can Delegate access to another user

When enabled, a user can delegate access to their account to another user, in the case where they are away from their place of employment eg. holidays, training, conference, etc.

The nominated user will be CCd on any email notifications that the user (who has assigned the delegate) receives from RiskMan, and will be able to assume their identity during the period of time that they have been allocated as a delegate.

The delegate option will appear in the menu under *My Workspace* > *Assign a Delegate*. Refer to the “RiskMan Personal Delegates Guide” for more information.

Administrative Permissions

Can modify Global Settings

Allows the user to access and change the Global Settings and other Settings under the *Administration* > *Configuration* menu, and also the Tools under the *Administration* > *Tools* menu - refer to the “RiskMan System Configuration & Tools Guide” for more information

Note

Strongly Recommend this option be turned on at the Administrator level ONLY

Can modify other users Delegates

Allows the user to add, modify or delete delegates on behalf of other users through the User Profiles. This can be done under the “Current/Pending Delegation” section that appears under the “Login Details” of any of the User Profile pages. This section displays all active and future delegations for or assigned to the selected user.

Can maintain Manager/Staff relationships

Allows the user to define Manager/Staff relations within RiskMan ie. who reports to who. Manager/Staff Relationships can be maintained through the menu option *Administration > Manager/Staff >Edit Staff.*

Note

The manager relationship may not correspond with any defined administrative/human resource hierarchy – it simply defines a line of reporting in RiskMan. This function can be used by Managers where the user has staff reporting to them in RiskMan.

Can maintain codes (eg Site / Location list)

Allows maintenance of the customisable drop down lists and the Tool Tips for for all Registers configured on your system. These lists are accessible from the menu options *Administration > List & Codes Maintenance.*

Can Broadcast Email

When enabled, the menu item *My Workspace > Broadcast Message*, will be available. The Broadcast Email page allows a user with this permission to send an email to a group of users. Broadcasting emails may include informing staff of:

- Up and coming training
- Scheduled Meetings
- Scheduled downtime

Can manage All Indicator Set

When enabled, and the user has the following Reporting permissions: **Can View Indicators** and **Can Create Indicator Set**; the user will be able to: Create individual Indicators under an existing set; Modify Indicators; Share Indicators to other users; Add charts to Individual indicators.

Can Send SMS

This setting enables the user to send alerts via SMS as well of, or instead of, via email. This setting should only be used in conjunction with RiskMan Support's guidance.

Can Edit 'General' User Profiles

Allows the user to access and change User Profile settings under the General tab only.

Can Edit 'General' User Templates

Allows the user to access and change User Template settings under the General Tab only.

Can Reset 'General' User Profiles

Allows the user to apply the changes that have been made to the General User Template to all users assigned to that template. This allows several changes to be made to a template before they are actually applied to the user profiles assigned to that template. Resetting user profiles is accessed through the menu *Administration > User Permissions > Apply Template Changes*.

Can Import List Data

Allows the user to import lists from a CSV file (file format saved from Excel™) into all non-RISKMAN lists in the List & Codes Maintenance (provided the Import button has been activated on the lists), negating the need to manually enter the data if it is saved in an Excel™ spreadsheet - refer to the "RiskMan Managing Lists Guide for more information"

Note:

If you would like to be able to import data into specific lists eg. Program, Department within the List & Codes Maintenance, the "Import" button needs to be set as active. To enable the "Import" button on a list please contact RiskMan Support – support@riskman.net.au

Can manage Homepage

Allows the user to modify panels available on the Homepage, and also which widgets are available to be displayed on the Homepage.

Can manage Roam Script Builder

Allows you to give the user access the tool that enables data capture from your system from a mobile device.

Can edit controls in Roam Script Builder

Technical script information that may be used with the assistance of the RiskMan Helpdesk

REGISTER PERMISSIONS

Basic Permissions

Can do Item entry

Allows the user to create a new record in the register

Can review own/subordinate’s entries

Allows the user to review their own records after they have initially submitted them. Also allows the user to review records entered by users for whom they are nominated as a manager.

Can apply Distribution Lists (if enabled)

Allows a user to create a Distribution List for a record, which grants other users permission to see that record.

Can mark an entry for "Personal Alerts" (change notification)

Allows the user to be able to activate a personal alert on a selected record. For the duration of time the user specifies, if any other user modifies that record, then an email will be sent to the user informing them that this took place.

The user will not be emailed about journals or attached documents.

Can see the Review History

Allows the user to see the Review History in records.

Can "Archive" entries

Allows the user to add a record to their Personal Archive. This has two effects:

- The record will be hidden from the user's *My Workspace* > *Review My* > *Register Name* page
- An entry will be placed in the Review History of the record to denote that the user added the record to their personal archive

This action does not affect any other user's ability to see the record.

Can prevent sending manager email notifications when saving an entry

This is a deprecated setting which is in the system for legacy purposes.

Can use the "Print Preview" report from an unposted entry

Allows the View **Printer Friendly Version** button to be displayed in the "Control Panel" of an existing record so that the record can be printed. The printed copy will only show the fields (and content) that the user has permission to view.

This button can be renamed through the *Administration* > *Configuration* > *Global Settings* under the "Reports" listing - items 110 and 120

Can create Linked entries

This permission allows a user to create a linked (grouped) record after the first record has been entered. It also displays the "Clone & Link" icon in the toolbar of the register list pages, to allow a linked record to be created from an existing record.

Can see risks on items *(Incident Register only, or enabled for other registers based on custom config)*

Allows the user to view the "Associated Risk" section on the Incident Notification and view any risks that have been associated with the displayed incident.

Can modify risks on items *(Incident Register only, or enabled for other registers based on custom config)*

If the **Associated Risk** section on the Incident Entry form is available *(and the permission **Can see risks on items** is enabled)* this allows the user to associate risks to incidents

Can create Shortcut

Allows a user to partially complete a new record, and save that as a shortcut on their Homepage.

Can share Shortcut

Allows a user to share a shortcut they have created with other users.

Can create Draft

Allows a user to save a partially completed form as a draft, to be completed at a later time. The draft will remain on the user's Homepage in the Shortcut section. Drafts can be set to expire after a certain number of days via the Global Setting *Item Entry Defaults | Shortcuts | Draft shortcut expiry time (days)*.

Can generate results using Letter Builder

Allows a user the ability to generate letters/documents based on the records they have permission to see in a register.

Reporting Permissions

Can modify Custom Reports

Allows you access to be able to access and create customised layouts.

Can restrict to Sentinel Events Only on Reports *(Incident Register only)*

Enables the filter option “Can restrict to Sentinel Events Only on Reports” on the report creation page.

Can exclude Incidents where Stratification Undefined on reports *(Incident Register only)*

Enables the filter option “Exclude incidents where Stratification is not defined” on the report creation page. Only has an effect if your organisation individually risk rates every incident.

Can view MyReports

Allows you to see reports for this register in Library and My Reports folders where you have at least the Read permission.

Can save MyReports

You are able to save any reports and access them via Reports > My Reports.

Can share MyReports

You are able to share the reports you have save with other users who have access to My Reports.

Can share MyReports created by others

If another user has shared a report with you, you can then share that report with other users.

Can schedule MyReports

Allows you to create schedules for generating reports automatically at the time frame you stipulate (if you are using the Scheduler option in your system).

Can Create Library Reports

When saving your report to MyReports, if you think it maybe of use to oters, you can save it in the library for other users to add to their MyReports.

Note

The above permissions related to My Reports will not be available if you have migrated to Reports V2

Can Save Reports to Library V2

Allows you to create reports and choose a folder in the Library as a save destination. You also need the permission “Can Create Reports V2”, and at least Read/Write permission to the desired folder.

Can View Reports V2

Allows you to see reports for this register in Library and My Reports folders where you have at least the Read permission.

Can Create Reports V2

Allows you to create reports for this register. This permission also allows you to edit existing reports (where you have at least the Read/Write folder permission).

Can Modify Custom Reports V2

Allows you to modify report layouts for this register.

Can Schedule Reports V2

Allows you to create schedules for generating reports automatically at the time frame you stipulate (if you are using the Scheduler option in your system).

Analyser Permissions (Incident Register only)

Can use "Analyser"

Allows a user to use the Incident Analyser, accessible via *Reports* > *Analyser*.

Can modify Views

Allows a user to modify an Analyser View to which they have permission.

Can save Views

Allows a user to save the Analyser setup as a “view”, for future use. This is the equivalent of a My Report.

Can share Views

Allows a user to share an Analyser View with other users.

Can delete Views

Allows a user to delete Analyser Views to which they have permission.

Can save Filters

Allows a user the ability to save their own filtering conditions in the Analyser.

Can share Filters

Allows a user to share filtering conditions they create in the Analyser with other users.

Can save Comparison Factors

Allows a user to create and maintain Comparison Factor tables in the Analyser. This data can also be referenced by Indicators.

Can import Comparison Factors

Allows a user to import Comparison Factor data en masse via a prescribed spreadsheet.

Can delete Comparison Factors

Allows a user to delete Comparison Factor tables that they have permission to see.

Can Modify shared Analyser Views and Filters

Allows a user to modify Analyser Views and Filters which have been shared with them by someone else.

Management Permissions

Can review entries in Inbox

In registers which use the Posting paradigm (usually incidents and feedback):

Allows the user to review the (Incident or Feedback) Inbox page. The Inbox is where a user posts a record. Posting a record allows it to appear in reports generated in RiskMan (please note that it is possible, depending on how they are configured, for indicators and InfoCentre widets to count unposted records if desired. However, a record will not appear in qualitative reports until it has been posted.

In registers which do not use the Posting paradigm:

Allows a user to view the (Register Name) Register page, eg. Risk Register.

Note

Irrespective of whether it is the incident or feedback inbox, or other Register page, the information displayed for a user is dependent on how that user's profile has been configured.

Can delete entries in Inbox

Allows a user to delete records in the *Management > Inbox > Incidents / Feedback* pages, or *Management > (Register Name)* Register pages. Users with this permission also have the ability to restore deleted records.

Can review Posted entries *(Incident / Feedback Registers only)*

Allows a user to view the posted incidents / feedback via the *Management > Enquiry > Posted Incidents / Feedback* pages.

Can edit Posted entries *(Incident / Feedback Registers only)*

Allows a user to makes changes to, and save, records that they can see in the Posted Incidents / Feedback pages.

Can delete Posted Items *(Incident / Feedback Registers only)*

Allows a user to delete records they can see in the Posted Incidents / Feedback pages. Users with this permission also have the ability to restore deleted records.

Can Group existing items

Allows a user to see the “Linked Records” icon in the toolbar on the list pages of a register, which allows them to:

- Link existing records together
- Unlink records
- Modify which record is considered the ‘Master’ record

Can always see Review Log Distribution List email Links

When a distribution list is created for a record, and a user enters a comment in the email, the comment is saved and can be made visible in the Review History of the record.

The following setting: *Administration* > Configuration > *Global Setting* under the *Item Entry Defaults | Distribution Lists | 30) Email notes for Distribution List emails display in Review History using this policy setting* has 3 options for displaying the distribution list comments

Do not Display – The comments are never visible in the Review History

Always Display – The comments are visible in the Review History to all users with access to the record

Only for Sender, Receiver – The comments are only visible in the Review History of the record to the sender and receiver of the distribution list

If this permission is enabled, then despite what is selected in the above Global Setting, the user will still see any Distribution List **<Email>** links in the Review History of the records they have permission to view.

Can Create and Edit Letter Builder items

Allows a user to create, modify, and delete customised letters for a register.

Administrative Permissions

Can modify User Profiles

Allows the user to access and change (create new, modify and delete existing) User Profile settings for a register.

Can modify User Templates

Allows the user to access and change (create new, modify and delete existing) User Template settings under the General Tab only.

Can Reset User Profiles

Allows the user to apply the changes that have been made to a User Template to all users assigned to that template. This allows several changes to be made to a template before they are actually applied to the user profiles assigned to that template. Resetting user profiles is accessed through the menu *Administration > User Permissions > Apply Template Changes.*

Can manage Alerts

Allows a user to create, modify, and delete Alerts for a register.

Can view Document Library

Files eg. documents, images, correspondence, etc. can be uploaded and attached to records, and are stored either in the RiskMan database, or a separate file system. The Document Library provides a listing of files which:

- Have been attached to records
- Have been attached to a new record, but never saved with the record – these are called “Orphaned” files
- Are deleted – these files are flagged as deleted but still remain in the database / in a file system

These files can be viewed and where required, “Orphaned” and “Deleted” files can be permanently deleted as required and therefore removed from the database or file system.

Users with this permission will be able to manage files that have been attached to records in a register. Users will only be permitted to view attached files from records that they have permission to view based on their restrictions in their User Profile eg. Organisation/Site, Campus/Location, or alerted record restrictions (refer to the “Document Library” Guide for more information).

Can maintain Classifications (RiskCat)

Depending on the configuration of your system, a register may be designed to use the “RiskCat” classification feature.

If RiskCat is used in a register, this permission allows the user to maintain and configure the classifications - Supergroups, Classes & Definitions. It also allows the user to re-map the classifications on existing records if there are changes to the RiskCat. This option is available via the menu option *Administration -> (Register) Classification Editor.*

Please refer to the “RiskMan Classification Editor Guide” for more information.

Can import Item data

Allows a user to import records to a register via the Data Import tool. This feature will only be visible if the user also has permission *Can Modify Global Settings* in the General tab, as it is accessed via the Tools menu by navigating *Administration > Tools > Database > Data Import.*

Please refer to the Data Import Tool section for further information.

Attach Document Permissions

The Attach Document Permissions allow you to set permissions on attaching, viewing and deleting files which are attached to records in a register. Users with access to attaching or viewing files will see a “Document” section at the bottom of the entry form.

Note

To activate the Attach Document functionality, the Administration > Attach Document Settings need to be configured – refer to the “RiskMan System Configuration & Tools Guide” for more information

Own: Can Attach, Delete

Allows a user to attach files to a record (and thus, by implication view those files), and delete files that only they have attached to record in a register.

Subordinates: View, Delete

Allows a user to view, delete files that have been attached by users that report to them. This permission only applies if your system is using Manager/Staff relationships to define your reporting pathways.

All: View, Delete

Allows a user to view, delete all files attached to any record they have permission to see in a register.

Journal Permissions

The Journal Permissions allow you to set permissions on creating, viewing, modifying and deleting Journal Entries. Users with permission to add or view Journals will see a “Journals” section towards the bottom of a record. If none of the permissions are checked, the “Journals” section will not display on the form for users assigned to that template.

Own: Add, View, Edit/Delete

Allows a user to add, view, or modify and delete journal entries they have entered.

Subordinates: View, Edit/Delete

Allows a user to view, modify and delete journal entries that have been entered by users who report to them. This permission only applies if your system is using Manager/Staff relationships to define your reporting pathways.

All: View, Edit/Delete

Allows a user to view, modify and delete journal entries that have been entered by other users.

Allocated Journals: View, Edit/Delete

If “View” is enabled, this will allow a user to view a Journal that has been allocated to them, even if they are restricted from seeing that Journal Type or they do not have access to add or view Journals. This permission is useful to give all staff within your organisation. If you check “Edit/Delete” then the user can also edit or delete the Journal that has been allocated to them.

Note

It is recommended that only high-level users eg. Administrators, Risk/Quality Managers have access to Edit/Delete journals as there is no history of modifications/deletions of journals. Once a journal is modified there is no record of what the journal contained prior to the modification, and once a journal is deleted it is no longer linked to that record. A Journal will appear on ALL versions of a record, regardless of which version of the record the journal was added.