Your one solution for Governance, Risk and Compliance

Risk & Controls Module

A Brief Guide for Users

Contents

Contents

1. Overview of the system

GRC ONE aims to provide an instant Risk Register for any organisation, with the individual governance items identified and allocated to your organisational structure.

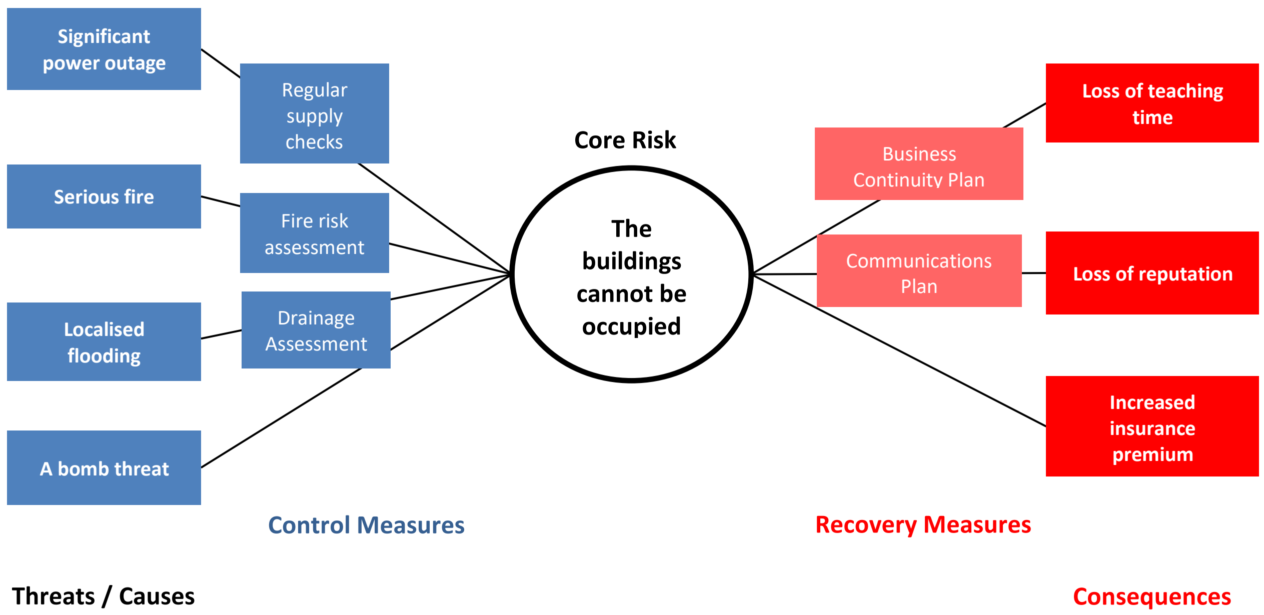
We have implemented both a traditional and a “Bow Tie” methodology for Risk Management, whereby the **Core Risk** is broken down into its underlying **Threats** (or causes).

Each Threat is scored as to the **Probability** of it happening (likelihood) and the **Impact** it will have in the event of it happening, giving you both an **Inherent** and **Residual** risk score.

Control Measures are implemented to reduce either the probability of the risk becoming an event or reducing the impact felt when an event happens.

Finally, if an event actually happens (regardless of the Control Measures that have been implemented), **Recovery Measures** are put in place to try to minimise the consequence.

A simple Risk illustrated by the Bow Tie Method:



You start the Risk Management process at the Risk register, a table of all Risks and Threats that have been identified to date. The register can be filtered to allow you to hone in on a particular Risk Type, Office, Impact Type and Owner etc.

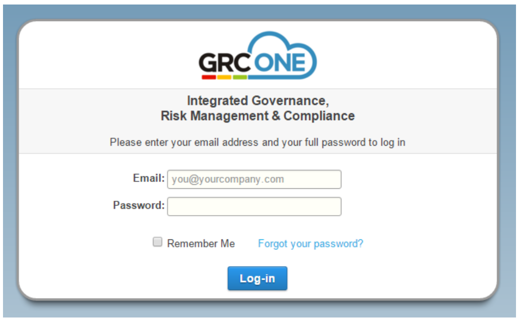
The Risk Type of ”Core Risk”, gives you the highest level of information, and each item can be clicked on to drill down to find more information, including the controls that mitigate a risk and any actions or incidents reported.

You have the choice as to how you wish to manage Risk within your Company. We can provide you with either a copy of software that has been pre-populated with example data, or a bank copy to which you can add your own data.

2. Log In

The GRC ONE Administrator will send you an e-mail with a link to the URL you should be logging into.

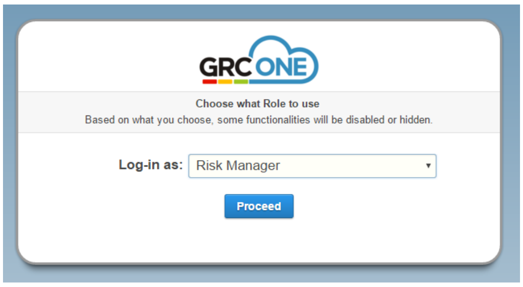
Included in this email will be a password which you can then use to log into the system.



At the login screen you will be asked to login using the email address you were registered with and for your full password.

3. Selecting your Role

If you have been given more than one Role within the system you will be presented with a Role selection option, otherwise you will go straight into your Home screen.



Each role gives the user access to different parts of the system.

The following table shows the functions which each Role within the system can perform:

Role within System	Basic User	Executive	Incident Manager	Risk Manager	Controls Manager
Risk Module					
Add, Edit and Delete own Risks	○	○	○	●	○
View Risk Register	○	●	○	●	○
Allocate Risks to other users	○	○	○	●	○
Link Risks to Controls	○	○	○	●	○
View Risk Matrix	○	●	○	●	○
Score and categorise risks	○	○	○	●	○
Print Risk Reports	○	●	○	●	○

Role within System	Basic User	Executive	Incident Manager	Risk Manager	Controls Manager
Add Actions to Risks	○	○	○	●	○
Controls Module					
Add and allocate Controls	○	○	○	●	●
Manage own Controls	○	○	○	●	●
View Controls Register	●	●	○	●	●
Manage Control Documentation	○	○	○	●	●
Print Controls Reports	●	●	○	●	●
Link Action to a Risk	○	○	○	●	○
Link Action to a Control	○	○	○	●	●
Receive email Alerts	●	●	●	●	●
Allocate Controls to other users	○	○	○	●	●
Set current control status	○	○	○	●	●
Add Actions to a Control	○	○	○	●	●
Assessment Module					
Create New Assessment	○	○	○	●	○
Approve and Close Assessments	○	○	○	●	○
Add Management Comments	○	○	○	○	○
View Assessment History	○	○	○	○	○
Print Assessment Reports	○	○	○	●	○
Actions Module					
Manage own Actions	●	●	●	●	●
Add new Action	●	●	●	●	●
Allocate Action to other user	●	●	●	●	●
Link Action to a Risk	○	○	○	●	○
Link Action to a Control	○	○	○	●	●
Receive email Alerts	●	●	●	●	●
Incident Module					
Record new Incident	●	●	●	●	●
Allocate Incidents to a User and	○	○	●	●	○
Updated to own Incidents status	●	●	●	●	●
Receive email Alerts	●	●	●	●	●
Documentation Module					
Add new Document	●	●	●	●	●
Manage own Documents	●	●	●	●	●
View Documents Register	●	●	●	●	●
Link a Document to a Risk \ Control or Incident	○	○	●	●	●

Role within System	Administrator
Tenant Administration	
Set Tenant default info	●
Manage Organisation set-up	●
Manage Email Preferences	●
Manage Users and Groups	●
Allocate User Roles	●
Manage Reference Data	●
Manage Assessment Templates	●
Import Assessment Data	●
Manage Assessment files	●
Manage Documents	●
Export Data for backup or external reporting \ analysis	●

4. Getting started - User

You will have been given a level of function to the system that is dependent on the role that your administrator has given you and the access to the data you are allowed to see.

On logging on you will open to your Home screen, which will be the Risk Register for the Risk Manager and Executive roles and the Controls Register for the Basic User role.

You can add and edit items within the system dependent on your access rights; however you can only delete items that you are the owner of.

The deep blue coloured bar are the Modules you have been given access to within the system. All Risk Module users can see the Control, Incidents, Actions and Calendar modules.

Each of the menus drops down to reveal the functions you are allowed to perform. If you select the Home menu item, it will return you the screen you first land on, and clear all the filters you may have set.

Each of the menu items will be discussed under the Menu section below.

5. Navigating the system

We hope navigating the system is self-explanatory.

Be aware that the system only automatically saves any changes you have made when you navigate away from a page using the 

button.

To navigate away without saving, use the  back button.

6. Changing your Password

Once you have logged in you can change your password by using the Change Password function at the top right hand side of the screen.

Your password needs to obey the following rules;

Your password must have:

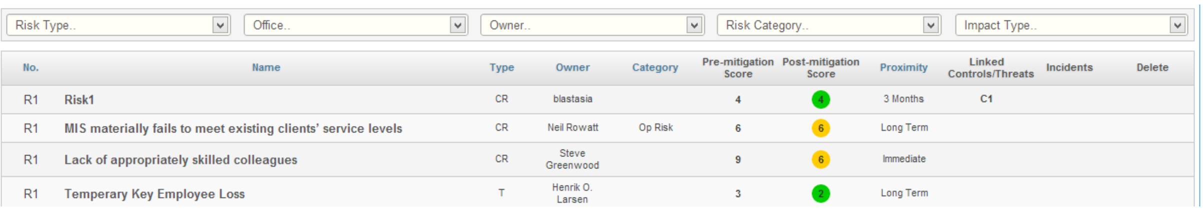
- A minimum of 8 and a maximum of 14 characters
- 1 upper case character
- 1 lower case character
- 1 number or symbol

Your password must not have:

- details from your name or e-mail address
- repetitions or sequences greater than 4 characters (AAAAA, ABCDE, 12345)
- no commonly used words (God, Pass, Love, Word, etc)
- weak or banned passwords (not specified)

7. Allocating Risks and Controls

The first task of the Risk manager is to review the 'Risk's and 'Controls' and allocate 'Owners' to each of them. Each owner will be required to manage the risks and/or controls allocated to them so it is important they understand when and how their responsibility should be completed. Of course they will need to have their own log in and password.



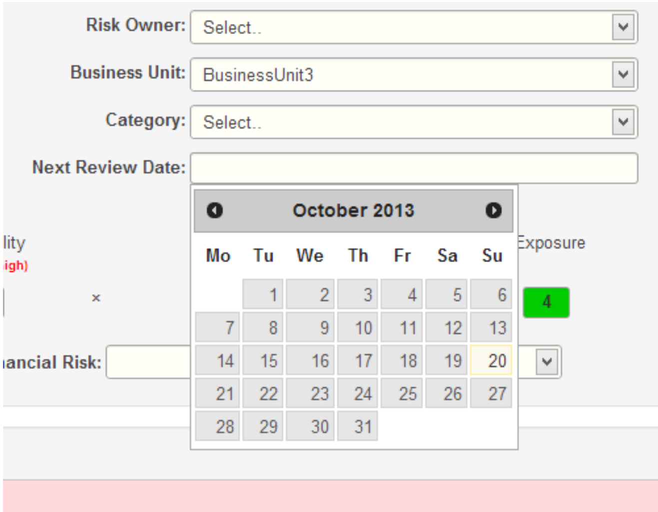
Risk Type.. | Office.. | Owner.. | Risk Category.. | Impact Type..

No.	Name	Type	Owner	Category	Pre-mitigation Score	Post-mitigation Score	Proximity	Linked Controls/Threats	Incidents	Delete
R1	Risk1	CR	blastasia		4	4	3 Months	C1		
R1	MIS materially fails to meet existing clients' service levels	CR	Neil Rowatt	Op Risk	6	6	Long Term			
R1	Lack of appropriately skilled colleagues	CR	Steve Greenwood		9	6	Immediate			
R1	Temperary Key Employee Loss	T	Henrik O. Larsen		3	2	Long Term			

You should discuss with the Control owner how regularly the review of each risk and control needs to take place, so the next review date can be populated on the Controls detail screen.

To re-allocate a Risk or Control, open the record you wish to amend and change the Owner name to the new user.

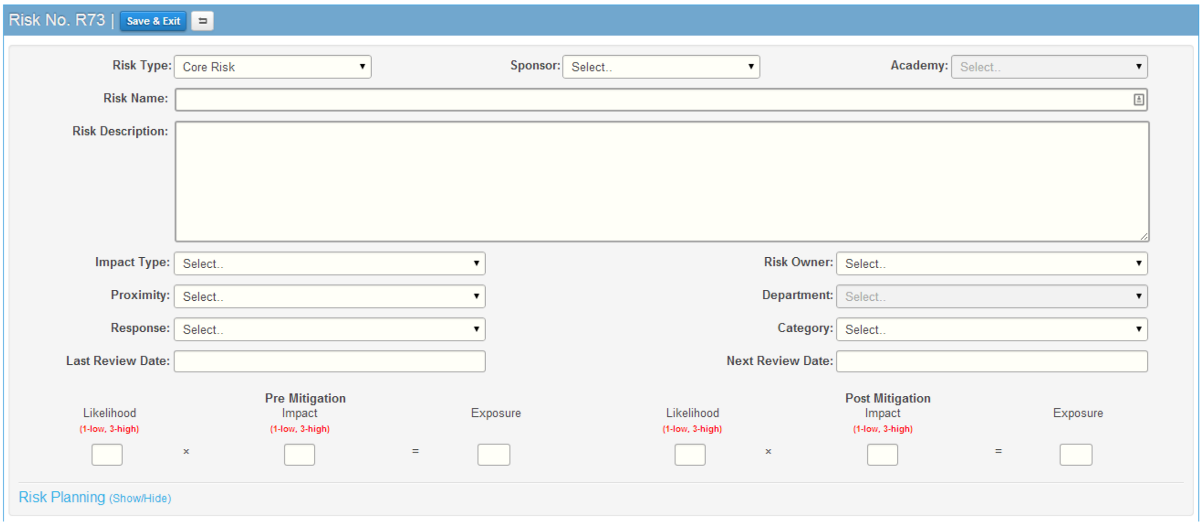
Please note that Basic users can only edit records that are owned by them, so only a Risk Manager can re-assign a record to someone else.



8. Adding a new Risk

Any data that has been provided in the Risk and Control registers is example data only and you may need to add additional Risks or Controls for your Company.

Select the Risk tab from the menu banner at the top of the page and then New Risk. You can then complete the Risk description. A new Risk number will appear (example Risk No. R11) Ensure you Save & Exit before moving on to create and/or link Controls.



You do not need to fill in all the fields at once, as only the Risk Name, Owner, Company, Company and Business Unit are mandatory fields.

If the values you would like to see are not present in the drop down boxes, please contact your Administrator who may be able to add them using the Reference files function.

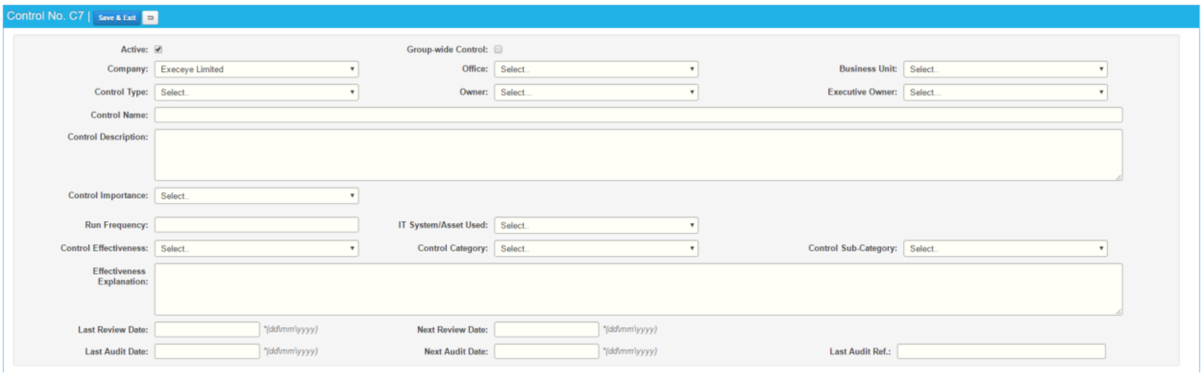
Once you have entered the amount of information you want to, press the Save and Exit button on the light blue menu bar.

9. Adding a new Control

You may wish to create a new Control to link to a Risk. If so, select Controls from the menu and select Controls/New Control where you will be given a New Control screen to complete.

You do not need to fill in all the fields at once, as only the mandatory fields such as Control Name, Owner, Company, Company and Business Unit.

Where a control is required by law or by an industry regulator, the Control Importance should be selected with the correct level, with any legislative requirements entered in the Control Description field.



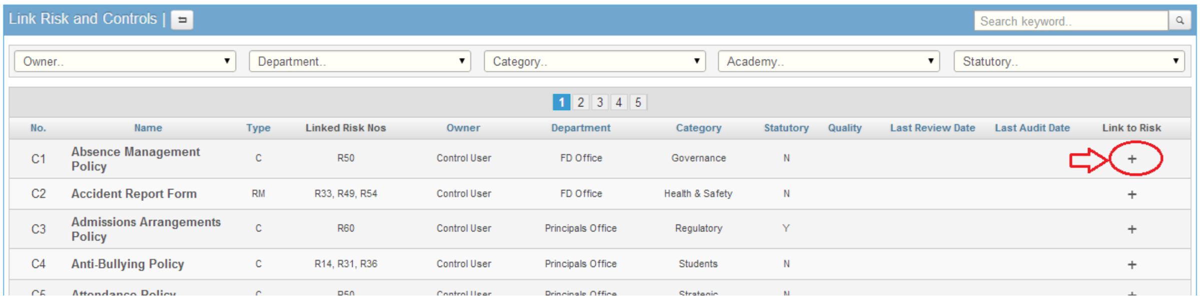
Once you have entered a new control, you will need to go back to the Risk Register and select the Risk that you want to link to the new Control.

Once you have entered the amount of information you want to, press the Save and Exit button on the light blue menu bar.

10. Linking Risks to a Control (s)

You may now link the Risk to a Control (s), for this you will see 'Link Controls' button at the top of the page.

Select this and scroll through the Controls selecting those that need linking by clicking on the '+' sign on the right hand side of the page.



No.	Name	Type	Linked Risk Nos	Owner	Department	Category	Statutory	Quality	Last Review Date	Last Audit Date	Link to Risk
C1	Absence Management Policy	C	R50	Control User	FD Office	Governance	N				+
C2	Accident Report Form	RM	R33, R49, R54	Control User	FD Office	Health & Safety	N				+
C3	Admissions Arrangements Policy	C	R60	Control User	Principals Office	Regulatory	Y				+
C4	Anti-Bullying Policy	C	R14, R31, R36	Control User	Principals Office	Students	N				+

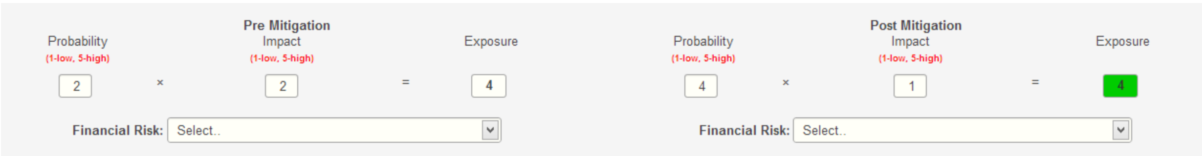
To remove a link to a control, you just reverse the process by selecting the '-' sign on the right hand side of the page.

11. Scoring a Risk

There are two scores for each Risk, Pre-Mitigation and Post Mitigation. Pre mitigation is before any controls or recovery measures have been implemented to reduce the risk probability or impact. The post mitigation score is the residual amount of risk remaining after your controls have been implemented.

Both scores use the same simple mechanism based on **1 = Low, 2 = Medium and 3 = High**.

The Risk score calculation = PROBABILITY x IMPACT = SCORE.



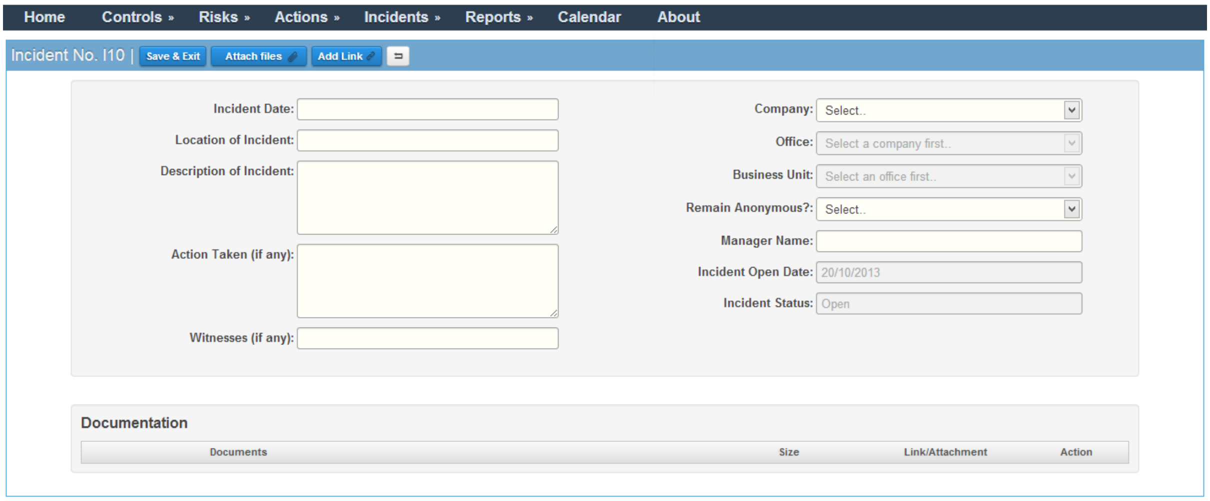
So the highest score a Risk can have either before or after your controls have been implemented is nine, and the lowest is 1.

12. Raising an Incident

Anyone who has a log in to the system may raise an incident.

Incidents can be raised anonymously by selecting the button of the same name.

Evidence of the incident can be attached either as a file (such as a photo) or as a link to a website.



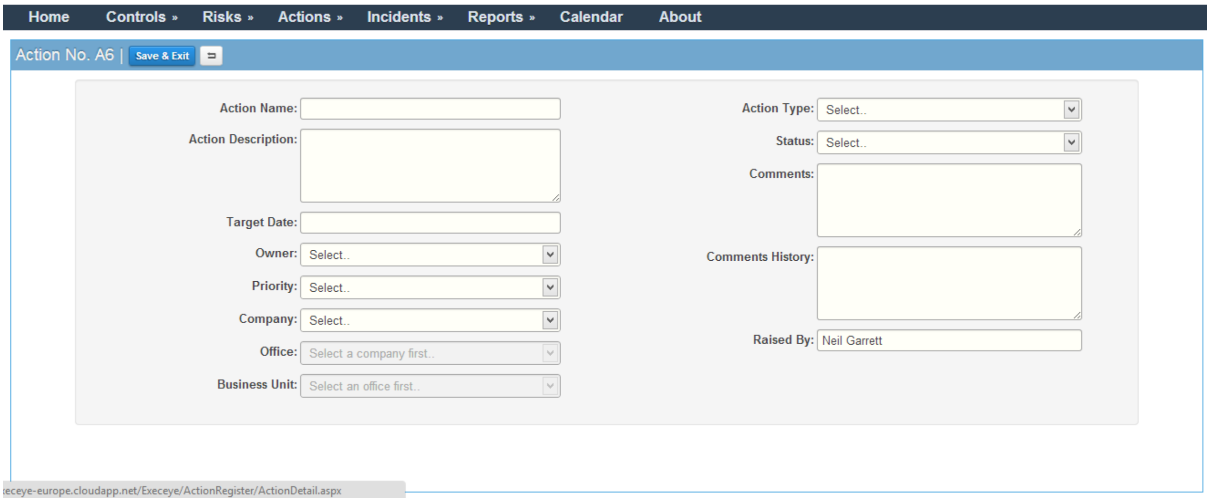
Once an incident has been raised the person with incident manager or risk manager role will be able to allocate the incident to a particular person and a particular risk.

13. Raising an Action

An action is a job or task to be done within the system (an example could be a Control requires improvement or review, a Risk that needs investigation etc.)

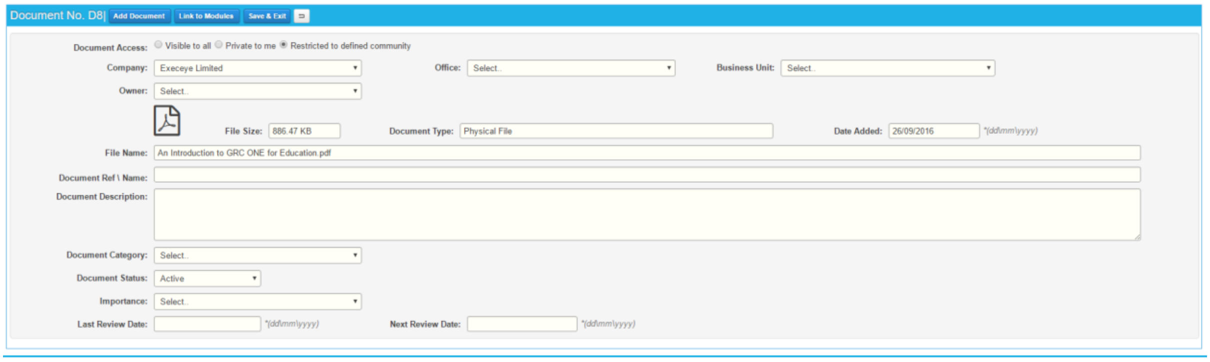
An action can be entered whilst in a Risk, a Control, an Incident or from the Actions menu.

An action can be allocated to any user within the system.



14. Adding a Document

A Document can be added to the system in the Documentation Module or via the “Add Documents” buttons on the various module details screens.



The first information required for a document is the access you wish it to have within the system. There are three options :

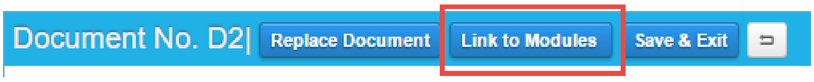
Visible to All = Any user within the "Company" can see the document.

Private to me = Only the user set in the Owner field will be able to view the document

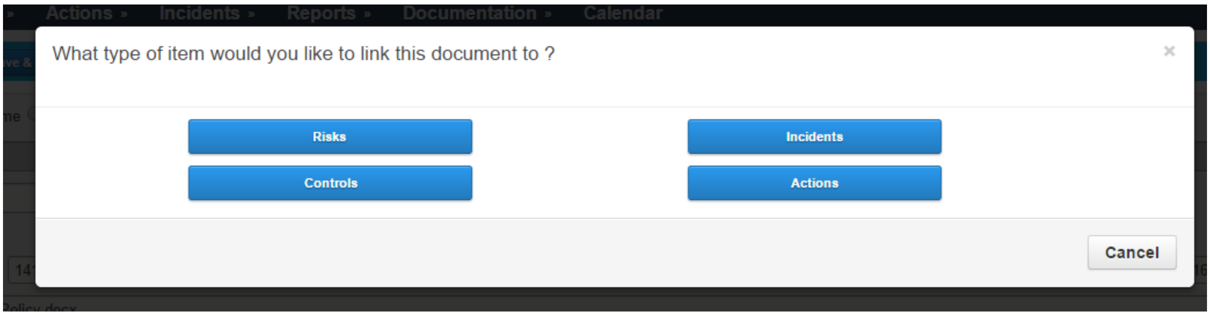
Restricted to defined community = The document will be available to be seen by only those users who have access to the set Company/Office/Business Unit combination.

15. Linking a Document to another Risk\Control\Incident or Action

Documents can be linked to another item in the system by using the Link to Modules button on the document menu bar.

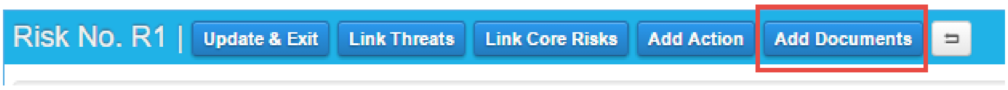


Once selected the button will give the user the opportunity to link the document to one or many items within the system.



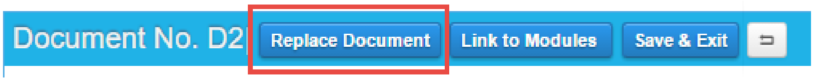
Any item that is linked will automatically show the document under its detail screen.

Alternatively, a document can be added or linked to an item from within the risk\controls and Incidents details screens using the "Add Documents" function button



16. Replacing a Document

Documents can be replaced within the system by using the simple function available on the menu bar

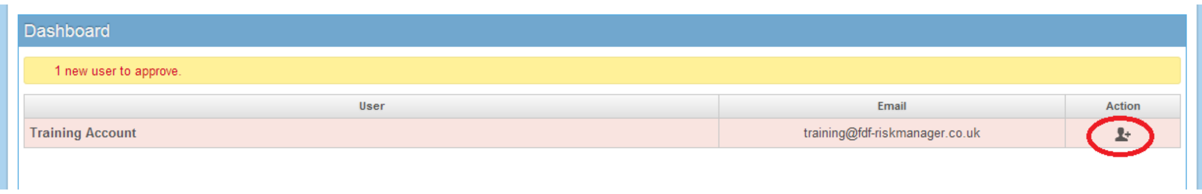


When a Document is replaced using this function, an old copy of the document will be saved in the Documents History bar below the detail screen and the new document will not show within any linked records in the system.

17. Administrator – Getting Started

The Administrator role is allocated by entering User Management and selecting the administrator button against the user name. Once this role has been allocated, the Administration menu will automatically appear on the menu bar.

If there are any users that have been locked out of the system or requiring approval, they will appear in user dashboard, and can be reactivated by selecting the Action button at the end of the item row.



The administrator Menu bar is very different to that of the other roles, and will have some options that are not required by just the Risk Management Module. Care should be taken to understand the impact a change in the Reference Files and Administration menus before any changes are attempted, as it is critical to the operating of the system that the right connections are maintained.

Note : you only have access to your Company reference data, and your changes will not affect any other Company.

18. Administrator - Understanding data access within the system

There are three parts to creating a user's access control within the system:

Reference Item	What	Set Where
Location	The combination of *Company + Country + Office + Business Unit*	***Administration>Company Structure>Location Management***

Firstly, the individual elements of reference data for Company, Country, Office and Business Unit need to be combined to make a Location. Example: Your home address is made up of four pieces of data House Name\No., Street, Town and Post Code. The combination of these pieces of data makes your address, but if not combined are meaningless.

By linking these pieces of data together we are saying that these particular Business Units are present at this Office, this Office is located in this Country.

Note: If a new Business Unit is added to the Reference Files, but not linked within a Location it will not be available in any of the drop down menus within the Risk and Controls register filters or on the detail screens.

Secondly, a Group is created so only the right users can work on a particular Business Units data.

Reference Item	What	Set Where
Group	One or more Location combined	**Administration > Group Management**

Example :

User 1 : needs to see only Finance risks for Company 1

User 2 : needs to see all Risks for Company 1, Office 1

User 3 : needs to see all Risks for Company 1, Office 2

User 4 : needs to see all Risks across all Companys

Three Groups are required to be created to allow this to be implemented:

Group 1 = Company 1 + Finance

Group 2 = Company 1 + Office 1 + All Business Units

Group 3 = Company 1 + Office 2 + All Business Units

User 4 doesn't need their own Group, but needs to be given access to Groups 2 & 3 then the Role is applied over this to give the functions the user can access.

And finally, the individual user is given a Role or Roles, which allows them to perform certain functions within the system.

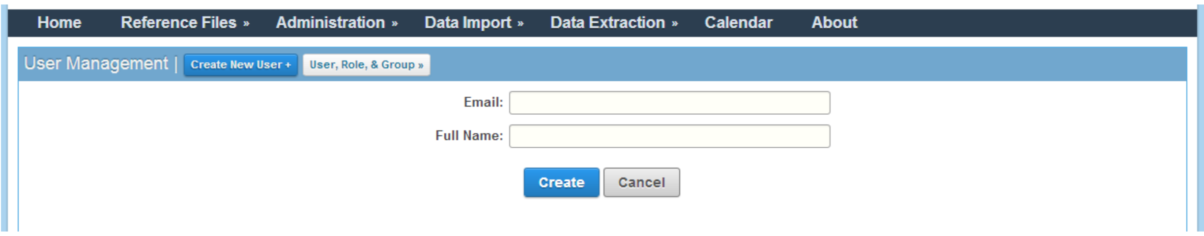
Reference Item	What	Set Where
Role	The Functions within the system can you can use :	Already set within the system

19. Administrator - Creating a new User

Only the Administrator role can create new users and reset passwords for the system.

To create new users go to the following from the home page;

Administration > Users > User Management



You will need to enter a unique

- First name
- Last name
- E-mail address

The new user will automatically receive an e-mail with a password which they will change as required.

If you wish to set up users but not automatically send them a password, you can use a dummy email account and then change it at a later date using the amend user function of the User Management screen.

20. Administrator – Changing a user's password

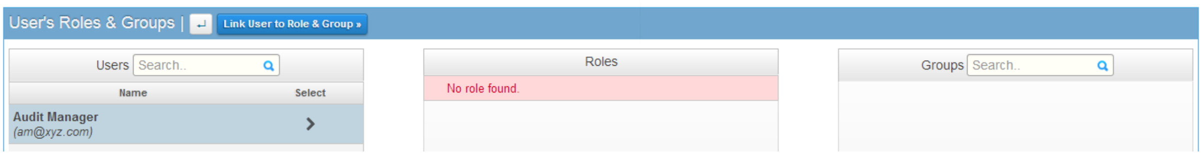
Other than the user themselves, only the Administrator role can change the users password.

The Administrator selects ***Administration > Users > User Management*** from the menu bar, then selects the far right Action icon against the user they wish to change the password for.

On the change of password, the user will receive an email communicating their password has changed; however they will not receive the new password. The administrator will need to contact the user in person to communicate the new password.

Note : This function is regarded as an emergency password change function only, and under normal circumstances the user should use the change password function in Change Password section above.

21. Administrator - Allocating User Role and Group



Only the Administrator can allocate a Role to the user.

To add a Role and Group select ***Administration > User > User Permissions*** from the menu bar then select the Manager User Permissions button.

First select the name of the User you wish to change by ticking the box against the correct line on the right hand side of the screen. Now hit the Proceed to Role Selection button at the bottom of the screen.

Next, select the Role that you wish the user to perform (for the data Group that you are setting them up for) by selecting the arrow against the role on the right hand side of the screen.

Finally, select the data group or groups that you want them to have access to for the role you have just selected. Then hit the Save or Save and Add More Role button at the bottom of the screen.

22. Administrator – Reference Files

The Tenant Administrator is a "super user" who can add, edit and remove the reference data, corporate structure of your Company and the way in which your copy of the application works.

Care should be taken when removing or changing reference data, as any records that utilise the data will change or in the worst case scenario become invisible to the users.

Underlying Risk and Control records utilise the reference data, so a basic understanding of how the data is being used is required before any changes should be made.

There are a number of fields (listed below) that the Tenant Admin can edit.

Name	Description	Where used	Risk of change or deletion
Country	A list of active countries within your whole Company	In the core data security model to create locations. Locations are used by groups to set the users access to system data.	Deselecting a country could have a catastrophic effect on your user's ability to see their data.
Company	Names of the companies within your Organisation	In the core data security model to create locations. Locations are used by groups to set the users access to system data.	High – renaming of the Company is low risk, however all records in the system currently using the existing Company name will be changed. Deleting the Company will have a catastrophic effect on your data.
Office	A list of Offices within your whole Company	In the core data security model to create locations. Locations are used by groups to set the users access to system data.	High – renaming of a Company is low risk, however all records in the system currently using the existing Company name will be changed. Deleting an

			Company will have a significant effect on your user's ability to see their data.
Business Unit	A list of Business Units within your whole Company	In the core data security model to create locations. Locations are used by groups to set the users access to system data.	High – renaming of a Business Unit is low risk, however all records in the system currently using the existing Business Unit name will be changed. Deleting a Business Unit could have a significant effect on your data.
Location Management	This is where the system links the Country, Company, Office and Business Units together to show which Business Units are present in which Offices, and which Offices are owned by which Company.	In the core data security model allow locations to be linked to Groups. Groups set the users access to system data.	High – changes to the Locations will affect the data that users can see within the system. Only people with experience of changing locations should attempt to make alterations in this menu item.
Rating	Bespoke Impact and Likelihood naming conventions for your Company.	Risk Matrix and reporting	Low – these rating will only take affect if they are selected in the Tenant Management screen under the Administration menu option.
IT System	A list of the IT systems used in your Company	Control detail screen to show the system a control is being run on	Low
Financial Risk	A list of value ranges used to highlight the monetary value a Risk can have	Risk and Threat detail screens and reports	Medium – depends on how much effort users have already put into allocating a financial value
Action Type	A list of the action types for use in filters, sort orders and reports	Action detail screen	Low
Risk Category	A list of areas of classification for Risks	Risk Detail and Risk Register screens, filters and on Risk reports	Medium – depends on how much effort users have already put into categorisation of risk

Control Category	A list of areas of classification for Controls	Control Detail and Control Register screens, filters and on Risk reports	Medium – depends on how much effort users have already put into categorisation of Controls