Risk Flow

Documentation

Updated 14/04/2023

Contents

1. Introduction

1.1. About the application

The Risk Flow application was created primarily to facilitate the work of all risk managers and analysts. Your time is too valuable to waste on formatting tables or headings. Nor should you waste your time on thankless copying of information between different documents. Risk Flow offers you the opportunity to focus only on the content. It takes care of formatting and checking for correct data entry for you. It also takes care of keeping track of defined deadlines. It emphasizes teamwork and the possibility of multiple people working on the same project or parts of it. Your clients will be able to view and participate in the analyses being performed. In addition to inappropriate methods, Risk Flow eliminates the unsecured sharing of files and documents needed to complete risk analyses. Increase the efficiency of your work and your employees and perform risk analyses and asset management simply and, most importantly, securely.

1.2. Main Funcionalities

User management will provide you with a clear and intuitive environment for managing access and permissions of users who will have access to the platform. In Client Management, you can enter and edit your clients and assign users to them. You can then create asset lists and create risk analyses for registered clients. Completed risk analyses are followed by a creation of a risk treatment plan. To facilitate the development of risk analyses and risk treatment plans, Risk Flow offers a risk catalog containing applicable risks, threats, vulnerabilities, measures, goals and metrics. As part of approval processes, clients then review risk analyses, prepared plans and other documents and add their comments to them. Until the client approves all flow parts, you as risk managers and analysts are still able to modify them. Audit and control activities are a very important part of a properly set up risk management. Within Risk Flow, you can manage the access of internal and external auditors and perform audit processes.

1.3. Licensing models

Risk Flow has three licensing models, that differ in the amount of available functionality and, of course, in price. This documentation only describes the application differences of the licensing models. For a complete list, including a price comparison, visit

> https://riskflow.cz/pricing.

For personal use	Team	Enterprise
Unlimited asset management	Everything in personal license	Everything in the team license
Unlimited analyses	Maximum of 5 active users	Unlimited number of active users
Unlimited risk treatment plans	Maximum of 5 clients	Unlimited number of clients
Unlimited flows	Option to run the instance on dedicated computing resources.	Customization of generated reports
Maximum of 2 active users		Customization application GUI
One active client		Using your own outgoing mail server
Multifactor authentication		Using you own domain
Operates in cloud		Integration with other tools via API
Instances with shared computing resources		Possibility of customization
Anti DDoS protection with Cloudflare		Priority support
Support through the ticketing system		

> 💡 **Tip**
>
> Instance administrators can quickly check the status of their license at any time by clicking the green `Check License` button in the left sidebar of the application. Then they will see information about its status in the right bottom corner. An example of the license status information for the `Team` variant can be seen below.
>
>
>
> ✓ **License active till March 2, 2024**   ✗
>
> License type: **Enterprise**
> Maximum of active users: **Unlimited**
> Maximum of clients: **Unlimited**
>
> *Fig. 1.1* Information about the active licence.

1.4. Support

If you discover any deficiency, you can contact our technical support by submitting a ticket in our helpdesk system. If you have an account, you can access our helpdesk and submit a ticket directly at https://riskflow.freshdesk.com or by

sending an email to support@riskflow.freshdesk.com.

1.5. Terms of Use

By using Risk Flow, you agree to the Terms and Conditions, which can be found at:

https://riskflow.cz/terms-of-use/

2. Entry to the application

Risk Flow is available in a web-based interface and requires only internet connection and computer with a web browser installed.
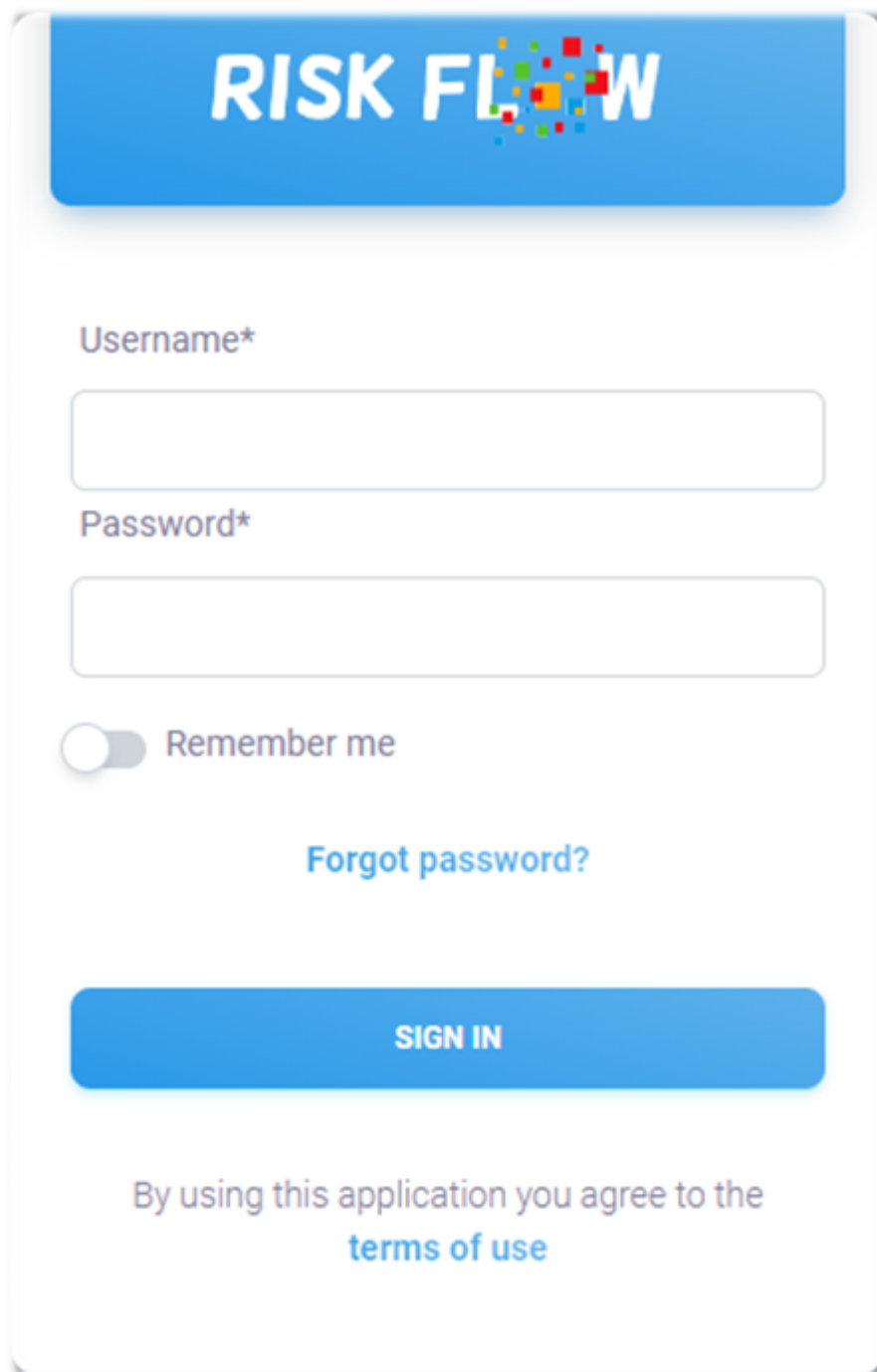
> 💡 **Use on various devices**
>
> The system is designed to be available on most devices with different types of displays. You can use Risk Flow comfortably on large screens as well as on smaller displays or standard laptops. The system also adapts to smaller screens on tablets or mobile phones, but using the app on these devices may not be as comfortable. This comes from the nature of the application, which works with a large number of tables and a wide range of information.

2.1. Language and localisation

The system can recognize the user's system-set language and adapt the application view to it. This means that if you are using, for example, Windows 10 in English, the website will automatically switch to English when you visit, and the same goes for Czech. The user can switch the language of the app at any time by clicking on the flag icon in the right top corner of the app environment or in the right bottom corner of the login screen.

2.2. Login

A login is always required to use the app. It is not possible to register to the system, the account has be created for a user by the instance administrator. After the user account is created, a link is sent to the specified email to verify the email and set a password. The user is then allowed to log in.

Fig. 2.1 Application log-in dialog.

Login with multi-factor authentication

If the user has a second factor authentication enabled, after entering the correct password, she/he will not be immediately redirected to the Risk Flow dashboard, but will be prompted to enter the security code from the application he/she is using for MFA (e.g. Microsoft Authenticator, Google Authentication, etc.). Once the security code is entered correctly, he/she will be redirected to the Risk Flow dashboard.

2.3. Forgotten password

If a user forgets his/her password, a password reset request can be generated. The link to the password reset request form can be found under the login form. Upon successful completion of the form, an email will be sent to the user's mailbox with a link to the password reset form. This link is valid for 24 hours, after which the user must submit a new password reset request. Until this process is fully completed, the user remains set to the old password.

2.4. Forgotten username

In the case of a forgotten username, the user must contact the administrator of their instance or Risk Flow Support.

2.5. Logging out of the app

You can log out of the application by clicking on the `Log out` button in the upper right part of the application environment or in the left sidebar.

3. Risk Flow dashboard

After successful login, the user is redirected to a dashboard of his Risk Flow instance. Here he/she will find summarized information relevant to his/her role in the system.

3.1. Admin's view

The Risk Flow dashboard provides summary information about the status of an instance. The administrator can see the number of open analyses and flows at the top, then the number of users and clients.
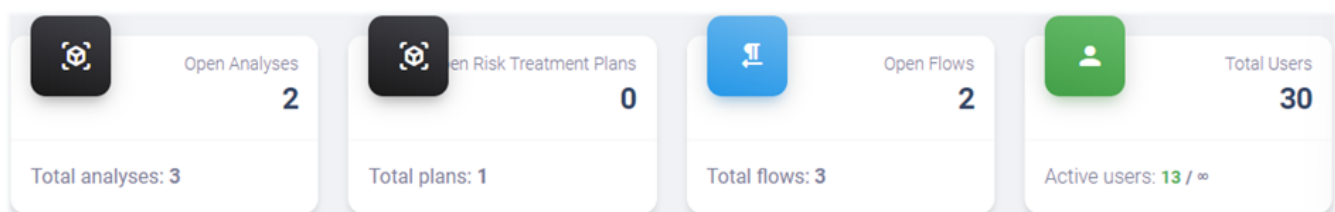

Fig. 3.1 Instance state summary.

At the bottom of the page, the pending risk analyses for all clients are displayed and sorted by their deadline. This provides the administrator with quick information if some risk analyzes are delayed to completion. Those are highlighted in red. He can then find the responsible manager to contact if necessary.

Fig. 3.2 Open analyses overview.

In addition to the summary of open risk analyses, the user will find the sam summary for risk treatment plans for all clients, sorted by their deadline. This gives the user quick information if some plans are overdue for completion. These are marked in red. He will also find the manager responsible for contacting them.

The administrator also sees all pending registered flows on his/her notice board. Again, the displayed records are sorted according to the due date and the manager responsible for contacting them is displayed.

Fig. 3.3 Open flows overview.

3.2. Risk Manager view

A user with the role of `Risk manager` has the same set of blocks available on their dashboard as the administrator, but risk analyses and flows are filtered according to the logged-in manager.

3.3. Risk analyst view

Users with the `Analyst` role has no rights to create, edit, or view the flows that are executed. Therefore, these actions are not shown to them in the dashboard. The displayed risk analyses are also filtered by the currently logged-in user with the analyst role.

3.4. Auditor view

The `Auditor` can see all the same as the `Administrator` of the instance in the system but cannot edit those entities. A user logged-in with this role will see the same content as the administrator of the instance on their dashboard.

3.5. Client´s user view

For users with the `Client's user` role, information about the total number of users of the Risk Flow instance is not displayed in the upper blocks of the dashboard. The content of the open risk analyses and pending flows sections is filtered according to the selected client.

4. User management

User management is only available to administrators of the instance and to auditors for review. The auditor has in this section only viewing rights and does not have rights to add, edit or delete users.

4.1. List of users

The list of users can be filtered by active/inactive users or by roles. Listings can be also sorted by username, role, or status in descending or ascending order using the red and blue arrows in the listing header. It is also possible to define the number of records to be listed per page before paging is enabled.

Fig. 4.1 User overview and management tool.

4.2. Create a new user

Create users with the role of manager, analyst and auditor

To create a Risk Flow user, click on the button in User Management `Add user` or by opening `https://NAZEV-INSTANCE.riskflow.cz/cs/users/create`. It is not possible to create client's users in this section.

Parameter	Required	Description
Email	Yes	Also used as a username. It must be unique within the instance.
First name	Yes	Person's first name.
Last name	Yes	Person's last name.
User's role	Yes	Available options: • Risk analyst *(default option)* • Risk manager • Auditor
E-mail	Yes	Language of e-mails generated by the application. Available options: • English *(default option)* • Czech
Active	No	Users can only log-in to the system if they are activated. By default, added users are deactivated.

After the user is successfully added, an e-mail is generated and sent to the user's email address. The user is then prompted to verify their account and set a password. Until the user account is verified, the user will not receive any informational emails. Unverified user accounts are distinguished in the user list by a warning next to their status.

Create a client's user

Adding a user for registered clients is possible in client management after selecting a specific client. The form for creating a new user is very similar to the process described above for adding analysts, managers, and auditors. The process differs in that the user role in this case is automatically set to the client user.

The form for creating a client's user can be found at `https://<NAZEV-ISTANCE>.riskflow.cz/en/clients/<CLIENT'S ID>/users/create` or by clicking on the "Add client's user" button.

Parameter	Required	Description
Email	Yes	Also used as username. It must be unique within the instance.
First name	Yes	Person's first name.
Last name	Yes	Person's last name.
E-mail language	Yes	Setting preferred language for sending informational emails. Available options: • English *(default option)* • Czech
Active	No	Users can only log into the system if they are activated. By default, added users are deactivated.

After the user is successfully added, an e-mail is generated and sent to the user's address. The user is then prompted to verify their account and set a password. Until the user account is verified, the user will not receive any informational emails. Unverified user accounts are distinguished in the user list by a warning next to their status.

4.3. Edit a user

User editing is possible in user management (or client management for client's users) after opening the edit form by clicking the `three dots` icon.
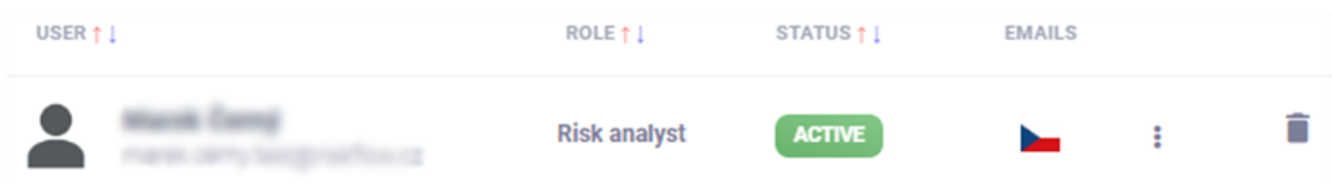
4.4. User activation and deactivation

Activation/deactivation is possible in user management (or client management for client's users) after opening the activation/deactivation form by clicking the button in the status column. This button can be green or grey and also indicates the status of a particular user.
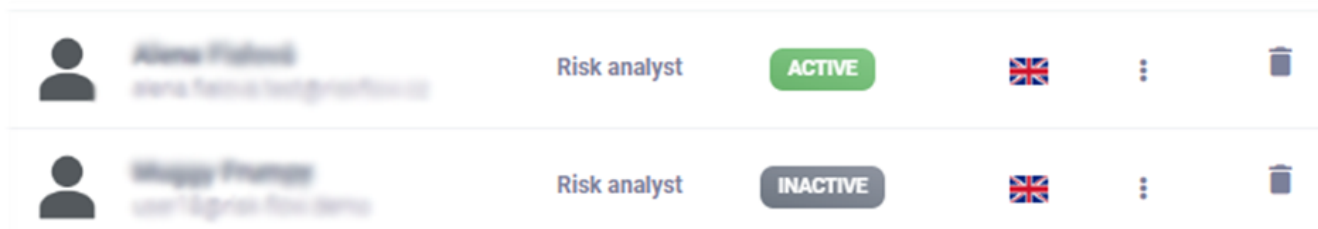
4.5. Setting a language preference for informative emails

etting the preferred language for informative emails is possible when creating a user or editing an existing user. The change is possible in the edit form and currently it is possible to choose between Czech and English.

4.6. Delete a user

Deleting users can be done in User Management (or Client Management for client's users) by clicking on the `trash can` icon. When deleting, it is necessary to confirm the action in the modal window that appears afterwards. Only users who are not assigned to any risk or flow analysis can be deleted. Otherwise, the user cannot be deleted, it can only be deactivated.

4.7. User roles

Administrator

A user with the administrator role has access to all modules of Risk Flow. Access to parts of the settings and application interfaces are limited by the active license:

- Dashboard
- User management – full access
- Client management – full access
- Asset management – full access
- Risk analyses – full access
- Risk treatment plans – full access
- Flows – full access

- Risk catalog – full access
- Documentation – read only access
- Settings – full access
- API – full access

Risk manager

A user with the Risk Manager role has access to the following Risk Flow modules:

- Dashboard
- Asset management – full access
- Risk analyses and risk treatment plans – may only manage risk analyses where is assigned as the responsible manager or analyst
- Flows – can only manage flows where is assigned as the responsible manager
- Risk catalog - read-only access, can use it to process risk analyses and risk treatment plans
- Documentation – read only access

Risk analyst

A user with the Risk Analyst role has access to the following Risk Flow modules:

- Dashboard
- Asset management – read only access
- Risk analyses and risk treatment plans – may participate in conducting risk analyses to which is assigned. Can add, edit and delete risk analysis row
- Risk catalog – read-only access, can use it to process risk analyses and risk treatment plans
- Documentation – read only access

Auditor

A user with the auditor role has access to the following Risk Flow modules:

- Dashboard
- User management – read only access
- Client management – read only access
- Asset management – read only access
- Risk analyses and risk treatment plans – read only access
- Flows:
    - Approval flows – read only access, can add comments
    - Audit flows – involved in conducting flow
- Risk catalog – read only access
- Documentation – read only access

Client's user

A user with the client's user role has access to the following Risk Flow modules:

- Dashboard
- Asset management – access to his company's assets only
- Risk analyses and risk treatment plans – has access only to analyses performed for his company. He/she has the possibility to add comments to them.
- Flows – involved in conducting approval flows
- Documentation – read only access

API user

A user with the API user role has access to the APIs only. He/she has access only to those application interfaces that have been explicitly granted to them. This will be described in more detail in the chapter about APIs.

4.8. Export of users

The export of users is possible in the user management (or in the users section in the client management) by clicking on the `Export` button and then selecting the export type.
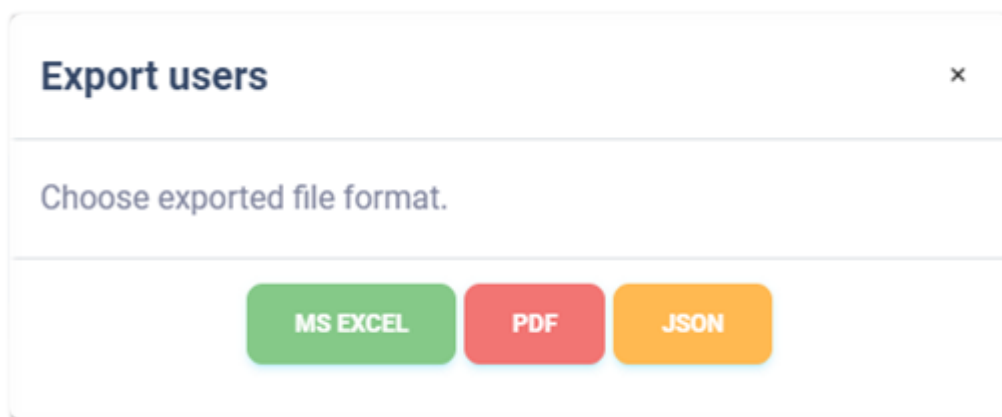
Export to MS Excel

The export of users is possible in the user management (or in the users section in the client management) by clicking on the `Export` button and then selecting the export type.

Column name	Description
#	Record number in the export.
Email	Username and contact email.
First name	User's first name.
Last name	User's last name.
Administrator	Information about whether user is instance administrator.
Role	Manager / Analyst / Auditor / Client' user.
Client	If the user's role is "Client's user", the client name will be listed here.
Status	Information about whether the user is active or inactive.
E-mails	Preferred language for information emails.
Created at	Date of record created.
Creation time	Time of record created.
Created by	Email of user who created the record.
Modified	The date record was last modified.
Modification time	The time record was last modified.
Modified by	Email of user who made last changes.

Export to PDF

Exporting users to PDF format contains a list of users similar to the listing in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export.
Email	Username and contact email.
First name	User's first name.
Last name	User's last name.
Role	Manager / Analyst / Auditor / Client's user.
Client	If the user's role is "Client's user", theclient's name will be listed here.
Status	Information about whether the user is active or inactive.
E-mails	Preferred language for information emails.

Export to JSON

Exporting users to JSON format is available only for instance administrators. This type of export can only be used with an Enterprise license. The exported file can be used as a simple backup or can be used to create custom templates for bulk user import.

4.9. Import users

Bulk importing of users can be done in the user administration via a modal form that is displayed to the user after clicking on the `Import` button.

Import users   ✕

You can create records in bulk here. You need to have a json file created in the correct format. You can find detailed information in **documentation**.

Restrictions

- Only files up to 5MB can be uploaded.
- Only files in json format can be uploaded.

Notice

- Lines containing invalid values will be ignored. You can find information about the imports **here**.

JSON file: **Browse…**   No file selected.

IMPORT ⬆

To conduct a bulk import of users, you must have a properly created data file. Only JSON format files can be imported, and the maximum size is limited to 5MB. Additionally, the uploaded file needs to be properly structured and to contain valid data. We recommend using the ready-made templates available at https://riskflow.cz/templates. The structure of a valid file with one valid record looks like this.

```
[
    {
        "first_name": "Jan",
        "last_name": "Novák",
        "email": "example1@riskflow.cz",
        "active": true,
        "role": "manager",
        "lang": "cs"
    }
]
```

Parameter	Accepted values
first_name	Alphanumeric string with special symbols
last_name	Alphanumeric string with special symbols
email	Alphanumeric string with special symbols
active	true / false
role	manager / auditor / analyst
lang	cs / en

Templates for bulk user import

Risk Flow prepares templates for its clients to create files for bulk import. These templates are publicly available at https://riskflow.cz/templates/. It is allowed to edit and use them for private and commercial purposes.

It is always recommended to verify the integrity of downloaded files. This verification ensures that the file has not been corrupted or altered during the download. To verify the success of the download, we use an MD5 hash that can be found in the download table.

Title	Type	Description	Language	Download	MD5
Users	Users	Template for bulk import of Risk Flow users - managers, analysts and auditors.	🇬🇧	Download	685ec6fb095a657fc6f6136da410bc25

For verification, you need to calculate the MD5 hash of the downloaded file and to compare it with the MD5 hash displayed on the download page. If the strings are identical, the file was not corrupted or altered in any way during the download.

Verification in MS Windows environment:
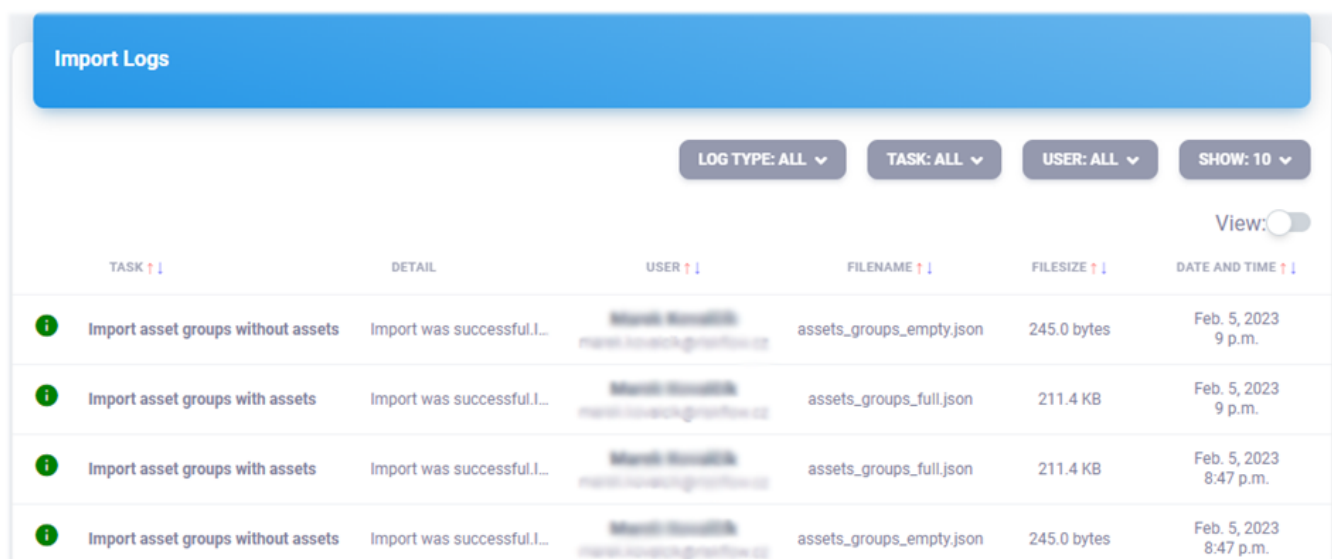
Verification in Linux environment:

Import success verification

The success of the specified bulk imports can be verified in the Log Entries module. This is available at `https://NAZEV-INSTANCE.riskflow.cz/imports/logs/` or it is possible to get to it through the modal window of bulk import forms.

By default, records are sorted by date and time the request was created and contain following information - status, task name, detailed description of the action result, the user who made the request, the name of the uploaded file and its size, and the date and time the request was created.

	Import was successful.
	Import finished. Some data failed to be imported, check the import log detail.
	Import failure.

5. User profile

The users can view their own profile by clicking on the appropriate link in the left sidebar. On the profile page they can see their name, email, company information and other information, available to edit.

At the same time, on this page the user can set the preferences of informational emails, including their preferred language, with a simple toggle switch. Currently the user can choose between Czech and English.

Furthermore, the user can choose the theme of the system - light or dark.

5.1. View another user's public profile

The username displayed in the system is also a link to the user's public profile. The user's public profile may display company, user or contact information, including links to social networks.

Profile information

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Phasellus enim erat, vestibulum vel, aliquam a, posuere eu, velit. Nulla turpis magna, cursus sit amet, suscipit a, interdum id, felis.

Mobile: +123 456 789

Email: ondrej.bohaty.test@riskflow.cz

Location: Praha, Česká republika

Social:

5.2. User password change

Any user can change his/her password at any time. They can do so by opening the appropriate form from their profile or by visiting `https://NAZEV-INSTANCE.riskflow.cz/cs/users/change-password/`. A password policy is required and is shown in form below.

Changing password

Old password*

New password*

- Your password can't be too similar to your other personal information.
- Your password must contain at least 8 characters.
- Your password can't be a commonly used password.
- Your password can't be entirely numeric.

New password confirmation*

CHANGE PASSWORD 💾

CANCEL ❌

* Fields marked with this symbol are required

5.3. Setting up multi-factor authentication

We recommend that all users should use the second authentication factor for login. This can be set up in the form opened from the user's profile, or at `https://NAZEV-INSTANCE.riskflow.cz/en/account/two_factor/setup/`.

Enable multifcator authentication

You are about to take your account security to the next level. Follow the steps in this wizard to enable two-factor authentication.

MFA SETUP 📱

CANCEL ⊗
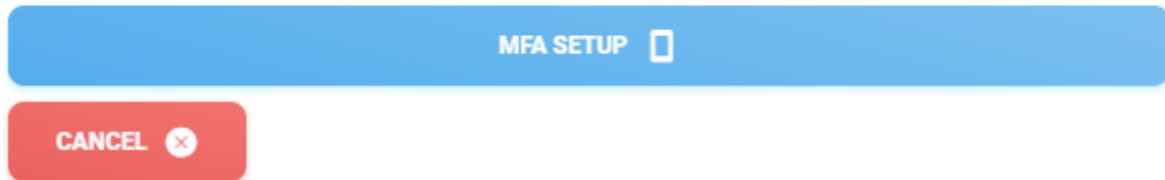
After pressing the MFA setup button shown above, the user will be presented with a page and the generated unique code to add to the third-party application. There are number of applications available that allow authentication through one-time generated codes. For example, we recommend using Microsoft Authenticator or Google Authenticator Both of these apps are available for Android and Apple iOS.

Now, open the Microsoft or Google Authenticator app on your phone and then add a new device (using the plus icon). Select the option to scan the QR code. Scan the generated QR code in Risk Flow into your mobile device and then

enter the generated six-digit code into the MFA setup form.

Enable Two-factor Authentication

To start using a token generator, please use your smartphone to scan the QR code below. For example, use Google Authenticator.

Alternatively you can use the following secret to setup TOTP in your authenticator or password manager manually.

TOTP secret: VH8HOFVMHATM0Y9KJP6EJOWKAJBJV9Q

Enter the token generated by the authentication app.

Token*

CONFIRM AND SET UP MFA

CANCEL

After successfully entering the code, you will see the following message on the screen with a link to the account security view.

Enable Two-factor Authentication

Congratulations, you've successfully enabled two-factor authentication.

SHOW ACCOUNT SECURITY

If you go to account security, you will see the option to generate backup codes. Backup tokens can be used when your primary and backup phone numbers are not available. Once the backup tokens have been generated, you will be prompted to store them securely. You can re-generate the tokens at any time.

You can also disable the use of MFA in Account Security Management.

Account security - Two-factor Authentication

Backup tokens

If you don't have any device with you, you can access your account using backup tokens. You have 0 backup tokens remaining.

SHOW BACKUP CODES

Disable Two-Factor Authentication

However we strongly discourage you to do so, you can also disable two-factor authentication for your account.

DISABLE TWO-FACTOR AUTHENTICATION

5.4. Account settings

On user's profile page, each user has the option to customize the behaviour of the app. For example, they can define which information email they wants to receive.

Risk Flow Settings

ACCOUNT

Write me about changes made in analyzes and flows

Email me when deadline is approaching

Email me when someone adds a comment to my analysis or flow

Notification of changes made to analyses and flows

The user is informed about the assignment of a role to analysis or flow, a change of status or a removal of the solver role.

Sending notifications of upcoming deadlines for analyses and flows

The user is informed when the deadline for solving an analysis or flow is approaching. This notification starts 3 days prior the defined resolution date.

Notification of newly added comments on analyses and flows

The user is informed about new comments on risk analyses and flows to which he has access - i.e., he/she is assigned to them as a manager, an analyst or he/she is a client user for whom the analyses or flows are processed.

Setting the app theme

The user can also set the light or dark theme of the app on their profile page. Setting the preferred language for informative emails

Setting the preferred language for informative e-mails

The user can also set their preferred language for email notifications on their profile page. Currently, there is an option to choose between Czech and Englis

6. Client management

Client management is only available to instance administrators and to auditors for review. The auditor has read only rights in this section and does not have rights to add, edit or delete users.

6.1. View list of clients

The client list contains information about client (name, logo) and its users. Listings in this section can be further sorted by client name. It is also possible to define the number of records to be listed per page before paging is enabled. The client list displays information about total number of its users and the number of its active users.

6.2. Adding a client

You can create a Risk Flow client by clicking on the `Add Client` button in the client management or by opening `https://NAZEV-INSTANCE.riskflow.cz/clients/create`.

Parameter	Required	Description
Client's name	Yes	It must be unique within the instance.
Logo	No	Only image files are accepted. The file name must not be longer than 100 characters.
Note	No	User to add additional notes.

6.3. Client editing

Editing a client is possible in client management after opening the edit form by clicking the icon `three dots`.

6.4. Deleting a client

Deleting clients is possible in client management by clicking on the `trash can` icon. When deleting, it is necessary to confirm the action in the modal window displayed afterwards. Only clients for which no assets, analyses or flows are recorded can be deleted.

6.5. Export of clients

Exporting clients is possible in the client management by clicking on the `Export` button and then selecting export type.
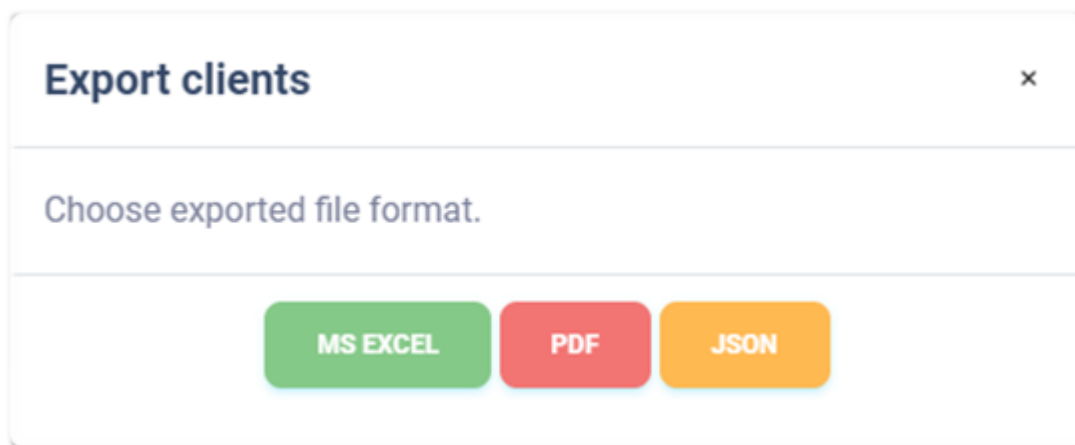
Export to MS Excel

Exporting clients to a Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export.
Name	Client's name.
Users	Number of registered users.
Active users	Number of registered active users.
Created at	Date of record created.
Creation time	Time of record created.
Created by	Email of user who created the record.
Modified	The date record was last modified.
Modification time	The time record was last modified.
Modified by	Email of user who made last changes.

Export to PDF

The clients export to PDF format contains a clients list similar to the listing in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Name	Client's name
Users	Number of registered users
Active users	Number of registered active users

Export to JSON

Exporting users to JSON format is available only for instance administrators. This type of export can only be used with an Enterprise license. The exported file can serve as a simple backup or can be used to create custom templates for bulk import.

6.6. Import clients

Bulk import of clients can be done in the client management via a modal form that is displayed to the user after clicking on the `Import` button.

To specify a bulk import of clients, a properly created data file must be ready. Only files in JSON format can be imported and the maximum size is limited to 5MB. Additionally, the uploaded file needs to be properly structured and to contain valid data. We recommend using the ready-made templates. The structure of a valid file with one valid record looks as follows:

```
[
    {
        "name": "Test Client"
    }
]
```

Parameter	Accepted values
name	Alphanumeric string with special symbols

It is possible to import clients simultaneously with their users. For this option, the following structure must be followed:

```json
{
    "name": "Test Client",
    "users": [
        {
            "first_name": "Jan",
            "last_name": "Novák",
            "email": "example1@riskflow.cz",
            "active": false,
            "lang": "en"
        },
        {
            "first_name": "Jana",
            "last_name": "Nováková",
            "email": "example2@riskflow.cz",
            "active": true,
            "lang": "cs"
        }
    ]
}
```

Parameter	Accepted values
name	Alphanumeric string with special symbols
first_name	Alphanumeric string with special symbols
last_name	Alphanumeric string with special symbols
email	Alphanumeric string with special symbols
active	true / false
lang	cs / en

Templates for bulk import of clients

Risk Flow prepares templates for its clients to create files intended to bulk import. These templates are publicly available at https://riskflow.cz/templates/. It is allowed to edit and use them for private and commercial purposes.

It is always a good idea to verify the integrity of downloaded files. This verification ensures that the file has not been corrupted or altered during the download. To verify the success of the download, we use an MD5 hash that can be found in the download table.

> 💡 **Tip**
>
> For instructions on how to verify the success of a downloaded file, please refer to the Templates for bulk user import section of this documentation.

Verification of the success of the specified import

Success of the specified bulk imports can be verified in the Log Entries module. This is available at `https://INSTANCE-NAME.riskflow.cz/cs/imports/logs` or it is possible to get to it through the modal window of bulk import forms.

By default, records are sorted by date and time the request was created and contain the following information - status, task name, detailed description of the action result, the user who made the request, name of the uploaded file and its size, and the date and time the request was created.

> 💡 **Tip**
>
> Detail of the provided information are described in section Import success verification of this documentation, dedicated to user managamenet.

6.7. Manage client's users

You can manage users of a specific client in the application `Client Management` -> `Client User Management`.

List of client's users

See the section List of users. The only difference is in the display of the user role and filtering options.

Adding client's users

See section Create a client's user.

Editing client's user

Editing of the client user is possible through the form available via the `three dots` icon next to the user record.

Activation and deactivation

Activation and deactivation is possible after opening the activation/deactivation form by clicking on the button in the status column. This button can be green or grey and also indicates the status of a particular user.

Setting preferred language for informative emails

Setting the preferred language for informative emails is possible while creating a user or editing an existing user. The change is possible in the edit form and currently you can choose between Czech and English.

Delete client's user

You can delete a client's user by clicking on the `trash can` icon. When deleting, it is necessary to confirm the action in the modal window displayed afterwards.

Export users of clients

Export users to Microsoft Excel workbook the following values. The language of the report is adapted by the currently used language of the application.
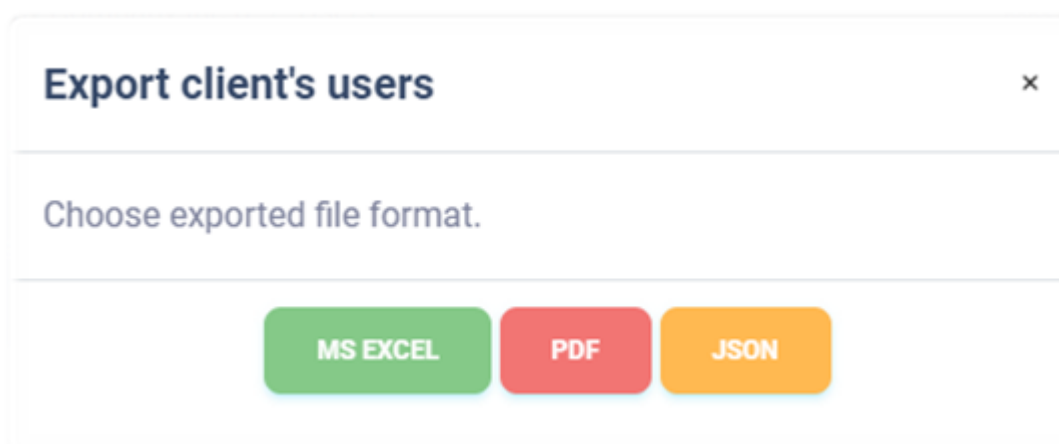
Export to MS Excel

Export users to Microsoft Excel workbook the following values. Language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client's name
Email	Username and contact email
First name	User's first name
Last name	User's last name
Status	Information about whether the user account is active or inactive.
Emails	Preferred language for informative emails
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date record was last modified.
Modification time	The time record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

Exporting client users to PDF format contains a list of users similar to the listing in the application. It contains the following information. The language of the report is adapted by the language currently used in the application.

Column name	Description
#	Record number in the export
Client	Client's name
Email	Username and contact email
First name	User's first name
Last name	User's last name
Status	Information about whether the user account is active or inactive.

Export to JSON

Exporting client users to JSON format is available only to instance administrators. This type of export can only be used with an Enterprise license. The exported file can be used as a simple backup or can be used to create custom templates for bulk user import.

Importing client's users

Bulk importing of users can be done in the user administration via a modal form that is displayed to the user after clicking on the `Import` button.

Import client's users

You can create records in bulk here. You need to have a json file created in the correct format. You can find detailed information in **documentation**.

Restrictions

- Only files up to 5MB can be uploaded.
- Only files in json format can be uploaded.

Notice

- Lines containing invalid values will be ignored. You can find information about the imports **here**.

JSON file: Browse… No file selected.

IMPORT ⬆

To specify a bulk import of clients, a properly created data file must be ready. Only files in JSON format can be imported and the maximum size is limited to 5MB. Additionally, the uploaded file needs to be properly structured and to contain valid data. We recommend using the ready-made templates at https://riskflow.cz/templates/. The structure of a valid file with one valid record looks following.

```json
[
    {
        "first_name": "Jan",
        "last_name": "Novák",
        "email": "example1@riskflow.cz",
        "active": false,
        "lang": "en"
    },
    {
        "first_name": "Jana",
        "last_name": "Nováková",
        "email": "example2@riskflow.cz",
        "active": true,
        "lang": "cs"
    }
]
```

Parameter	Accepted values
first_name	Alphanumeric string with special symbols
last_name	Alphanumeric string with special symbols
email	Alphanumeric string with special symbols
active	true / false
lang	cs / en

Templates for bulk import of client's users

Risk Flow prepares templates for its clients to create files intended to bulk import. These templates are publicly available at https://riskflow.cz/templates/. It is allowed to edit and use them for private and commercial purposes.

It is always recommended to verify the integrity of downloaded files. This verification ensures that the file has not been corrupted or altered during the download. To verify the success of the download, we use an MD5 hash that can be found in the download table.

> 💡 **Tip**
>
> A tutorial on how to perform this verification can be found in section Templates for bulk user import

Verification of the success of the specified import

Success of the specified bulk imports can be verified in the Log Entries module. This is available at `https://INSTANCE-NAME.riskflow.cz/imports/logs` or it is possible to get to it through the modal window of bulk import forms.

By default, records are sorted by date and time the request was created and contain the following information - status, task name, detailed description of the action result, the user who made the request, name of the uploaded file and its size, and the date and time the request was created.

> 💡 **Tip**
>
> Detail of the provided information are described in section Import success verification of this documentation, dedicated to user managamenet.

7. Asset management

Asset management is available to all Risk Flow users. Client users have access only to the groups and assets registered for them. Managers and administrators can see all asset groups and their assets and can simultaneously edit them. Users with an analyst or auditor role have read only access to all groups and their assets.

7.1. Clients

For users with the role of administrator, manager, analyst or auditor, a list of registered clients is displayed when you open asset management. In this list, you can find the total number of asset groups and the total number of recorded assets.

Export to MS Excel

Export the following values to a Microsoft Excel workbook. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client's name
Assets groups	Total number of asset groups
Assets	Total number of assets
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

The export to PDF format contains an inventory similar to the listing in the application. It contains the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client's name
Assets groups	Total number of asset groups
Assets	Total number of assets

7.2. Asset groups

After selecting a specific client, a list of its asset groups is displayed. For users with the role `client's user` this inventory will be displayed directly when accessing asset management. The list contains information about the name of the group, which must be unique within the client. There is also information about the number of assets entered and whether the group is active. Only assets from active groups can be used in risk analyses.
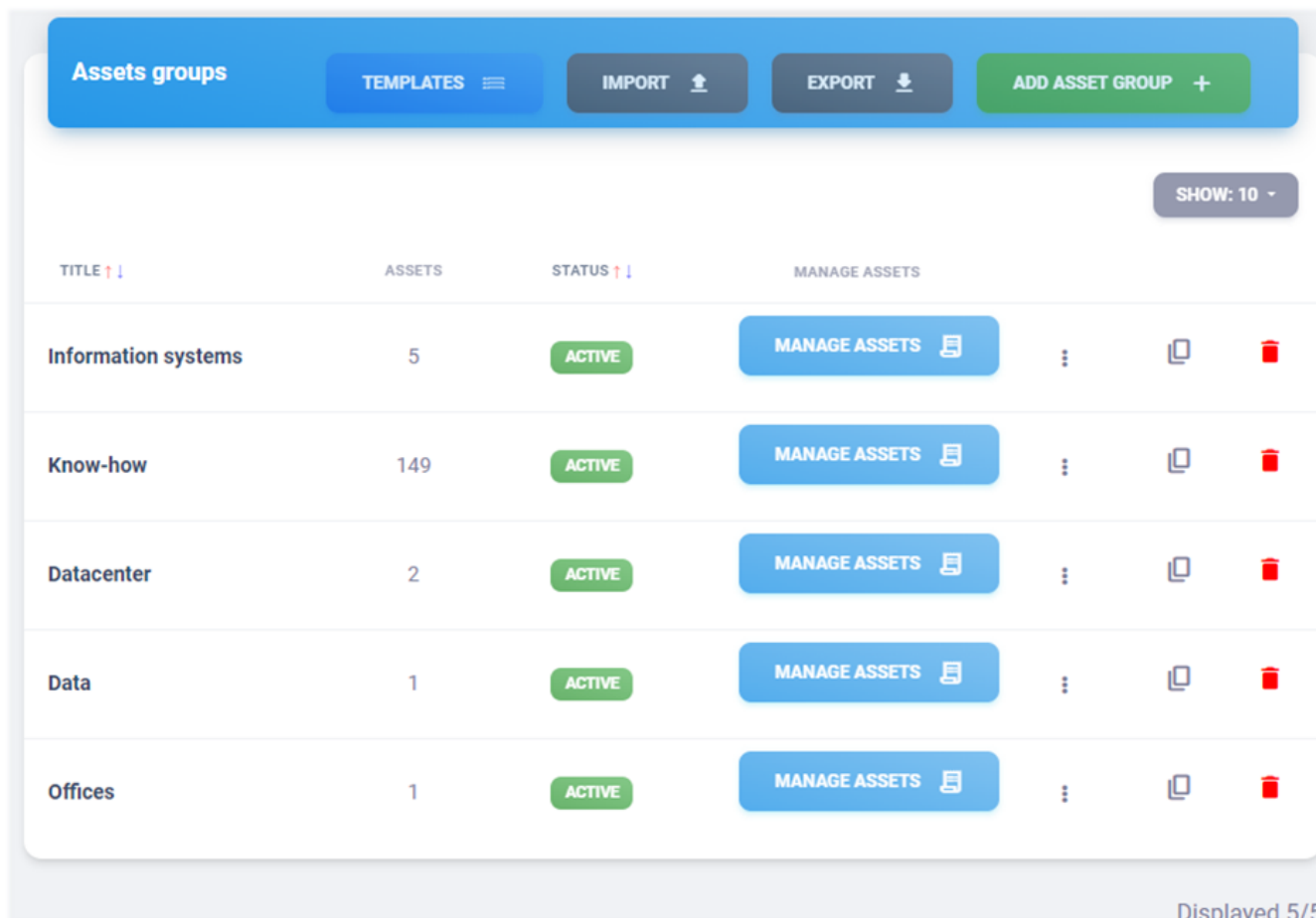
Adding asset group

The form for adding an asset group can be found at `https://INSTANCE-NAME.riskflow.cz/risks/assets/clients/` or after clicking on the "Add asset group" button.

Parameter	Required	Description
Group name	Yes	Name of the asset group. It must be unique withing the client.
Active	No	An asset group can only be used in the analysis if it is activated.

Creating a copy of an asset group

An authorised user can create copies of asset groups via the copy icon shown in the image below. During the copying process, copies are also created in the asset group of record.

TITLE ↑↓	ASSETS	STATUS ↑↓	MANAGE ASSETS			
Datacenter 1	149	ACTIVE	MANAGE ASSETS	⋮	▣	🗑

Editing and asset group

Editing an asset group is possible after opening the edit form by clicking the `three dots` icon.

Asset group activation and deactivation

Activation and deactivation is possible after opening the activation/deactivation form by clicking on the button in the status column. This button can be green or grey and also indicates the status of a particular asset group. Only assets from active groups can be further used for risk analysis.

Deleting an asset group

You can delete asset groups by clicking on the `trash can` icon. When deleting, it is necessary to confirm the action in the modal window displayed afterwards. Only groups with no assets used in risk analyses can be deleted.

Export of asset groups

Export of asset groups is possible in the asset management by clicking on the `Export` button and then selecting the export type.
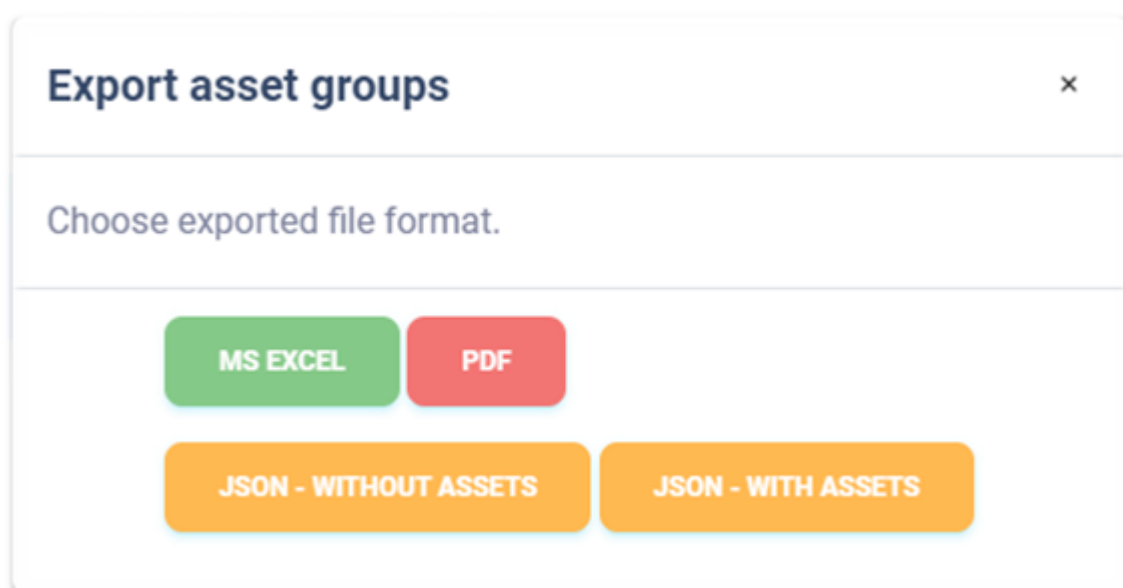
Export to MS Excel

Exporting asset groups of a specific client to a Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export
Title	Asset group name
Assets	Number of assets in the group
Status	Active / Inactive
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date record was last modified.
Modification time	The time record was last modified.
Modified by	Email of user who made last changes.

Export to PDF

Exporting asset groups of a selected client to PDF format contains a list of asset groups similar to the listing in the application. It contains the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Title	Asset group name
Assets	Number of assets in the group
Status	Active / Inactive

Export to JSON

Exporting asset groups to JSON format is only available to instance administrators. This type of export can only be used with an Enterprise license. The exported file can serve as a simple backup or can be used to create custom templates for bulk import.

Asset groups can be exported to JSON format in two ways:

- Without assets
- With assets

Import of assets groups

Bulk import of asset groups can be performed in the asset management of the selected client via a modal form that is displayed to the user after clicking on the `Import` button.

To specify a bulk import of users, a properly created data file must be prepared. Only JSON format files can be imported, and the maximum size is limited to 5MB. Additionally, the uploaded file needs to be properly structured and to contain valid data. We recommend using the ready-made templates at https://riskflow.cz/cs/templates/. The structure of a valid file with two records looks following.

```
[
    {
        "title": "Group 1",
        "active": true
    },
    {
        "title": "Group 2",
        "active": false
    }
]
```

Parameter	Accepted values
title	Alphanumeric string with special symbols
active	true / false

Asset groups can be imported in bulk together with the corresponding assets. For this option, you need to have a file ready for import in the following format.

```json
[
  {
    "asset_groups": [
      {
        "title": "Group 1",
        "active": true,
        "assets": [
          {
            "identifier": "AS1",
            "title": "Asset 1",
            "type": "primary",
            "short_description": "short description",
            "long_description": "detailed description",
            "owner": "Pokey Trippy",
            "guarantor": "Randy Sleepy",
            "availability": "low",
            "integrity": "high",
            "confidentiality": "critical"
          },
          {
            "identifier": "AS2",
            "title": "Asset 2",
            "type": "auxiliary",
            "short_description": "short description",
            "long_description": "detailed description",
            "owner": "Squirrely Baggy",
            "guarantor": "Cloudy Baggy",
            "availability": "critical",
            "integrity": "low",
            "confidentiality": "low"
          }
        ]
      }
    ]
  }
]
```

Parameter	Accepted values
asset_groups	Array of asset groups
active	True / false
assets	Array of assets in a particular group
identifier	It must be unique within the group. It can be empty. Alphanumeric string special symbols.
title	Alphanumeric string with special symbols
type	Primary / auxiliary
short_description	Alphanumeric string with special symbols
long_description	Alphanumeric string with special symbols, can be empty
owner	Alphanumeric string with special symbols
guarantor	Alphanumeric string with special symbols
availability	low / medium / high /critical
integrity	low / medium / high /critical
confidentiality	low / medium / high /critical

Templates for bulk import of client's users

Risk Flow prepares templates for its clients to create files for bulk import. These templates are publicly available at https://riskflow.cz/templates/. It is allowed to edit and use them for private and commercial purposes.

Verification of the success of the specified import

Success of the specified bulk imports can be verified in the Log Entries module. This is available at https://INSTANCE-NAME.riskflow.cz/imports/logs or it is possible to get to it through the modal window of bulk import forms

By default, records are sorted by date and time the request was created and contain the following information - status, task name, detailed description of the action result, the user who made the request, name of the uploaded file and its size, and the date and time the request was created.

> 💡 **Tip**
>
> Detail of the provided information are described in section Import success verification of this documentation, dedicated to user managamenet.

7.3. Assets

After selecting an asset group, a listing of the specific assets recorded in that group is displayed. Instance administrators, managers and client users can edit these assets. Analysts and auditors and can only view them. The assets created can be edited and their impact on availability, integrity and confidentiality can be assessed directly in this listing.

Creating an asset

The form to add an asset group can be found at `https://NAZEV-INSTANCE.riskflow.cz/cs/risks/assets/<ID KLIENTA>/groups/<ID SKUPINY>/assets/create` or by clicking on the `Add asset` button.

Parameter	Required	Description
Identification	Ne	Asset identification for better orientation. Must be unique within the asset group.
Title	Yes	Asset name
Asset type	Yes	• Primary – represents information or service processed or provided by an information and communication system. At the same time, these primary assets often create value for the organization. Examples of primary assets include data, information or services provided. • Auxiliary – represents technical assets, employees and contractors involved in the operation, development, administration or security of the information and communication system.
Short description	Yes	Brief description of the asset. It is displayed in the assets inventory.
Detailed description	No	Detailed description of the asset. It is displayed in the asset detail.
Asset owner	Yes	Identification of the person, organization or department that owns the asset.
Asset guarantor	Yes	The cybersecurity guarantor is a security role responsible for ensuring the development, usage and security of assets. An asset guarantor is also a person who promotes ensuring the confidentiality , availability and integrity of the asset of which it is the custodian. It is appropriate for the guarantor to control the assessment of the asset, as he/she is most familiar with it.

Edit asset

Editing the asset is possible after opening the edit form by clicking the `three dots` icon. It is also possible to edit assets directly in the listing of all assets. The availability, integrity and confidentiality of the asset is also evaluated in this listing. These three values are then used to calculate the final value of the asset, which is considered when calculating the value at risk in the analysis.

View asset details

Users who do not have the ability to edit assets can view a listing of assets and their details by clicking on the asset identifier or description. Users with editing rights can view the full asset detail in the edit form by clicking the `three dots` icon.

Availability

Availability of information means that the information, including the required information systems, must be accessible to any authorised person at any time and usable (functional) to the extent required. If the system fails or is not accessible, the requested information is not available. In certain cases, this can lead to disruptions with far-reaching consequences, for example in process maintenance. The Risk Flow provides the following scale for assessing availability.

Disruption of the availability of the asset is not important, and in the event of an outage, a longer time for correction is normally tolerated (approx. up to 1 week).

Disruption of the availability of the asset should not exceed the duration of a working day, a longer outage leads to a possible threat to the legitimate interests of the liable person.

Disruption of asset availability should not exceed a few hours. The outage must be resolved immediately. Assets are considered to be very important.

Disruption of asset availability is not permitted. Even short-term unavailability leads to a serious threat to the interests of the liable person. Assets are considered to be critical.

LOW   MEDIUM   HIGH   CRITICAL

Integrity

The technical term integrity is associated with several requirements:

- Unintentional changes to information must be impossible or at least detectable and traceable.
- The reliability of data and systems must be guaranteed.
- The completeness of the information must be guaranteed.

Risk Flow provides the following scale for assessing integrity.

The asset does not require integrity protection. Violation of the integrity of the asset does not threaten the legitimate interests of the obligee.

An asset may require integrity protection. Violation of the integrity of the asset may lead to damage to the legitimate interests of the liable party and may have less serious consequences.

The asset requires integrity protection. Violation of the integrity of the asset leads to damage to the legitimate interests of the obligee with substantial consequences.

The asset requires integrity protection. Violation of the integrity of the asset leads to very serious damage to the legitimate interests of the obligated person with direct and very serious impacts on the primary assets.

| LOW | MEDIUM | HIGH | CRITICAL |

Confidentiality

The aim is to protect confidential data from unauthorised access, whether on the grounds of data protection laws or on the grounds of commercial confidentiality, which is covered, for example, by the Trade Secrets Act. Therefore, the confidentiality of information and sensitive data is ensured if only persons who are authorised to access it have an access to it. Access means, for example, reading, editing or even deleting.

The measures taken must therefore ensure that only authorised persons have access to confidential information - unauthorised persons never. This also applies to information on paper, which may be lying unprotected on a desk and inviting to be read, or to the transmission of data that cannot be accessed in the course of processing.

Risk Flow provides the following scale for assessing confidentiality.

The assets are publicly available or have been intended to be publicly available. Violation of the confidentiality of assets does not threaten the legitimate interests of the obligated person. No protection required.

The assets are not publicly accessible and constitute the know-how of the liable party, asset protection is not required by any legal regulation or contractual agreement. Access control tools are used to protect confidentiality.

Assets are not publicly accessible and their protection is required by law, other regulations or contractual agreements (for example, trade secrets or personal data). Means of control and recording of access are used for protection. Information transmissions through communication channels are protected by cryptographic means.

The assets are not publicly accessible and require a higher level of protection than the previous category (for example, strategic trade secrets, special categories of personal data). To protect confidentiality, means are used to ensure control and logging of access. It also provides protection against abuse of assets by administrators. Information transmissions through communication channels are protected by cryptographic means.

| LOW | MEDIUM | HIGH | CRITICAL |

Value of the asset

The asset value is calculated from the specified availability, integrity and confidentiality values and is calculated as the maximum value of these monitored parameters.

```
Asset value = max(availability, integrity, confidentiality)
```

Value	Description
1	The asset is of low value to the organisation. This applies if all its factors are rated low.
2	The asset is of medium value to the organisation. This applies if it is at least one factor from the trio of accessibility, integrity, confidentiality rated medium.
3	The asset is of high value to the organisation. This applies if at least one factor of the triad of availability, integrity, confidentiality is rated high.
4	The asset is of critical value to the organisation. This applies if at least one factor of the triple of availability, integrity, confidentiality is rated critical.

Delete asset

You can delete assets by clicking on the `trash can` icon. When deleting, it is necessary to confirm the action in the modal window displayed afterwards. Only assets that are not used in risk analyses can be deleted.

Export assets

Export to MS Excel

Exporting assets to a Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export
ID	An asset identification
Short description	Brief description of the asset
Asset type	Primary / Auxiliary
Owner	Asset owner
Guarantor	Asset guarantor
Availability	Low / Medium / High / Critical
Integrity	Low / Medium / High / Critical
Confidentiality	Low / Medium / High / Critical
Asset value	1 / 2 / 3 / 4
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export do PDF

Exporting assets to PDF format contains an asset inventory similar to the listing in the application. It contains the following information. The report language is adapted by the language currently used in the application.

Column name	Description
#	Record number in the export
ID	An asset identification
Short description	Brief description of the asset
Asset type	Primary / Auxiliary
Owner	Asset owner
Guarantor	Asset guarantor
Availability	Low / Medium / High / Critical
Integrity	Low / Medium / High / Critical
Confidentiality	Low / Medium / High / Critical
Asset value	1 / 2 / 3 / 4

Export to JSON

Exporting assets to JSON format is only available to instance administrators. This type of export can only be used with an Enterprise license. The exported file can serve as a simple backup or can be used to create custom templates for bulk import.

Import of assets

Bulk import of assets can be performed in the asset management of the selected client via a modal form that is displayed to the user after clicking on the `Import` button.

Import assets

You can create records in bulk here. You need to have a json file created in the correct format. You can find detailed information in **documentation**.

Restrictions

- Only files up to 5MB can be uploaded.
- Only files in json format can be uploaded.

Notice

- Lines containing invalid values will be ignored. You can find information about the imports **here**.

JSON file: Browse… No file selected.

IMPORT

To specify a bulk import of assets, a properly created data file must be prepared. You can only import files in JSON format, the maximum size of which is limited to 5MB. It is also necessary that the uploaded file has the correct structure and contains valid data. We recommend using the templates available at https://riskflow.cz/templates/. The structure of a valid single record file is following.

```
[
    {
        "identifier": "A1",
        "title": "Asset 1",
        "type": "primary",
        "short_description": "short description",
        "long_description": "detailed description",
        "owner": "Pokey Trippy",
        "guarantor": "Randy Sleepy",
        "availability": "low",
        "integrity": "high",
        "confidentiality": "critical"
    }
]
```

Parameter	Accepted values
identifier	Alphanumeric string with special symbols
title	Alphanumeric string with special symbols
type	Primary / auxiliary
short_description	Alphanumeric string with special symbols
long_description	Alphanumeric string with special symbols
owner	Alphanumeric string with special symbols
guarantor	Alphanumeric string with special symbols
availability	low / medium / high / critical
integrity	low / medium / high / critical
confidentiality	low / medium / high / critical

Templates for bulk import of assets

Risk Flow prepares templates for its clients to create files for bulk import. These templates are publicly available at https://riskflow.cz/templates/. It is allowed to edit and use them for private and commercial purposes.

It is always recommended to verify the integrity of downloaded files. This verification ensures that the file has not been corrupted or altered during the download. To verify the success of the download, we use an MD5 hash that can be found in the download table.

> 💡 **Tip**
>
> A tutorial on how to perform this verification can be found in section Templates for bulk user import

Verification of the success of the specified import

Success of the specified bulk imports can be verified in the Log Entries module. This is available at `https://INSTANCE-NAME.riskflow.cz/imports/logs` or it is possible to get to it through the modal window of bulk import forms.

By default, records are sorted by date and time the request was created and contain the following information - status, task name, detailed description of the action result, the user who made the request, name of the uploaded file and its size, and the date and time the request was created.

> **💡 Tip**
>
> Detail of the provided information are described in section Import success verification of this documentation, dedicated to user managamenet.

8. Risk catalog

The risk catalog serves as a knowledge base, which users subsequently use when processing risk analyses and risk treatment plans. It contains data, which are subsequently automatically suggested to users for completion in relevant forms, thus making their work in the system more efficient. In addition to the catalog supplied by Risk Flow, users have the opportunity to build and develop their own catalog, thanks to the ability to add their own texts when performing actions in the application.

8.1. View catalog

After going to the `Risk catalog` module, user will see a list of all available texts. Distribution of permissions in this case is as follows:

Role	Rights
Admin	Full rights.
Manager	Read-only rights and ability to use catalog knowledge in forms.
Analyst	Read-only rights and ability to use catalog knowledge in forms.
Client	No rights.
Auditor	Read-only rights.

The risk catalog is used to store knowledge that is subsequently used in the creation of risk analyses and risk treatment plans. During their processing, Risk Flow suggests values from this catalog, and thus Risk Flow facilitates work in the system. The basic Risk Flow catalog can be expanded during processing of risk analyses and risk treatment plans, in such a way that the user in the form of adding or editing lines of the analysis or plan allows the addition of the processed data to this catalog. You can thus build your own risk catalog. The catalog contains only unique records and only instance administrators has the right to edit it.

There is a minimal Risk Flow catalog on this demo instance.

8.2. Add text to the catalog

Text can be added to the catalog by clicking the `Add record` button or by opening `https://NAME-INSTANCE.riskflow.cz/en/risks/catalog/create`.

| Parameter	Required	Description
Type	Yes	Risk / Threat / Vulnerability / Measures / Description of measures / Goals and benefits / Metrics for evaluation
Text	Yes	The text, which must be unique in combination with the type within the catalog.
Active	No	Only active texts will be suggested to users when filling out the appropriate forms.

8.3. Edit text in catalog

Text editing is possible in the update form, which the administrator can open in the list via the "three dots" icon.

8.4. Delete text from the catalog

Deletion is possible in the list of available texts in the catalog. An authorized user can delete any texts. Texts are not tied to already existing data, they are only used in the `help` when processing the appropriate forms.

8.5. Export

Export is possible in the appropriate module by clicking on the `Export` button.
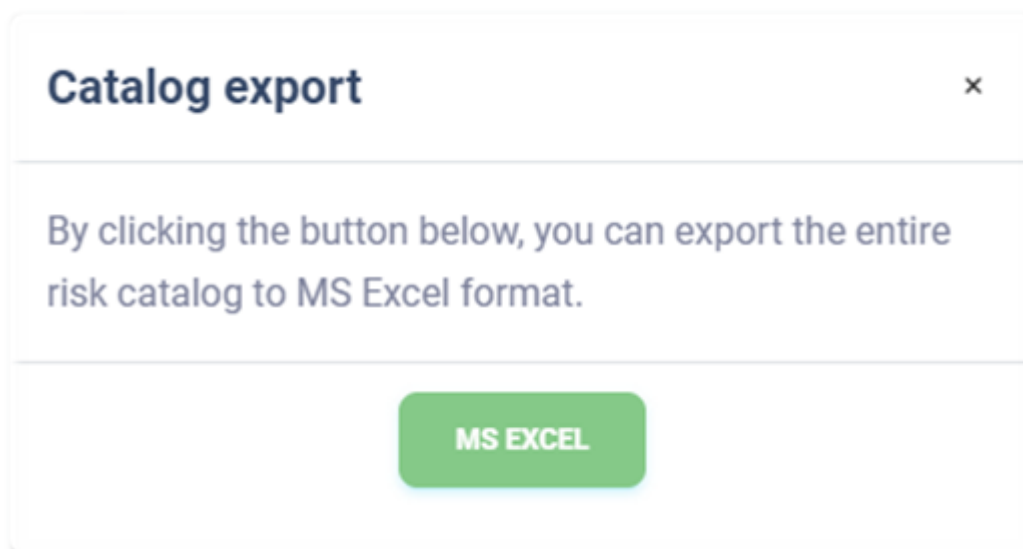
Export to MS Excel

Exporting a risk catalog to a Microsoft Excel workbook has the following values. The report language adapts to the currently used application language.

Column name	Description
ID	Identifier of the text in the catalog
Text	Text
Type	Risk / Threat / Vulnerability / Measures / Description of measures / Goals and benefits / Metrics for evaluation
Active	Yes / No
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

8.6. Import catalog

Bulk import of the catalog can be done in the appropriate module after opening the catalog import form. The import also serves as an update of an already existing catalog. The Risk Flow team regularly updates and delivers its current risk catalog to clients. Contact Risk Flow support or your contact person to obtain current data.

Verification of the success of the specified import

Success of the specified bulk imports can be verified in the Log Entries module. This is available at `https://INSTANCE-NAME.riskflow.cz/imports/logs` or it is possible to get to it through the modal window of bulk import forms.

By default, records are sorted by date and time the request was created and contain the following information - status, task name, detailed description of the action result, the user who made the request, name of the uploaded file and its size, and the date and time the request was created.

> 💡 **Tip**
>
> Detail of the provided information are described in section Import success verification of this documentation, dedicated to user managamenet.

9. Risk analyses

Supporting the execution of risk analysis is the most important feature of the Risk Flow platform. This module describes in detail the used methodology.

9.1. View a list of risk analyses

After navigating to the `Analyses` module, the user is presented with a list of all risk analyses to which they have rights to access. The distribution of permissions in this case is as follows:

Admin	Has rights to see and edit all available unfinished analyses.
Manager	He has rights to see and edit the risk analyses, that he has created and to which he has been assigned by the administrator. A user with the manager role also has all the privileges of an analyst.
Analyst	Has the rights to perform the risk analysis, to which he is assigned. Does not have rights to edit risk analysis parameters but can edit analysis lines and request manager approval. Can add comments.
Client	Has the rights to view and comment on the risk analyses that have been created for his Company.
Auditor	Has read-only access to all sections, can add comments.

9.2. Create risk analysis

It is possible to create a risk analysis on the Risk Flow platform by clicking on the button `Start a new analysis` or by opening `https://NAZEV-INSTANCE.riskflow.cz/cs/analysis/create`.

Parameter	Required	Description
Client	Yes	Selecting client for whom the risk analysis will be performed.
Analysis title	No	Title of the risk analysis. It is used for better orientation in the system.
Responsible	Yes	Only users with the `Risk Manager` role manager can be selected. Only active users can be selected. If a user with the role `Risk manager` is creating a risk analysis, he is automatically assigned to it.
Risk analysts	No	Users with the role `Risk manager` or `Risk Analyst`. Only active users can be selected. Multiple analysts can be assigned to collaborate on the analysis.
Deadline	Yes	Setting a deadline to resolve. Cannot be set in the past or at today's date.
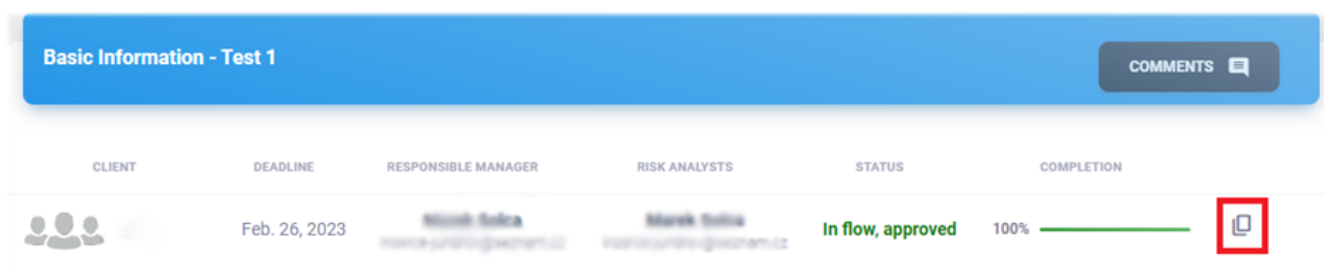
After successful creation of the risk analysis, the assigned analysts and manager are notified by email. The user who triggered the action does not receive an informational email, i.e., if the manager creates the analysis, he does not receive an informational email about the assignment to the risk analysis. In this way, Risk Flow tries to minimize the number of informational emails.

9.3. Edit risk analysis

Editing the risk analysis is possible in the update form, which the user can open in the list analyses via the `three dots` icon or in the risk analysis detail via the `Edit` button.

9.4. Copying risk analysis

A user with editing rights to a specific risk analysis can create copies of it. When copying a risk analysis, the same parameters must be set as in time of creating a new risk analysis. In this process, all rows of the risk analysis are duplicated. This feature is very useful when revising previously completed risk analyses. Copying a risk analysis can be done via the `copy` icon in the list of all available risk analyses or in the details of a specific risk analysis. The responsible manager and analysts are notified by email of the assignment to the analysis.

9.5. Delete risk analysis

You can delete a risk analysis in the list of available risk analyses or in the details of a specific analysis. An authorized user can delete those risk analyses that are not part of any approval processes.

9.6. Export risk analyses

Export of analyses is possible in the appropriate module by clicking on the `Export` button and selecting the export type.
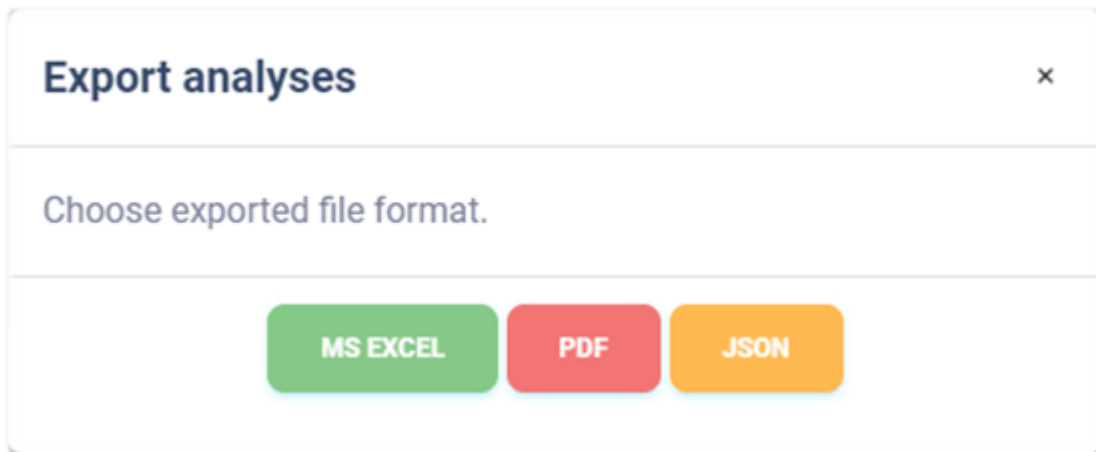
Export to MS Excel

Exporting a list of risk analyses to a Microsoft Excel workbook has the following values. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client name
Deadline	Deadline date
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the risk analysis.
Analysts	List of users with the role `Risk analysts` who are/were involved in performing risk analysis.
Stav	**Established** - analysis has been established, not yet in progress. **In progress** - analysis is being processed. **Waiting for approval** - the analysis has been completed and is awaiting approval by the responsible manager. **Approved** - analysis is completed and approved by the responsible manager. **Not approved** - analysis is completed, but not yet approved by the responsible manager, returned for refinement. **In Flow** - completed and approved risk analysis as part of the approval process. **In Flow, not approved** - completed analysis that was returned by the client as part of the approval process to be completed. **In Flow, approved** - risk analysis completed, approved by the responsible manager and the relevant client.
Completion	Analysis progress expressed in %.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

Exporting the analysis list to PDF format contains a list similar to the list in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client name
Deadline	Deadline date
Responsible manager	A user with the role of "Risk Manager" who is responsible for completing the risk analysis.
Analysts	List of users with the role "Risk analysts" who are/ were involved in performing risk analysis.
Stav	**Established** - analysis has been established, not yet in progress. **In progress** - analysis is being processed. **Waiting for approval** - the analysis been completed and is awaiting approval by the responsible manager. **Approved** - analysis is completed and approved by the responsible manager. **Not approved** - analysis is completed but not yet approved by the responsible manager, returned for refinement. **In Flow** - completed and approved risk analysis as part of the approval process. **In Flow, not approved** - completed analysis that was returned by the client part of the approval process to be completed. **In Flow, approved** - risk analysis completed, approved by the responsible manager and the relevant client.
Progress	Analysis progress expressed in %.

Export to JSON

Exporting assets to JSON format is available only to instance administrators. This type of export can only be used with an Enterprise license. The exported file can serve as a simple backup or can be used to import into third-party applications.

9.7. Risk analysis detail

Authorized persons may consult the risk analyses available to them. The administrator or responsible persons can add and edit risk analysis rows. Users with edit permissions can edit not yet approved risk analyses directly in the risk analysis detail, just as asset management works.

Adding risk analysis row

The form for adding risk analysis row can be found at `https://INSTANCE-NAME.riskflow.cz/en/analysis/<ANALYSIS ID>/row/create` or by clicking on the `Add Row` button.

In this form, you can take advantage of the Risk Flow catalog, from which specific texts describing risks, threats and vulnerabilities can be drawn. Searching the catalog works after entering at least three characters and its use is demonstrated in the following image.

Use of the risk catalog is possible in this form for the following fields – Risk description, Threat, Vulnerability.

Managers and analysts can add to the risk catalog by leaving the `Add to risk catalog` box checked. The catalog can be used by all managers and analysts for all risk analyses, and therefore texts specific to the client being processed should not be added to the catalog. Only the instance administrator has rights to edit the catalog.

Parameter	Required	Description
Identification	Ne	The identifier is used to improve user orientation in the system. It is limited to 10 characters.
Asset group	Yes	To select an asset, you must first select an asset group. This list is filtered to show only the asset groups of the respective client.
Asset	Yes	Selection of the asset to which the recorded risk applies. Can only be selected after selecting the asset group. This list is filtered to show only the assets of the selected group. In risk analysis it is only possible to use assets, which are fully evaluated in terms of availability, integrity and confidentiality.
Risk description	Yes	Brief description of the risk recorded – for example, leakage of sensitive information, infiltration of the system or application, unavailability of services, etc.
Detailed description of the risk	No	Detailed description of the recorded risk.
Threat	Yes	A threat exploits the vulnerability of an asset and can cause damage or disruption to it. Threats can be, for example, natural disasters, accidents, social phenomena, economic phenomena or individual behavior. It is always necessary to consider the threats relevant to the asset and the context of the organization.
Detailed threat description	No	Detailed description of the threat.
Vulnerability	Yes	A vulnerability is a weakness (lack) of an asset or a weakness (lack) of a security measure that can be exploited by one or more threats.
Detailed description of vulnerability	No	Detailed description of the vulnerability.

| Measure | No | A method of protecting an asset to mitigate the magnitude of risk. |

Edit analysis row

An authorized user can edit risk analysis rows directly in the risk analysis detail or in the detail of the specific row after opening the respective form by clicking on the `three dots` icon. It is possible to use the advantages of the Risk Flow catalog, as when adding an analysis line.

Delete analysis row

An authorized user can delete rows of a risk analysis not yet approved directly in the detail of the risk analysis of a specific line after opening the relevant form by clicking on the `trash bin` icon and then confirming in the modal window.

Evaluation

Only assets that are fully rated for availability, integrity and confidentiality in asset management can be used in risk analysis. To calculate the risk value of an analysis line, three values are required - asset value, threat value, vulnerability value. Since the asset value is calculated by creating and rating the asset in asset management, the threat and vulnerability values remain to be defined in this step.

The value at risk is calculated as follows:

`RISK = ASSET x THREAT x VULNERABILITY`

Threat assessment

Risk Flow uses the following scale to assess threats.

The threat does not exist or is unlikely. The expected realization of the threat is not more frequent than once every five years.

The threat is unlikely to probable. The expected realization of the threat is in the range from 1 year to 5 years.

The threat is probable to very probable. The expected realization of the threat ranges from 1 month to 1 year.

The threat is very likely or nearly certain. The expected realization of the threat is more frequent than once a month.

| LOW | MEDIUM | HIGH | CRITICAL |

Vulnerability assessment

Risk Flow uses the following vulnerability rating scale.

Vulnerability does not exist or exploitation of vulnerabilities is unlikely. Security measures are in place that are able to detect potential vulnerabilities or possible attempts to exploit them in time.

The exploitation of the vulnerability is unlikely to probable. Security measures are implemented, the effectiveness of them is regularly checked. The ability of the security measures to detect possible vulnerabilities in time or possible attempts to overcome the measures is limited. No successful attempts to overcome the security measures are heard.

Exploitation of the vulnerability is likely to very likely. Security measures are in place, but their effectiveness does not cover all necessary aspects and is not regularly checked. Partial attempts to overcome security measures are known.

The exploitation of the vulnerability is very likely or nearly certain. Security measures are not implemented or their effectiveness is greatly limited. There is no control of the effectiveness of security measures. There are known successful attempts to overcome security measures.

LOW   MEDIUM   HIGH   CRITICAL

Risk calculation and acceptance

When all the necessary data is defined for an analysis row, Risk Flow calculates the risk value. This is an integer falling in one of the following ranges.

1-11 - The risk is considered acceptable.

12-32 - The risk can be reduced by less demanding measures, or in the case of more demanding measures, the risk is acceptable.

33-46 - The risk is unacceptable in the long term and systematic steps must be taken to mitigate it.

47-64 - The risk is unacceptable and steps must be taken to mitigate it immediately.

Risk may or may not be accepted. It is based on the final risk assessment and the scale is defined as follows.

1-32 - Risk is accepted

33-64 - Risk not accepted

Exporting risk analysis details

Export of risk analysis details is possible by clicking on the `Export` button and then selecting the type exports.

Export to MS Excel

Exporting the risk analysis detail to a Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export.
ID	The identifier is used to improve user orientation in the system.
Risk desc.	Brief description of the risk recorded - for example, leakage of sensitive information, infiltration of the system or application, unavailability of services, etc.
Detailed description of the risk	Detailed description of the recorded risk.
Asset	Selection of the asset, to which the recorded risk applies. Can only be chosen after selecting the asset group. This list is filtered to show only the assets of the selected group. Only assets that are fully rated for availability, integrity and confidentiality in asset management can be used in risk analysis. In risk analysis it is only possible to use assets, which are fully evaluated in terms of availability, integrity and confidentiality.
Asset value	1 / 2 / 3 / 4
Threat	A threat exploits the vulnerability of an asset and can cause damage or disruption to it. Threats can be, for example, natural disasters, accidents, social phenomena, economic phenomena or individual behavior. It is always necessary to consider other threats relevant to the asset and the context of the organization.
Detailed threat description	Detailed threat description.
Value	Low / Medium / High / Critical
Vulnerability	A vulnerability is a weakness (lack) of an asset or a weakness (lack) of a security measure that can be exploited by one or more threats.
Detailed description of the vulnerability	Detailed description of the vulnerability.
Value	Low / Medium / High / Critical
Risk	Calculated risk value, a number from the interval <1, 64>.
Accepted	Yes / No

Measure	A method of protecting an asset to mitigate the magnitude of risk.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date the record was last modified.
Modification time	The time the record was last modified.
Modified by	Email of user who made last changes.

Export to PDF

Exporting the risk analysis details to PDF format contains a list similar to the listing in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
ID	The identifier is used to improve user orientation in the system.
Risk desc.	Brief description of the risk recorded - for example, leakage of sensitive information, infiltration of the system or application, unavailability of services, etc.
Asset	Selection of the asset, to which the recorded risk applies. Can only be selected after selecting the asset group. This list is filtered to show only the assets of the selected group. Only assets that are fully rated for availability, integrity and confidentiality in asset management can be used in risk analysis. In risk analysis it is only possible to use assets, which are fully evaluated in terms of availability, integrity and confidentiality.
Asset value	1 / 2 / 3 / 4
Threat	A threat exploits the vulnerability of an asset and can cause damage or disruption to it. Threats can be, for example, natural disasters, accidents, social phenomena, economic phenomena or individual behaviour. It is always necessary to consider other threats relevant to the asset and the context of the organization.
Value	Low / Medium / High / Critical
Vulnerability	A vulnerability is a weakness (lack) of an asset or a weakness (lack) of a security measure that can be exploited by one or more threats.
Value	Low / Medium / High / Critical
Risk	Calculated risk value, a number from the interval <1, 64>.
Accepted	Yes / No
Measure	A method of protecting an asset to mitigate the magnitude of risk.

Export to JSON

Exporting risk analysis rows to JSON format is only available to instance administrators. This type of export can only be used in the Enterprise license. The exported file can serve as a simple backup or can be used to import into third-

party applications.

9.8. Risk analysis approval

Once all risk analysis lines have been completely evaluated and the risk analysis progress parameter shows a value of 100%, the analysis can proceed to approval.

Request for approval of completed risk analysis

A user with the role of manager or analyst can submit a request for approval of an analysis. The responsible manager is notified of the request by email and prompted to take action.

Approval or return for refinement

Approval of implementation is made by the responsible manager of the specific analysis. Once an analysis is approved, it is locked for editing and can be further used in approval flows. Until the analysis is approved by the responsible manager, it can be further edited. As long as the analysis is not part of an approval flow, the responsible manager can withdraw his approval and return the analysis to the analysts for refinement.

9.9. Comments

View comments

Authorized users can add comments to all risk analyses. All comments can be viewed by clicking on the `Comments` button, which opens a page with a list of existing comments and a form to add a new one.

Adding comment

You can add a comment after filling in the appropriate field for entering the text of the comment and submitting it by clicking the `Add comment` button.

Internal and public comments

Users can add internal and public comments. Internal comments are not displayed to the clients for whom the risk analysis is processed. Administrators, managers, analysts and auditors can see all registered comments and attachments.

Attachments

You can add attachments to each comment. To select multiple attachments, hold down the CTRL key and left-click to select multiple files to upload, or select all files to upload and drag them with the mouse into the file upload box.

10. Risk treatment plans (RTP)

The follow-up document to a risk analysis is the risk treatment plan (abbreviated as RTP). This is a document containing the objectives and benefits of security measures for managing individual unaccepted risks, the designation of the person ensuring the enforcement of security measures for risk management, the necessary financial, technical, human and information resources, the date of their implementation, a description of the links between risks and relevant security measures and the method implementation of security measures.

Security measures are implemented in accordance with this risk treatment plan. Documents based on the risk assessment, including the risk assessment itself, must be regularly updated and must take into account not only significant changes, but also changes in the scope of the ISMS, measures according to § 11 ZKB and cyber security incidents, including previously resolved ones.

10.1. List of risk treatment plans

After going to the `Risk treatment plans` module, user will be presented with a list of all the plans to which they have access rights. The distribution of permissions in this case is as follows:

Role	Rights
Admin	Has rights to see and edit all available unfinished plans.
Manager	He/she has rights to see and edit the plans he/she created and assigned to by the administrator. A user with the manager role also has all permissions as an analyst.
Analyst	He/she has rights to participate in the creation of plans to which he/she has been assigned. He/she does not have the right to edit plans parameters, but can edit rows of plans and request approval from the manager. Can add comments.
Client	Client has rights to view and comment on plans that have been created for his/her company.
Auditor	Has read access to all sections, can add comments.

10.2. Create new RTP

Creating an RTP on the Risk Flow platform is possible by clicking on the `New risk treatment plan` button or by opening `https://INSTANCE-NAME.riskflow.cz/en/risks/risk-plan/create`.

Parameter	Required	Description
Client	Yes	Selects the client for which the RTP will be processed.
Analysis	Yes	Selection of a completed and manager approved risk analysis for which a risk treatment plan will be prepared.
Type	Yes	Choose from the following options: • import from the analysis only risks that have been marked as unacceptable, • import all risks from the analysis.
Title	No	Name of risk treatment plan. It serves for better orientation.
Responsible manager	Yes	Only users with the `Risk Manager` role can be selected. Only active users can be selected. If the risk analysis is created by a user with the role `Risk manager`, he is automatically assigned to it.
Risk analysts	No	Only users with the role `Risk manager` or `Risk analyst` can be selected. Only active users can be selected. Multiple analysts can be assigned to collaborate on RTP processing.
Deadline	Yes	Setting a deadline to resolve. It cannot be set to the past or to today's date.

Upon successful creation of a risk treatment plan, assigned analyst and manager are notified by email. The information email will not be sent to the user who triggered the action, i.e. if the plan is created by a manager, he/she will not receive an informational email about being assigned to the plan. In this way, Risk Flow tries to minimize the amount of informational emails.

10.3. Edit RTP

Editing of plans is possible in the update form, which the user can open in the RTP list via the `three dots` icon or in the details of the risk management plan via the `Edit` button.

10.4. Copy RTP

A user with edit rights to a specific RTP can create copies of it. When copying, it is necessary to set the same parameters as when establishing a new risk management plan. All RTP rows are duplicated in this process. This feature is very useful when performing revisions of previously completed RTPs. Copying is possible via the `copying` icon in the list of all available RTPs or in the detail of a specific RTP. The responsible manager and analysts are informed by email about the assignment to RTP.

10.5. Delete RTP

RTP deletion is possible in the list of available plans or in the detail of a specific risk treatment plan. An authorized user can delete plans that are not part of any approval processes.

10.6. Export RTP

Plans can be exported in the appropriate module by clicking on the `Export` button and selecting the type of export.

Export do MS Excel

Export of risk treatment plans to a Microsoft Excel sheet has the following structure. Language of the export is set according to the user's language settings.

Column	Description
#	Record number in the export
Client	Client's name
Deadline	Date
Title	Title of the risk treatment plan
Responsible manager	A user with the role `Risk Manager` who is responsible for completing the RTP.
Analysts	List of users with the role `Risk Analysts` who participate/participated in the creation of the plan.
Stav	**Started** - the plan has been established, it is not yet in progress. **In Progress** – The plan is being processed. **Waiting for approval** - The plan has been completed and is awaiting approval by the responsible manager. **Approved** – the plan has been and approved by the responsible manager. **Not approved** - plan completed but not yet approved by responsible manager, returned for revision. **In Flow** – a completed and approved risk treatment plan that is part of the approval process. **In Flow, not approved** – a completed plan that was returned by the client for revision as part of the approval process. **In Flow, Approved** – Completed plan, approved by both responsible manager and relevant client.
Completion	Plan completion progress expressed in %.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date the record was last modified.
Modification time	The time the record was last modified.
Modified by	Email of user who made last changes.

Export do PDF

The schedule list export to PDF format contains an inventory similar to the listing in the application. It contains the information below. The report language adapts to the currently used application language.

Column	Description
#	Record number in the export
Client	Client's name
Deadline	Date
Title	Title of the risk treatment plan
Responsible manager	A user with the role `Risk Manager` who is responsible for completing the RTP.
Analysts	List of users with the role `Risk Analysts` who participate/participated in the creation of the plan.
Stav	**Started** - the plan has been established, it is not yet in progress. **In Progress** - The plan is being processed. **Waiting for approval** - The plan has been completed and is awaiting approval by the responsible manager. **Approved** – the plan has been completed and approved by the responsible manager. **Not approved** - plan completed but not yet approved by responsible manager, returned for revision. **In Flow** – a completed and approved risk treatment plan that is part of the approval process. **In Flow, not approved** - a completed plan that was returned by the client for revision as part of the approval process. **In Flow, Approved** – Completed plan, approved by both responsible manager and relevant client.
Completion	Plan completion progress expressed in %.

Export do JSON

Exporting plans to JSON format is only available to instance administrators. This type of export can only be used in the Enterprise license. The exported file can serve as a simple backup or can be used to import into third-party

applications.

10.7. RTP detail

Authorized users can view the risk treatment plans available to them. Administrator or responsible persons can add and edit row. Users with edit permission can edit plans that have not yet been approved directly in its detail, just as asset management works.

Adding rows

When a new risk treatment plan is created, all unacceptable risks from the relevant risk analysis are automatically imported to it, or also acceptable ones depending on the type of risk treatment plan being created. Acceptable risks can be added and removed from the plan. Unacceptable risks cannot be omitted from the risk management plan.

The form for adding a risk can be found at `https://INSTANCE-NAME.riskflow.cz/cs/risks/risk-plan/\<ID RTP\>/row/create/` or by clicking the `Add to plan` button. In this form, you can take advantage of the Risk Flow catalog, from which you can draw specific texts describing measures, their goals and benefits, and evaluation metrics. Searching the catalog works after entering at least three characters and its use is demonstrated in the following image.

Parameter	Required	Description
Risk analysis row	Yes	Selection of the risk of the relevant risk analysis for which th security measures will be proposed.

Edit RTP row

An authorized user can edit the rows of the plan directly in its detail or in edit form of a specific row. In this form, you can take advantage of the Risk Flow catalog, from which you can draw specific texts describing measures, their goals and benefits, and evaluation metrics. Searching the catalog works after entering at least three characters and its use is demonstrated in the following image.

Use of the risk catalog is possible in this form for the following fields – Measures, Description of measures, Objectives and benefits, Metric for evaluation.

Managers and analysts can add to the risk catalog by leaving the `Add to risk catalog` box checked. The catalog can be used by all managers and analysts for all risk analyses, and therefore texts specific to the client being processed should not be added to the catalog. Only the instance administrator has rights to edit the catalog.

Parameter	Required	Description
Identification	Yes	Identifier to improve orientation in the system.
Measure	Yes	Name of the security measure.
Measure description	Yes	Detailed description of the proposed security measure.
Goals and benefits	Yes	List of what the implementation of the measure will achieve.
Responsible manager	Yes	Person, department, or company responsible for implementing the security measure.
Implementation deadline	Yes	Deadline for the implementation of measure.
Technical sources	Yes	Inventory of necessary equipment, space, etc., required to successfully implement the measure.
Financial sources	Yes	Estimate of the financial cost of implementing measure.
Human sources	Yes	Estimation of the time required toimplement measures (e.g. MD - man-days)
Evaluation metric	Yes	Definition of a measurable way to verify the effectiveness of the applied security measure.

Delete RTP row

An authorized user can delete the rows of a plan not yet approved directly in its detail in the detail of a specific row after opening the relevant form by clicking on the `trash can` icon and then confirming in the modal window.

10.8. RTP approval

Once all the lines are completely filled in and the risk treatment plan completion shows a value of 100%, the plan can proceed for approval.

Request for completed RTP approval

A user with a manager or analyst role can submit an RTP approval request. The responsible manager is notified of the request by email and invited to take action.

Approval or return for completion

Approval is done by the responsible manager of the specific plan. Once the plan is approved, it is locked for editing and can be further used in approval flows. Until the plan is approved by the responsible manager, it is possible to edit it further. As long as the plan is not part of the approval flow, the responsible manager can withdraw his approval and return the plan to the analysts for further development.

10.9. Comments

Authorized users can add comments to plans. All comments can be viewed by clicking on the `Comments` button, which opens a page with a list of existing comments and a form for adding a new one.

Add comment

It is possible to add a comment after filling in the appropriate field for entering the text of the comment and sending it with the `Add comment` button.

Internal and public comments

Users can add internal and public comments. Internal comments are not displayed to clients for whom a risk treatment plan is being processed. Administrators, managers, analysts and auditors can see all recorded comments and attachments.

Attachments to comments

Attachments can be added to each comment. To select multiple attachments, hold down the CTRL key and left-click to select multiple files to insert, or select all files to upload and drag them to the file upload field.

11. Flows

Flows represent processes that the Risk Flow platform can effectively help users with. The application can work with two types of flows - approval and audit. Their principles will be described in detail in this chapter.

11.1. View list of flows

After navigating to the `Flows` module, the user will be presented with a list of all the flows they have rights to access. The distribution of permissions in this case is as follows:

Role	Rights
Admin	Rights to see all flows and edit all available flows.
Manager	Rights to see and edit the flows that he created and to which he has been assigned by the administrator.
Analyst	Rights to rights this section of the application.
Client	Rights to view and to comment on flows that have been created for his company.
Auditor	Read-only rights to all sections, can add comments. Participates in the processing of audit flows.

11.2. Start new flow

You can start a flow on the Risk Flow platform by clicking on the `Start new flow` button and then selecting the type - approval or audit. In both cases, the same parameters are needed to start a new flow, which are described in the following table.

Parameter	Required	Description
Client	Yes	Selecting the client for whom the flow will be processed.
Flow title	No	Is used for better orientation in the system.
Responsible manager	Yes	Only users with the `Risk Manager` role can be selected. Only active users can be selected. If a flow is created by a user with the `Risk manager` role, this user is automatically assigned.
Deadline	Yes	Setting a deadline to finish flow. Cannot be set with the past or today's date.

After a successful flow creation, users assigned to it are notified by an email. In the case of an approval flow, the assigned manager and the clients for whom the flow was created are notified. In the case of an audit flow, all active users with the `Auditor` role are notified about its creation. The informational email does not come to the user who triggered the action, i.e. if a manager creates the analysis, he does not receive an informational email about the assignment to the risk analysis. In this way, Risk Flow tries to minimize the amount of informational emails.

11.3. Edit flow

Editing the flow is possible via the update form, which can be opened by an authorized user in the list flows via the `three dots` icon or in the risk analysis detail through the `Edit` button.

11.4. Copy flow

A user with editing rights to a specific flow can create copies of it. When copying a flow, the same parameters are set as while creating a new one. In this process, all flow rows are duplicated. This feature is very useful when revising previously completed flows. You can copy a flow via the `copy` icon in the list of all available flows or in the details of a specific flow. The responsible persons are informed when a new flow is created. In the case of an approval flow, the assigned manager and the clients for whom the flow is being processed are notified of its creation. In the case of an audit flow, all active users with the `Auditor` role are notified of its creation. An informational email is not sent to the

user who triggered the action, i.e. if the analysis is created by a manager, he does not receive an informational email about the assignment to the risk analysis. In this way, Risk Flow tries to minimize the amount of informational emails.

11.5. Delete flow

Deleting a flow is possible in the list of available flows or in the details of a specific flow. To preserve the audit trail, it is possible to delete only:

- Approval flows – which are not yet approved by the client.
- Audit flows - which audit has not been completed.

11.6. Export flows

Exporting flows is possible in the appropriate module by clicking on the `Export` button and selecting the export type.
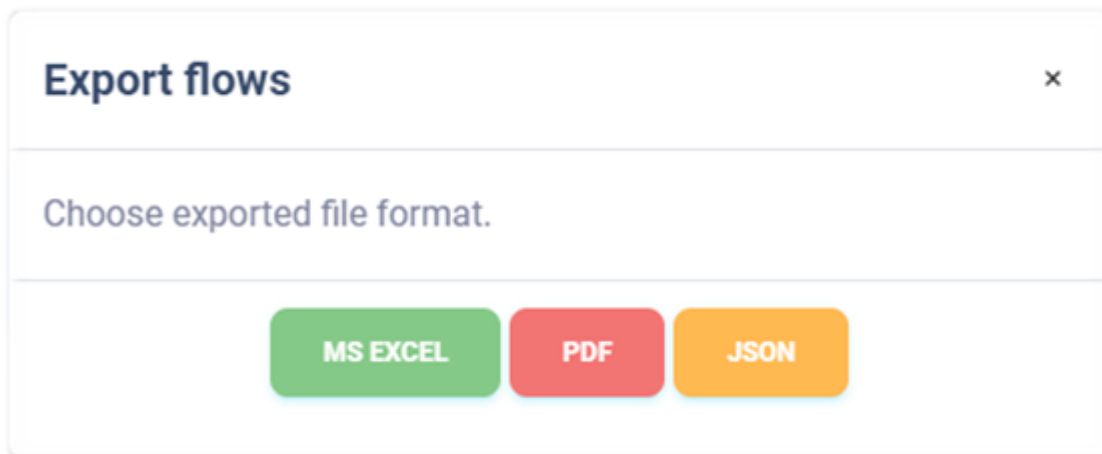
Export to MS Excel

Exporting a list of flows to a Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export.
Client	Client's name.
Deadline	Deadline date.
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Status	**Started** - flow has been established, not yet in progress. **In progress** - flow is processed. **Waiting for approval** - all subparts are complete and awaiting final confirmation: - by client in case of approval flow, - by auditor in case of audit flow. **Not approved** - returned with comments for refinement. **Approved** - flow completed.
Type	Approval flow / Audit flow.
Completion	Flow progress expressed in %.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

Exporting the list of flows to PDF format contains an inventory similar to the listing in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
#	Record number in the export
Client	Client's name
Deadline	Deadline date
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Status	**Started** - flow has been established, not yet in progress. **In progress** - flow is processed. **Waiting for approval** - all subparts are complete and awaiting final confirmation: - by client in case of approval flow, - by auditor in case of audit flow. **Not approved** - returned with comments for refinement. **Approved** - flow completed.
Type	Approval flow / Audit flow
Completion	Flow progress expressed in %.

Export to JSON

Exporting flows to JSON format is available only to instance administrators. This type of export can only be used in the Enterprise license. The exported file can serve as a simple backup or can be used to import into third-party applications.

11.7. Approval flow

The approval flow is the process by which completed and manager-approved risk analyses, risk management plans and other documents are presented to the client. This flow can include several risk analyses and plans that are presented to the client for approval at once. The client can view and examine these parts in detail. Each of them can be commented on and approved or sent back for revision. If all partial risk analyses, risk treatment plans and any other documents are approved, the client can close the approval flow.

Detail - manager's point of view

After opening the approval flow detail, the user sees the following listing. He/she can edit the parameters flow, add risk analysis, RTPs and other documents for approval and add comments.

Detail - client's point of view

After opening the details of the approval flow, the user sees the following statement. Has permission to approve risk analyses, risk treatment plans and other documents in this flow, view their detail and add comments.

EPC diagram

EPC diagram is used for process descriptions and workflow modelling. It looks like this for the approval flow.

Adding parts of the approval process

Adding parts to the approval flow is possible in the flow detail after clicking the `Add` button and then selecting what you want to add – Analysis, Risk treatment plan or Document.

Add risk analysis

Parameter	Required	Description
Identification	Yes	Identification of added risk analysis. Used for better orientation.
Analysis	Yes	Selection of risk analysis to be added to the approval flow. Only completed risk analyses that have been prepared for this client and approved by the responsible manager will be displayed in this list. Each analysis can be added to the approval flow only once.

Add risk treatment plan

Parameter	Required	Description
Identification	Yes	Identification of the added plan. It serves for better orientation.
Risk treatment plan	Yes	Select the RTP to add to the approval flow. Only completed and manager-approved plans that have been processed for this client will appear in this list. Each plan can be added to the approval flow only once.

Add document

Parameter	Required	Description
Identification	Yes	Identification of attachments being added. It serves for better orientation.
Attachment	Yes	To select multiple attachments, hold down the CTRL key and left-click to select multiple files to insert, or select all files to upload and drag them to the file upload box. It is possible to upload files in `pdf`, `png`, `jpg`, `doc`, `zip`, `docx`, `xlsx`, `txt` and `csv` formats. The size of one file is limited to 10MB.

Removal of part of the approval process

An authorized user can remove a risk analysis, risk treatment plan or document from the approval flow by clicking on the `trash bin` icon and then confirming in the modal window.

Approval of individual parts

The client has the ability to review, comment and approve parts of the approval process. If the flow contains any part that is still waiting for approval, it is highlighted with a gray exclamation point in the table header.

After clicking the `Approval` button, the client is given the option to approve or disapprove the part. In case of disapproval, the part is returned for completion and open for editing. The client should add comments to it describing why they did not approve this part. As long as the approval flow is not closed, the client can take back his approval or disapproval.

Approval and completion of flow

At the moment when all parts of the flow are approved by the client, the client is given the option to close the approval flow through the `Approval` button in the flow detail header.

Completion and final approval of the approval flow must still be confirmed in the modal window.

Comments

Authorized users can add comments to all the flows. All comments can be viewed by clicking on the `Comments` button, which opens a page with a list of existing comments and a form to add a new one.

Adding comment

It is possible to add a comment after filling in the appropriate field for entering the text of the comment and sending it with the `Add comment` button.

Internal and public comments

Users can add internal and public comments. Internal comments are not displayed to the clients for which the flow is processed. Administrators, managers, analysts, and auditors can see all logged comments and attachments.

Comments attachments

You can add attachments to each comment. To select multiple attachments, hold down the CTRL key and left-click to select multiple files to upload, or select all files to upload and drag them with the mouse into the file upload box.

Export flow

The export flow details is possible by clicking on the `Export` button and then selecting the export type.
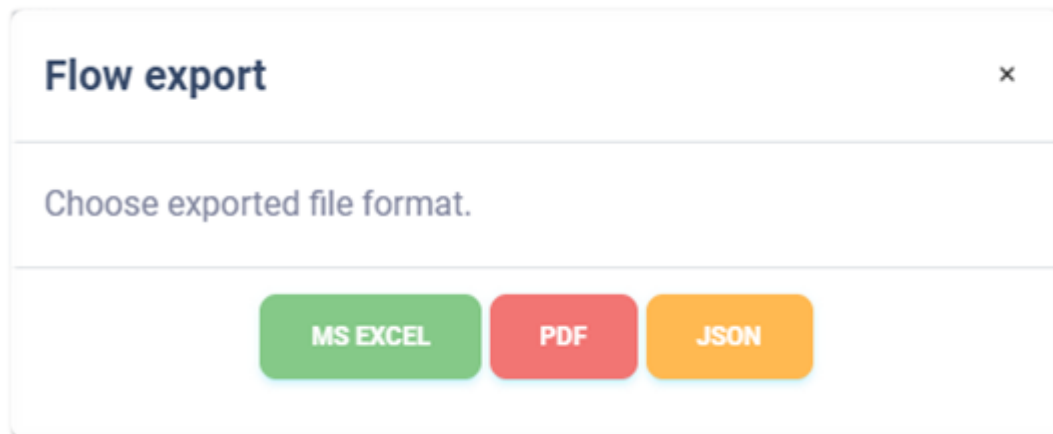
Export to MS Excel

The approval flow detail export to a Microsoft Excel workbook has three sheets of the following values. The report language adapts to the currently used application language.

> **Sheet 1 – Risk analyses**

Column name	Description
#	Record number in the export.
ID	An identifier is used to improve user orientation in the system.
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Risk analysts	List of users with the role `Risk analysts` who are/ were involved in performing risk analysis.
Client approval	Awaiting approval / Approved / Not approved.
Approved by	User of the client who approved/disapproved the analysis.
Approval date	Date of approval.
Approval time	Time of approval.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Sheet 2 – Risk treatment plans

Column name	Description
#	Record number in the export.
ID	An identifier is used to improve user orientation in the system.
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Risk analysts	List of users with the role `Risk analysts` who are/ were involved in performing risk analysis.
Client approval	Awaiting approval / Approved / Not approved.
Approved by	User of the client who approved/disapproved the analysis.
Approval date	Date of approval.
Approval time	Time of approval.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Sheet 3 – Other documents

Column name	Description
#	Record number in the export.
ID	An identifier is used to improve user orientation in the system.
Client approval	Awaiting approval / Approved / Not approved.
Approved by	User of the client who approved/disapproved the analysis.
Approval date	Date of approval.
Approval time	Time of approval.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

Exporting the flow detail list to PDF format contains a list similar to the listing in the application. It includes the following information. The language of the report is adapted by the currently used language of the application.

Analyses in the flow

Column name	Description
ID	An identifier is used to improve user orientation in the system.
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Risk analysts	List of users with the role `Risk analysts` who are/were involved in performing risk analysis.
Status	**In Flow** – a completed and approved risk analysis that is part of the approval process. **In Flow, not approved** - a completed analysis that was returned by the client for revision as part of the approval process. **In Flow, approved** - Completed risk analysis, approved by both responsible manager and relevant client.
Client approval	Awaiting approval / Approved / Not approved. This field includes information about which user took the action and when.

Risk treatment plans

Column name	Description
ID	An identifier is used to improve user orientation in the system.
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Risk analysts	List of users with the role `Risk analysts` who are/ were involved in performing risk analysis.
Status	**In Flow** – a completed and approved risk analysis that is part of the approval process. **In Flow, not approved** - a completed analysis that was returned by the client for revision as part of the approval process. **In Flow, approved** - Completed risk analysis, approved by both responsible manager and relevant client.
Client approval	Awaiting approval / Approved / Not approved. This field includes information about which user took the action and when.

> **Other documents**

Column name	Description
ID	An identifier is used to improve user orientation in the system.
Created	Creation date and time
Client approval	Awaiting approval / Approved / Not approved. This field includes information about which user took the action and when.

Export to JSON

Exporting flow details to JSON format is available only to instance administrators. This type of export can only be used in the Enterprise license. The exported file can serve as a simple backup, or it can be used to import into third-party applications.

11.8. Audit flow

The audit flow is a process, by which users with the `Auditor` role can perform auditing activities on already completely approved risk analyses. These are analyses that have passed the approval flow. An audit flow can include multiple approval flows, where each single approval flow can contain multiple risk analyses prepared for a given client.

Detail – manager's point of view

After opening the audit flow detail, the manager can see the following statement. He/she can edit the parameters flow, add completed audit approval processes and add comments.

Detail – auditor's perspective

After opening the flow detail, the auditor can see the following statement. He/she has permission to close the audit of the subparts in this flow, view their detail and add comments.

EPC diagram

The EPC diagram is used for process descriptions and workflow modelling. It looks like this for the audit flow.

Adding a completed approval flow

Adding the approval flow to an audit one is possible in the flow details by clicking `Add flow`.

Parameter	Required	Description
Identification	No	Identification of the added approval flow. Used for better orientation.
Flows	Yes	Only completed and client-approved approval flows can be added to an audit flow. Each record can be added to the flow only once.

Removing the approval flow

An authorized user can remove the approval flow from an audit flow by clicking the `trash can` and then confirm it in the modal window.

Audit of individual approval flows

Auditor has the ability to review, comment on and close audit records in the audit flow.

After clicking on the `Finish Audit` button, a modal window is opened for the auditor to confirm the completion Audit.

An approval flow whose audit has been completing is displayed in the audit flow detail as follows.

Completing audit flow

When the audit of all approval flows is completed, the auditor is given the option to close the audit flow via the `Finish Audit` button in the flow detail header.

You must still confirm the completion of the audit in the modal window.

Comments

Authorized users can add comments to all the flows. All comments can be viewed by clicking on the `Comments` button, which opens a page with a list of existing comments and a form to add a new one.

Adding comment

You can add a comment after filling in the appropriate field for entering the text of the comment and submitting it by clicking the `Add comment` button.

Internal and public comments

Users can add internal and public comments. Internal comments are not displayed to the clients for which the flow is processed. Administrators, managers, analysts, and auditors can see all logged comments and attachments.

Attachments to comments

It is possible to add attachments to each comment. To select multiple attachments, hold down the CTRL key and left-click to select multiple files to upload, or select all files to upload and drag them with the mouse into the file upload box.

Export flow

Export of the flow detail is possible in the appropriate module by clicking on the `Export` button and selecting the type exports.
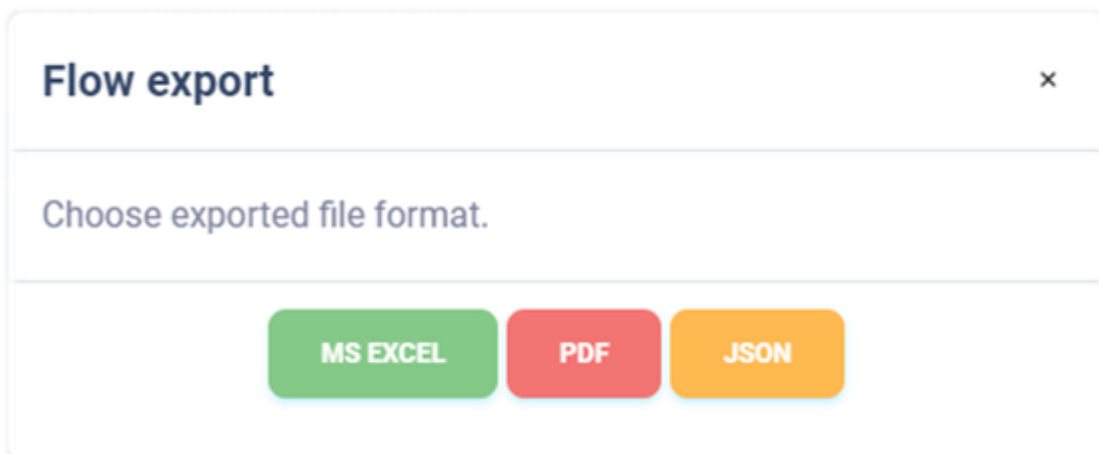
Export to MS Excel

The export of the flows detail to the Microsoft Excel workbook has the following values. The report language is adapted by the currently used application language.

Column name	Description
#	Record number in the export
ID	Identification for better orientation in the system
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Client's approval	Status - only approved flows can be in this flow type. If this column contained a value other than `Approved`, there's a mistake somewhere.
Approval by	The user of the client who approved the analysis.
Approval date	Date of the approval
Approval time	Time of the approval
Status	Waiting for audit / Audit completed.
Audited by	Auditor, who completed the audit of this section.
Audit completed date	Date of completion of the audit part.
Audit completed time	Time of completion of the audit part.
Created at	Date the record was created.
Creation time	Time the record was created.
Created by	Email of user who created the record.
Modified	The date when record was last modified.
Modification time	The time when record was last modified.
Modified by	Email of user who made the last changes.

Export to PDF

Exporting the flow detail to PDF format contains an inventory similar to the listing in the application. Includes the following information. The language of the report is adapted by the currently used language of the application.

Column name	Description
ID	Identification for better orientation in the system
Deadline	Date for processing
Responsible manager	A user with the role of `Risk Manager` who is responsible for completing the flow.
Client's approval	Status - only approved flows can be in this flow type. If this column contained a value other than `Approved`, there's a mistake somewhere. The column contains information about the client that approved the flow and also information about when the action was taken.
Stav	Audit completion status. In the case of a completed audit, this column additionally contains information about which auditor completed the audit and when they took this action.

Export to JSON
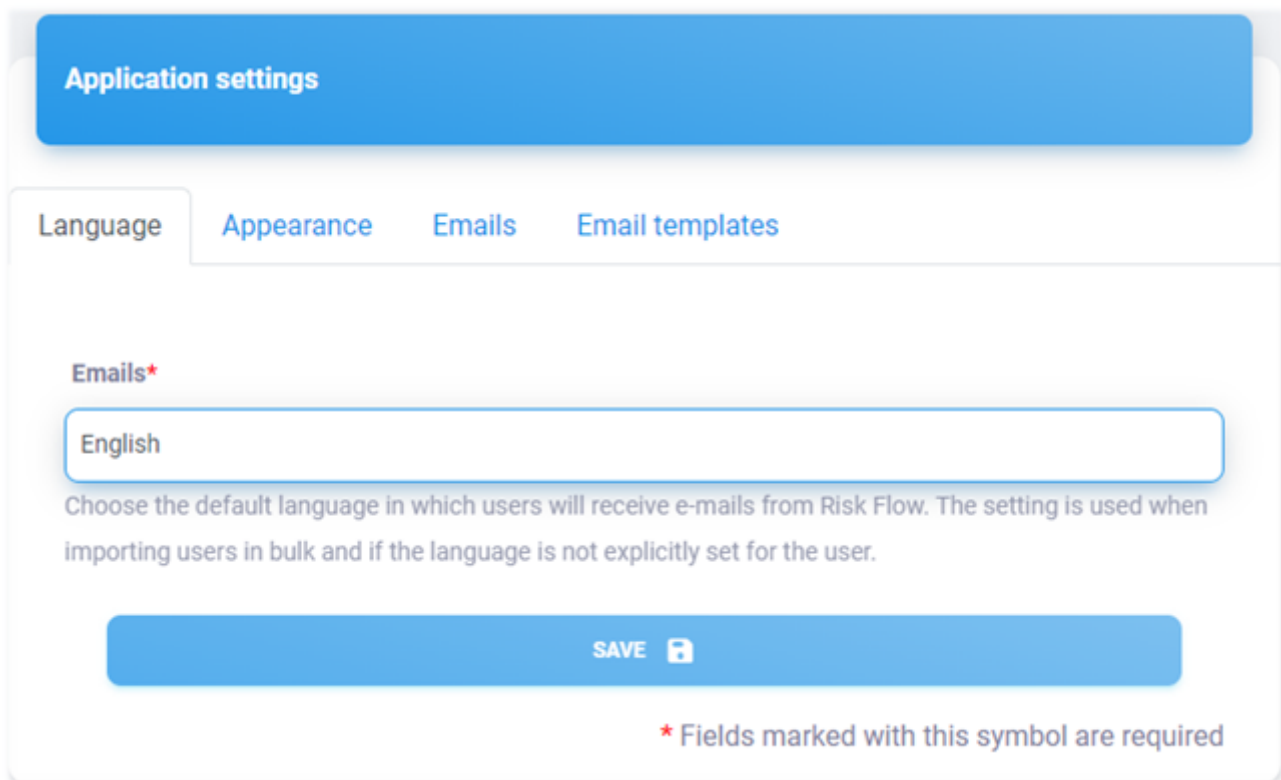
Exporting flow details to JSON format is available only to instance administrators. This type of export can only be used in the Enterprise license. The exported file can serve as a simple backup or can be used to import into third-party applications.

12. Settings

Only instance administrators have the access to the `Settings` module. In this section it is possible to customize the behaviour of the application. The amount of options for customizing the application settings depend on the type of the current license.

12.1. Default language for email notifications

In the `Settings` -> `Language` section, the administrator can define the default language for creating new users. This option is used especially for bulk user imports. Currently, it is possible to choose between Czech and English.

12.2. Appearance customization

In the `Settings` -> `Appearance` section, administrators can set the display of the organization's own logo in the Risk Flow sections. Here, it is possible to define different logos to display in the sidebar of the application, on the login screen and in exported PDF documents. It is also possible here to define the default theme of the application for new users - light or dark. This setting is only available with an Enterprise license.

User interface theme

Each user can choose to use the app in light or dark mode. They can make this choice in their profile settings.

12.3. Server setup for outgoing mails

In `Settings` -> `E-mails` you can set up your own server for outgoing mail. With the green button `Send test email` you can check the functionality of your settings by sending a test email to your email given address. At any

time, you can use the option to reset your settings to their original form by selecting `Reset Settings` and then confirm it in the modal window. This configuration option is only available in the Enterprise license.

13. E-mail notifications

Risk Flow sends notification emails to users according to the action triggered and according to their set preferences in the user profile. Below you can find a list of notification emails that Risk Flow sends.

| #	Email type	Description	Receivers
1	SMTP configuration test	Email to verify SMTP settings.	Administrator
2	New user created	This email informs new user that an account has been created and prompts them to set a password.	New user
3	Assignment of the responsible manager to the analysis	This email will notify the user with the manager role of their assignment to risk analysis.	Responsible manager
4	Assigning an analyst to an analysis	This email will notify the user with the analyst role of their assignment to risk analysis.	Analysts
5	Request for approval of the risk analysis	This email will notify the responsible analysis manager of the requirement to approve the risk analysis.	Responsible manager
6	Notice of removal of the Analysis Manager role	This email will notify the manager of the removal of responsibility for the risk analysis.	Responsible manager
7	Notice of removal of the Analysis Analyst role	This email will notify the analyst of the removal of the risk analysis role.	Analysts
8	New approval flow created	This email will notify the client that a new approval flow has been created.	Client
9	New audit flow created	This email will notify all users with the auditor role of the new audit flow.	Auditors
10	Comments added to a risk analysis	This email will alert the manager, analysts, and client users to the new comment. The user who added the comment will not receive a notification about the new comment.	Responsible manager, analysts, client

11	Comment added to a flow	This email will alert the manager and client users in the case of approval flow, or users with the auditor role in the case of audit flow, of the new comment. The user who added the comment will not receive a notification about the new comment.	Responsible manager, client
12	Flow approval notice	Information for the responsible manager on the client's approval of the flow.	Responsible manager
13	Audit completion notice	Information for the responsible manager on the completion of the audit flow.	Responsible manager
14	Analysis deadline changed	Information for the responsible manager and risk analysts regarding the change in the deadline for processing.	Responsible manager, analysts
15	Flow deadline changed	Information for the responsible manager and flow clients, and possibly auditors, regarding the change in the deadline for processing.	Responsible manager, Client, Auditor
16	Responsibility manager role removed notice	This email will notify the manager about removal of responsibility for the flow.	Responsible manager
17	License expiration is approaching	This email will notify the administrator that the current license expires in 7 days.	Administrators
18	License expiration notice	This email will notify the administrator that the license has been terminated.	Administrators
19	Analysis deadline is approaching	Information about the risk analysis not completed, which is approaching the deadline for resolution.	Responsible manager, Analysts

20	Analysis deadline exceeded	Information about the risk analysis yet not finished, which has exceeded its deadline.	Responsible manager, Analysts
21	Flow deadline is approaching	Information on a pending flow that is close to its deadline for resolution.	Responsible manager, Client, Auditor
22	Flow deadline exceeded	Information about a pending flow that has reached its deadline for resolution.	Responsible manager, Client, Auditor
23	Assignment of responsible manager to the flow	This email will notify the user with the manager role of their assignment to flow.	Responsible manager
24	Assigning a responsible manager to the risk treatment plan	This email will notify the manager user of the assignment to the risk treatment plan.	Responsible manager
25	Assigning an analyst to a risk treatment plan	This email will notify a user with the analyst role of being assigned to a risk treatment plan.	Analysts
26	Request for approval of the risk treatment plan	This email will notify the responsible analysis manager of the request for approval of the risk treatment plan.	Responsible manager
27	Risk treatment plan manager role removal notice	This email will notify the manager of the removal of responsibility for the risk treatment plan.	Manager
28	Notice of removal of the risk treatment plan analyst role	This email will notify the analyst of the removal of the role in the execution of the risk treatment plan.	Analysts
29	The deadline for resolving the risk treatment plan is approaching	Information about the pending risk treatment plan, which is approaching the deadline for resolution.	Responsible manager, Analysts
30	The deadline for resolving the risk treatment plan exceeded	Information about a pending risk treatment	Responsible manager, Analysts

		plan, which has exceeded its deadline for resolution.	
31	Change of the deadline for treatment the risk management plan	Information for the responsible manager and analysts of the risk treatment plan regarding the change of the due date.	Responsible manager, Analysts
32	Adding a comment to the risk treatment plan	This email will notify the client's manager, manager, analysts, and users of the new comment. The user who added the comment will not receive a notification about a new comment.	Responsible manager, Analysts, Client

Although the email notifications differ in content, they have a consistent look and feel, which is as follows.
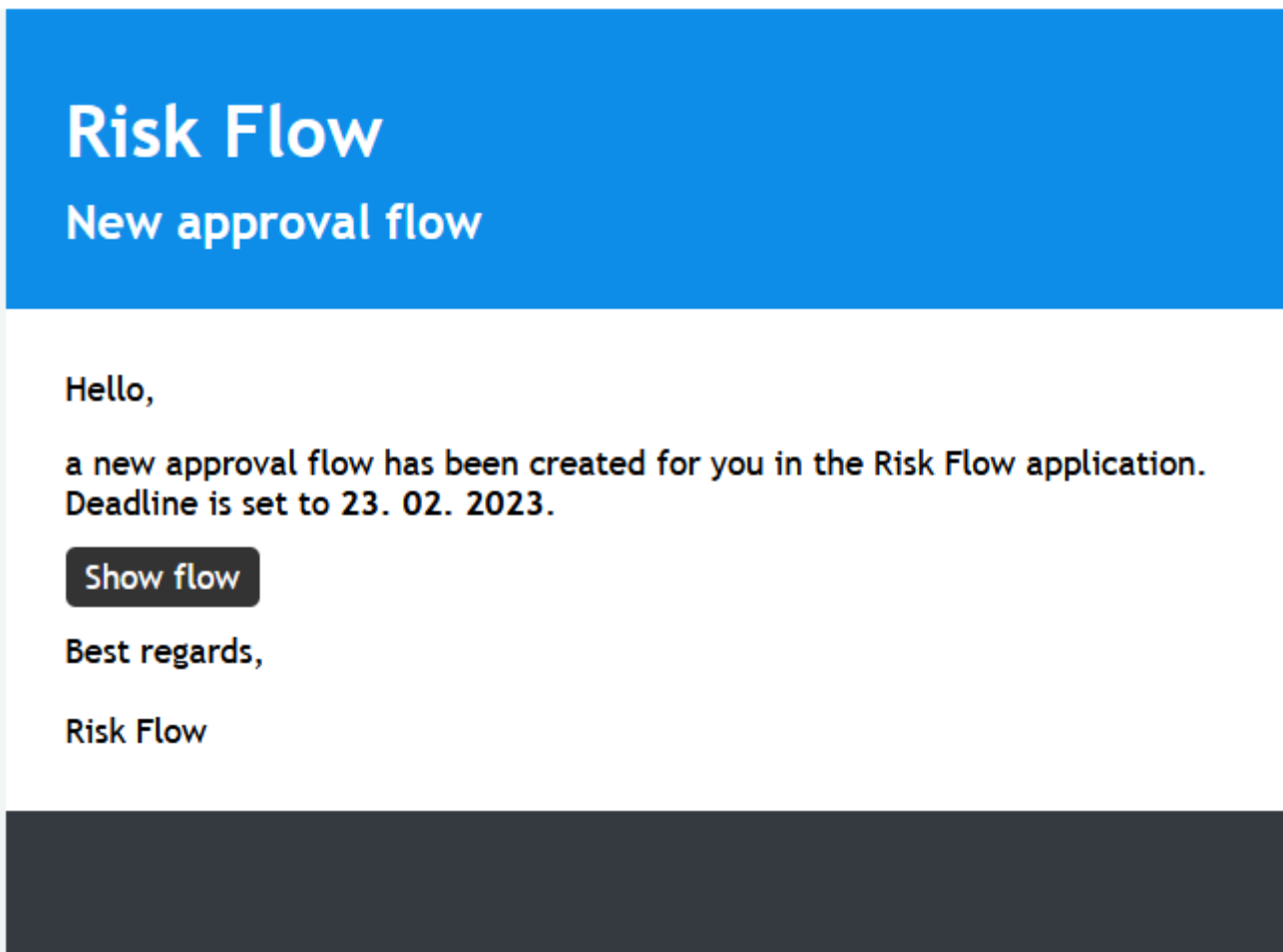
14. API

This module is accessible only to instance administrators and can be accessed from the side panel by selecting the `API` module. This module is only available with the Enterprise license.

14.1. API users

Apart from the instance administrator, only explicitly defined API users have the access to the application interfaces. These users can be managed in the `API` -> `API Users` section. These users are only used to access the application interfaces and do not have any other permissions to access the system.

Create API user

You can create an API user by clicking on the green `Add User` button and filling in the appropriate form.

Parameter	Required	Description
Name	Yes	The API login name of the user. To maintain maximum compatibility with third-party applications, we recommend choosing simple names without diacritics. For example: apiuser1, api_user_2, …
Activate	No	Only active API users can use the available application interface.
Description	No	It is used to improve orientation in the system.

Once a user is created, a unique secret is created for them, which can be viewed via the icon `show` in the list of API users. This secret serves as a password to access the application interfaces.

Edit API user

Editing the API user is possible in the update form, which can be opened by the authorized user in the API user list via the `three dots` icon.

API user activation and deactivation

Whether a user is active or inactive, it is indicated by the `Status` column in the API user listing. At the same time, the administrator can navigate to the activation/deactivation form via this button. Only active API users can use the available APIs.

Reset API user secret

The user's API secret serves as a login password to access the available APIs. This can be reset by the administrator via the `Reset` button.

14.2. API management

Risk Flow offers a simple management of application interfaces that looks like this.

Assign API access to API user

For each API, you must explicitly define the users, who can access it. You can edit this via the edit form by clicking on the `Edit User` button. You can assign any or multiple API users to an API.

API activation and deactivation

The application interface can be activated and deactivated via the activation/deactivation form. Only active APIs can be accessed by API users.

Test API in browser

Each application interface can be tested in the browser by clicking on the `Test API` button.

Example of using API using Postman

Postman is an application used for testing application interfaces of other systems. This section will demonstrate connecting the API to a third-party application and displaying the available data.

All available application interfaces are described in the following chapter – Available APIs. To demonstrate the functionality of the application interface, a request will be made to list all users of the first client. First, we need to find out the ID of the client for which we want to get a list of users. So we will make a request for the appropriate application interface with the following parameters. First, we set the authentication data correctly – name, password and url address of the required API.

After sending such a request, we get a list of all registered clients and information about their users.

```json
{
    "id": 1,
    "name": "Klient 1",
    "users": [
        {
            "id": 35,
            "first_name": "Ondřej",
            "last_name": "Bohatý",
            "email": "ondrej.bohaty.test@riskflow.cz",
            "active": true,
            "lang": "en"
        },
        {
            "id": 36,
            "first_name": "Jakub",
            "last_name": "Chudý",
            "email": "jakub.chudy.test@riskflow.cz",
            "active": true,
            "lang": "en"
        }
    ]
},
```

Now we know the client identifier from the name `Klient 1` and we can use this knowledge to make other requests. We create a new request in the Postman application and set the same authentication and authorization values as in the previous request. In this case, we add another parameter specifying the selected client. We will use the API to find all available analyses for this client.
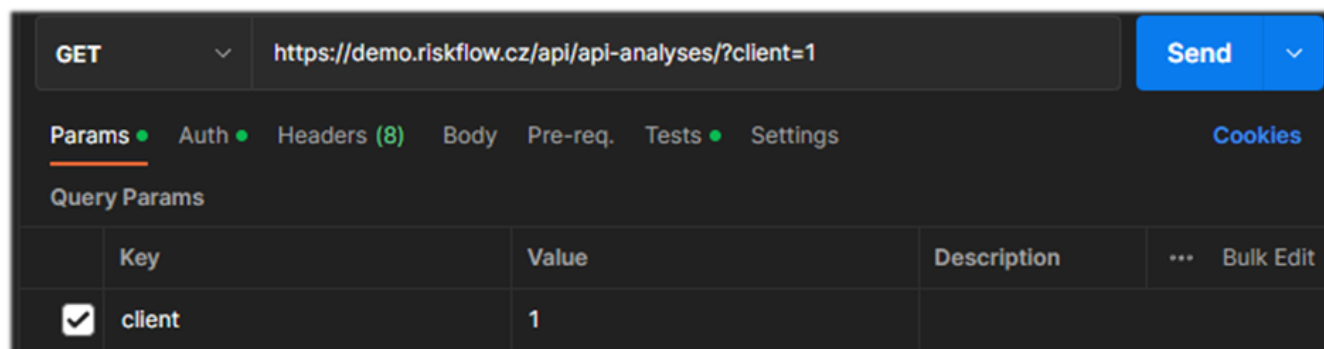
After sending such a request, we will get a result containing a list of available risk analyses for this client. Which APIs are available and which parameters they accept is described in the following chapter.

```json
{
    "id": 6,
    "title": "Prvotní analýza",
    "client": "Klient 1",
    "deadline": "2023-05-04",
    "manager": "iva.cervena.test@riskflow.cz",
    "analysts": [
        "libor.modry.test@riskflow.cz",
        "marek.cerny.test@riskflow.cz"
    ],
    "status": "inflowapproved",
    "completion": 100
},
{
    "id": 7,
    "title": "Další analýza",
    "client": "Klient 1",
    "deadline": "2023-06-01",
    "manager": "jana.zelena.test@riskflow.cz",
    "analysts": [
        "lenka.zlata.test@riskflow.cz",
        "jana.zelena.test@riskflow.cz"
    ],
    "status": "inprogress",
    "completion": 1
},
```

14.3. Available APIs

Risk Flow provides a standard REST API. The following interfaces can be used. Some interfaces accept additional http GET parameters. Parameters marked in red are mandatory.

The URLs of the individual application interfaces are available at `https://INSTANCE-NAME.riskflow.cz/api/`

Title	Description	Additional parameters
Users	List Risk Flow users.	**role** Accepts values "manager", "analyst", "auditor", "client". **active** Receives values „true" or Accepts values `true` or `false`. Returns active or inactive based on the selected value. **lang** Accepts values `en` or `cs`. Returns users with the preferred language of notification emails selected.
Clients	List of all clients.	
Client's users	List all user of a specific client.	**client** Accepts client ID. Returns a list of users of the selected client. **active** Receives values „true" or Accepts values `true` or `false`. Returns active or inactive based on the selected value. **lang** Accepts values `en` or `cs`. Returns users with the preferred language of notification emails selected.
Asset groups	List of asset groups for a specific client.	**client** Receives client ID. Returns a list of asset groups for the selected client.
Assets	List of assets and groups for a specific client.	**group** Accepts asset group IDs. Returns a list of assets of the selected groups. **availability**

Accepts values `low`, `medium`, `high`, `critical`, `not-set`. Returns a list of assets according to the selected value.

integrity

Accepts values `low`, `medium`, `high`, `critical`, `not-set`. Returns a list of assets according to the selected value.

confidentiality

Accepts values `low`, `medium`, `high`, `critical`, `not-set`. Returns a list of assets according to the selected value.

type

Accepts values `primary`, `auxiliary`

value

Accepts values `1`, `2`, `34`, `0`. Value of 0 filters out assets that have not yet been valued.

Analyses	List of risk analyses.	**client**

client

Accepts client ID. Returns a list of risk analyses for the selected client.

manager

Email of the user who is the responsible manager of the analysis.

analyst

E-mail of the user who works as an analyst in the analysis.

status

Accepts values `started`, `inprogress`, `finished`, `waitingforapproval`, `approved`, `notapproved`, `inflow`,

		`inflownotapproved`, `inflowapproved`.
Risk analysis	Specific risk analysis detail.	**analysis** Accepts ID risk analysis. Returns the detail of the selected analysis.
Risk analysis comments	List of all comments for a specific risk analysis.	**analysis** Accepts ID risk analysis. Returns the comments of the selected analysis.
Flows	List of all flows.	**client** Accepts client's ID. Returns a list of flows of the selected client. **manager** Email of the user who is the responsible manager at flow. **status** Accepts values `started`, `inprogress`, `finished`, `waitingforapproval`, `approved`, `notapproved`, `done",``auditdone`  **type**  It accepts `approval` or `audit` values and filters the list of flows based on the selected type.
Approval flow	Approval flow	**flow** Receives flow ID. Returns the detail of the selected flow.
Audit flow	Audit flow	**flow** Receives flow ID. Returns the detail of the selected flow.
Flow comments	List of all comments for a specific flow	**flow** Receives ID flow. Returns comments of the selected flow.
All assets and groups of clients	List of all clients, their asset groups and all relevant assets.	**client** Receives client's ID. Returns a list of asset groups and their

		assets for the selected client.
Import logs	Records of imports and description of potential errors.	
Risk treatment plans	List of risk treatment plans	**client** Accepts client ID. Returns a list of risk treatment plans for the selected client. **manager** Email of the user who acts as the responsible manager for the plan. **analyst** E-mail of the user who acts as an analyst for the plan. **status** Accepts values `started`, `inprogress`, `finished`, `waitingforapproval`, `approved`, `notapproved`, `inflow`, `inflownotapproved`, `inflowapproved`.
Risk treatment plan	Detail of risk ma treatment plan	**plan** Accepts the risk treatment plan ID. Returns the detail of the selected plan.
Risk treatment plan comment	Comments on a specific risk treatment plan	**plan** Accepts risk management plan ID. Returns the comments of the selected plan.