

OpRiskControl System Administrators' Guide

5.5.0

Approval and Publishing History:

OpRiskControl® System Administrators' Guide

Version 5.0.0	Edited, Approved and Published	March 2014
Version 5.1.0	Updated, Approved and Published	June 2014
Version 5.2.0	Updated, Approved and Published	January 2015
Version 5.3.0	Updated, Approved and Published	June 2015
Version 5.4.0	Updated, Approved and Published	March 2016
Version 5.4.1	Updated, Approved and Published	April 2016
Version 5.5.0	Updated, Approved and Published	November 2016

Disclaimer of Warranty

Mitrates Holdings, Inc. (Mitrates) makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Mitrates reserves the right to not support non-standard or non-default functionality and extended functionality available in third-party software, unless specifically documented as supported or certified in the Mitrates product documentation. For further information regarding third-party non-standard or non-default functionality, please contact Mitrates Support.

This document, along with the software that it describes, is furnished under licence and may be used or copied only in accordance with the terms of such licence. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Mitrates.

The following document is for OpRiskControl™ only. Though every effort was made to ensure that the information in this document is correct and reliable, Mitrates does not assume any liability for any errors encountered in this document.

If you need support for OpRiskControl™, please contact the Mitrates support team by sending an email to: support@mitrates.com.

For more information about Mitrates, visit our web site: <http://www.mitrates.com>.

Government Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Mitrates licence agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (Feb 2012) FAR 12.212(a) (1995), FAR 52.227-19 (Dec 2007), or FAR 52.227-14, as applicable.

Contents

1.	Introduction.....	1
1.1.	Welcome.....	1
1.2.	Purpose Of The Software	1
1.3.	Database And Application Backup	1
2.	Overview Of Functionality.....	3
2.1.	Functionality.....	3
2.2.	Context View of Risks	3
2.3.	Security – Single Sign-on	3
2.4.	Role Based Security (RBS)	3
2.5.	Approval Process.....	4
2.6.	Report Wizard	4
2.7.	Charting Wizard	4
3.	Risk Matrix Options	5
3.1.	5x5x5 Risk Matrix	5
3.2.	Triage Style Risk Matrix.....	5
3.3.	Select Matrix Type.....	6
3.3.1.	Numeric Value.....	6
3.3.2.	Custom.....	6
3.3.3.	Triage	7
3.3.4.	5x5x5 Numeric Matrix.....	7
3.3.5.	Change Matrix.....	7
3.3.6.	Set Up A Custom 5x5x4 Matrix.....	7
3.3.7.	Set Up A Custom 5x5x5 Matrix.....	8
3.3.8.	Edit Risk Ratings For Numeric Value Matrix	8
3.4.	Activating The Matrix	8
3.5.	Risk Matrix Descriptions.....	9
3.5.1.	Likelihood Descriptions	9
3.5.1.1.	Triage	9
3.5.2.	Consequence Descriptions.....	9
3.5.2.1.	Triage	10
3.5.3.	Risk Rating Descriptions	10
3.5.4.	Risk Rating Levels	11
3.5.5.	Excess Risk Ratings.....	11
3.5.6.	Removing A Likelihood Level	11
3.5.7.	Removing A Consequence Level.....	11
4.	Risk And Action Entry Overview.....	13
4.1.	Risk Entry Forms	13
4.1.1.	My Form Settings.....	13
4.1.2.	Default Form Settings	14
4.2.	Action Entry Form	16
5.	Risk Form.....	17
5.1.	Tabbed Form	17
5.2.	Custom Forms	17
5.2.1.	Risk Level.....	18
5.2.2.	Action Level.....	19
5.2.3.	Using A Custom Form.....	20

6.	System Settings	21
6.1.	General Tab	21
6.1.1.	Welcome Message	21
6.1.2.	Localisation.....	21
6.1.3.	Other Settings	22
6.2.	Reporting Tab	22
6.2.1.	Reporting	22
6.3.	History Tab.....	24
6.3.1.	Optional History.....	24
6.3.2.	Automatic Risk And Action History	24
6.3.3.	History Location	24
6.4.	Security Tab	25
6.5.	Workflow Tab	26
6.5.1.	Workflow Forms	27
6.5.2.	Tabbed Form Settings	28
6.5.2.1.	Tabbed Risk Form	28
6.5.2.2.	Tabbed Action Form	28
6.5.2.3.	Organization Structure.....	29
6.5.2.4.	Reference Data.....	29
6.5.2.5.	Rating Information	29
6.5.3.	Notification Manager.....	30
6.5.3.1.	Alerts And Escalations	30
6.5.3.1.1.	Alerts	31
6.5.3.1.2.	Escalations	31
6.5.3.2.	Updates And Reminders	32
6.5.3.2.1.	Setup Updates	32
6.5.3.2.2.	Setup Compliance	33
6.5.3.2.3.	Setup Deactivations	33
6.5.3.2.4.	Setup Incidents	33
6.5.3.2.5.	Key Indicators	34
6.5.4.	Notification Settings.....	34
6.5.5.	Process Management.....	34
6.5.6.	User Permissions	34
6.6.	Formula Tab.....	35
6.7.	Options Tab	37
6.7.1.	Options.....	37
6.7.2.	Incident Logging	38
6.8.	Setup Tab.....	38
6.8.1.	Menu Tabs	39
6.8.2.	Menu Ribbons And Sub-Menu Items	40
6.8.3.	Panel Headers And Borders	41
6.8.4.	Panel Tabs	42
6.8.5.	Panel Content.....	42
6.8.6.	Page Banner	44
6.8.7.	Page Headers.....	44
6.8.8.	Grid Column Headers.....	44
6.8.9.	Grid Items	45
6.8.10.	Alternate Grid Items.....	46
6.8.11.	Footer	46
6.8.12.	Buttons.....	47
6.9.	Refresh System Settings	47
6.10.	Save Website Appearance	47
6.11.	Restore Saved Website Appearance.....	47

7.	Role Based Security.....	49
7.1.	Overview.....	49
7.2.	RBS Permissions.....	49
7.2.1.	Permission Allocation.....	49
7.3.	RBS Roles.....	49
7.3.1.	Role Permissions	49
7.3.2.	RBS Users	49
7.4.	RBS User Interface Functionality	50
8.	System Security	51
8.1.	Roles.....	51
8.1.1.	Role Definition Tab.....	51
8.1.2.	Role Permissions Tab	52
8.1.3.	Role Users Tab.....	53
8.2.	Users	53
8.2.1.	User Roles Tab.....	54
8.2.2.	User Permissions Tab.....	54
8.2.2.1.	Permissions Configured.....	55
8.2.3.	User Details Tab	56
8.3.	System Security Settings.....	56
8.3.1.	Row Level Security.....	56
8.4.	Example Of Row Level Security.....	57
8.4.1.	Multiple Roles.....	58
8.4.2.	Access All Areas	58
8.5.	Troubleshooting.....	59
8.5.1.	No Roles Appearing For Division/Department/Location/Asset	59
8.5.2.	Access Not Granted	59
8.5.3.	Error Message	59
9.	System Data	61
9.1.	Likelihood.....	61
9.2.	Consequence	61
9.3.	Consequence Factor Setup.....	62
9.3.1.	Automatic Consequence Factor Setup	63
9.3.2.	Manually Create Consequence Factors	64
9.3.3.	Using Likelihood And Consequence Factors.....	64
9.4.	Rating	65
9.5.	Willingness	65
9.6.	Impact.....	66
9.7.	Appetite Matrix.....	66
9.7.1.	Changing The Appetite Rating Level	67
9.8.	Appetite Rating.....	67
9.8.1.	Changing The Appetite Rating Colour.....	68
9.8.2.	Changing The Appetite Rating Name.....	68
9.9.	Enterprise Rating	68
9.10.	Control Effectiveness	69
9.11.	Likelihood Rating Conversion	69
9.12.	Change Matrix.....	70
9.12.1.	Numeric Value.....	70
9.12.2.	Edit Risk Ratings For Numeric Value Matrix	71
9.12.3.	Activating The Matrix	71

9.12.4. Custom.....	72
9.12.5. Triage.....	72
9.13. Global Translator	72
9.14. Risk Status.....	73
9.15. Structure Filter.....	73
9.16. Action Type.....	74
10. System Content	75
10.1. Manage Content	75
10.2. Manage Links.....	75
10.3. Import Logo	76
11. System Email Templates	77
11.1. Making Changes To Email Templates.....	77
12. Manage Users	79
12.1. Users And Contacts.....	79
12.1.1. When Employees Leave The Organisation.....	79
12.1.1.1. Imported Users	79
12.1.1.2. Manually Created Users.....	80
12.1.2. Print List.....	80
12.1.3. Change Layout.....	80
12.1.4. New User.....	80
12.1.4.1. Title	81
12.1.4.2. Given Name.....	81
12.1.4.3. Middle Initials	81
12.1.4.4. Family Name	81
12.1.5. Select	82
12.1.6. User Details	82
12.1.6.1. Back To List.....	82
12.1.6.2. New User	82
12.1.6.2.1. Title	82
12.1.6.2.2. Given Name	83
12.1.6.2.3. Middle Initials	83
12.1.6.2.4. Family Name	83
12.1.6.3. Deactivate/Activate	83
12.1.6.4. Edit.....	83
12.1.7. Risks Tab	83
12.1.7.1. Reassign Risks	83
12.1.8. Actions Tab	83
12.1.8.1. Reassign Actions.....	84
12.1.9. User Groups Tab	84
12.1.9.1. Add A User To A Group.....	84
12.1.10. Where Used Tab	84
12.1.11. Where Used.....	84
12.1.12. Documents Tab	85
12.2. User Groups	85
12.3. User Import	85
13. Manage Documents	87
13.1. Attach Hyperlink.....	87
13.2. Attach Document.....	88

14. Manage Reference Data	89
14.1. Action Code.....	89
14.2. Action Frequency	90
14.3. Assets.....	90
14.4. Asset Types.....	91
14.5. Departments	92
14.6. Divisions.....	93
14.7. Division Groups.....	93
14.8. Exposure Periods.....	94
14.9. Function	94
14.10. History Types	94
14.11. Project.....	95
14.12. Locations	95
14.13. Responsible Parties	95
14.14. Review Frequencies.....	96
14.15. Risk Events	96
14.16. Other Classification.....	99
14.17. Event Context	99
14.18. Risk Types.....	99
14.18.1. Manually Create Likelihood And Consequence Factors.....	100
14.19. Standards.....	101
14.19.1. Add A Standard	101
14.19.2. Attach A Document To A Standard	101
14.20. Timeframe.....	101
14.21. Categories.....	102
14.22. Risk Capacity	102
14.23. Correlation To Strategy	102
15. Manage Risk Data	105
16. Manage Lookups	107
16.1. Risk Lookups	107
16.2. Action Lookups	108
17. Options	111
17.1. Processes.....	111
17.2. Process Management.....	111
17.2.1. Global Edit	112
17.2.2. Export	112
17.2.3. Edit.....	113
17.3. Risk Templates.....	113
17.3.1. Manage Templates	113
17.3.1.1. Create A New Template.....	113
17.3.1.2. Edit An Existing Template	114
17.3.2. Create Risks From Templates.....	114
18. Additional Information.....	117
18.1. Risk Locking	117
18.1.1. Risk Locks Enabled	117
18.1.2. Risk Locks Disabled.....	117

1. Introduction

1.1. Welcome

This System Administrator's Guide contains the information you need to implement a risk management structure, to supervise others in the use of the OpRiskControl software, and to carry out advanced operations on the database.

Any reference to Microsoft® Outlook may be considered a reference to other popular email systems such as Lotus Notes, GroupWise®, Microsoft® Outlook Express or Microsoft® Exchange Client.

In some risk management environments, users responsible for managing risk refer to *hazards* and *controls* rather than *risks* and *actions*. To clarify, we understand that risks relate to hazards, and those hazards or risks may be mitigated in some way. Mitigation may be in the form of an existing control or a new action.

So as not to make the database too complex, the schema has been simplified in that a risk source (e.g. risk event code) may be a hazard or a risk or a risk related to a hazard. Likewise an action in the database may be an existing control.

1.2. Purpose Of The Software

OpRiskControl simplifies the task of managing general operational risks. This software allows you to enter an unlimited number of risks by *division* (which may be renamed to *client* or *campus*, for example), *department*, *function* (for example *sub-department*), *project*, *location*, and *asset* (a tangible or intangible asset).

With OpRiskControl you can quickly evaluate the most critical and expensive Risks, and then take Action to reduce the likelihood or consequence of an event.

1.3. Database And Application Backup

It is assumed that your I.T. Department will do a daily backup of your data in the SQL Server database.

Because OpRiskControl allows documents to be attached to Risks and Actions, and those documents are located in the *Output* sub-directory, it is also assumed that your I.T. Department will do a daily backup of the *Output* directory.

It is also assumed that your I.T. Department will do a weekly or monthly backup of the whole application directory to save your configured company logo, home page, licence keys and so on.

2. Overview Of Functionality

This software package is used to manage general organisational risks.

It provides a generic framework for establishing the context, identification, analysis, evaluation, action, monitoring and communication of risk.

A five-step risk management process can be used with the monitoring and communication of risks. The stages are:

1. Establish the context.
2. Identify Risks.
3. Analyse Risks.
4. Evaluate Risks.
5. Treat Risks.

2.1. Functionality

OpRiskControl provides the following functionality:

- Risk name, description, dates logged, reviewed and closed, potential loss (or gain), Risk status, types of Risk and more.
- Risk context by department, division, location, project, process, asset or user defined code.
- Up to nine levels of likelihood (most customers use five) and nine levels of consequence (most customers use five) giving greater granularity of Risk Rating.
- Any number of Actions, with a name, description and estimated cost.
- A record of the names of three users associated with the Risk: Recorded by, Contact and the Owner.
- A link to related documents at both Risk and Action levels.
- The effectiveness of each Action which adjusts the Residual Risk when the Action is completed.

2.2. Context View of Risks

Each user may edit their *Context Profile* to set the default Risk Search criteria. From that point on they only see Risks in their context. When they run a report or display a Risk matrix, they only see their section's Risks and Actions. However, if they wish to see if another department is managing a Risk, they can override their context to view other Risks. To block this override completely, see "[Role Based Security \(RBS\)](#)" below.

2.3. Security – Single Sign-on

OpRiskControl uses Windows authentication to validate users' access to the application – there is no need to set up different access control mechanisms.

2.4. Role Based Security (RBS)

OpRiskControl supports Role Based Security which means Roles are created and then users are assigned to the Roles. It is then easy to change a user's Role if they get promoted or move departments or divisions. System users will gain access to programs and data as allowed by the Role to which they belong. A user may have multiple Roles such as *Finance Department User* and *Audit Department Officer*.

2.5. Approval Process

Risks can be first given a status of *Input* and are then not formally included in the system until an authorized user verifies them and updates their status to *Active*.

2.6. Report Wizard

The Report Wizard starts with basic report structures and then allows the user to select the data they want to report on, the data columns they want to see, the sort order, and the number of records they want to print.

2.7. Charting Wizard

In a large organisation senior executive need to know where their high risks are; where people are not managing their Risks; and how exposed they are. OpRiskControl has many charts that provide information by Division, Business Unit, Asset, Location, Risk Type and Risk Level. Chart types may be column, pie, bar and X-Y plots.

3. Risk Matrix Options

You have a choice of many Risk matrices. Before you begin to use OpRiskControl, you need to decide which Risk matrix you wish to use. A 9x9x9 (9 levels of Likelihood, 9 levels of Consequence and 9 levels of Risk Rating) matrix gives you the most granularity and flexibility. The 5x5x5 matrix (five levels of Likelihood, five levels of Consequence and five levels of Risk Rating) is simpler and the most popular.

If you work in the health industry, you may find that a Triage style Risk matrix may be more acceptable. With the Triage style Risk matrix, a rating of one is the highest Risk and four the lowest. The matrix is the reverse of the normal matrix.

The choice is yours, but it must be made before you enter any Risks. If you decide to use a 5x5 or 9x9 matrix, you will be able to alter the level at which Risk Ratings start, however such a change is system wide and will affect all Users of the system.

3.1. 5x5x5 Risk Matrix

The OpRiskControl default configuration uses a 5 by 5 Risk matrix. The 5x5x5 matrix gives a maximum rating of 25.

5x5	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain					
Likely					
Possible					
Unlikely					
Rare					

You are able to adjust the levels at which Risk Ratings start, so you can increase (or decrease) the number of cells that are high or extreme Risks. You are then able to rename (or translate) the *Likelihood*, *Consequence* and *Rating* labels to suit your methodology.

The Risk Rating is usually calculated by multiplying the values for the *Likelihood* and the *Consequence* (although it can be set to the sum of the *Likelihood* and the *Consequence* [see "Formula Tab" on page 35](#)). The Residual Risk is calculated from the Risk Rating less the effectiveness (as a percent or level reduction) of any completed Actions. The Residual Risk is the rating which is often used on executive reports.

3.2. Triage Style Risk Matrix

When OpRiskControl is initially configured, the System Administrator may elect to use the Triage Style matrix and change it from the default 5x5x5 to a 5x5x4 matrix (five levels of Likelihood, five levels of Consequence and four levels of Risk Rating). The Triage 5x5x4 matrix gives a maximum rating of 1.

Triage5by5	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Frequent					
Likely					
Possible					
Unlikely					
Rare					

The system is delivered with a predetermined mapping of *Likelihood* and *Consequence* to give Risk Ratings. If this mapping is not to your liking, configure the matrix so it meets your requirements.

3.3. Select Matrix Type

Decide which matrix type best suits your operation.

On the *System* tab, select *System Data* and select *Change Matrix* from the menu.

The password is *changematrix* (one word). This password protects the matrix if you are not using RBS.

3.3.1. Numeric Value

The *Numeric Value* Risk matrix relies on cut-off values specified on the Risk Rating table. To use it, select *Numeric Value* then click *Activate the Matrix*. If required, select *Edit Risk Ratings* and change the levels at which the Risk Rating changes.

3.3.2. Custom

Customers have different Risk matrix requirements. If their requirements are not met by the default 5x5x5 matrix, they can use the *Custom* Risk matrix.

For example, customers who do not want to use the standard five levels of Risk Rating can use a *Custom* matrix.

3.3.3. Triage

A *Triage* style Risk matrix is reversed so that 1 is the highest Risk Rating. If you want to use a Triage matrix, you will have to configure the matrix, the Likelihood descriptions and the Consequence descriptions.

3.3.4. 5x5x5 Numeric Matrix

To use the dynamic 5x5x5 matrix, select *Numeric Value* and specify the cut-off values in the Risk Rating table.

3.3.5. Change Matrix

After changing the type of matrix from, for example, *Custom* to *Numeric Values*, click *Change Matrix* to display the appropriate configuration options for the selected matrix.

If you select *Custom* or *Triage* and click *Change Matrix*, the form will expand so that you can change the intersection of *Likelihood* and *Consequence* to specify the desired *Risk Rating*.

ID	Likelihood	Consequence	Rating
1	1 Rare	1 Insignificant	1 Insignificant
2	2 Unlikely	1 Insignificant	1 Insignificant
3	3 Possible	1 Insignificant	2 Low
4	4 Probable	1 Insignificant	2 Low
5	5 Almost certain	1 Insignificant	3 Medium
6	1 Rare	2 Minor	1 Insignificant
7	2 Unlikely	2 Minor	2 Low
8	3 Possible	2 Minor	3 Medium
9	4 Probable	2 Minor	3 Medium
10	5 Almost certain	2 Minor	3 Medium
11	1 Rare	3 Moderate	2 Low
12	2 Unlikely	3 Moderate	3 Medium
13	3 Possible	3 Moderate	3 Medium
14	4 Probable	3 Moderate	3 Medium
15	5 Almost certain	3 Moderate	4 High
16	1 Rare	4 Major	2 Low
17	2 Unlikely	4 Major	3 Medium
18	3 Possible	4 Major	3 Medium
19	4 Probable	4 Major	4 High
20	5 Almost certain	4 Major	5 Extreme
21	1 Rare	5 Critical	3 Medium
22	2 Unlikely	5 Critical	3 Medium
23	3 Possible	5 Critical	4 High
24	4 Probable	5 Critical	5 Extreme
25	5 Almost certain	5 Critical	5 Extreme

Edit the column named *Rating* to declare which rating you want to appear in that cell.



Note: You will not be able to delete a Level (for example, Level 5 if you have decided to use just 4 Levels of Risk) if that Level appears in this table. Change the Levels so that, for example, Level 5, does not appear in this table. You will then be able to delete Level 5.

When you have edited the list, click *Activate the Matrix* to save the changes. Exit the browser and re-start the application. If you have any problem activating the matrix, refer to “[Activating The Matrix](#)” on page 8.

3.3.6. Set Up A Custom 5x5x4 Matrix

A 5x5x4 matrix has five levels of Likelihood, five levels of Consequence and 4 levels of Risk Rating. Place a number from 1 to 4 in the *Rating* column (for a 4 level Risk Rating) as an indicator that such a Risk Rating will apply for that intersection of *Likelihood* and *Consequence*.

3.3.7. Set Up A Custom 5x5x5 Matrix

A 5x5x5 matrix has five levels of Likelihood, five levels of Consequence and five levels of Risk Rating. In the *Rating* column place a number from 1 to 5 (for a five Level Risk Rating) as an indicator that such a Risk Rating will apply for that intersection of likelihood and consequence.

3.3.8. Edit Risk Ratings For Numeric Value Matrix



Note: This section applies only if you have selected *Numeric Value* for your matrix. It does not apply if you have selected a Custom or Triage matrix.

If you want to change the levels at which Risk Ratings cut in, then use *Edit Risk Ratings* to change the cut-off values as shown below.

Normal		Insignificant	Minor	Moderate	Major	Catastrophic		Rating Level
		1	2	3	4	5		
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	10
Possible	3	3	6	9	12	15	Medium	5
Unlikely	2	2	4	6	8	10	Low	3
Rare	1	1	2	3	4	5	Insignificant	0

Option 2		Insignificant	Minor	Moderate	Major	Catastrophic		Rating Level
		1	2	3	4	5		
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	15
Possible	3	3	6	9	12	15	Medium	10
Unlikely	2	2	4	6	8	10	Low	5
Rare	1	1	2	3	4	5	Insignificant	0

Option 3		Insignificant	Minor	Moderate	Major	Catastrophic		Rating Level
		1	2	3	4	5		
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	14
Possible	3	3	6	9	12	15	Medium	8
Unlikely	2	2	4	6	8	10	Low	4
Rare	1	1	2	3	4	5	Insignificant	0

The top settings show a Risk Rating of 0-2 is Insignificant, 3-4 is Low, 5-9 is Medium, 10-19 is High and 20 or higher is Extreme. The Risk Rating is usually calculated by multiplying the values for the *Likelihood* and the *Consequence*, (see "Formula Tab" on page 35 for more information).

3.4. Activating The Matrix

If you have edited the Risk Rating levels, click the *Activate the Matrix* button to save your changes.

Exit all browser sessions and then restart OpRiskControl.

Select the *System* tab, select *System Settings*, then, at the bottom of any page, press *Refresh System Settings*.

Refresh System Settings

This causes a refresh of the system settings.



Note: It is often necessary to restart IIS. If you are not able to restart IIS due to other live web applications, then Stop and Start the website itself.

To finish activating the matrix, select the *Manage* tab, select *Risk Data* and click on the option *Recalculate risk values if risk matrix altered (applies to ALL risks, ignoring filter criteria above)*.

Go to *Dashboard* to check the matrix. If the labels are not as you want them, follow instructions in ["Risk Matrix Descriptions"](#) on page 9.

3.5. Risk Matrix Descriptions

3.5.1. Likelihood Descriptions

If you are *not* using five levels of likelihood, you will have to either delete the likelihood levels you do not need (starting from the highest – see ["Removing A Likelihood Level"](#) on page 11), or add the *Likelihood* levels you need.

If you wish to change the *Likelihood* Names (not normally changed) and Descriptions (changes are often made) you will need to change the values (select the *System* tab, then select *System Data* and select *Likelihood* from the menu).

LIKELIHOOD DEFINITIONS

Likelihood	Name	Description	
1	Rare	May occur only in exceptional circumstances, can expect 1 event every 20 to 50 years	Edit
2	Unlikely	Could occur at some time, can expect 1 event every 5 to 20 years	Edit
3	Possible	Might occur at some time, can expect 1 event every 1 to 5 years	Edit
4	Probable	Will probably occur in most circumstances, can expect 1 event every year	Edit
5	Almost certain	Is expected to occur in most circumstances, can expect more than 1 event every year	Edit

With five levels of *Likelihood* there will be five rows numbered 1 to 5.

3.5.1.1. Triage

For a Triage matrix, you will have to edit the descriptions so that 1 is *Almost certain* and 5 is *Rare*.

3.5.2. Consequence Descriptions

If you are not using five levels of *Consequence*, you will have to delete the consequence levels you do not need, starting from the highest (see ["Removing A Consequence Level"](#) on page 11), or add the *Consequence* levels you need.

The *Consequence Descriptions* are not normally changed. However, if you decide they should be changed, click the *System* tab, select *System Data* and then select *Consequence* from the menu. Click on the *Select* link text beside the Consequence Description you want to edit. See ["Consequence"](#) on page 61 for more information about editing the Consequence Description.

With five levels of *Consequence* there will be five rows numbered 1 to 5.

The *Cut-off Value* should have values that are consistent across the Enterprise. The *Cut-off Value* is not used in calculations. If the *Cut-off Value* is shown, it should be consistent with the Enterprise Rating *Cut-off Values* which are used in the calculation of the Enterprise Rating.

CONSEQUENCE

	Consequence	Description	
1		Insignificant	Select
2		Minor	Select
3		Moderate	Select
4		Major	Select
5		Critical	Select

[Rename Consequence Labels](#)

The 13 *Consequence Labels* can be changed by clicking the *Rename Consequence Labels* button. To change these settings, select the *System* tab, select *System Data*, and select *Consequence* from the menu. The *Rename Consequence Labels* button is below the Consequence descriptions.

3.5.2.1. Triage

For Triage matrix you will have to edit the descriptions so that 1 is *Catastrophic* and 5 is *Insignificant*.

3.5.3. Risk Rating Descriptions

If you are using fewer than five levels of Risk Rating, you will have to delete the Rating levels you do not need, starting from the highest. If you are using more than five levels of Risk Rating, you will have to add the Rating levels you need. However because 4 levels of Rating is quite popular, level five may be deleted from within the application. The best way to handle this is to configure the matrix, ignoring level 5 and delete it when everything is configured.

The Risk Rating Descriptions are not normally changed. The Management Criteria are often changed. Both can be changed by the System Administrator selecting the *System* tab, then selecting *System Data* and selecting *Rating* from the menu.

With five levels of Rating there will be five rows numbered 1 to 5.

ID	Description	Management Criteria	Colour	Code	
1	Insignificant	Acceptable	Chartreuse	I	Edit
2	Low	Monitor	Chartreuse	L	Edit
3	Medium	Monitor	Yellow	M	Edit
4	High	Treatment Required	Red	H	Edit
5	Extreme	Immediate Treatment	Red	E	Edit

You may select the colour associated with each Rating.

You should enter the one-character code for each description. This is used in the one-character short columns (S-A-R-T) in the Risk Search form. Being one character, if you have description names that start with the same letter, you will have to compromise or use numerals 1-5.

For a Triage matrix you will have to edit the descriptions so that 1 is *Extreme* and 5 is *Negligible*.

For a 4-level Triage matrix just have 1-4 going from *Extreme* to *Low*.

3.5.4. Risk Rating Levels



Note: If you are using the *Custom* or *Triage* Risk matrix, set all Rating levels to zero as they are not used with Custom or Triage matrix types.

The Rating Level is used in the formula for the dynamic *Numeric Value* 5x5x5 Risk matrix to determine what cells in the Risk matrix are used for extreme, high, moderate, low and negligible. If the mathematical product of the *Likelihood* and *Consequence* is equal to or greater than a *Rating Level* but less than the next highest *Rating Level* that cell (intersection point) will be deemed to be that Risk Rating.

The Rating Levels must be set to 0 if Custom or Triage is used otherwise they may confuse Users.

Thus, if the Extreme Risk *Rating Level* is set to 20, then only intersections of 4x5, 5x4 and 5x5 will be rated extreme. The *Rating Levels* must be in ascending order, must start from zero and the must not be higher than 25.

3.5.5. Excess Risk Ratings

If you have a custom matrix and you have less than five levels of Risk Rating, the Risk matrix on the dashboard and in the Risk Matrix report will appear correctly.

However, if you select the *System* tab, select *System Data* and select *Rating* from the menu, you might see Level 5 (which you do not want). Delete Level 5 after you have configured the matrix correctly.

3.5.6. Removing A Likelihood Level

If you are absolutely sure you want to reduce the Likelihood levels to 4 levels (and not the Risk Rating levels to 4 levels), do this with Database Administrator's assistance:

1. First, back up the database.
2. Search for Risks that have a Likelihood equal to Level 5 and change the Likelihood to Level 4.
3. The Database Administrator should then delete row 5 in the database table *tblLikelihood*.
4. Select the *System* tab, select *System Data* and select *Change Matrix* from the menu. Enter the password *changematrix* and click the *Sign in* button.
5. Check the Risk matrix mapping is using the *Custom* matrix. If it is not, change it to *Custom*. Check all the intersections between Likelihood and Consequence are correctly mapped. If they are not, *Edit* the line and correct it.
6. Click the *Activate the Matrix* button (at the bottom of the screen, on the right).
7. Close all browser sessions and re-start OpRiskControl to check the matrix looks correct in the Risk *Dashboard*.



Note: If you are reducing the *Likelihood* to three levels, remove level 4 as well.

3.5.7. Removing A Consequence Level

If you are absolutely sure you want to reduce the *Consequence* levels to four (not the Risk Rating levels to four), do this with Database Administrator's assistance:

1. First, back up the database.
 2. Search for Risks that have a *Consequence* equal to Level 5 and change the *Consequence* to Level 4.
 3. The Database Administrator should then delete row 5 in the database table *tblConsequence*.
 4. Select the *System* tab, select *System Data* and select *Change Matrix* from the menu. Enter the password *changematrix* and click the *Sign in* button.
 5. Check the Risk matrix mapping is using the *Custom* matrix. If it is not, change it to *Custom*. Check all the intersections between *Likelihood* and *Consequence* are correctly mapped. If they are not, *Edit* the line and correct it.
 6. Click the *Activate the Matrix* button (at the bottom of the screen, on the right).
 7. Close all browser sessions and re-start OpRiskControl to check the matrix looks correct in the Risk *Dashboard*.
-



Note: If you are reducing the *Consequence* to three levels, remove level 4 as well.

4. Risk And Action Entry Overview

4.1. Risk Entry Forms

The following image shows the Tabbed Risk Form.

RISK DETAILS: ASSET AUDIT LOG REVEALS MISSING ASSETS

◀ Back to Search Results

Risk		Action	KRI	History	Analysis	Documents	Stakeholders
Context		Rating	Ownership and Dates	Financial			
Business Unit							
Division:	All Divisions						...
Department:	All Departments						...
Function:							...
Project:							...
Location:	All Locations						...
Category of Threat							
Risk Type	Human Failure						...
Event Type:	Failure to effectively operate						...
Area Threatened							
Asset Type:	Asset/Infrastructure						...
Asset:	Information Systems						...
Relative Value:	Medium						...
Other Categories							
Classification:	Strategic						
<div>Print Replicate Replicate with Actions Route To Staple</div> <div>Edit</div>							
Description		Controls and Actions		Custom Fields		Custom Lookups	
Risk Status:	Open	Item ID:	62	Other Ref No:			
Title:	Asset Audit Log reveals missing assets						
Description:	Missing Asset						
Categories:	Financial Crime						
Cause:							
Existing Controls:							
Early Warning Trigger:							
Action Strategy:							
<div>Default Form Settings</div> <div>My Form Settings</div>							

The *Workflow Form* (select the *System* tab, select the *System Settings* tab and select the *Workflow* tab) section of the page includes the options for selecting the type of Risk Form. For details on the Tabbed Risk entry form, refer to the *OpRiskControl User Guide*.

4.1.1. My Form Settings

The System Administrator may configure the *Default Form Settings* (on the *Risk Details* page) which selects which fields to show and hide.

Users who have permission to change their own form will see the link *My Form Settings* on the *Risk Details* page.

Click *My Form Settings* on the *Risk Details* page to see a panel that allows you to change your settings. Greyed-out items have been disabled by the System Administrator.

The right and lower panels allow you to hide data items and buttons that are not needed, while the panel at top left allows you to show data items and tabs.



Note: You can reset your form back to the arrangement set up by the System Administrator at any time by selecting *Restore Default* (in *Edit* mode) and then clicking the *Save* button.

4.1.2. Default Form Settings

The System Administrator may restrict data items and tabs using the *Default Form Settings*. View a Risk, and click the *Default Form Settings* link on the *Risk Detail* page.

The *Default Form Settings* page is displayed.

Default Form Settings

Activate all settings / Deactivate all settings ☐

Tabbed Form Settings	
Tabbed Risk Form	
Allow Financial Tab:	<input checked="" type="checkbox"/>
Allow Custom Text Fields:	<input checked="" type="checkbox"/>
Allow Custom Lookups:	<input checked="" type="checkbox"/>
Tabbed Action Form	
Allow Custom Text Fields:	<input checked="" type="checkbox"/>
Allow Custom Lookups:	<input checked="" type="checkbox"/>
Organization Structure	
Manage Projects:	<input checked="" type="checkbox"/>
Manage Function (e.g. sub-department):	<input checked="" type="checkbox"/>
Other Tab Settings	
Hide Controls and Actions Tab:	<input type="checkbox"/>
Hide Action Tab:	<input type="checkbox"/>
Hide History Tab:	<input type="checkbox"/>
Hide Analysis Tab:	<input type="checkbox"/>
Hide Documents Tab:	<input type="checkbox"/>
Hide Stakeholders Tab:	<input type="checkbox"/>

Field Settings	
Hide Action Reductions by Level/Percentage:	<input type="checkbox"/>
Hide Approved By and Date Approved:	<input type="checkbox"/>
Hide Assessed By:	<input type="checkbox"/>
Hide Asset Type (use only Asset):	<input type="checkbox"/>
Hide Date Exception Expires:	<input type="checkbox"/>
Hide Other Categories:	<input type="checkbox"/>
Hide Other Rating Information:	<input type="checkbox"/>
Hide Raised By:	<input type="checkbox"/>
Hide Relative Value:	<input type="checkbox"/>
Hide Residual Risk:	<input type="checkbox"/>
Hide Review Frequency and Dates:	<input type="checkbox"/>
Hide Risk Type (use only Event Type):	<input type="checkbox"/>
Hide Set for Opportunity:	<input type="checkbox"/>
Hide Target Residual:	<input type="checkbox"/>

Button Settings	
Hide Replicate Button:	<input type="checkbox"/>
Hide Routing Button:	<input type="checkbox"/>
Hide Stapled Button:	<input type="checkbox"/>

Apply these settings to all users who use the default form Edit



Note: When items are disabled on the *Workflow* tab (select the *System* tab, select the *System Settings* tab and select the *Workflow* tab) they are greyed-out here and they cannot be selected.

When the *Default Form Settings* are changed, Users must re-apply the default settings via their own *My Form Settings* link (on the Risk view page) by selecting *Restore Default*.

4.2. Action Entry Form

The following image shows the Action form.

RISK DETAILS - ACTION CODE OF RISK: FAILURE TO SIGN OFF PROJECT

◀ Back to Search Results

Risk | **Action** | KRI | History | Analysis | Documents | Stakeholders

[New Action](#)

Action Code	Stage	Action Owner	Due Date	Completed Date	Action Status	Test Result	Control Effectiveness		
Employee Training	In Progress				Active			History	Delete

[Edit](#)

Ownership and Dates

Ownership and Dates

Recorded By:

Date Recorded:

Action Owner:

Timeframe:

Due Date:

Action Approved By:

Date Approved:

Responsible Party:

Percent Complete:

Completed Date:

Action Management

Existing Control: ☐

Preferred Action: ☐

Frequency:

Last Completed:

Description | Custom Fields | Lookup

Action Status: Action ID:

Action Code:

Action Details:

Categories:

Status Details:

Test Result:

Test Result History:

Action Document:

Action Hyperlink:

[Print](#) [Route To](#) [Edit](#)

When viewing a Risk, you can select the *Action* tab to see a list of mitigation Actions that have been attached to the Risk. If you want to add an Action, click the *New Action* button.

5. Risk Form

OpRiskControl provides a standard tabbed form and custom forms allowing administrators to create Risk forms which are suitable for your business.

5.1. Tabbed Form

The tabbed form provides up to 70 fields to record a Risk. However, if the Risks your company will log do not require this many fields, Custom Forms can be created to tailor the information logged to OpRiskControl (see “[Custom Forms](#)”, below).

RISK DETAILS: ASSET AUDIT LOG REVEALS MISSING ASSETS

Back to Search Results

Risk Action KRI History Analysis Documents Stakeholders

Context Rating Ownership and Dates Financial

Business Unit

Division: All Divisions ...

Department: All Departments ...

Function: ...

Project: ...

Location: All Locations ...

Category of Threat

Risk Type: Human Failure ...

Event Type: Failure to effectively operate ...

Area Threatened

Asset Type: Asset/Infrastructure ...

Asset: Information Systems ...

Relative Value: Medium

Other Categories

Classification: Strategic

Edit

Description Controls and Actions Custom Fields Custom Lookups

Risk Status: Open Item ID: 62 Other Ref No:

Title: Asset Audit Log reveals missing assets

Description: Missing Asset

Categories: Financial Crime ...

Cause:

Existing Controls:

Early Warning Trigger:

Action Strategy:

Edit

Print Replicate Replicate with Actions Route To Staple

Default Form Settings My Form Settings

5.2. Custom Forms

An example custom form is shown below.

RISK DETAILS: FRAUDULENT USE OF EXPENSES

Back to Search Results

Risk Action KRI History Analysis Documents Stakeholders

Event Type: Fraud

Division: Across all Divisions

Department: Across all Departments

Function:

Project:

Asset: Expenses

Location: Across all Locations

Criminal Act

Title: Fraudulent use of expenses

Description: Fraudulent use of expenses

Risk Status: Open

Cause:

Likelihood: Unlikely ...

Consequence: Moderate ...

Risk Rating: Medium

Risk Recorded By: Alison Heard

Categories:

Print Replicate Staple Route To

Edit

To configure a custom form, select the *System* tab, select *System Settings* and then select the *Workflow* tab.

Click the *Edit* button at the bottom of the page, select *Custom Forms* and click the *Save* button. Now that Custom Forms has been enabled, you can create Custom Forms. Click the *Custom Forms* button. Click *Add new form* and then enter a name for the new custom form and a description. Click *Save* and then click *Back to list*.

5.2.1. Risk Level

To change the fields which are part of the new custom form, in the Risk Level column, click *Edit*. A dialog is displayed reminding you to make sure no one is using the form you are editing.

FORM RISK : SHORT FORM - RISK LEVEL

[◀ Back to List](#)

Click Sort button to apply the changes

Field Name	Display	Order	Mandatory	Original Name
Division	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Division
Department	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Department
Function	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Function
Project	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Project
Asset	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Asset
Event Type	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Risk Event
Location	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Location
Title	<input checked="" type="checkbox"/>	01	<input checked="" type="checkbox"/>	Title
Description	<input checked="" type="checkbox"/>	02	<input checked="" type="checkbox"/>	Statement
Categories	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Categories
Cause	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Cause
Consequence	<input checked="" type="checkbox"/>	99	<input checked="" type="checkbox"/>	Consequence
Likelihood	<input checked="" type="checkbox"/>	99	<input checked="" type="checkbox"/>	Likelihood
Risk Rating	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Risk Rating
Risk Recorded By	<input checked="" type="checkbox"/>	99	<input checked="" type="checkbox"/>	Risk Recorded By
Risk Status	<input checked="" type="checkbox"/>	99	<input checked="" type="checkbox"/>	Status
Acceptable	<input type="checkbox"/>	99	<input type="checkbox"/>	Acceptable
Action Reductions	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Reductions
Action Strategy	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Strategy
Alert Date	<input type="checkbox"/>	99	<input type="checkbox"/>	Alert Date
Assessed By	<input type="checkbox"/>	99	<input type="checkbox"/>	Assessed By
Assessor Rating	<input type="checkbox"/>	99	<input type="checkbox"/>	Assessor Rating
Classification	<input type="checkbox"/>	99	<input type="checkbox"/>	Classification
Compliance Alert To	<input type="checkbox"/>	99	<input type="checkbox"/>	Compliance Alert To

This screen lists all the fields which can be added to a custom form. The following fields must be present on the custom form and cannot be removed:

- Division
- Department
- Function (If *Show Additional Enterprise Structure* is set)
- Project (If *Show Additional Enterprise Structure* is set)
- Asset
- Even Type
- Location
- Title
- Description
- Consequences
- Likelihood

Select a field to include it on the form, or clear the selection to remove it from the form. The *Mandatory* option is used to ensure that, when the field is included on the form, it must be completed before the Risk can be saved. Clear the *Mandatory* option if you want users to be able to save the Risk without completing the field.

The placement of the fields on the form is set by the *Order* field. Some fields cannot be moved, these fields have N/A in the order field. Change the values in the *Order* fields so the

fields appear in the required order on the form. To create the custom form displayed earlier, the following settings were used.

[◀ Back to List](#)

Click Sort button to apply the changes

Field Name	Display	Order	Mandatory	Original Name
Division	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Division
Department	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Department
Function	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Function
Project	<input checked="" type="checkbox"/>	N/A	<input type="checkbox"/>	Project
Asset	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Asset
Event Type	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Risk Event
Location	<input checked="" type="checkbox"/>	N/A	<input checked="" type="checkbox"/>	Location
Title	<input checked="" type="checkbox"/>	01	<input checked="" type="checkbox"/>	Title
Description	<input checked="" type="checkbox"/>	02	<input checked="" type="checkbox"/>	Statement
Risk Status	<input checked="" type="checkbox"/>	03	<input checked="" type="checkbox"/>	Status
Cause	<input checked="" type="checkbox"/>	04	<input type="checkbox"/>	Cause
Likelihood	<input checked="" type="checkbox"/>	05	<input checked="" type="checkbox"/>	Likelihood
Consequence	<input checked="" type="checkbox"/>	06	<input checked="" type="checkbox"/>	Consequence
Risk Rating	<input checked="" type="checkbox"/>	07	<input type="checkbox"/>	Risk Rating
Risk Recorded By	<input checked="" type="checkbox"/>	08	<input checked="" type="checkbox"/>	Risk Recorded By
Categories	<input checked="" type="checkbox"/>	09	<input type="checkbox"/>	Categories
Acceptable	<input type="checkbox"/>	99	<input type="checkbox"/>	Acceptable
Action Reductions	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Reductions
Action Strategy	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Strategy

Click *Sort* and *Save* to re-order the fields in to the requested order and to save the changes to the form.

5.2.2. Action Level

Click *Back to List* and click *Edit* under *Action Level* for the new Custom Form. This screen lists all the fields which can be added to a custom Action form.

[◀ Back to List](#)

Click Sort button to apply the changes

Field Name	Display	Order	Mandatory	Original Name
Action Code	<input checked="" type="checkbox"/>	01	<input checked="" type="checkbox"/>	Action Code
Details	<input checked="" type="checkbox"/>	02	<input checked="" type="checkbox"/>	Details
Completed Date	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Completed Date
Consequence (%)	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Consequence (%)
Control Effectiveness	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Control Effectiveness
Due Date	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Due Date
Reduce Likelihood (%)	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Reduce Likelihood (%)
Test Result	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Test Result
Test Result History	<input checked="" type="checkbox"/>	99	<input type="checkbox"/>	Test Result History
Action Approved By	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Approved By
Action Cost	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Cost
Action Custom 1	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 1
Action Custom 10	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 10
Action Custom 2	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 2
Action Custom 3	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 3
Action Custom 4	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 4
Action Custom 5	<input type="checkbox"/>	99	<input type="checkbox"/>	Action Custom 5

The fields displayed on the Action form can be configured in the same way as the Risk Form. The following fields must appear on the Action form and cannot be removed.

- Action Code
- Details
- Due Date
- Completed Date

Select the fields you want to appear on the Action form for the Custom form, using the *Order* field to set the order the fields appear on the form. Click *Sort and Save* to re-order the fields in to the requested order and to save the changes to the action form.

5.2.3. Using A Custom Form

When the Custom Form has been designed, it must be associated with the Risk Type it can be used with. Select the *Manage* tab, then select *Reference Data* and then select *Risk Types*. Click on the *Edit* link beside the Risk Type you want to use the new Custom Form. Then select the Custom Form from the drop down list. Click the *Save* link to save the change.

Risk Type	Short Name		Risks	L	C	
Criminal Act	Criminal Act	All Short form	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Save Cancel
Human Failure	Human Failure		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit

In a similar way, link the Custom Form to other Risk Types as required.

When both tabbed forms and custom forms are used, click *New Risk* to create a new Risk using the tabbed form, or click *New Risk (Custom Form)* to create a new Risk using the Custom Form linked to the Risk Type selected.



Note: To use Custom Forms only, ensure every Risk Type is associated with a Custom Form before disabling Tabbed Forms.

6. System Settings

System Settings allows the System Administrator to change system wide settings. These pages may vary at your installation due to licence key settings.

This information is normally available to, and should only be changed by, the System Administrator.

6.1. General Tab

SYSTEM SETTINGS - GENERAL

General Reporting History Security Workflow Formula Options Setup

Welcome Message

Organisation: Mitrates Holdings, Inc.

Title:

Message:

Localisation

Culture: English (United Kingdom)

Other Settings

Autogenerate Codes: ☒ Prefix:

Also copy prefix to changed risks: ☒

Enable Google Links: ☐

Hide Logo: ☐

[Refresh System Settings](#) [Edit](#)

6.1.1. Welcome Message

If required, enter your company name in *Organisation*.

Title and *Message* may be used to display a message-of-the-day or important message from the System Administrator. If both are left blank there will be no pop-up box on the Home page at login.

Other Options Preferences

close

Organisation

Title

Message



Note: The Welcome Message is displayed only when the *Home Page* is set as the *Startup Page*. Select the *Preferences* tab, select *Context Profile*, click *Edit* and, for the option *Startup Page*, select *Home Page*. Click *Save*.

6.1.2. Localisation

Selecting the *Culture* determines the currency symbol (for example, £) and numeric value separators. It is not involved in system wide translation.

6.1.3. Other Settings

Select *Autogenerate Codes* to configure the system to automatically generate Risk IDs.

If required, enter a *Prefix* in the box. For example, entering *Risk* in the *Prefix* box causes new Risks to be numbered (for example) Risk100, Risk101.

Select *Also copy prefix to changed risks* to cause the configured *Prefix* to be added to the Risk ID when a Risk (which does not have the *Prefix* in its Risk ID) is changed. A suggested use of this feature is to change the *Prefix* to be the last 2 digits of the year and separate with a colon (for example 13:). It will then be easy to see which Risks have been updated this year.



Note: The *Prefix* is ignored when searching for a Risk by its ID.

Google Links is provided for access to the Google Toolbar which includes a spellchecker.

If you select *Hide Logo*, the logo at the top of the page is hidden on many of the pages allowing you more space on your working forms.

6.2. Reporting Tab

The screenshot shows the 'Reporting' configuration tab. It contains several input fields and checkboxes. The 'Title' field is set to 'Mitrates Holdings, Inc.' and has a checkbox 'Use Division Name in Risk Management report title'. The 'Top Right' field is set to 'OpRiskControl'. The 'Bottom Left' field is set to 'Copyright (c) 2017 Mitrates Holdings, Inc.' and has a checkbox 'Use Division Name in Risk Management report footer'. There are checkboxes for 'Include Risk List Report in HTML Format' (unchecked) and 'Show reports in new window' (checked). Below these are radio buttons for 'Show Risk Matrix' with options: 'Likelihood on left of matrix' (selected), 'Consequence on left of matrix' (unchecked), and 'Inverted' (unchecked). At the bottom, there is a checkbox 'Ask to include Department objectives in reports grouped by Department' (unchecked).

6.2.1. Reporting

Specify headers and footers to be used on reports (these fields are included on most, but not all, reports).

- *Title* – Provide the text to appear in the top left of the report. (*Title* is not used when *Use Division Name in report title* is selected – see below.)
- *Top Right* – Provide the text to appear in the top right of the report.
- *Bottom Left* – Provide the text to appear in the bottom left of the report. (*Bottom Left* is not used when *Use Division Name in report footer* is selected – see below.)
- *Include Risk List Report in HTML Format*: – When selected and when the Risk List Report is selected, an extra print button is provided: *Print Using HTML*. This button displays an HTML version of the *Risk List Report*.
- *Show reports in new window* – Select if you want reports to be displayed in a new browser window. When cleared, the current browser window is used. Use the *back* button to return to OpRiskControl.
- *Show Risk Matrix* – Whenever the selected report includes a Risk Matrix:
 - *Likelihood on left of matrix* – *Likelihood* is shown on the left side of the Risk Matrix (as shown in the examples below).
 - *Consequences on left of matrix* – *Consequence* is shown on the left side of the Risk Matrix.

- *Inverted* – When selected, for the *Likelihood*, *Rare* appears at the top and *Almost certain* is at the bottom.

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Rare	6	2	0	0	0
Unlikely	0	1	0	0	0
Possible	0	4	3	0	0
Probable	0	0	0	0	0
Almost certain	0	0	0	0	0

When cleared, *Almost certain* appears at the top and *Rare* appears at the bottom.

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Almost certain	0	0	0	0	0
Probable	0	0	0	0	0
Possible	0	4	3	0	0
Unlikely	0	1	0	0	0
Rare	6	2	0	0	0

- *Ask to include Department objectives in reports grouped by Department* – Some reports have the option to *Group By* (for example, the *Action Status Report* and the *Risk List Report*). When *Ask to include Department objectives in reports grouped by Department* is selected and when *Group By* is set to *Department*, an extra option appears in the Report Wizard which allows you to select *Append objectives to group name*. When *Append objectives to group name* is selected, any item in the selected Report which is assigned to a Department which has an Objective configured, shows the department's Objective appended to the Department name on the Report. See ["Departments" on page 92](#) for information on adding an Objective to a Department.
- *Use Division Name in Risk Management report title* – Select if you want reports to use the relevant *Division Name* **instead** of *Title* in the Risk Management report.
- *Use Division Name in Risk Management report footer* – Select if you want reports to use the relevant *Division Name* instead of *Bottom Left* in the Risk Management report.

6.3. History Tab

Many Risk and Action events are automatically logged to the Risk History page or the Action History page, as appropriate. However, other history items are optional and can be selected here.

Optional Risk History		Optional Action History	
Log change of Approval:	<input checked="" type="checkbox"/>	Log any change of Approval:	<input checked="" type="checkbox"/>
Log any change of Division:	<input checked="" type="checkbox"/>	Log any change of Effectiveness:	<input checked="" type="checkbox"/>
Log any change of Department:	<input checked="" type="checkbox"/>	Log any change of Dates:	<input checked="" type="checkbox"/>
Log any change of Location:	<input checked="" type="checkbox"/>	Log any change of Status:	<input checked="" type="checkbox"/>
Log any change of Asset:	<input checked="" type="checkbox"/>	Log any change of Action Owner:	<input checked="" type="checkbox"/>
Log any change of Function:	<input checked="" type="checkbox"/>	Log who changes an Action Record:	<input checked="" type="checkbox"/>
Log any change of Project:	<input checked="" type="checkbox"/>	Log any change of Action Details:	<input checked="" type="checkbox"/>
Log any change of Owner:	<input checked="" type="checkbox"/>	Log any change of Action Status Details:	<input checked="" type="checkbox"/>
Log any change of Contact:	<input checked="" type="checkbox"/>	Log Action Notifications:	<input checked="" type="checkbox"/>
Log who changes a Risk Record:	<input checked="" type="checkbox"/>	Log any change of Categories:	<input checked="" type="checkbox"/>
Log Risk Notifications:	<input checked="" type="checkbox"/>		
Log Overall Effectiveness:	<input checked="" type="checkbox"/>		
Log any change of Categories:	<input checked="" type="checkbox"/>		
Log any change of Documents:	<input checked="" type="checkbox"/>		
Log any change of Stakeholders:	<input checked="" type="checkbox"/>		
Automatic Risk History		Automatic Action History	
Initial Rating		Action Recorded	
Risk Review (rating or date)		Action Completed	
Status Change		Action Deleted	
Risk History Location		Action History Location	
Log action history to risk form:	<input type="checkbox"/>	Log action history to action form:	<input checked="" type="checkbox"/>

6.3.1. Optional History

When the *Optional Risk History* option *Log any changes of Owner* is selected, not only are manual changes of a Risk owner logged to the history page, but so are any bulk Risk reassignment in User Management (see ["Reassign Risks" on page 83](#) and see ["Reassign Actions" on page 84](#) for more information on reassigning Risks and Actions). The same applies to *Log any change of Contact* and *Log any change of Action Owner*.

6.3.2. Automatic Risk And Action History

The items listed in this section are always logged and cannot be disabled.

6.3.3. History Location

Two settings are provided to allow you to decide where the Action history is logged.

- *Log action history to risk form*
- *Log action history to action form*

You can decide to:

- *Clear* both options, and not log the Action history.
- Select *Log action history to risk form* to log the Action history to the Risk page. To view an Action's History on the Risk page, perform a Risk Search, *View* a Risk and select the History tab. All Action History since this option was selected is listed on this page. If this option is cleared, no more Action History is logged here.
- Select *Log action history to action form* to log the Action history to the Action page. To view an Action's History on the Action page, perform a Risk Search, then *View* a Risk, select the *Action* tab and click the *History* link. All Action History since this option was selected is listed on this page. If this option is cleared, no more Action History is logged here.
- Select both options to log the Action history to both the Action and the Risk pages.

6.4. Security Tab

The screenshot shows the 'SYSTEM SETTINGS - SECURITY' interface. The 'Security' tab is active. Under the 'Role Based Security' section, there are five options, each with an unchecked checkbox:

- Limit Risk Access By Division:
- Limit Risk Access By Department:
- Limit Risk Access By Location:
- Limit Risk Access By Asset:
- Limit User List By Division:

Below these is a text input field with the placeholder text 'Reset all User Search Criteria to use "My..." whenever applicable:' and an unchecked checkbox.

The *Security* tab allows the System Administrator to specify the level of business unit security on the system. Most customers limit access to Division only.

- Select *Limit Risk Access by Division* and then, in RBS, assign people to the relevant Division.



Note: If you want a User to have access to more than one Division you will need to assign them to each Division.

- Select *Limit Risk Access by Department* and then, in RBS, assign people to the relevant Department.



Note: If you want a User to have access to more than one department you will need to assign them to each Department.

- *Limit Risk Access by Location* is rarely used. In RBS, assign people to the relevant Location.



Note: If you want a User to have access to more than one location you will need to assign them to each Location.

- *Limit Risk Access by Asset* is rarely used. In RBS, assign people to the relevant Asset.



Note: If you want a User to have access to more than one asset you will need to assign them to each Asset.

If you want to have access to all Divisions or Departments or Locations or Assets, you can assign yourself to *All Divisions* or *All Departments* or *All Locations* or *All Assets* in RBS.

You can allow some Users to have read-only access to a common set of Risks by Division, such as a pseudo-division named *Across all Division*. To do this, edit that Division record via the *More* link and select *Allow this division to be viewed by all users*. You can then assign that division to the Users who need access to all the Risks in that Division.

To reduce the size of user picklists, you can assign a Division to each User and then enable *Limit User List by Division* (see ["Example Of Row Level Security" on page 57](#)). When entering Risks, the list will then be filtered to show only Users in the selected Division.

- *Reset all Search Criteria to use "My..." whenever applicable* – When one or more of the *Limit Risk Access By* options have been selected and a User has been assigned to a Division, Department, Location and/or Asset, as appropriate, the Risk Search page labels the fields *My Divisions*, *My Departments*, *My Locations* and/or *My Assets*, as appropriate.

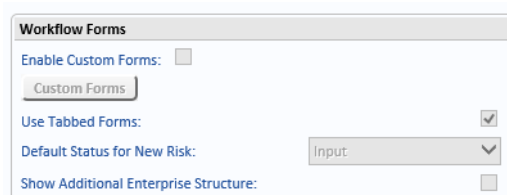


Note: *Reset all Search Criteria to use "My..." whenever applicable* is used when at least one of the following options is selected: *Limit Risk Access By Division*, *Limit Risk Access By Department*, *Limit Risk Access By Location* and/or *Limit Risk Access By Asset*.

6.5. Workflow Tab

Workflow Forms Enable Custom Forms: <input type="checkbox"/> <input type="button" value="Custom Forms"/> Use Tabbed Forms: <input checked="" type="checkbox"/> Default Status for New Risk: <input type="text" value="Input"/> Show Additional Enterprise Structure: <input checked="" type="checkbox"/>	Notification Manager Notification Monitor: <input type="text" value="Mitrates Support"/> Enable Automated Email: <input checked="" type="checkbox"/> Setup: <input type="button" value="Alerts and Escalation"/> 20 settings Setup: <input type="button" value="Updates and Reminders"/> 13 settings Primary Contact Alert To: <input type="radio"/> Contact <input checked="" type="radio"/> Owner												
Tabbed Form Settings Tabbed Risk Form Allow Financial Tab: <input checked="" type="checkbox"/> Allow Custom Text Fields: <input checked="" type="checkbox"/> Allow Custom Lookups: <input checked="" type="checkbox"/> Tabbed Action Form Allow Custom Text Fields: <input checked="" type="checkbox"/> Allow Custom Lookups: <input checked="" type="checkbox"/> Organization Structure Manage Projects: <input checked="" type="checkbox"/> Manage Function (e.g. sub-department): <input checked="" type="checkbox"/> Reference Data Allow Risk Type: <input checked="" type="checkbox"/> Allow Asset Type: <input checked="" type="checkbox"/> Allow Classification: <input checked="" type="checkbox"/> Rating Information Allow Residual Risk: <input checked="" type="checkbox"/> Allow Target Residual: <input checked="" type="checkbox"/> Allow Other Rating Information: <input checked="" type="checkbox"/> Allow Effectiveness Information: <input checked="" type="checkbox"/>	<table border="1"> <thead> <tr> <th>Notification Settings</th> <th>Days</th> </tr> </thead> <tbody> <tr> <td>Risk Review Due Period:</td> <td><input type="text" value="7"/></td> </tr> <tr> <td>Mitigation Action Due Period:</td> <td><input type="text" value="30"/></td> </tr> <tr> <td>Reminders Due Period:</td> <td><input type="text" value="2"/></td> </tr> <tr> <td>Recurring Action Reset (Days):</td> <td><input type="text" value="10"/></td> </tr> <tr> <td>Compliance Due Period:</td> <td><input type="text" value="7"/></td> </tr> </tbody> </table> Process Management <input type="button" value="Role Based Security"/> <input type="button" value="Business Rules Manager"/>	Notification Settings	Days	Risk Review Due Period:	<input type="text" value="7"/>	Mitigation Action Due Period:	<input type="text" value="30"/>	Reminders Due Period:	<input type="text" value="2"/>	Recurring Action Reset (Days):	<input type="text" value="10"/>	Compliance Due Period:	<input type="text" value="7"/>
Notification Settings	Days												
Risk Review Due Period:	<input type="text" value="7"/>												
Mitigation Action Due Period:	<input type="text" value="30"/>												
Reminders Due Period:	<input type="text" value="2"/>												
Recurring Action Reset (Days):	<input type="text" value="10"/>												
Compliance Due Period:	<input type="text" value="7"/>												
	User Permissions Allow Risk Delete by Recorder: <input checked="" type="checkbox"/> Allow Unapproved Risk Delete by Recorder: <input checked="" type="checkbox"/> Allow Risk Delete by Owner: <input checked="" type="checkbox"/> Allow Risk Delete by Contact: <input checked="" type="checkbox"/> Allow User to Disable Filter: <input type="checkbox"/>												

6.5.1. Workflow Forms



You may select from various form types:

- *Custom Forms* (for any special requirements).
- *Tabbed Forms* (most commonly used).

At least one form type must be selected.



Note: When you want to use Custom Forms only, you must associate every Risk Type with a Custom Form. If there are any Risk Types which are not associated with a Custom Form, when you try to save the configuration (with *Enable Custom Forms* selected and *Use Tabbed Forms* cleared), you will see the following message:

There are existing risks without an associated custom form. To disable tabbed forms, each existing risk must have an associated custom form. Select Risk Types on the Manage tab and assign a custom form to each Risk Type.

See [“Using A Custom Form” on page 20](#) for information on assigning a Custom Form to a Risk Type.

The Custom Forms currently in use are listed under the *Custom Forms* button.

Activation of Custom Forms requires activation in the OpRiskControl Licence key and must be activated here before you may access the *Custom Forms* button.

The *Default Status for New Risk* will normally be *Input*, but you may change the default status to *Open*. When the *Default Status* is set to *Input*, Risks are validated before being set to *Open*. When the *Default Status* is set to *Open*, new Risks do not go through a validation process.

When *Show Additional Enterprise Structure* is cleared, the following search fields are available on the *Risk Search* form: *Division*, *Business Unit*, *Asset*, *Risk Type*, *Event Type*, *Status*, *Location* and *Owner*.

When *Show Additional Enterprise Structure* is selected, the search fields *Project*, *Function* and *Class* are included in addition to the search fields listed above.

6.5.2. Tabbed Form Settings

Tabbed Form Settings	
Tabbed Risk Form	
Allow Financial Tab:	<input checked="" type="checkbox"/>
Allow Custom Text Fields:	<input checked="" type="checkbox"/>
Allow Custom Lookups:	<input checked="" type="checkbox"/>
Tabbed Action Form	
Allow Custom Text Fields:	<input checked="" type="checkbox"/>
Allow Custom Lookups:	<input checked="" type="checkbox"/>
Organization Structure	
Manage Projects:	<input checked="" type="checkbox"/>
Manage Function (e.g. sub-department):	<input checked="" type="checkbox"/>
Reference Data	
Allow Risk Type:	<input checked="" type="checkbox"/>
Allow Asset Type:	<input checked="" type="checkbox"/>
Allow Classification:	<input checked="" type="checkbox"/>
Rating Information	
Allow Residual Risk:	<input checked="" type="checkbox"/>
Allow Target Residual:	<input checked="" type="checkbox"/>
Allow Other Rating Information:	<input checked="" type="checkbox"/>

If *Tabbed Forms* is activated, this panel is displayed so that extra Risk and Action data entry pages may be activated by each User.

Even though these pages are enabled here, some Users may have no need for these pages and therefore need not activate these extra pages in their *My Form Settings*.

6.5.2.1. Tabbed Risk Form

- *Allow Financial Tab* – The *Financial* tab is available when creating and viewing Risks.
- *Allow Custom Text Fields* – The *Custom Fields* tab is available when creating and viewing Risks.
- *Allow Custom Lookups* – The *Custom Lookups* tab is available when creating and viewing Risks.



Note: If these tabs are not available when creating or viewing a Risk, check the appropriate options are set in both *Default Form Settings* and in *My Form Settings*.

6.5.2.2. Tabbed Action Form

- *Allow Custom Text Fields* – The *Custom Fields* tab is available when creating and viewing Actions.
- *Allow Custom Lookups* – The *Lookups* tab is available when creating and viewing Actions.



Note: If these tabs are not available when creating or viewing an Action, check the appropriate options are set in both *Default Form Settings* and in *My Form Settings*.

6.5.2.3. Organization Structure

- *Manage Projects* – A field called *Project* is added to the Risk screen. *Projects* are added by selecting the *Manage* tab, selecting *Reference Data* and selecting *Project* from the menu. See “*Project*” on page 95 for more information.
- *Manage Functions (e.g. sub-department)* – A field called *Function* is added to the Risk screen. *Functions* are added by selecting the *Manage* tab, selecting *Reference Data* and selecting *Function* from the menu. See “*Function*” on page 94 for more information.

6.5.2.4. Reference Data

- *Allow Risk Type* – When selected, on the Risk form, in the *Category of threat* section, both *Risk Type* and *Event Type* fields are available. When cleared, only *Risk Event* is available.



Note: When *Allow Risk Type* is cleared, the option *Hide Risk Type (use only Event Type)* in *My Form Settings* is automatically selected and cannot be edited until this option is selected again. Therefore, if you later select this *Allow Risk Type*, every User must update their *My Form Settings*.

- *Allow Asset Type* – When selected, on the Risk form, in the *Area Threatened* section, both *Asset Type* and *Asset* fields are available. When cleared, only *Asset* is available.



Note: When *Allow Asset Type* is cleared, the option *Hide Asset Type (use only Asset)* in *My Form Settings* is automatically selected and cannot be edited until this option is selected again. Therefore, if you later select this *Allow Asset Type*, every User must update their *My Form Settings*.

6.5.2.5. Rating Information

- *Allow Residual Risk* – When viewing or creating a Risk, the *Residual Risk (with Existing Controls)* section is included on the *Rating* tab.



Note: When *Allow Residual Risk* is cleared, the option *Hide Residual Risk* in *My Form Settings* is automatically selected and cannot be edited until this option is selected again. Therefore, if you later select this *Allow Residual Risk*, every User must update their *My Form Settings*.

- *Allow Target Residual* – When viewing or creating a Risk, the *Target Residual (with new Actions)* section is included on the *Rating* tab.



Note: *Allow Target Residual* can be selected only when *Allow Residual Risk* has been selected.



Note: When *Allow Target Residual* is cleared, the option *Hide Target Residual* in *My Form Settings* is automatically selected and cannot be edited until this option is selected again. Therefore, if you later select this *Allow Target Residual*, every User must update their *My Form Settings*.

- *Allow Other Rating Information* – When viewing or creating a Risk, the *Other Rating Information* section is included on the *Rating* tab.

6.5.3. Notification Manager

The activation of *Automated Notifications* requires the installation of a Windows Service, activation in the OpRiskControl Licence key, and it also needs to be activated here before it will operate.

Alerts and escalations may be set up for reviews that are due and overdue, Actions that are due and overdue, and the assignment of a Risk contact, Risk Owner or Risk Stakeholders.

In edit mode, select a Notification Monitor from the drop-down list. The Notification Monitor can be sent Alerts and Escalations. See [“Alerts And Escalations” on page 30](#) for details.

Select *Enable Automated Email* to enable the Notifications. When this option is *cleared*, no email notifications are sent and the Notification settings configured via the Alerts and Escalations button are ignored.

Click *Alerts and Escalations* to configure who will receive emails and alerts when items are overdue or have been changed. The number of currently selected tick-boxes on the *Alert and Escalation* page is shown to the right of the *Alerts and Escalation* button.

Alerts are sent to the Primary Contact (when configured on the *Alert and Escalation* page). Here, select either the Risk Contact or Owner to determine the *Primary Contact*. The Risk's Owner and Contact are both configured on the Risk's *Ownership and Dates* tab.

6.5.3.1. Alerts And Escalations

Click *Edit* on the line you want to make changes to.

Setup Notifications		Alerts			Escalations								
Notification	Residual Level	Primary Contact	Every x days	Owner	Notification Monitor	Function Manager	Project Manager	Department Manager	Division Manager	Asset Level	Days Delay	Every x days	
Review due	Insignificant	<input checked="" type="checkbox"/>	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6	6	Edit
Review due	Low	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review due	Medium	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review due	High	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review due	Extreme	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review overdue	Insignificant	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review overdue	Low	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review overdue	Medium	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Review overdue	High	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		3	Edit
Review overdue	Extreme	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		3	Edit
Action due	Insignificant	<input type="checkbox"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action due	Low	<input type="checkbox"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action due	Medium	<input type="checkbox"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action due	High	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action due	Extreme	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action overdue	Insignificant	<input type="checkbox"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action overdue	Low	<input type="checkbox"/>	12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action overdue	Medium	<input type="checkbox"/>	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		12	Edit
Action overdue	High	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit
Action overdue	Extreme	<input type="checkbox"/>	3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		6	Edit

[Refresh](#)
[Back to System Settings](#)

There are four types of Notifications:

- *Review due* – the *Date Next Review* (configured on the *Ownership and Dates* tab on the Risk details form) is approaching. The number of days is set in the *Risk Review Due Period*. See [“Notification Settings” on page 34](#) for more information.
- *Review overdue* – the *Date Next Review* (configured on the *Ownership and Dates* tab on the Risk details form) has passed and the Risk has not yet been reviewed.
- *Action due* – the *Action Due Date* (configured on the *Action’s Ownership and Dates* tab) is approaching. The number of days is set by the *Mitigation Action Due Period*. See [“Notification Settings” on page 34](#) for more information.
- *Action overdue* – the *Action Due Date* (configured on the *Action’s Ownership and Dates* tab) has passed and the Action has not yet been completed.

For each type of Notification, the list of Risk Ratings is provided. It is therefore possible to have different notifications and alerts configured for each of the risk ratings for each of the types of Notification listed above.

6.5.3.1.1. Alerts

Alerts are displayed on the user’s *Alerts* tab.

For each *Residual Level* in each Notification type (*Review due*, *Review overdue*, *Action due* and *Action overdue*), select whether the *Primary Contact* will receive an alert (the *Primary Contact* is configured on the *Workflow* page on the *System Settings* tab. See [“Notification Manager” on page 30](#) for more information.

Set the frequency of Alerts. For example, set 6 to ensure the Primary Contact receives an Alert every 6 days until the Risk Review is completed or the Action is completed. This number is ignored if the *Primary Contact* option is *cleared*.

6.5.3.1.2. Escalations

- *Owner* – the Owner of the Risk or Action (as appropriate) is sent an email. The Owner is set on the Risk or Action’s *Ownership and Dates* tab, as appropriate.
- *Notification Monitor* – the *Notification Monitor* is sent an email. The *Notification Monitor* is set on the *Workflow* tab, on the *System Settings* tab. See [“Notification Manager” on page 30](#) for more information.
- *Function Manager* – The *Function Manager* for the Function configured for the Risk is sent an email. If there is no *Function* configured for the Risk, or if there is no *Function Manager* configured for the Risk’s Function, then no email is sent.
- *Project Manager* – The *Project Manager* for the Project configured for the Risk is sent an email. If there is no *Project* configured for the Risk, or if there is no *Project Manager* configured for the Risk’s Project, then no email is sent.
- *Department Manager* – The *Department Manager* for the Department configured for the Risk is sent an email. If there is no *Department* configured for the Risk, or if there is no *Department Manager* configured for the Risk’s Department, then no email is sent.
- *Division Manager* – The *Division Manager* for the Division configured for the Risk is sent an email. If there is no *Division* configured for the Risk, or if there is no *Division Manager* configured for the Risk’s Division, then no email is sent.
- *Asset Level* – The *Asset* configured for the Risk is sent an email. If there is no *Asset* configured for the Risk, then no email is sent.
- *Days Delay* – Enter the number of days (after the escalation occurred) before the first email is sent. For example, if you enter 3, then the first email is sent 3 days after a Risk’s Review or Action was due or a Risk review or Action became overdue.
- *Every x days* – Enter the number of days between subsequent emails. For example, if you enter 2, then, after the first email, more emails are sent every two days.



Note: When Alerts or Escalations are set for a *Review due*, the alerts and escalations stop when the Review is completed or becomes overdue.

When Alerts or Escalations are set for a *Review overdue*, the alerts and escalations stop when the Review is completed.

When Alerts or Escalations are set for an *Action due*, the alerts and escalations stop when the Action is completed or becomes overdue.

When Alerts or Escalations are set for an *Action overdue*, the alerts and escalations stop when the Action is completed.

6.5.3.2. Updates And Reminders

This screen is used to configure if emails should be sent to the Notification Manager and other users when specific events have occurred.

Setup Updates		Alert User	Alert Notification Monitor	
Notification	Single Alert	Single Alert	Single Alert	
Contact assigned	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Owner assigned	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Action owner assigned	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Stakeholder assigned	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Update to stakeholder	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Risk raised - exemption expired	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Owner that Action completed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Setup Compliance		Alert User	Alert Notification Monitor	
Notification	Single Alert	Single Alert	Single Alert	
Compliance Due	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Compliance Overdue	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit
Setup Deactivations		Alert User	Alert Notification Monitor	
Notification	Single Alert	Single Alert	Single Alert	
Alert Deactivated User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Setup Incidents		Alert User	Alert Notification Monitor	
Notification	Single Alert	Single Alert	Single Alert	
Internal Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Insurance Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Safety Regulator Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Company Regulator Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Environmental Regulator Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Other Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Key Indicators		Alert User	Alert Notification Monitor	
Notification	Single Alert	Single Alert	Single Alert	
Monthly Key Indicator Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Edit

[Refresh](#) [Back to System Settings](#)

6.5.3.2.1. Setup Updates

The first section is used to set email notifications about updates to Risks. Emails can be sent to a user assigned to the Risk as the Contact, Owner, Action Owner, etc. and/or to the Notification Monitor. (The *Notification Monitor* is set on the *Workflow* tab, on the *System Settings* tab. See "[Notification Manager](#)" on page 30 for more information.)

- *Contact assigned* – Send an email to the *Contact* assigned to a Risk and/or to the Notification Monitor.

- *Owner assigned* – Send an email to the *Owner* assigned to a Risk and/or to the Notification Monitor.
- *Action owner assigned* – Send an email to the *Owner* assigned to a Risk's *Action* and/or to the Notification Monitor.
- *Stakeholder assigned* – Send an email to the *Stakeholder* assigned to a Risk and/or to the Notification Monitor.
- *Update to stakeholder* – Send an email to the updated *Stakeholder* assigned to a Risk and/or to the Notification Monitor.
- *Risk raised - exemption expired* – Send an email to the *Owner* assigned to a Risk and/or to the Notification Monitor when an exemption has expired. The *Date Exemption Expires* is set on the Risk's *Ownership and Dates* tab.
- *Owner that Action completed* – Send an email to the Action Owner and/or the Notification Monitor when an Action is completed.

6.5.3.2.2. Setup Compliance

There are two Compliance notifications.

- *Compliance Due* – Send an email to the user configured for *Compliance Alert To* (set on the Risk's *Ownership and Dates* tab) and/or to the Notification Monitor when the Alert is approaching. The number of days is set in the *Compliance Due Period*. See "[Notification Settings](#)" on page 34 for more information.
- *Compliance Overdue* – Send an email to the user configured for *Compliance Alert To* (set on the Risk's *Ownership and Dates* tab) and/or to the Notification Monitor when the Alert date has passed.

6.5.3.2.3. Setup Deactivations

There is one deactivation notification:

- *Alert Deactivated User* – Send a single email to the Notification Monitor when a user account is deactivated.

6.5.3.2.4. Setup Incidents

There are six incident notifications:

- *Internal Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Internal Email* field regarding an Incident.
- *Insurance Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Insurance Email* field regarding an Incident.
- *Safety Regulator Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Safety Regulator Email* field regarding an Incident.
- *Company Regulator Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Company Regulator Email* field regarding an Incident.
- *Environmental Regulator Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Environmental Regulator Email* field regarding an Incident.
- *Other Email* – Send an email to the Notification Monitor when an email is sent to the email address configured on the *Options* tab of the *System Settings* tab in the *Other Email* field regarding an Incident.

6.5.3.2.5. Key Indicators

There is one key indicator notification:

- *Monthly Key Indicator Email* - Send a monthly email to the Owner assigned to the *Key Indicator* and/or to the Notification Monitor.

6.5.4. Notification Settings

Notification Settings	Days
Risk Review Due Period:	7
Mitigation Action Due Period:	30
Reminders Due Period:	2
Recurring Action Reset (Days):	10
Compliance Due Period:	7

Specify how many days before a Risk review, an Action is due, and a recurring Action is due, the responsible UserFigure 14.2, "Action Frequency," on page 90s are sent a reminder.

- *Risk Review Due Period* – Set the number of days before a Risk Review is due that a reminder is sent (if configured).
- *Mitigation Action Due Period* – Set the number of days before an Action is due that a reminder is sent (if configured).
- *Reminders Due Period* – Set the number of days before a Reminder is due that a reminder is sent (if configured).
- *Recurring Action Reset (Days)* – Set the number of days before a recurring Action's *Due Date* that its *Completed Date* is cleared. This must be a *negative* number. For example, consider a recurring Action with the *Frequency* set to *Annually*. If this *Annually* recurring Action was last Completed on 1st January 2014 and *Recurring Action Reset (Days)* is set to -10, the Action's *Completed Date* of 1/1/2014 will be cleared 10 days before its *Due Date* of 1st January 2015 (as the default value for a Year is 365 days – see *Manage, Reference Data, Action Frequency* for information on changing this). The date of reset will be 22nd December 2014. As the *Completed Date* is now blank, it is eligible for a reminder to be sent. Once the *Mitigation Action Due Period* for an action is reached, an email will be sent.
- *Compliance Due Period* – Set the number of days before a Compliance is due that a reminder is sent (if configured).

6.5.5. Process Management

Click *Role Base Security* to navigate to the *Role Permissions* tab on the *Security* page on the *System* tab.

6.5.6. User Permissions

Select what the Risk Owner, Recorder and Contact can delete.

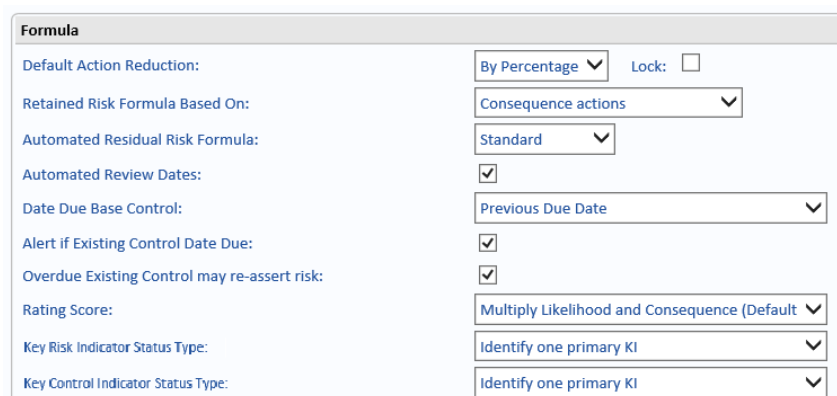
If RBS is active and the user has the RBS Administration permission *Super User Edit or Delete any Risk/Incident* selected, the user will be able to delete all Risks regardless of the settings on the *Workflow* tab. If the RBS permission *Super User Edit or Delete any Risk/Incident* is cleared,

the *Workflow* tab settings are considered. (This RBS setting can be overridden by the administration settings in the web.config file.)

TABLE 1. User Permissions

User Permission	Setting	Permissions
Allow Risk Delete By Recorder	Selected	The user set in the <i>Recorded By</i> field in the Risk can delete the Risk.
	Cleared	The user set in the <i>Recorded By</i> field in the Risk <i>cannot</i> delete the Risk (unless they have the RBS permission to delete all Risks).
Allow Unapproved Risk Delete By Recorder	Selected	The user set in the <i>Recorded By</i> field in the Risk can delete the Risk if the Risk is unapproved. A Risk is unapproved if the <i>Date Approved</i> and <i>Approved By</i> fields have not been completed.
	Cleared	The user set in the <i>Recorded By</i> field in the Risk <i>cannot</i> delete the Risk (unless they have the RBS permission to delete all Risks).
Allow Risk Delete by Owner	Selected	The user set in the <i>Owner</i> field in the Risk can delete the Risk.
	Cleared	The user set in the <i>Owner</i> field in the Risk <i>cannot</i> delete the Risk (unless they have the RBS permission to delete all Risks).
Allow Risk Delete by Contact	Selected	The user set in the <i>Contact</i> field in the Risk can delete the Risk.
	Cleared	The user set in the <i>Contact</i> field in the Risk <i>cannot</i> delete the Risk (unless they have the RBS permission to delete all Risks).

6.6. Formula Tab



Formula

Default Action Reduction: By Percentage ☐ Lock: ☐

Retained Risk Formula Based On: Consequence actions

Automated Residual Risk Formula: Standard

Automated Review Dates: ☒

Date Due Base Control: Previous Due Date

Alert if Existing Control Date Due: ☒

Overdue Existing Control may re-assert risk: ☒

Rating Score: Multiply Likelihood and Consequence (Default)

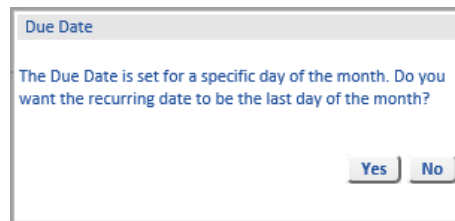
Key Risk Indicator Status Type: Identify one primary KI

Key Control Indicator Status Type: Identify one primary KI

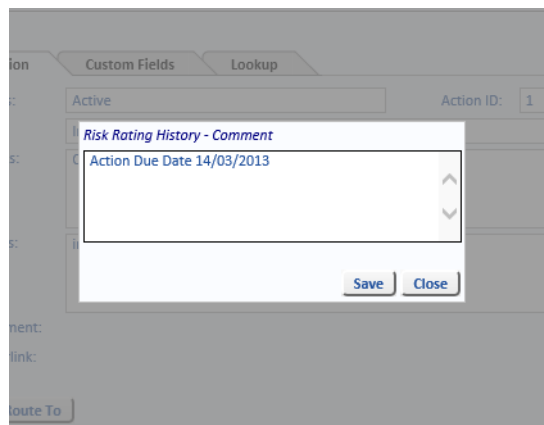
Various formulas are used in the system and those settings are made here.

- *Default Action Reduction* – Defines whether, when an Action is completed, the Risk is reduced by a *Percentage* amount or by a *Level* (from High to Medium, for example). When *Lock* is selected, this setting cannot be overridden on a per-Risk basis. When *Lock* is cleared, this setting can be overridden on a per-Risk basis.

- *Retained Risk Formula Based On* – Select *Consequence actions* to use only the *Consequence* in the Retained Risk Formula. Select *Likelihood & consequence actions* to use both *Consequence* and *Likelihood* in the Retained Risk Formula.
- *Automated Residual Risk Formula* – Select *None* to manually set the Residual Risk. Select *Standard* to automatically calculate the Residual Risk.
- *Automated Review Dates* – When the *Review Frequency* is changed on the Risk's *Ownership and Dates* tab, the *Date Next Review* is updated automatically. When cleared, the *Date Next Review* must be entered manually.
- *Date Due Base Control* - Determines whether the *Action Frequency* is calculated from the *Last Completed Date* or the *Previous Due Date*. Click the *Edit* button to enable the frequency *Date Due Base Control* selections. The *Action Frequency* can be set to a specific date in a month or the last day of the month, irrespective of the number of days in the month, see "[Action Frequency](#)" on page 68 for more details. When the *Due Date* or the *Last Completed Date* (for the *Risk Action* and *Incident Action*) is set to 28th February, or 29th and 30th of other months, the following message will be displayed:



- *Alert if Existing Control Date Due* – when selected, a pop-up is displayed when the *Due Date* of an Existing Control is passed.



- *Overdue Existing Control may re-assert risk* – When selected, Existing Controls which are Overdue will still affect the Risk Rating. When cleared, Existing Controls which are Overdue will not affect the Risk Rating.
- *Rating Score* – *Multiply Likelihood and Consequence (Default)* is often used to calculate the Risk Rating Score. Alternatively, the Risk Rating Score can be calculated by adding the *Likelihood* and *Consequence* values (*Add Likelihood and Consequence*). Select *None* to manually enter the Risk Rating value.
- *Key Risk Indicator Status Type* – There are three Key Risk Indicator Status Type choices: *Identify one primary KI* - this selection will only display the Primary Key Indicator. *Roll-up of all KI statuses* - this selection will display a Roll-up of all KI statuses similar to a majority rule. *Display worst KI status* - this selection will display the worst KI status.
- *Key Control Indicator Status Type* – There are three Key Control Indicator Status Type choices: *Identify one primary KI* - this selection will only display the Primary Key Indicator. *Roll-up of all KI statuses* - this selection will display a Roll-up of all KI statuses similar to a majority rule. *Display worst KI status* - this selection will display the worst KI status.

6.7. Options Tab

Options	
Activate Risk Stapling:	<input checked="" type="checkbox"/>
Activate Replicate Button:	<input checked="" type="checkbox"/>
Activate Scenario Analysis:	<input checked="" type="checkbox"/>
Activate Control Effectiveness Matrix:	<input checked="" type="checkbox"/>
Activate Key Indicators:	<input checked="" type="checkbox"/>
Activate Risk Appetite:	<input checked="" type="checkbox"/>
Activate Processes:	<input checked="" type="checkbox"/>
Activate Compliance Alerts:	<input checked="" type="checkbox"/>

Incident Logging	
Activate Incident Logging	<input type="checkbox"/>
Internal Email:	<input type="text"/>
Insurance Email:	<input type="text"/>
Safety Regulator Email:	<input type="text"/>
Company Regulator Email:	<input type="text"/>
Environmental Regulator Email:	<input type="text"/>
Other Email:	<input type="text"/>

[Refresh System Settings](#)
[Edit](#)

6.7.1. Options

These options require activation in the OpRiskControl Licence key even though they may not be a billable option.

- *Activate Risk Stapling* – *Stapled Risks* appear on the Risks menu, and a *Staple* button appears at the bottom of any Risk form. See *Staple Button* in the *Risks* chapter of the *OpRiskControl Users' Guide*.
- *Activate Replicate Button* – The *Replicate* buttons enable Users to create a new Risk based on an existing Risk. See *Replicate Button* and *Replicate With Actions Button* in the *Risks* chapter of the *OpRiskControl Users' Guide*.
- *Activate Scenario Analysis* – *Scenario Analysis* appears on the Risk Analysis page. See *Scenario Analysis Button* in the *Risk Analysis* chapter of the *OpRiskControl Users' Guide*.
- *Activate Control Effectiveness Matrix* – Two extra items appear on the Risk and on the Action forms. They are *Design Effectiveness* and *Implementation Effectiveness*. Also, an extra item (*Control Effectiveness*) appears in the *System Data* menu. Control Effectiveness enables you to set up a control effectiveness matrix. If you are using *Custom Forms* you will need to enable *Design Effectiveness* and *Implementation Effectiveness*.
- *Activate Key Indicators* – *Key Indicators* appears on the main *Risk* tab.
- *Activate Risk Appetite* – Selecting this option enables all *Risk Appetite* functionality.
- *Activate Processes* – Select to display *Processes* and *Process Management* when the *Options* tab is selected.
- *Activate Compliance Alerts* – Compliance alert options are added to the Risk form (on the *Ownership and Dates* tab). The Risk creator can then select a User from the drop-down list and a date. On the selected date, when the selected User selects the *Alerts* tab and selects *Compliance Due*, they will see an alert for the Risk.



Note: When the Job Scheduler is installed and running, Key Indicators are updated daily.

6.7.2. Incident Logging

- *Activate Incident Logging* – When selected, *Log an Incident* and *Search Incidents* appear on the *Risk* tab. These options allow you to log Incidents and to track claims and losses. Please refer to the *OpRiskControl Users' Guide* for more information on *Logging an Incident*.
- *Email Addresses* – You can configure the following default email addresses:
 - *Internal Email*.
 - *Insurance Email* – This is automatically used as the *Broker Email* on the Incident Claim page.
 - *Safety Regulator Email*.
 - *Company Regulator Email*.
 - *Environment Regulator Email*.
 - *Other Email*.

To enable Incident Logging for a User, ensure the following steps have been completed:

1. Select the option *Activate Incident Logging* and enter default email addresses (if required).
2. Ensure the Role the user belongs to has the correct security settings. To create Incidents, the User must be in a Role which has the option *View Risks/Incidents* and the option *Edit Risks/Incident Events* (both in the *Reference Data* section of the permissions) selected.
3. Enable Event Notifications for a Risk Event. Select the *Manage* tab and click on *Reference Data*. Select *Risk Events* from the menu. Click *Edit*, select the required email types and click *Save*.

The screenshot displays the 'RISK EVENT' configuration interface. At the top, there are tabs for Home, Risks, Alerts, Charts, System, Manage, Other, Options, Preferences, and Links. Below these are sub-tabs for Users, Documents, Reference Data, Risk Data, Risk Lookups, and Action Lookups. The 'RISK EVENT' section contains the following fields and options:

- Name:** Earthquake
- Description:** Earthquake
- Type:** Natural Hazard
- Default likelihood:** [Empty field]
- Event Context:** [Empty field]
- Short Name:** Earthquake
- Default Consequence:** [Empty field]
- Acceptable Risk Level:** [Empty field]
- Standard:** [Empty field]
- Custom Report Order:** 0
- Email Notifications (all checked):**
 - Internal Email: ☒
 - Insurance Email: ☒
 - Other Email: ☒
 - Safety Regulator Email: ☒
 - Company Regulator Email: ☒
 - Environmental Regulator Email: ☒

4. Automatic emails can be sent from the Notification Manager service. See ["Setup Incidents" on page 33](#) for a description of the notification settings.

6.8. Setup Tab

Home Page – Select the Home page layout from the drop-down list. A new Home page can be created by selecting the *System* tab, clicking *Content* and selecting *Manage Content* from the menu. See ["Manage Content" on page 75](#) for more information.

Display Home Tab – Select to display the Home tab.



– Clear to hide the Home tab.



Set Risk IDs to start numbering from – Sets the start number for new Risks. This value must be set higher than the highest automatically numbered Risk.

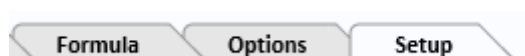
Set Action IDs to start numbering from – Sets the start number for new Actions. This value must be set higher than the highest automatically numbered Action.

Each section on this page is described below.

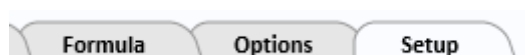
6.8.1. Menu Tabs

Tab Style – Select one of the following styles for the tabs:

ABRUPT SLOPE



SMOOTH SLOPE



Tab Colour – Cannot be changed.

Selected Tab Colour – Cannot be changed.

Font – Select the font you want to use for the text on the tabs.

Weight – Select the weight of the selected font you want to use for the text on the tabs.

Text Size – Select size (in points) of the selected font you want to use for the text on the tabs.

Text Colour – Select the colour of the selected font you want to use for the text on the *unselected* tabs. Purple is selected in the example below.

Selected Text Colour – Select the colour of the font you want to use for the text on the *selected* tab. Cyan is selected in the example below.

Hover Text Colour – Select *Underline* if you want the text to be underlined when the mouse hovers over it. Select the colour of the selected font you want to use for the text on the tab the mouse is hovering over. Orange is selected in the example below.



6.8.2. Menu Ribbons And Sub-Menu Items

Tab Colour – Cannot be changed.

Selected Tab Colour – Cannot be changed.

Font – Select the font you want to use for the text on the menu items.

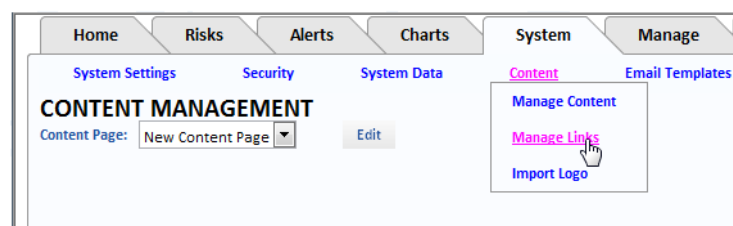
Weight – Select the weight of the font you want to use for the text on the menu items.

Text Size – Select the size of the font you want to use for the text on the menu items.

Text Colour – Select the colour of the font you want to use for the text on the *unselected* tabs. Purple is selected in the example below.

Selected Text Colour – Select the colour of the font you want to use for the selected text.

Hover Text Colour – Select *Underline* if you want the text to be underlined when the mouse hovers over it. Select the colour of the font you want to use for the text on the menu item the mouse is hovering over. Fuchsia is selected in the example below.



6.8.3. Panel Headers And Borders

Panel Headers and Borders

Header Background: ☒ HEX E6E6E6

Header Font: Calibri

Header Weight/Style: bold

Header Font Size: 12

Header Font Colour: ☐ HEX Black

Label Background Colour: ☒ HEX FAFDFF

Text Background Colour: ☐ HEX White

Border Colour: ☒ HEX BFBFBF

Border Weight: 1

Header Background – Select the colour of the background of the panel headers. Bisque is selected in this example below.

Header Font – Select the font you want to use for the text on the panel headers.

Header Weight/Style – Select the weight and style of the font used on the panel headers.

Header Font Size – Select the size of the font used for the panel headers.

Header Font Colour – Select the colour of the text used in the panel headers. Brown is selected in the example below.

Label Background Colour – Select the background colour to be used with labels. Powder Blue is selected in the example below.

Text Background Colour – Select the colour you want used for the background of text boxes used in panels. Thistle (pink) is selected in the example below.

Border Colour – Select the colour you want used for the panel borders. Dark Magenta is selected in the example below.

Border Weight – Enter the point weight of the panel borders. The weight has been set to 5 in the example below.

Context **Rating** **Ownership and Dates** **Financial**

Department

Division: Corporate

Department: Across all Business Units

Location: Head Office

Category of Threat

Risk Type: Natural Hazard

Event Type: Flood

Area Threatened

Asset: Liabilities

Relative Value: Medium

6.8.4. Panel Tabs

Panel Tabs

Tab Colour: E6E6E6

Selected Tab Colour: FAFDFF

Font: Calibri

Weight/Style: bold

Text Size: 12

Text Colour: ☐ HEX

Selected Text Colour: ☐ HEX

Hover Text Colour: ☒ Underline ☐ HEX

Tab Colour – Cannot be changed.

Selected Tab Colour – Cannot be changed.

Font – Select the font you want used on the Panel tabs.

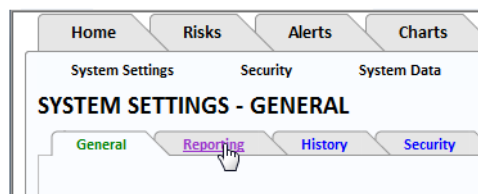
Weight/Style – Select the weight and style of the font you want used on the panel tabs.

Text Size – Select the font size you want used on the Panel tabs.

Text Colour – Select the text colour you want used on *unselected* Panel tabs. Blue is selected in the example below.

Selected Text Colour – Select the text colour you want used on the *selected* Panel tab. Dark Green is selected in the example below.

Hover Text Colour – Select the text colour you want used when the mouse hovers over a Panel tab. Dark Orchid is selected in the example below.



6.8.5. Panel Content

Panel Content

Panel Background Colour: ☒ HEX FAFDFF

Label Font: Calibri

Label Weight/Style: normal

Label Size: 12

Label Colour: ☒ HEX 22529E

Text Font: Calibri

Text Weight Style: normal

Text Size: 12

Text Colour: ☒ HEX 22529E

Drop Down Font: Calibri

Drop Down Weight/Style: normal

Drop Down Size: 12

Search Drop Down Colour: ☐ HEX

Search Drop Down Background: ☐ HEX

Panel Background Colour – Select the colour you want used for the panel background. Yellow is selected in the example below.

Label Font – Select the font to be used for the field labels in the panel.

Label Weight/Style – Select the weight and style of the field label font.

Label Size – Select the size of the field label font.

Label Colour – Select the colour of the field label text. Green is selected in the example below.

Text Font – Select the font to be used for the text which has been entered in the text boxes.

Text Weight/Style – Select the weight and style of the font to be used for the text which has been entered in the text boxes.

Text Size – Select the size of the font to be used for the text which has been entered in the text boxes.

Text Colour – Select the font colour to be used for the text which has been entered in the text boxes. Dark Blue is selected in the example below.

The screenshot shows the 'SYSTEM SETTINGS - GENERAL' panel. The background is yellow. The 'System Administrator Message' section has the following fields:

- Business Name:** Business Name
- Bold Header:** Bold Header
- Login Message:** Login Message
- Show Banner:** ☐

Drop Down Font – Select the font to be used in the drop-down menus.

Drop Down Weight/Style – Select the weight and style of the font to be used in the drop-down menus.

Drop Down Size – Select the size of the font to be used in the drop-down menus.

Search Drop Down Colour – Select the colour of the font to be used in the drop-down menus. White is selected in the example below.

Search Drop Down Background – Select the background colour to be used in the drop-down menus. Orange is selected in the example below.

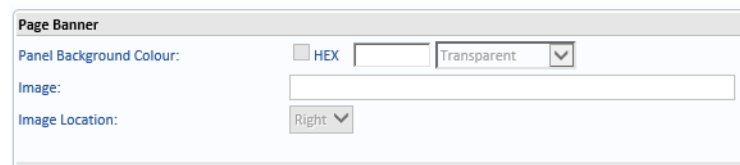
The screenshot shows the 'RISK SEARCH' panel. The background is orange. The 'RISK SEARCH' section has the following filters:

- Division:** Corporate
- Risk Type:** Across all Divisions
- Location:** Operational Project
- Department:** All Departments
- Event Type:** All Events
- Asset:** All Assets
- Owner:** All Owners
- Status:** Open

Below the filters is a table of selected risks:

Item ID	S	A	R	T	Act	Title	Description	Likelihood	Consequence	Rating	Residual	View	Delete
18	O	M				0/1 Clear Corporate Priorities	Clear Corporate Priorities...	Unlikely	Moderate	Medium	Insignificant	View	Delete

6.8.6. Page Banner

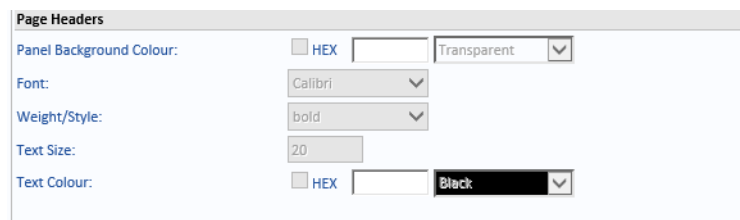


Panel Background Colour – Select the colour you want to appear at the top of the screen – where the company logo is shown.

Image – Select the image you want to appear on the right side of the banner.

Image Location – Cannot be changed from *Right*.

6.8.7. Page Headers




Panel Background Colour – Select the colour you want to use for the page header banner background. Aquamarine is selected in the example below.

Font – Select the font you want to use for the text in the page header banner.

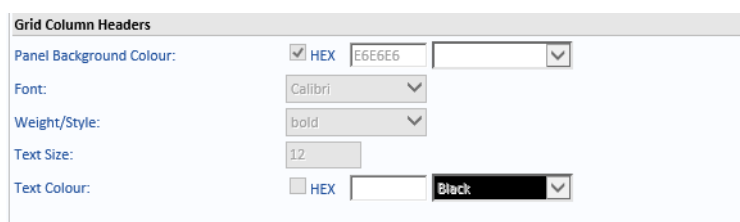
Weight/Style – Select the weight and style of the font you want to use for the text in the page header banner.

Text Size – Select the font size you want to use for the text in the page header banner.

Text Colour – Select the colour you want to use for the text in the page header banner. Orange is selected in the example below.



6.8.8. Grid Column Headers



Panel Background Colour – Select the colour to be used for the background of the grid header text. Yellow is selected in the example below.

Font – Select the font to be used for the grid header text.

Weight/Style – Select the weight and style of the font to be used for the grid header text.

Text Size – Select the font size to be used for the grid header text.

Text Colour – Select the font colour to be used for the grid header text. Brown is selected in the example below.

The screenshot shows a web application interface with a top navigation bar (Home, Risks, Alerts, Charts, System, Manage, Other) and a sub-navigation bar (Risk Search, Recently Viewed, Report Wizard, New Risk, Stapled Risks). The 'Risk Search' section contains filters for Division, Function, Risk Type, Location, Department, Project, Event Type, and Categories. Below this is a 'Selected Risks' section with a table showing risk details.

S	A	R	T	Title	Likelihood	Consequence	Rating
O	H	M	I	A Substantial Financial Loss from Interest Rate Changes	Almost certain	Moderate	High

6.8.9. Grid Items

The 'Grid Items' configuration panel includes settings for Panel Background Colour (HEX: FAFDFF), Font (Calibri), Weight/Style (normal), Text Size (12), and Text Colour (HEX: 22529E).

Panel Background Colour – Select the background colour to be used for the odd number rows in a grid display. Light Cyan is selected in the example below.

Font – Select the font to be used for the text in the odd number rows in a grid display.

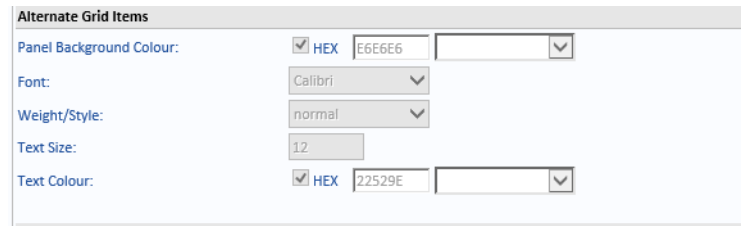
Weight/Style – Select the weight and style of the font to be used for the text in the odd number rows in a grid display.

Text Size – Select the font size to be used for the text in the odd number rows in a grid display.

Text Colour – Select the font colour to be used for the text in the odd number rows in a grid display. Dark Turquoise is selected in the example below.

Item ID	S	A	R	T	Act	Title	Description
18	O	M	I	I	0/1	Clear Corporate Priorities	Clear Corporate Priorities....
13	O	H	M	I	1/2	Climate Change Implications	Southbridge needs to assess the potential long term impact of climate change to ensure the continued provision of appropriate services in light of potentially higher costs, extreme weather patterns, flood, drought, heatwaves etc. and determine measures which could reduce emissions etc
17	O	H	M	I		Financial Management Information	Financial Management Information...
11	O	H	M	I	0/3	Health and Safety	Failure of proper H&S management and systems could lead to: - exposure to legal action; - financial impact; - reduction in reputation; - increased exposure to H&S risks.

6.8.10. Alternate Grid Items



Alternate Grid Items

Panel Background Colour: ☒ HEX E6E6E6

Font: Calibri

Weight/Style: normal

Text Size: 12

Text Colour: ☒ HEX 22529E

Panel Background Colour – Select the background colour to be used for the even number rows in a grid display. Blue is selected in the example below.

Font – Select the font to be used for the text in the even number rows in a grid display.

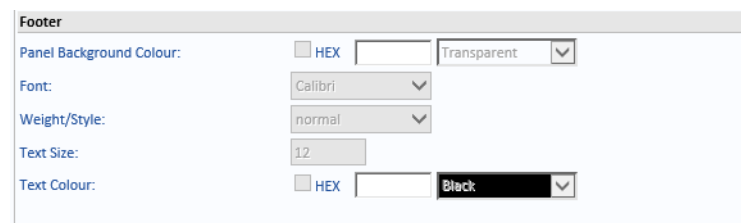
Weight/Style – Select the weight and style of the font to be used for the text in the even number rows in a grid display.

Text Size – Select the font size to be used for the text in the even number rows in a grid display.

Text Colour – Select the font colour to be used for the text in the even number rows in a grid display. Dark Blue is selected in the example below.

Item ID	S	A	R	T	Act	Title	Description
18	O	M	I	I	0/1	Clear Corporate Priorities	Clear Corporate Priorities....
13	O	M	M	I	1/2	Climate Change Implications	Southbridge needs to assess the potential long term impact of climate change to ensure the continued provision of appropriate services in light of potentially higher costs, extreme weather patterns, flood, drought, heatwaves etc. and determine measures which could reduce emissions etc
17	O	S	M	I		Financial Management Information	Financial Management Information...
11	O	M	M	I	0/3	Health and Safety	Failure of proper H&S management and systems could lead to: - exposure to legal action; - financial impact; - reduction in reputation; - increased exposure to H&S risks.

6.8.11. Footer



Footer

Panel Background Colour: ☐ HEX Transparent

Font: Calibri

Weight/Style: normal

Text Size: 12

Text Colour: ☐ HEX Black

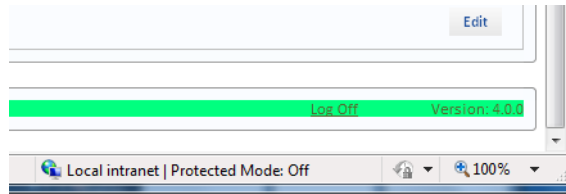
Panel Background Colour – Select the footer background colour. Light green is selected in the example below.

Font – Select the font to be used for the text in the footer.

Weight/Style – Select the weight and style of the font to be used for the text in the footer.

Text Size – Select the font size to be used for the text in the footer.

Text Colour – Select the font colour to be used for the text in the footer. Dark green is used in the example below.



6.8.12. Buttons

 A screenshot of a 'Buttons' configuration window. It contains the following settings:

- Background Colour Upper:** Checked, HEX F9F9F9
- Background Colour Lower:** Checked, HEX E8E8E8
- Font:** Calibri
- Weight/Style:** bold
- Text Size:** 12
- Text Colour:** Checked, HEX 22529E

Background Colour Upper – Select the colour to be used for the top of the buttons. Cornflower blue is used in the example below.

Background Colour Lower – Select the colour to be used for the bottom of the buttons. Dark blue is used in the example below.

Font – Select the font to be used for the text on the buttons.

Weight/Style – Select the weight and style of the font to be used for the text on the buttons.

Text Size – Select the size of the font to be used for the text on the buttons.

Text Colour – Select the colour to be used for the text on the buttons. Pale blue is used in the example below.

 A screenshot of the 'Options' tab in a system settings window. It shows a search filter section with 'Asset' set to 'All Assets' and 'Status' set to 'Open'. There are three empty dropdown menus on the left. At the bottom right are buttons for 'Clear', 'Search', and 'New Risk'.

6.9. Refresh System Settings

Click *Refresh System Settings* to reload all the System Settings.

6.10. Save Website Appearance

Click *Save website appearance* to save the current settings.

6.11. Restore Saved Website Appearance

Click *Restore saved website appearance* to restore the last saved settings.

7. Role Based Security

7.1. Overview

Role-based security (RBS) refers to a type of authorisation process that allows a User to access some resources and not others, and/or to perform specific tasks, based on their *Role*.

A Role may be the User's job title or position in the organisation, or may refer to a group or part of the organisation to which the User belongs. A Role may simply exist to denote Users who need access to identical resources within the software.

The advantage of setting permissions against Roles is that once a Role is set up, Users can simply be added to that Role in order to gain the permissions set against the Role. And if the scope of permission required by a Role changes, this can simply be performed against the Role with all Role Users automatically inheriting the change.

7.2. RBS Permissions

Permissions in RBS can be thought of as describing a task or action. Typical examples of permissions may be *Can view risks* or *Can edit risks*. In RBS, permissions have a name and a description.

7.2.1. Permission Allocation

A permission becomes useful when it is allocated to a User or Role:

- Allocating a permission to a User allows that User to perform the action represented by that permission. So, for example, if a User called *John* is allocated the permission *Can create invoice*, the application would allow John to create an invoice.
- Allocating a permission to a Role allows all Users who are in that Role to perform the action represented by that permission. So, for example, if a Role called *Account Managers* was given the permission *Can create invoice*, and Users *John*, *Margaret* and *Rajesh* were members of that *Account Managers* Role, then John, Margaret and Rajesh would automatically be allowed to create invoices in the application.

7.3. RBS Roles

A Role in RBS is simply a container within which to group Users who perform that Role.

The Role must be given a name, and can be given a description.

A Role can contain many Users, and a User may belong to more than one Role.

7.3.1. Role Permissions

A Role is allocated permissions, thus providing all Users within that Role those permissions.

If a User is a member of more than one Role, they inherit all the permissions from all the Roles to which they belong. When permissions allocated to their Roles coincide, a User may actually inherit a permission more than once.

7.3.2. RBS Users

A User may also be allocated permissions directly. This is useful if a particular User requires all the permissions of a particular Role, plus a few extra permissions, possibly on a temporary basis. For example, if a manager is off sick, one of his employees may be required to assume part of his Role for the day, but not get all the permissions from that Role. Rather than set up a

new Role just for that day, it is possible to allocate only those additional permissions required directly to the employee only.

7.4. RBS User Interface Functionality

Select the *System* tab and then select the appropriate option from the *Security* menu.

The following chapter describes the RBS pages.

After permissions or Roles have been changed for a User, the User will need to log out of OpRiskControl, and log back in before the changes take effect.

8. System Security

The following sections describe the available RBS configuration screens. After permissions or Roles have been changed for a User, they will need to log out of OpRiskControl and then log back in before the changes take effect.

8.1. Roles

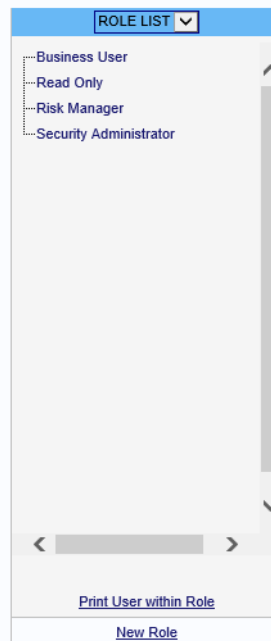
Select the *System* tab, then select *Roles* from the *Security* menu to display the Role List screen.

The RBS Role List screen allows the creation, navigation and maintenance of Roles. Roles are generally defined by a System Administrator, although, depending on the specific implementation of the software, it is possible for some Roles to be automatically generated by the application. For more information on automatically generating Roles, see [“Example Of Row Level Security” on page 57](#).

A tree containing the Roles is displayed on the left. These Roles are defined by the System Administrator.

Clicking on a Role anywhere within the list displays the details of that Role in the detail section on the right side of the page.

Clicking on the *New Role* link text creates a new Role.



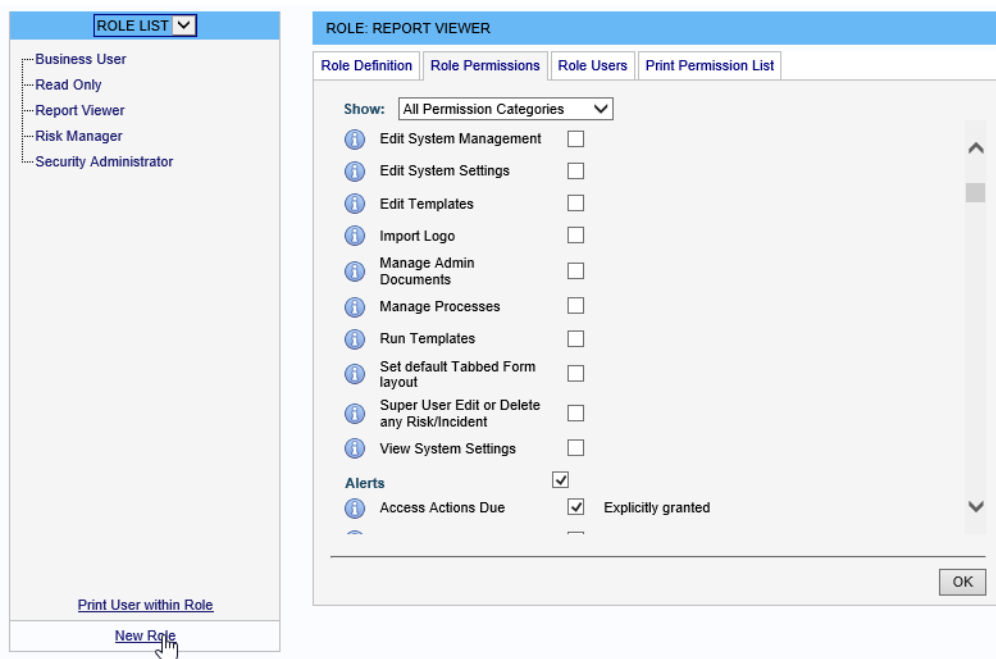
The right side of the page contains four tabs: Role Definition, Role Permissions, Role Users, Print Permission List.

8.1.1. Role Definition Tab

The *Role Definition* tab displays the following fields and buttons:

- *Role Name* – the name of the Role.
- *Role Description* – this is used as a ToolTip in other parts of RBS.
- *Delete* – click to delete the Role. A confirmation prompt is displayed prior to deletion.
- *Edit* – click to edit the Role.

This screen is also used to enter new Roles after clicking the *New Role* link in the Role tree on the left of the screen.



8.1.2. Role Permissions Tab

Permissions allocated to a particular Role are entered via the *Role Permissions* tab. Initially, the whole set of possible permissions is displayed, grouped by permission category.

The drop-down list at the top of the screen allows the view to be filtered by permission category. (Permission categories are simply convenient groupings of permissions.) By default, the filter is set to show *All Permission Categories*.

Each permission is displayed with an icon adjacent to it. Hovering over the icon with the mouse displays a ToolTip giving a further description of that permission.

A tick-box is displayed beside each permission. If this tick-box is selected, that particular permission is allocated to the Role. If the tick-box is cleared, the Role does not have that permission.

To allocate a Permission to a Role, click the *Edit* button at the bottom of the screen. Any permissions that the Role does not yet have may now be applied simply by clicking the tick-box. A tick-box is also provided by the permission category name – selecting this box simply allocates all permissions in that category to the Role. Once editing is complete, click the *OK* button.

Not all permissions are specifically allocated to the Role. Some permissions may already be selected because they may be triggered by other permissions which are checked (see the RBS Permissions section for further information about permission triggering). In this case, it is not possible to remove that permission. The cause of the permission must be adjusted instead.

Displayed to the right of each *selected* permission is a message explaining how the permission was allocated. This allows the System Administrator to determine how the permission was set. The message will be one of the following:

- *Explicitly granted* – The permission was allocated explicitly to this Role. The permission can hence be removed from the Role, simply by clearing the tick-box.
- *Implied by permission: Permission name* – Another permission allocated to the Role has triggered this permission. For instance, the permission *View Departments* is triggered by the permission *Edit Departments*, since you would need to view a department definition

in order to edit it. Triggered permissions cannot be removed without removing the triggering permission. In the screen shot below, the tick-box for the *View Departments* is dimmed.

ROLE: BUSINESS USER

Role Definition | **Role Permissions** | Role Users | Print Permission List

Show: All Permission Categories

	Edit User Classifications	<input type="checkbox"/>	
	Manage Countries	<input type="checkbox"/>	
	View Action Frequency	<input type="checkbox"/>	
	View Assessed By	<input type="checkbox"/>	
	View Asset/Area	<input type="checkbox"/>	
	View Asset/Area Types	<input type="checkbox"/>	
	View Departments	<input checked="" type="checkbox"/>	Implied by permission: Edit Departments
	View Division	<input type="checkbox"/>	
	View Division Groups	<input type="checkbox"/>	
	View Evaluation Criteria	<input type="checkbox"/>	
	View Exposure Periods	<input type="checkbox"/>	
	View Function	<input type="checkbox"/>	
	View History Types	<input type="checkbox"/>	

OK

In some cases, a permission can be allocated from *Multiple Sources*. In this case, a drop-down list is displayed detailing each source of the permission. Selecting an item in the drop-down list navigates to the source of the permission, if applicable.

8.1.3. Role Users Tab

The *Role Users* tab displays a list of Users who have been added to the selected Role.

Users can be *Added* to the Role or *Removed* from the Role by clicking the appropriate text link.

ROLE LIST

- Business User
- Read Only
- Report Viewer
- Risk Manager
- Security Administrator

[Print User within Role](#)

[New Role](#)

ROLE: REPORT VIEWER

Role Definition | Role Permissions | **Role Users**

User	
Alison Heard	Remove
Mitrtech Support	Add

The screen shot shows one User has the Role *Report Viewer*.

8.2. Users

Select *Users* from the *Security* menu to display the *User List* page.

You can navigate between Roles and Users from the drop-down list.

Select a name from the left-hand pane to see their Roles, Permissions and Details.

To add a new User, go to *Manage*, select *Users* and click the *New User* button.

The right side of the page contains three tabs: User Roles, User Permissions and User Details.

8.2.1. User Roles Tab

The Roles to which a User belongs are displayed on the *User Roles* tab. Additional Roles can be added to the User simply by selecting a Role from the drop-down list and clicking the *Add* button.

The User can be removed from a Role by clicking the *Remove* button against that Role.



Note: The *Remove* button removes the User from that Role, it does not delete the Role.

8.2.2. User Permissions Tab

Select the *System* tab, select *Security* and select *Users* from the menu. The *User Permissions* tab is on the right.

Permissions allocated to a particular User are entered via the *User Permissions* tab. Initially, all the permissions are displayed, grouped by permission category.

The drop-down list at the top of the screen allows the view to be filtered by permission category. (Permission categories are simply convenient groupings of permissions.) By default, the filter is set to show *All Permission Categories*.

Each permission is displayed with an icon adjacent to it. Hovering over the icon with the mouse displays a ToolTip giving further description of that permission.

A tick-box is displayed beside each permission. If this tick-box is selected, that permission has been allocated to the User. If the tick-box is cleared, the User does not have that permission.

To allocate a permission explicitly to a User, click the *Edit* button at the bottom of the screen. Any permissions the User does not yet have may now be applied simply by selecting the tick-box. A tick-box is also provided beside the permission category name – selecting this box

allocates all permissions in that category to the User. Once editing is complete, click the *OK* button.

Usually, permissions are not specifically allocated explicitly to the User but are inherited from their Roles. The User might have specific permissions selected because:

- They may be inherited from one or more Roles of which the User is a member.
- They may be triggered by other permissions which are checked.

If a permission is implied by either of the above scenarios, it is not possible to remove that permission. The cause of the permission must be adjusted instead.

To assist with this, displayed to the right of each permission that has been allocated is a message explaining how the permission was allocated. This allows the System Administrator to determine how the permission came to be set, and will be one of three messages:

- *Explicitly Granted* – This means that the permission was actually allocated explicitly to this User. The permission can hence be removed from the User, simply by clearing the tick-box.
- *Implied by permission: Permission name* – This means that another permission that the User has triggered this permission. For instance, the permission *View Departments* is triggered by the permission *Edit Departments*, since you would need to view a department definition in order to edit it. Triggered permissions cannot be removed without removing the triggering permission. As you can see, the tick-box for the *View Departments* is greyed out.
- *Inherited from Role: Role name* – This means that a Role of which the User is a member has this permission, and the User has inherited it from the Role. In this case, a *View* link is provided which navigates directly to that subordinate Role for convenience.

In some cases, a permission can be allocated from *Multiple Sources*. In this case, a drop-down list is displayed detailing each source of the permission. Selecting an item in the drop-down list navigates to the source of the permission, if applicable.

The screenshot displays the 'USER: STAN' configuration page. On the left, a 'USER LIST' dropdown shows a list of users: Abul Khair, Alison Heard (Super User), Chris Priest, Craig Wright, Hitec Support, Karim Rabi-laleh, and Stan Pattenden. Below this list are links for 'Print Role within User' and 'New User'. The main panel is titled 'USER: STAN' and has tabs for 'User Roles', 'User Permissions', and 'User Details'. The 'User Permissions' tab is active. It features a 'Show:' dropdown set to 'Risks/Incidents'. Below this, a list of permissions is shown, each with an information icon, a checkbox, a description of the source, and a 'View' link. The permissions listed are: Allow Manual Routing, Approve Risk/Incident, Approve Treatment/Action, Change Action Status, Change Risk/Incident Status, Custom Forms, Delete Documents, Delete History, Delete Manual Routing, Delete Treatments/Actions, and Delete unapproved Risks/Incidents. The first nine permissions are inherited from the 'Business User' role. The last two, 'Delete History' and 'Delete Treatments/Actions', are marked as 'Multiple sources...' and have a dropdown menu. An 'Edit' button is located at the bottom right of the permissions list.

8.2.2.1. Permissions Configured

Permissions define tasks that can be performed in OpRiskControl, not data that can be accessed. Permissions are global in scope, and apply regardless of Department, Division, Location and Function/Area. That is, they do not apply at database row level. Row level

security is applied after permissions are checked. See [“Example Of Row Level Security” on page 57](#) for further details.

OpRiskControl checks relevant permissions prior to granting access to screens, buttons, menu items and tabs. This means that for a particular User, if there are no permissions granted to view anything on a particular page, the page does not appear as a menu option. If no menu options appear for a menu, the menu does not appear. If there are no permissions granted to view anything on a tab, the tab does not appear.

If a User does not have permission to see a page, not only will it not be present within the menu structure, but they also cannot access it via the URL or bookmarks. In these cases, an *access denied* message is displayed.

8.2.3. User Details Tab

The *User Details* tab provides a link to the User definition screen. Click *View Application User Details* to navigate to the *User Details* page. See [“Manage Users” on page 79](#) for more information.

8.3. System Security Settings

Select the *System* tab, then select the *System Settings* tab and select the *Security* tab.

8.3.1. Row Level Security

Customers who have purchased an RBS licence have access to four tick-boxes on the *Security* tab (select the *System* tab, select *System Settings* and then select the *Security* tab):

- Limit Access by Division
- Limit Access by Department
- Limit Access by Location
- Limit Access by Asset
- Limit User List by Division

The screenshot displays the 'SYSTEM SETTINGS - SECURITY' configuration page. The top navigation bar includes tabs for Home, Risks, Alerts, Charts, System, Manage, Other, Options, and Preferences. Under the 'System' tab, there are sub-tabs for System Settings, Security, System Data, Content, and Email Templates. The 'Security' sub-tab is active, showing further sub-tabs: General, Reporting, History, Security, Workflow, Formula, Options, and Setup. The 'Security' sub-tab is selected, revealing a 'Role Based Security' section with five tick-boxes: 'Limit Risk Access By Division', 'Limit Risk Access By Department', 'Limit Risk Access By Location', 'Limit Risk Access By Asset', and 'Limit User List by Division'. A checkbox for 'Reset all User Search Criteria to use "My..." whenever applicable:' is also present. At the bottom, there are buttons for 'Refresh System Settings', 'Refresh Permissions', and 'Edit'.

The purpose of these tick-boxes is to restrict access to Risk related information based on whether the User is in the same Division, Department, Location or Asset as the Risk itself.

To facilitate this, OpRiskControl automatically creates RBS Roles to represent Divisions, Departments, Locations or Assets. These Roles are read-only, and may not be altered within RBS.

Then when a User attempts to access Risk related information, OpRiskControl:

1. Checks the User has the *View risk* permission (and other permissions relevant to the page) either directly or via one of the User's Roles.
2. Checks the User is a member of the Role for the Division/Department/Location/Asset to which the Risk in question belongs.



Note: While check 1 is always carried out for customers using RBS, check 2 is only carried out when the relevant tick-box in *System Settings* is selected. If either check fails, the User is denied access to that risk.

This is best illustrated by example.

8.4. Example Of Row Level Security

In this example, a Risk manager wants to allocate each User to a Division, and only wants each User to view Risks linked to their own Division.

This is achieved as follows:

1. Select the *System* tab, select the *System Settings* tab and then select the *Security* tab.
2. Click *Edit*. Select the *Limit Risk Access by Division* tick-box and clear the other three *Limit...* tick-boxes. Click *Save*.

Role Based Security

Limit Risk Access By Division: ☐

Role Based Security

Limit Risk Access By Division: ☒

3. OpRiskControl then automatically creates a Role in RBS for *each Division* in OpRiskControl. It conveniently groups all the new Division Roles under a parent Role called *All Division*.

ROLE LIST

- [-] All Division
 - Divn: Across all Divisions
 - Divn: Division - Tech Pubs
 - Divn: R&D
- Business User
- Read Only
- Risk Manager
- Security Administrator

ROLE: DIVN: ACROSS ALL DIVISIONS

Role Definition | Role Users

Role Name: Divn: Across all Divisions

Role Description: Division: Across all Divisions

4. Ensure that each User has the *View Risks/Incidents* permission either directly, or indirectly via any Roles to which the User already belongs.

The screenshot shows the 'ROLE LIST' on the left with a tree view containing 'All Division', 'Divn: Across all Divisions', 'Divn: Corporate', 'Divn: Operational', 'Divn: Project', 'Business User', 'Read Only', 'Risk Manager', and 'Security Administrator'. The 'Business User' role is selected. The right pane shows 'ROLE: BUSINESS USER' with tabs for 'Role Definition', 'Role Permissions', 'Role Users', and 'Print Permission List'. The 'Role Permissions' tab is active, showing a list of permissions. The 'View Risks/Incidents' permission is highlighted with a red box, showing it is checked and set to 'Multiple sources...'.

5. Ensure that each User is also placed in the Role created for their respective Division.

The screenshot shows the 'ROLE LIST' on the left with a tree view containing 'All Division', 'Divn: Across all Divisions', 'Divn: Corporate', 'Divn: Operational', 'Divn: Project', 'Business User', 'Read Only', 'Risk Manager', and 'Security Administrator'. The 'Divn: Corporate' role is selected. The right pane shows 'ROLE: DIVN: CORPORATE' with tabs for 'Role Definition' and 'Role Users'. The 'Role Users' tab is active, showing a list of users: Alison, Anu, Chris, and Craig, each with a 'Remove' button. An 'Add' button is at the bottom.

6. When a User attempts to view a Risk, OpRiskControl first checks they have the *View Risks/Incidents* permission either directly or via one of their Roles. Then OpRiskControl notes the Division the Risk is in and checks the User is in the Role created for that Division. If either check fails, they are denied access to that Risk.

The process is similar for limiting permissions by Location, Department and Asset.

8.4.1. Multiple Roles

It is possible (via Roles) for a User to be a member of more than one Division, Department, Location or Asset, with access to Risks being restricted to, for example, three Departments or two Locations. Simply add the User to more than one of the Roles concerned.

If the Roles for Division, Location, Department or Area are not present in the RBS Role List screen, then the relevant tick-box in the *System Settings* screen is not checked.

8.4.2. Access All Areas

If a User is to have access to Risks regardless of, for example, Location, there are two choices:

The first is to leave the *Limit Risk Access by Location* tick-box in *System Settings* cleared, thus not limiting any Users by location.

The second is to select the *Limit Risk Access by Location* tick-box, but add certain Users to all of the Location Roles.

The same methodology applies to Department, Division and Asset.

8.5. Troubleshooting

8.5.1. No Roles Appearing For Division/Department/Location/Asset

If you are trying to restrict access by Division, but there are no Roles appearing for Divisions in the Role List screen, ensure the *Limit Risk Access by Division* tick-box is selected within *System Settings*. The Division Roles will appear in the Role list under a Role called *Division Roles*. (Similarly for Department, Location and Asset.)

8.5.2. Access Not Granted

If you have changed a permission but you are still not granted access, close the browser and re-open it. Ensure that the permission is selected for the User in the RBS User List screen. If the permission is against a Role, ensure the User is a member of the Role.

8.5.3. Error Message

The error message *You have not been assigned any [Department/Division/Location/Asset] Roles* is displayed on one or more of the Risk related screens.

This message is displayed if:

- The system is set up to apply row level security by Department/Division/Location/Asset but the User has not been placed in a Role relating to the Department/Division/Location/Asset.
- The row level security to be applied is set on the *System Settings* screen, and membership of Roles is set on the *Role List* screen or the *User List* screen. For example, a User who is not a member of any *Location Roles* is not allowed access to the Risk Search screen if they are not assigned to any Locations.

9. System Data

To access *System Data*, select the *System* tab.

9.1. Likelihood

To edit Likelihood descriptions, select the *System* tab, select *System Data* and select *Likelihood* from the menu. The values displayed here are displayed when a User is Viewing a Risk or entering a new Risk and clicks the ... button to the right of the *Likelihood* field on the *Ratings* tab.

LIKELIHOOD DEFINITIONS

Likelihood	Name	Description	
1	Rare	May occur only in exceptional circumstances, can expect 1 event every 20 to 50 years	Edit
2	Unlikely	Could occur at some time, can expect 1 event every 5 to 20 years	Edit
3	Possible	Might occur at some time, can expect 1 event every 1 to 5 years	Edit
4	Probable	Will probably occur in most circumstances, can expect 1 event every year	Edit
5	Almost certain	Is expected to occur in most circumstances, can expect more than 1 event every year	Edit

Click the *Edit* link text beside the Likelihood you want to edit. You can edit the *Name* and you can edit the *Description*. Click *Save* to save your changes, or *Cancel* to discard your changes. Repeat for other Likelihood descriptions, as required.

For Triage matrix you will have to swap the descriptions so that *1* is *Almost certain* and *5* is *Rare*.

9.2. Consequence

The Consequence descriptions are not normally changed. However, if you decide they should be changed, click the *System* tab, select *System Data* and then select *Consequence* from the menu. Click on the *Select* link text beside the *Consequence* description you want to edit.

CONSEQUENCE DETAILS

Consequence:	Insignificant	Cutoff Value:	10,000
Health & Safety:	Injury not requiring first aid treatment	Financial:	Assets not at risk
Customers:	No appreciable economic loss	Infrastructure:	No appreciable performance loss
Production:	No customer issues	Legal:	No equipment safety, obsolescence and/or support issues
Reputation:	No external or environmental issues	Consequence Type H:	No access restrictions
Consequence Type I:		Consequence Type J:	
Consequence Type K:		Consequence Type L:	
Consequence Type M:			

[Back To List](#)
[Edit](#)

Edit the fields, as required.

The information on this screen is displayed in tabular form when a User clicks the ... button to the right of the *Consequence* field on the *Rating* tab when viewing a Risk or entering a new Risk.

If you are using Enterprise Rating or using different cut-off values across the enterprise, delete any cut-off values from this table.

For a Triage matrix, you will have to swap the descriptions so that 1 is *Catastrophic* and 5 is *Insignificant*.

Up to 13 aspects of Consequence are provided (for example, on the screen above, these are: Health & safety, Financial, Customers, Infrastructure and so on). These labels can be renamed. Select the *System* tab, select *System Data* and select *Consequence* from the menu. Click the *Rename Consequence Labels* button.

RENAME CONSEQUENCE LABELS

Note 1: Have a backup of your database taken before running this program.

Note 2: If you run any of these changes, you normally run them in the order specified below. The 'To' column is only a suggestion, and you may rename as you wish but be careful to spell correctly and use a capital for the first character. If you are happy with the current naming of the framework you should not do any of these changes

Note 3: Be careful not to change a label to something that will get changed further down. For example, if you changed "Division" to "Department", it would get changed again when you change "Department" to "Function". Contact support if you are not sure what to do.

Note 4: If you make a simple change in error, you may be able to reverse the change and then check the application forms to confirm all is ok. If you make a major error, you will need to restore the database.

The changes will be applied to: Consequence Labels

Show Translations

1. Change	Consequence Type A	to	Health & Safety	Go	<input type="checkbox"/>
2. Change	Consequence Type B	to	Financial	Go	<input type="checkbox"/>
3. Change	Consequence Type C	to	Customers	Go	<input type="checkbox"/>
4. Change	Consequence Type D	to	Infrastructure	Go	<input type="checkbox"/>
5. Change	Consequence Type E	to	Production	Go	<input type="checkbox"/>
6. Change	Consequence Type F	to	Legal	Go	<input type="checkbox"/>
7. Change	Consequence Type G	to	Reputation	Go	<input type="checkbox"/>
8. Change	Consequence Type H	to	Consequence Type H	Go	<input type="checkbox"/>
9. Change	Consequence Type I	to	Consequence Type I	Go	<input type="checkbox"/>
10. Change	Consequence Type J	to	Consequence Type J	Go	<input type="checkbox"/>
11. Change	Consequence Type K	to	Consequence Type K	Go	<input type="checkbox"/>
12. Change	Consequence Type L	to	Consequence Type L	Go	<input type="checkbox"/>
13. Change	Consequence Type M	to	Consequence Type M	Go	<input type="checkbox"/>

Backup structure now



Caution: Before you rename any Labels, create a backup of the database.

For each Label you want to change, enter a new Label in the second text box and then click Go for that row. Continue until you have renamed all the Consequence Labels you want to change.

9.3. Consequence Factor Setup

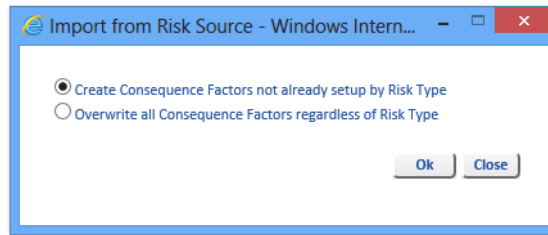
It is possible to create Risk Type Factors for the inherent (assessed) *Consequence* ratings. Instead of entering a single value for the *Consequence* ratings, you can enter several. When several values are entered, the highest rating is then used. (See ["Using Likelihood And Consequence Factors"](#) on page 64 on how to use *Consequence* and *Likelihood* factors once they have been configured.)

There are two ways to configure *Consequence Factors*: automatically or manually. To configure *Consequence Factors* automatically, see ["Automatic Consequence Factor Setup"](#) below. To configure *Consequence Factors* manually, see ["Manually Create Consequence Factors"](#) on page 64.

9.3.1. Automatic Consequence Factor Setup

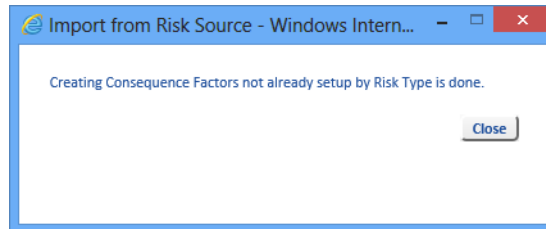
Consequence Factors can be created automatically from the *Consequence* details. See ["Consequence" on page 61](#) for more information on the *Consequence* details.

On the *System* tab, select *System Data* and select *Consequence Factor Setup* from the menu.



- Select *Create Consequence Factors not already setup by Risk Type* to create Consequence values for Risk Types which have not already had values configured.
- Select *Overwrite all Consequence Factors regardless of Risk Type* to create Consequence values for all Risk Types, overwriting any Consequence values already created.

A dialog is displayed when the *Consequence Factors* have been created.



To see the *Consequence Factors* which have been created, click the *Manage* tab, select *Reference Data* and select *Risk Types* from the menu. Click on the *Factors* link text beside the Risk Type for which you want to review and select *Consequence Factor* from the dialog. In this example, the *Risk Type* Human Failure is selected. The *Consequence Factors* which were created automatically, are displayed.

CONSEQUENCE FORMULA DETAIL ON RISK TYPE: HUMAN FAILURE

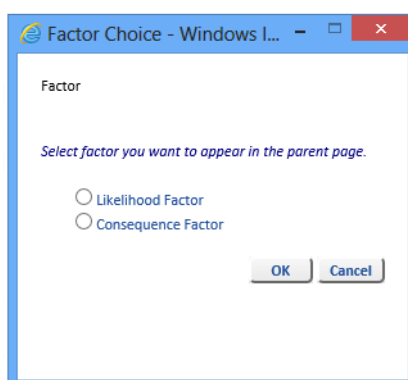
Factor	Very High (5)	High (4)	Medium (3)	Low (2)	Very Low (1)		
Consequence Type	No access	Major access restrictions	Frequent access restrictions	Minor access restrictions	No access restrictions	Edit	Del
Customers	Unacceptable business or project financial loss	Major business or project financial loss	Appreciable business or project financial loss	Minor business or project financial loss	No appreciable economic loss	Edit	Del
Financial	Assets at unacceptable risk	Assets at major risk	Assets at risk	Assets at minor risk	Assets not at risk	Edit	Del
Health & Safety	Death of large numbers of people	Major injuries resulting in loss of facility (arm, leg, eyesight, hearing)	Multiple injuries requiring medical treatment	Injury requiring medical treatment	Injury not requiring first aid treatment	Edit	Del
Infrastructure	Unacceptable delay or performance loss	Major delay or performance loss	Appreciable delay or performance loss	Minor delay or performance loss	No appreciable performance loss	Edit	Del
Legal	Unacceptable equipment safety issues, risk of explosion	Major equipment safety, obsolescence and/or support issues	Moderate equipment safety, obsolescence and/or support issues	Minor equipment safety, obsolescence and/or support issues	No equipment safety, obsolescence and/or support issues	Edit	Del
Production	Unacceptable customer issues	Major customer issues	Frequent customer issues	Minor customer issues	No customer issues	Edit	Del
Reputation	Unacceptable breach of environmental issues and/or corporate/brand image issues	Major breach of environmental issues and/or corporate/brand image issues	Frequent environmental issues and/or corporate/brand image issues	Minor environmental issues and/or corporate/brand image issues	No external or environmental issues	Edit	Del
Back To List						Add Factor	

9.3.2. Manually Create Consequence Factors

To create *Likelihood* and *Consequence Factors* manually, select the *Manage* tab, select *Reference Data* and select *Risk Types* from the menu.

Risk Type	Short Name	Risks		L	C	
Criminal Act	Criminal Act	1 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
Human Failure	Human Failure	1 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
Malicious Act	Malicious Act	0 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
Natural Hazard	Natural Hazard	0 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
Process Failure	Process Failure	0 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
System Failure	System Failure	6 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
Technical Failure	Technical Failure	0 Events	Factors	<input type="checkbox"/>	<input type="checkbox"/>	Edit Del
						Add

Click the *Factors* link text next to the appropriate *Risk Type* (for example, *Criminal Act*) and select *Consequence Factor*.



A dialog box titled "Factor Choice - Windows I..." with a close button. It contains the text "Factor" and "Select factor you want to appear in the parent page." Below this are two radio buttons: "Likelihood Factor" and "Consequence Factor". At the bottom are "OK" and "Cancel" buttons.

By default, there are no *Consequence Factors* configured.

Click the *Add Factor* button to configure the factors, for the selected *Risk Type* (Criminal Act in this example). Enter a name for the factor (Financial, in this example) and descriptive text for each of the ratings: *Very High*, *High*, *Medium*, *Low* and *Very Low*.

CONSEQUENCE FORMULA DETAIL ON RISK TYPE: CRIMINAL ACT

Factor	Very High (5)	High (4)	Medium (3)	Low (2)	Very Low (1)	
Financial	£1,000,000 loss	£500,000 loss	£100,000 loss	£50,000 loss	£10,000 loss	Edit Del

[Back To List](#)
[Add Factor](#)

Repeat these steps to add as many other *Factors* as required.

Then repeat these steps for other *Risk Types* for which you want to create *Consequence Factors*.

9.3.3. Using Likelihood And Consequence Factors

When *Likelihood* and/or *Consequence Factors* have been configured, (*Factors*) appears beside the *Likelihood* and/or *Consequence* fields (on the *Rating* tab of the Risk Form). Click (*Factors*) to open the Formula table. Enter Rating values for each of the configured *Factors*. Click the *Recalculate Formula* button to calculate the Rating. The highest entered Rating is used. Click the *Use Rating* button to populate the *Likelihood* or *Consequence* field with the calculated value.

9.4. Rating

To edit the Risk Rating definitions, select the *System* tab, select *System Data* and select *Rating* from the menu.

ID	Description	Management Criteria	Colour	Code	
1	Insignificant	Acceptable	Chartreuse	I	Edit
2	Low	Monitor	Chartreuse	L	Edit
3	Medium	Monitor	Yellow	M	Edit
4	High	Treatment Required	Red	H	Edit
5	Extreme	Immediate Treatment	Red	E	Edit

This information is included in a table which is displayed when the ... button is clicked to the right of the *Rating* field when a Risk is viewed or a new Risk is entered.

The *ID* cannot be changed. (The *ID* is displayed as *Code* when the ... button is clicked to the right of the *Rating* field when a Risk is viewed or a new Risk is entered.)

The *Description* can be changed. (The *Description* is displayed as the *Risk Rating* when the ... button is clicked to the right of the *Rating* field when a Risk is viewed or a new Risk is entered.)

The *Management Criteria* can be edited. (The *Management Criteria* is displayed as the *Rating* when the ... button is clicked to the right of the *Rating* field when a Risk is viewed or a new Risk is entered.)

You can change the *Colour* associated with each Risk Rating. This colour is used when results are returned from a Risk Search and the SART columns are displayed. It is also used in matrices and charts.

For a Triage matrix you will have to swap the descriptions so that 1 is *Extreme* and 5 is *Negligible*. For a 4-level Triage matrix, make sure there are just entries for IDs 1-4, going from Extreme to Low.

9.5. Willingness

To edit the *Willingness* definition, select the *System* tab, select *System Data* and select *Willingness* from the drop-down menu.

Willingness	Name	
1	Very Unwilling	Edit
2	Unwilling	Edit
3	Willing	Edit
4	Very Willing	Edit

To change a *Willingness Name*, select *Edit* next to the one you want to alter. You are now able to change the name field.

When you have finished typing the new name, select *Save* to keep the change or *Cancel* to revert back to the current name.



Note: The *Willingness* numerical value in the left column cannot be changed.

9.6. Impact

To edit the *Impact* definition, select the *System* tab, select *System Data* and select *Impact* from the drop-down menu.

Impact	Name	
1	Insignificant	Edit
2	Minor	Edit
3	Moderate	Edit
4	Major	Edit

To change an *Impact* Name, select *Edit* adjacent to the one you want to alter. You are now able to change the name field.

When you have changed the new name, select *Save* to keep the change or *Cancel* to revert back to the current name.



Note: The *Impact* numerical value in the left column cannot be changed.

9.7. Appetite Matrix

The Appetite Matrix is a 4x4 matrix. That is, four levels of *Willingness* and four levels of *Impact* which then calculates an overall rating.

The default levels are:

Willingness (see "*Willingness*" on page 65)

1. Very Unwilling
2. Unwilling
3. Willing
4. Very Willing

Impact (see "*Impact*" on page 66)

1. Insignificant
2. Minor
3. Moderate
4. Major

Appetite Rating is displayed as numbers and text with corresponding colour highlights. The default settings can be configured to a users requirements, see ["Changing The Appetite Rating Colour"](#) on page 68 and ["Changing The Appetite Rating Name"](#) on page 68.

Willingness	Impact	Appetite Rating	
1 Very Unwilling	1 Insignificant	1 Low	Edit
2 Unwilling	1 Insignificant	1 Low	Edit
3 Willing	1 Insignificant	1 Low	Edit
4 Very Willing	1 Insignificant	1 Low	Edit
1 Very Unwilling	2 Minor	1 Low	Edit
2 Unwilling	2 Minor	1 Low	Edit
3 Willing	2 Minor	2 Medium	Edit
4 Very Willing	2 Minor	2 Medium	Edit
1 Very Unwilling	3 Moderate	1 Low	Edit
2 Unwilling	3 Moderate	2 Medium	Edit
3 Willing	3 Moderate	3 Medium-High	Edit
4 Very Willing	3 Moderate	3 Medium-High	Edit
1 Very Unwilling	4 Major	1 Low	Edit
2 Unwilling	4 Major	2 Medium	Edit
3 Willing	4 Major	3 Medium-High	Edit
4 Very Willing	4 Major	4 High	Edit

[Edit the Willingness](#)
[Edit the Impact](#)
[Edit the Appetite Rating](#)

9.7.1. Changing The Appetite Rating Level

Select *Edit* to the right of the Appetite Rating you want to alter. From the drop down list of list you can choose a new level to associate with the Appetite Rating.

Appetite Rating

Low
 Medium
 Medium-High
 High

When you have changed the Appetite Rating level, select *Save* to keep the change or *Cancel* to revert back to the previous level.

- Selecting the *Edit the Willingness* button will open the Willingness Definitions page, see ["Willingness"](#) on page 65.
- Selecting the *Edit the Impact* button will open the Impact Definitions page, see ["Impact"](#) on page 66.
- Selecting the *Edit the Appetite Rating* button will open the Appetite Rating Definitions page, see ["Appetite Rating"](#) on page 67.

9.8. Appetite Rating

The Appetite Rating *Name* and *Colour* can be configured from the *System* tab, select *System Data* and then select Appetite Rating from the drop-down menu.

ID	Name	Colour	Code	
1	Low	Chartreuse	L	Edit
2	Medium	Gold	M	Edit
3	Medium-High	DarkOrange	MH	Edit
4	High	Red	H	Edit



Note: The *ID* numerical value in the left column cannot be changed. The *Code* column to the right of the *Colour* column is not utilised in *Appetite Rating*.

9.8.1. Changing The Appetite Rating Colour

Select *Edit* adjacent to the colour you want to alter. From the drop down list of colours you can choose a new colour to associate with the Appetite Rating.



Select *Save* to keep the change or *Cancel* to revert back to the previous colour.

9.8.2. Changing The Appetite Rating Name

Select *Edit* adjacent to the Name you want to alter. You are now able to change the name field.

When you have finished typing the new name, select *Save* to keep the change or *Cancel* to revert back to the current name.

9.9. Enterprise Rating

To edit the Enterprise Rating values, select the *System* tab, select *System Data* and select *Enterprise Rating* from the menu.

Rating	Cutoff Value	
1	10,000	Edit
2	50,000	Edit
3	500,000	Edit
4	5,000,000	Edit
5	999,999,999,999	Edit
6	999,999,999,999	Edit
7	999,999,999,999	Edit
8	999,999,999,999	Edit
9	999,999,999,999,999	Edit

[Update Consequence cut-off values](#)

The highest level of rating must be populated with a number higher than you would ever use for Potential loss.

After updating the values, press the *Update Consequence cut-off values* button to update the Consequence cut-off values for the relevant levels. This means that when a User displays the Consequence pop-up when editing Risks, the value will show correctly.

9.12. Change Matrix

Select the *System* tab, select *System Data* and select *Change Matrix* from the menu.

Before you can access the Change Matrix page, you must first sign in. Enter the password *changematrix* (all one word) in the *Password* text box and click the *Sign In* button.

The default matrix is a 5x5x5 matrix. That is, five levels of *Likelihood*, five levels of *Consequence* and five levels of *Risk Rating*. The default levels are:

Likelihood (see "[Likelihood](#)" on page 61)

1. Rare
2. Unlikely
3. Possible
4. Likely
5. Almost certain

Consequence (see "[Consequence](#)" on page 61)

1. Insignificant
2. Minor
3. Moderate
4. Major
5. Critical

Rating (see "[Rating](#)" on page 65)

1. Insignificant
2. Low
3. Medium
4. High
5. Extreme

9.12.1. Numeric Value

Select *Numeric Value* and click the *Change Matrix* button to change the settings for the Numeric Value matrix. See "[Risk Matrix Options](#)" on page 5 for more information about the selecting the type of matrix.

9.12.2. Edit Risk Ratings For Numeric Value Matrix



Note: This section applies only if you have selected *Numeric Value* for your matrix. It does not apply if you have selected a Custom or Triage matrix.

If you want to change the levels at which Risk Ratings cut in, then use *Edit Risk Ratings* to change the cut-off values.

RATING DEFINITIONS

ID	Rating Level	Description	Management Criteria	Colour	Code	
1	0	Insignificant	Acceptable	Chartreuse	I	Edit
2	3	Low	Monitor	Chartreuse	L	Edit
3	5	Medium	Monitor	Yellow	M	Edit
4	10	High	Treatment Required	Red	H	Edit
5	20	Extreme	Immediate Treatment	Red	E	Edit

Edit the Rating Level to change when a Risk Rating changes level (from Insignificant to Low, for example). The examples below show how changing these values affect the matrix.

Normal		Insignificant	Minor	Moderate	Major	Catastrophic		
		1	2	3	4	5		Rating Level
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	10
Possible	3	3	6	9	12	15	Medium	5
Unlikely	2	2	4	6	8	10	Low	3
Rare	1	1	2	3	4	5	Insignificant	0

Option 2		Insignificant	Minor	Moderate	Major	Catastrophic		
		1	2	3	4	5		Rating Level
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	15
Possible	3	3	6	9	12	15	Medium	10
Unlikely	2	2	4	6	8	10	Low	5
Rare	1	1	2	3	4	5	Insignificant	0

Option 3		Insignificant	Minor	Moderate	Major	Catastrophic		
		1	2	3	4	5		Rating Level
Almost certain	5	5	10	15	20	25	Extreme	20
Likely	4	4	8	12	16	20	High	14
Possible	3	3	6	9	12	15	Medium	8
Unlikely	2	2	4	6	8	10	Low	4
Rare	1	1	2	3	4	5	Insignificant	0

The top settings show a Risk Rating of 0-2 is Insignificant, 3-4 is Low, 5-9 is Medium, 10-19 is High and 20 or higher is Extreme. The Risk Rating is usually calculated by multiplying the values for the *Likelihood* and the *Consequence* (see ["Formula Tab" on page 35](#) for more information).

9.12.3. Activating The Matrix

If you have edited the Risk Rating levels, click the *Activate the Matrix* button to save your changes.

Exit all browser sessions and then restart OpRiskControl.

Select the *System* tab, select *System Settings*, then, at the bottom of any page, press *Refresh System Settings*.

[Refresh System Settings](#)

This causes a refresh of the system settings.



Note: It is often necessary to restart IIS. If you are not able to restart IIS due to other live web applications, then Stop and Start the website itself.

To finish activating the matrix, select the *Manage* tab, select *Risk Data* and click on the option *Recalculate risk values if risk matrix altered (applies to ALL risks, ignoring filter criteria above)*.

Go to *Dashboard* to check the matrix. If the labels are not as you want them, follow instructions in ["Risk Matrix Descriptions" on page 9](#).

9.12.4. Custom

Select *Custom* and click the *Change Matrix* button to change the settings for the Custom matrix. See ["Risk Matrix Options" on page 5](#) for more information about the selecting the type of matrix.

If you select *Custom* or *Triage* and click *Change Matrix*, the form will expand so that you can change the intersection of *Likelihood* and *Consequence* to specify the desired Risk Rating.

ID	Likelihood	Consequence	Rating
1	1 Rare	1 Insignificant	1 Insignificant
2	2 Unlikely	1 Insignificant	1 Insignificant
3	3 Possible	1 Insignificant	2 Low
4	4 Probable	1 Insignificant	2 Low
5	5 Almost certain	1 Insignificant	3 Medium
6	1 Rare	2 Minor	1 Insignificant
7	2 Unlikely	2 Minor	2 Low
8	3 Possible	2 Minor	3 Medium
9	4 Probable	2 Minor	3 Medium
10	5 Almost certain	2 Minor	3 Medium
11	1 Rare	3 Moderate	2 Low
12	2 Unlikely	3 Moderate	3 Medium
13	3 Possible	3 Moderate	3 Medium
14	4 Probable	3 Moderate	3 Medium
15	5 Almost certain	3 Moderate	4 High
16	1 Rare	4 Major	2 Low
17	2 Unlikely	4 Major	3 Medium
18	3 Possible	4 Major	3 Medium
19	4 Probable	4 Major	4 High
20	5 Almost certain	4 Major	5 Extreme
21	1 Rare	5 Critical	3 Medium
22	2 Unlikely	5 Critical	3 Medium
23	3 Possible	5 Critical	4 High
24	4 Probable	5 Critical	5 Extreme
25	5 Almost certain	5 Critical	5 Extreme

Edit the column named *Rating* to declare which rating you want to appear in that cell.

9.12.5. Triage

Select *Triage* and click the *Change Matrix* button to change the settings for the Triage matrix. See ["Risk Matrix Options" on page 5](#) for more information about the selecting the type of matrix.

9.13. Global Translator



Note: Should you need to rename any fields once the system has gone live, please contact the Help desk for advice and guidance on how to do this.

When renaming fields, keep a note of the original name and the new name so this documentation can still be used.

9.14. Risk Status

The *Risk Status* short codes are:

Status Name	Short Label	
Cancelled	X	Edit
Closed	C	Edit
Input	I	Edit
Open	O	Edit
Suspended	S	Edit

These may be edited by selecting the *System* tab, selecting *System Data* and selecting *Risk Status* from the menu. Status codes that are essential to the system cannot be deleted.

Status codes can be added and deleted (unless they have been used in the system). Risks with non-system status codes are counted in the Dashboard under *Other/Active* and the system will not automatically process them in any way.

9.15. Structure Filter

The *Structure Filter* maintains the relationship between two levels of organisational structure (Division and Department).

Your database will contain separate data tables containing your organisation's divisions and departments. Normally they are not linked in any hierarchical structure. However, your System Administrator may link them to make data entry easier.

The System Administrator may switch this filter on or off as desired using the *Allow Filtering* tick box at top left of the form. The System Administrator may add new relationships using the data entry fields at the bottom of this filter form.

STRUCTURE FILTER

Allow Filtering: ☒ [Print](#)

Division	Department		
Corporate	Corporate	Edit	Del
Corporate	Engineering	Edit	Del

[Add](#)

In this example, the Division Corporate has been configured with two Departments – *Corporate* and *Engineering*. When a new Risk is created and the Division is set to Corporate, only the Departments Corporate and Engineering are available.

RISK DETAILS:

Risk

Context Rating Ownership and Dates Financial

[Clear Context]

Department

Division: Corporate

Department: Corporate

Function: Engineering

However, if a different *Division* is selected, all *Departments* are available because there is no other Structure defined.

RISK DETAILS:

Risk

Context Rating Ownership and Dates Financial

[Clear Context]

Department

Division: Operational

Department:

Function:

Project:

Location:

Risk Type

Event Type:

Asset Type:

Asset:

Classification:

Across all Business Units

Corporate

Engineering

Finance

Fusion

Human Resources

Information Technology

Internal Audit

Manufacturing

Occupational Health and Safety

Office of the CEO

Professional Services

Program Office/Projects

Research and Development

Risk Management

Sales and Marketing

Security

Strategy and Planning

Click the *Add* link text to create a new entry. Select the *Division* from the first drop-down list then select the *Department* from the second drop-down list. Continue until you have created the Structure you require.

Select *Allow Filtering* to use the Structure you have created. Clear *Allow Filtering* to ignore the structure you have created (that is, all *Departments* will be available when any *Division* is selected). When this option is cleared, the Structure you defined is hidden. However, it has not been deleted – it is displayed when the *Allow Filtering* option is selected.

9.16. Action Type

The *Action Type* is used to define the *Action Codes* which are defined by selecting the *Manage* tab, then selecting *Reference Data* and selecting *Action Code* from the menu. See “[Action Code](#)” on page 89 for more information.

To add a new *Action Type*, enter,

- a numeric value for the *Order* in which the new entry should appear in the list of *Action Types*.
- a name for the *Action Type*.
- a description of the *Action Type*.
- a description of the *Time Frame*.

and then click the *Add* link text.

To delete an *Action Type*, click the *Delete* link text next to the *Action Type* you want to delete.

You can only delete *Action types* you have created. System *Action Types* cannot be deleted.

To edit the *Action Type*, click the *Edit* link text next to the *Action Type* you want to edit.

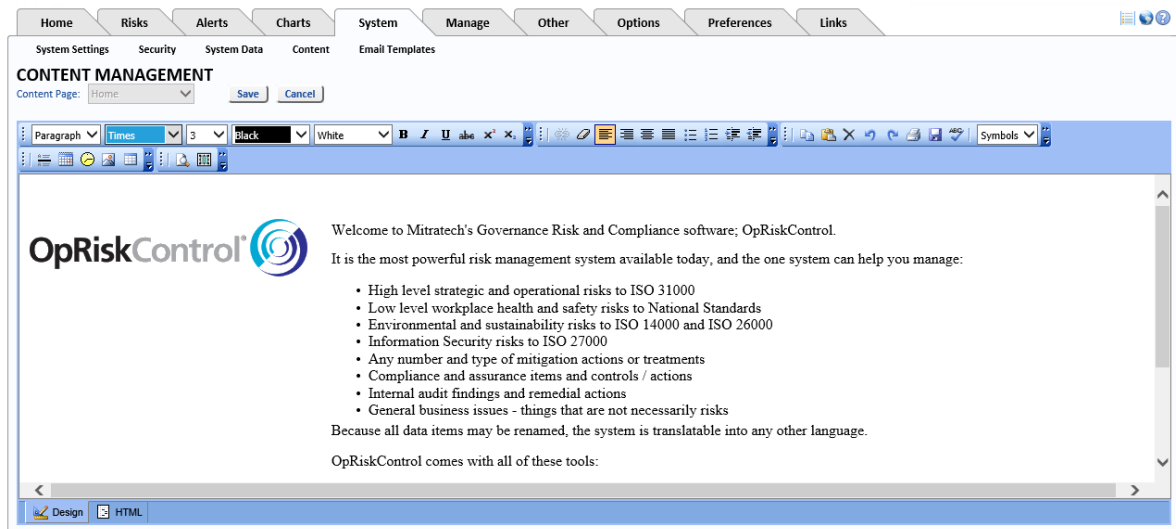
10. System Content

10.1. Manage Content

Select the *System* tab and then click *Content* and select *Manage Content* from the menu.



Caution: Edit the Home Page with care. The *Manage Content* option should only be used by an experienced HTML editor.



To create a *new* Content Page, select *New Content Page* from the drop-down list and click *Edit*. When you have created the new Content Page, enter a name for it in the text box and click *Save* to save the changes or *Cancel* to discard the changes.

To edit an *existing* Content Page, select it from the drop-down list and click *Edit*. After making the required changes, click *Save* to save the changes or *Cancel* to discard the changes.

10.2. Manage Links

Select the *System* tab and then click *Content* and select *Manage Links* from the menu.

Content Management allows the System Administrator to link to internal Intranet or external Internet web sites, edit the home page, upload documents and link to them, and to import the company logo.

Name	Link Type	Link			
Mitrates	Web Link	http://www.mitrates.com	Edit	Del	<input type="checkbox"/>
Google	Web Link	http://google.co.uk	Edit	Del	<input type="checkbox"/>

Link Type: Web Link

Name:

Complete URL (including http://):

[Save](#)

Documents and URLs added here will appear in the *Links* tab.

10.3. Import Logo

Select the *System* tab and then click *Content* and select *Import Logo* from the menu.

If you want your corporate logo on the top right of the banner, there are two ways to add the corporate logo. (The logo should not be more than 55 pixels high.)

- Your DBA may enter the name of the logo in the database table tblControl.[Co Brand Logo] and copy the logo into \RiskManager\ClientFiles\Images\Branding.
- Alternatively, you can select the *System* tab, select *Content* and select *Import Logo* from the menu. Click the *Browse* button to find the logo, then *Import* the logo.



The screenshot shows a dialog box with a light blue header containing the text "Please specify logo that will be used on this system." Below the header is a form with a label "Logo:" followed by a text input field. To the right of the input field are two buttons: "Browse..." and "Import".

11. System Email Templates

You can configure the emails generated by the system. Select the *System* tab and then select *Email Templates*.

This allows the System Administrator to edit emails for:

- Action Completed/Due/Overdue/Owner Assigned
- Ad-hoc Action/Reminder/Risk Email
- Claim Email
- Compliance Due and Overdue (if Compliance Interface activated)
- Contact Assigned
- Deactivated User
- Key Indicator Reminder
- Owner Assigned
- Review Due/Overdue
- Risk Email
- Risk Exemption Expired
- Risk Reminder
- Stakeholder Alert

11.1. Making Changes To Email Templates

Each Email Template can be edited by adding, deleting or editing a line. Each line can contain text and data fields. Empty lines can be added between lines of text. In the example below, regular text indicates text typed in by the Administrator and bold text is a data field.

The screenshot shows the 'Review Due' email template configuration. At the top, there is a 'Template Name' dropdown set to 'Review Due' and a 'Restore Default' button. Below this, the 'Subject' field contains 'Risk update required for - Risk Name' with an 'Edit Subject' button. The 'Body' field contains several lines of text: 'Please provide an update for this risk: Risk Name', 'Date last reviewed: Date Last Reviewed', and 'Last Residual Assessment: Residual'. Each line has 'Edit Line' and 'Delete' links to its right. At the bottom right of the body field is an 'Add New Line' button. Below the body field, a red message states: 'This email will have an active link to the item itself. The email recipient will need a login to the system to access the details.'

12. Manage Users

Select the *Manage* tab and then select *Users*.

12.1. Users And Contacts

The *User And Contacts* page is used to maintain both a list of current system Users and the names of all people involved in Risk management.

USERS AND CONTACTS

Users And Contacts User Groups User Import

Filter to show users or contacts whose name contains:

User Name	Telephone	E-Mail	Job Title	Login	Imported	Active	
John Doe		john.doe@company.com	Manager	john.doe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Select Delete
Jane Smith		jane.smith@company.com	Analyst	jane.smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Mike Johnson		mike.johnson@company.com	Analyst	mike.johnson	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select
Sarah Lee		sarah.lee@company.com	Analyst	sarah.lee	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
David Kim		david.kim@company.com	Analyst	david.kim	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Emily White		emily.white@company.com	Analyst	emily.white	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Chris Brown		chris.brown@company.com	Analyst	chris.brown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Alex Green		alex.green@company.com	Analyst	alex.green	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Mia Black		mia.black@company.com	Analyst	mia.black	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Noah Grey		noah.grey@company.com	Analyst	noah.grey	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Olivia Pink		olivia.pink@company.com	Analyst	olivia.pink	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Liam Blue		liam.blue@company.com	Analyst	liam.blue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Ava Yellow		ava.yellow@company.com	Analyst	ava.yellow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Ethan Purple		ethan.purple@company.com	Analyst	ethan.purple	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Sophia Teal		sophia.teal@company.com	Analyst	sophia.teal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Lucas Silver		lucas.silver@company.com	Analyst	lucas.silver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Gold		isabella.gold@company.com	Analyst	isabella.gold	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Bronze		benjamin.bronze@company.com	Analyst	benjamin.bronze	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Copper		charlotte.copper@company.com	Analyst	charlotte.copper	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Iron		william.iron@company.com	Analyst	william.iron	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Steel		amelia.steel@company.com	Analyst	amelia.steel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Tin		james.tin@company.com	Analyst	james.tin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Lead		harper.lead@company.com	Analyst	harper.lead	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Zinc		robert.zinc@company.com	Analyst	robert.zinc	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Nickel		evelyn.nickel@company.com	Analyst	evelyn.nickel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Cobalt		christopher.cobalt@company.com	Analyst	christopher.cobalt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Manganese		madison.manganese@company.com	Analyst	madison.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Vanadium		christopher.vanadium@company.com	Analyst	christopher.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Chromium		isabella.chromium@company.com	Analyst	isabella.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Molybdenum		benjamin.molybdenum@company.com	Analyst	benjamin.molybdenum	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Selenium		charlotte.selenium@company.com	Analyst	charlotte.selenium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Niobium		christopher.niobium@company.com	Analyst	christopher.niobium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Isabella Manganese		isabella.manganese@company.com	Analyst	isabella.manganese	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Benjamin Vanadium		benjamin.vanadium@company.com	Analyst	benjamin.vanadium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Charlotte Chromium		charlotte.chromium@company.com	Analyst	charlotte.chromium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
William Tellurium		william.tellurium@company.com	Analyst	william.tellurium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Amelia Bismuth		amelia.bismuth@company.com	Analyst	amelia.bismuth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
James Antimony		james.antimony@company.com	Analyst	james.antimony	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Harper Arsenic		harper.arsenic@company.com	Analyst	harper.arsenic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Robert Cadmium		robert.cadmium@company.com	Analyst	robert.cadmium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Evelyn Barium		evelyn.barium@company.com	Analyst	evelyn.barium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Christopher Strontium		christopher.strontium@company.com	Analyst	christopher.strontium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Select Delete
Madison Zirconium		madison.zirconium@company.com	Analyst	madison.zirconium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

responsible parties), therefore the System Administrator or Risk coordinator should add or edit their records here.

12.1.1.2. Manually Created Users

If an employee leaves the organisation and has never had any association with Risks in this database, they may be *Deleted*. If they have been associated with information in the system, they cannot be deleted (because you would lose a valuable audit trail). Therefore, they must be set to *Inactive*. See ["Deactivate/Activate" on page 83](#) for more information.

12.1.2. Print List

The *Print List* button on the *Users and Contacts* page has options to display all Users and contacts, Users only, non-users only, de-activated Users with open/active Risks, de-activated Users with open/active controls/Actions. This list can then be printed by selecting *Print* from the *File* menu.

12.1.3. Change Layout

Clicking the *Change Layout* button opens the *User Preferences – User List* page. The default layout includes the following columns:

- User Name
- Telephone
- E-Mail
- Job Title
- Login
- Imported
- Active.

Any of these columns can be hidden by selecting edit, selecting the field(s) you want hidden and then clicking the < button.

In addition, the following columns can be added:

- Cost Account
- Department
- Division
- Location1
- Location2
- Manager
- Mobile Phone
- User Form

To add a column, click *Edit*, select the columns you want to be visible and click the > button.

Click *Save* to save your layout changes, or *Cancel* to discard them.

You can use the *Restore Defaults* button to restore the default layout settings.

Click *Back* to return to the *Users and Contacts* page.

12.1.4. New User

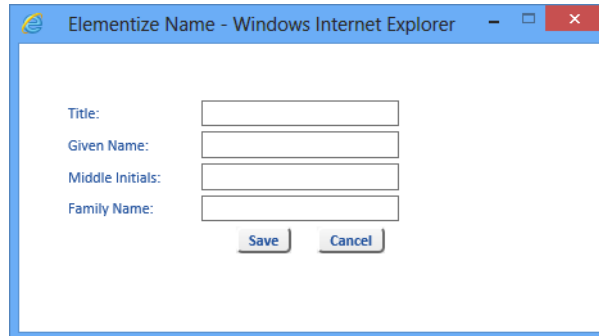
Click the *New User* button to create a new User.

This screen allows you to enter information in the following fields:

- Name (click the ... button to configure – see below)

- Phone Number
- E-Mail
- Job Title
- User Name
- Allow user to Disable Filter
- Approval Level
- Active – (see ["Deactivate/Activate" on page 83](#))
- Division
- Mobile Phone
- Department
- Manager
- Location 1
- Cost Account
- Location 2
- User's Form (cannot be changed)

Click the ... button next to *Name* to open the *Name* dialog. *Name* is the only mandatory field on this page. Click *Save* to save your changes or *Cancel* to discard your changes.



12.1.4.1. Title

Optional: If required, enter a Title such as Miss, Mr or Mrs.

12.1.4.2. Given Name

Required: Enter the given name of the User.

12.1.4.3. Middle Initials

Optional: If required, enter the middle initials of the User.

12.1.4.4. Family Name

Required: Enter the family name of the User.

12.1.5. Select

Click *Select* to view the User Details for that User.

Name:	Mitrates Support	Phone Number:	01628 6900900
E-Mail:	support@mitrates.com	Job Title:	
User Name:	headoffice\mitrates	Allow User to Disable Filter:	<input type="checkbox"/>
Approval Level:		Active:	<input checked="" type="checkbox"/>
Division:		Mobile Phone:	
Department:		Manager:	
Location 1:		Cost Account:	
Location 2:		User's Form:	Tabbed Form

[Back To List](#)
[New User](#)
[Deactivate](#)
[Edit](#)

The *User Details* page includes many optional data items. The only mandatory data item is the *Name*, and, although the name would normally be an employee, it may be an external person or a business role such as *Mitrates Support*.

If an email address is not included, the User will not receive email notifications.

A valid login name in *Domain Username* is required to allow a User to log in to OpRiskControl.

If operating without RBS, there will be a check-box named *Allow User to Translate Screens*. If this is checked for any User, that User may translate forms and reports.

If the structure filter is activated at the system level, the User may be allowed to disable the structure filter that links department to division.

When the *Select* link text is clicked, the *User Details* for the selected User is displayed. See ["User Details" on page 82](#) for more information.

12.1.6. User Details

12.1.6.1. Back To List

Click the *Back To List* button to return to the *Users and Contacts* page.

12.1.6.2. New User

Click the ... button next to *Name* to open the *Name* dialog. *Name* is the only mandatory field on this page. Click *Save* to save your changes or *Cancel* to discard your changes.

Elementize Name - Windows Internet Explorer

Title:

Given Name:

Middle Initials:

Family Name:

[Save](#) [Cancel](#)

12.1.6.2.1. Title

Optional: If required, enter a Title such as Miss, Mr or Mrs.

12.1.6.2.2. Given Name

Required: Enter the given name of the User.

12.1.6.2.3. Middle Initials

Optional: If required, enter the middle initials of the User.

12.1.6.2.4. Family Name

Required: Enter the family name of the User.

12.1.6.3. Deactivate/Activate

Click the *Deactivate* button to change a User's status from *Active* to *Inactive*. *Inactive* Users do not appear in lookup lists for *new* Risks, but still appear in lookup lists for *existing* Risks.

Click *Activate* to make an *Inactive* User, *Active*.

12.1.6.4. Edit

Click *Edit* to edit any of the fields on the *User Detail* page. Click *Save* to save your changes or *Cancel* to discard your changes.

12.1.7. Risks Tab

12.1.7.1. Reassign Risks

The *Risks* tab is displayed when a User has been selected from the *Users And Contacts* page and the *Select* link text is clicked.

If an employee leaves the organisation or is reassigned to another business unit, it will normally be necessary to reassign the Risks for which they were responsible.

RISKS FOR NATALIE FITZHUGH

User Details Risks Actions User Groups Where Used Documents

Risk Filter: All

Status	Risk	Risk Event	Owner	Contact	
Open	Failure to align financial resources with key priorities	Finances	Natalie FitzHugh	Financial Systems Manager	View Risk

[Back To List](#)
[Globally change](#)
Natalie FitzHugh to

[Cancel](#)
[Reassign Risks](#)

Select the *User*, then click on the *Risks* tab to see all the Risks assigned to that User. Change the *Owner* or *Contact* and then click *Reassign Risks*. Alternatively, use the *Globally change* button to change *all occurrences* of the selected User to the new User. (It is not necessary to reassign closed or cancelled Risks.)

12.1.8. Actions Tab

The *Actions* tab is displayed when a User has been selected from the *Users And Contacts* page and the *Select* link text is clicked.

12.1.8.1. Reassign Actions

If an employee leaves the organisation or is assigned to a different business unit, it will normally be necessary to reassign the Actions for which they were responsible.

ACTIONS FOR NATALIE FITZHUGH

User Details Risks **Actions** User Groups Where Used Documents

Risk	Action	Due	Responsible Party	Owner	
Shareholders fraud risk	Employee Training			Natalie FitzHugh	View Action
Anti-money laundering	Employee Training	31/07/2012		Natalie FitzHugh	View Action
Anti-money laundering	Monitor and Review			Natalie FitzHugh	View Action

[Back To List](#)
 Globally change Natalie FitzHugh to
[Cancel](#) [Reassign Actions](#)

Select the *User*, then click on the *Actions* tab to see all the Actions assigned to that User. Change the *Owner* and then click *Reassign Actions*. Alternatively, use the *Globally change* button to change *all occurrences* of the selected User to the new User. (It is not necessary to reassign closed or cancelled Actions.)

12.1.9. User Groups Tab

The *User Groups* tab is displayed when a User has been selected from the *Users And Contacts* page and the *Select* link text is clicked.

When a User has been selected on the *Users and Contacts* tab, the *User Groups* tab displays all the Groups to which the selected User belongs.

12.1.9.1. Add A User To A Group

To add the selected User to a Group, select the Group from the drop-down list and click *Add*. See “[User Groups](#)” on page 85 for information on creating new User Groups.

Click *Back To List* to return to the *Users and Contacts* page.

12.1.10. Where Used Tab

The *Actions* tab is displayed when a User has been selected from the *Users And Contacts* page and the *Select* link text is clicked.

When a User has been selected on the *Users and Contacts* tab, the *Where Used* tab displays all the Groups and Functions to which the selected User belongs.

Click *Back To List* to return to the *Users and Contacts* page.

12.1.11. Where Used

You may display a page that shows any User’s associations. If the User is associated with the following objects, they are listed on a page so the object may be edited and the User removed: Division Manager, Department Manager, Function Manager, Initiative Manager, User Group, Processes and Risk Stakeholder.

The screenshot shows the 'User Details' tab with the following fields:

Department Manager	
Finance	View
User Group	
Project Managers	View

A User may not normally be removed as the recorder of a Risk or associated history.

12.1.12. Documents Tab

The *Actions* tab is displayed when a User has been selected from the *Users And Contacts* page and the *Select* link text is clicked.

12.2. User Groups

User Groups can be created so that Risks and Actions can have their Owner set to a Group rather than an individual.

If a Risk is appropriate for all business units or all projects, it need only be recorded once and the Risk contact or Risk owner or Action owner may be a User Group rather than an actual person. Automatic notifications are then sent to all Users belonging to that group, and people may belong to multiple Groups.

The first step is to create the Groups. From the *Users and Contacts* tab, select *User Groups*. Enter the new Group name in the text box and click *Add* to create the new Group. When a new Group is created, you will find that Group name is also in the User list, and the system will have automatically linked the two records.

The screenshot shows the 'User Groups' tab with the following form:

Group Name	Edit	List	Del
Project Managers			
<input type="text"/>			Add

The next step is to add Users to the Group – see “[Add A User To A Group](#)” on page 84.

In the following image, Alison Heard belongs to Project Managers.

USER GROUPS FOR ALISON HEARD

The screenshot shows the 'User Groups' tab with the following form:

Group Name	Remove
Project Managers	
Select...	Add

In this way, the effort in recording and managing Risks is greatly reduced.

12.3. User Import

If the Active Directory Import is enabled, you will see a tab named *User Import*. This page allows you to configure Users to be automatically imported *Daily* or *Weekly*.



Note: When the *Import Frequency* is set to *Off*, no Users are imported.

We recommend using the *Daily* schedule.

To configure User Import, select the *Import Frequency*, then scroll down the list of *Users Found In Active Directory*, and *Exclude* any users you *do not* want to be imported.

Click *Save and Import*. The system will exclude the selected Users every time it performs the *Daily* (or *Weekly*) Import.

13. Manage Documents

The *Manage* tab can be used to access *Documents* which opens the *Admin Documents* page.

The screenshot shows the 'ADMIN DOCUMENTS' page. At the top, there are tabs: Home, Risks, Alerts, Charts, System, Manage, Other, Options, Preferences, and Links. Below these are sub-tabs: Users, Documents, Reference Data, Risk Data, Risk Lookups, and Action Lookups. The 'Manage' tab is selected. The main area contains a table with the following data:

Document Name	Created	Author	Revised	Version	Attached By	Security Class	Status
http://www.mitrates.com	23/01/2017				Peter Beard		

Below the table is a form with the following fields:

- Document Name:
- Created:
- Author:
- Revised:
- Version:
- Attached By:
- Security Class:
- Status:

At the bottom right of the form are 'Cancel' and 'Save' buttons.

This section can be used to upload documents for use by the System Administrator.

13.1. Attach Hyperlink

To add a document, click the *Attach Hyperlink* button.

The screenshot shows the 'ADMIN DOCUMENTS' page. At the top, there are tabs: Home, Risks, Alerts, Charts, System, Manage, Other, Options, Preferences, and Links. Below these are sub-tabs: Users, Documents, Reference Data, Risk Data, Risk Lookups, and Action Lookups. The 'Manage' tab is selected. The main area contains a table with the following data:

Document Name	Created	Author	Revised	Version	Attached By	Security Class	Status
OpRiskControl System Administrator's Guide.pdf	21/01/2014	Peter Beard		23/01/2017	Peter Beard		

Below the table is a form with the following fields:

- Full Hyperlink:
- Created:
- Author:
- Revised:
- Version:
- Attached By:
- Security Class:
- Status:

At the bottom right of the form are 'Cancel' and 'Save' buttons.

Enter the hyperlink address in the *Full Hyperlink* text box. Values for any of the following fields, as required: *Version*, *Created*, *Author*, *Security Class*, *Revised*, and *Status*. The name of the User who attached the hyperlink is automatically put in the *Attached By* field.

Click *Save* to save the attached hyperlink or *Cancel* to cancel the hyperlink addition.

13.2. Attach Document

To add a document, click the *Attach Document* button.

The screenshot shows the 'ADMIN DOCUMENTS' interface. The top navigation bar includes tabs for Home, Risks, Alerts, Charts, System, Manage, Other, Options, Preferences, and Links. The sub-navigation bar includes Users, Documents, Reference Data, Risk Data, Risk Lookups, and Action Lookups. The main content area is titled 'ADMIN DOCUMENTS' and contains a large empty box for document content. At the bottom, there are input fields for 'Document Name' (with a 'Browse...' button), 'Created' (with a date picker showing '23/01/2017'), 'Author' (with a text input), 'Revised' (with a date picker), 'Version' (with a text input), 'Attached By' (with a dropdown menu showing 'Peter Beard'), 'Security Class' (with a text input), and 'Status' (with a text input). There are 'Cancel' and 'Save' buttons at the bottom right.

Click the *Browse* button (beside *Document Name*) to select the document you want to add. Values for any of the following fields, as required: *Version*, *Created*, *Author*, *Security Class*, *Revised*, and *Status*. The name of the User who attached the document is automatically put in the *Attached By* field.

Click *Save* to save the attached document or *Cancel* to cancel the document upload.

14. Manage Reference Data

Reference Data items can be selected from the menu which is displayed when the mouse hovers over the option *Reference Data* on the Manage tab. Alternatively, click on *Reference Data* on the Manage tab to display buttons. Select the item you want to view.

REFERENCE DATA

Action Code	Action Frequency	Asset	Asset Types
Departments	Divisions	Division Groups	Exposure Periods
Function	History Types	Project	Locations
Responsible Parties	Review Frequencies	Risk Events	Other Classifications
Event Contexts	Risk Types	Standards	Timeframe
Categories	Risk Capacity	Correlation to Strategy	

To print the Reference Data for any item, select the appropriate item from the menu and click the *Print List* button (as shown below *Action Codes*).

14.1. Action Code

Select *Action Code* from the *Reference Data* menu to add a *New Action Code*, *Edit* and *Delete Action Codes*. If an Action Code is being used on any Risk, you will not be allowed to delete it.

Action Code	Description	Action Type		
Employee Training	Conduct employee training	Administrative Controls	Select	Delete
Existing Controls	Administrative Controls	Select	Delete
Inspection	Conduct inspection	Administrative Controls	Select	Delete
Insurance	Insurance policy ...	Administrative Controls	Select	Delete
Monitor and Review	Monitor and Review	Administrative Controls	Select	Delete
Scheduled Maintenance		Administrative Controls	Select	Delete

[Print List](#)
 Show rows per page [Change](#)
[New Action Code](#)



Note: The information displayed on this page is determined by configuring the *Action Code List* on the *Preferences* tab. Please refer to the *OpRiskControl Users' Guide* for more information.

Action Codes are a list of common Action measures. The *Action Code* description automatically populates the *Risk Control* or *Action* description where it may be edited to be specific to the Risk being controlled.

Likewise, if an *Action Code* has an attached document or web site link, this information is copied to the *Risk Control* or *Action*.

You may nominate the effectiveness of any mitigation type by a percentage or level reduction for Likelihood, Consequence or Risk transfer.

Click *Select* to edit an *Action Code*.

Click the *New Action Code* button to add a new *Action Code*.

14.2. Action Frequency

You may set up action frequencies (apart from Risk review frequencies) and nominate the number of days or months between actions.

The default setting for action frequencies is *Monthly* notifications. The system will alert you every month with this setting.

To change monthly action frequencies, select *Edit* for the *Months* frequency desired (annually, six monthly, etc.) then select *Use Months* tick-box and click *Save* to confirm. With months selected, the system will alert you on the same day of the month, depending on the frequency selected.

Action Frequency	Days	Months	Use Months	
Annually	365	12	<input type="checkbox"/>	Edit
Monthly	30	1	<input type="checkbox"/>	Edit
Not Applicable	0	0	<input type="checkbox"/>	Edit
Quarterly	90	3	<input type="checkbox"/>	Edit
Six-Monthly	182	6	<input type="checkbox"/>	Edit
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add

[Print List](#)



Note: Application software prior to version 5.4.0.

The default setting for action frequencies was set to *Days* with *Monthly* notifications. The system alerted you every 30 days with this setting.

14.3. Assets

Select *Assets* from the *Reference Data* menu to add, change and delete records. If the reference data is being used on any Risk you will not be allowed to delete it.

ASSET

Asset Type:

Asset	Type	Location	Manager	Critical	Risks		
Accounts Payable	Financial			<input type="checkbox"/>	0	Select	Delete
Accounts Receivable	Financial			<input type="checkbox"/>	0	Select	Delete
Business Continuity	Business Operations			<input type="checkbox"/>	5	Select	Delete
Business Strategy	Business Operations			<input type="checkbox"/>	3	Select	Delete
Compliance/Governance	Compliance/Governance			<input type="checkbox"/>	0	Select	Delete
Employee Health	Employees/Workplace			<input type="checkbox"/>	1	Select	Delete
Employee Safety	Employees/Workplace			<input type="checkbox"/>	2	Select	Delete
Expenses	Financial			<input type="checkbox"/>	0	Select	Delete
Financial Investment	Financial			<input type="checkbox"/>	7	Select	Delete
IAS Compliance	Compliance/Governance			<input type="checkbox"/>	0	Select	Delete
Information Networks	Asset/Infrastructure			<input type="checkbox"/>	0	Select	Delete
Information Systems	Asset/Infrastructure			<input type="checkbox"/>	8	Select	Delete
Investors/Shareholders	Community and Public			<input type="checkbox"/>	1	Select	Delete
Liabilities	Legal			<input type="checkbox"/>	1	Select	Delete
OH&S	Employees/Workplace			<input type="checkbox"/>	0	Select	Delete

[Previous] Page 1 of 2 [Next]

[Print List](#) [Print grouped by Type](#) Show 15 rows per page [Change](#) [New Asset](#)

Assets may be real assets or intangible assets. They are the things that may be harmed if the Risk eventuates. They are not the hazards. For the hazards, refer to Risk Types and Risk Events below.

Asset Title:	Accounts Payable	Asset Type:	Financial
Location: ...		Asset Owner:	
Critical?	<input type="checkbox"/>	Escalate To:	<input type="text"/> Division
Asset Description:			
Business Objective:			
Current Phase:	<input type="text"/>	Due Date:	<input type="text"/>
At Risk (\$):	<input type="text"/>	Relative Value:	Medium
Relative Value Note:			
Asset ID:			
Date Last Inspected:	<input type="text"/>		
Physical Address:			
Network Address:			
Asset Custom 1:			
Asset Custom 2:			
Asset Custom 3:			

An Asset must have an Asset Type. Asset Types are often aligned exactly with the Consequence table descriptions.

The rest of the data items are optional and some are provided for very advanced reporting and analysis – they are not needed for basic Risk management. Only use the following data items as described:

- Use *Location* only when the asset is a physical asset. Do not use *Location* if the Asset is a general Asset, such as Employees, or an intangible asset, such as Revenue.
- Use Owner only when there is a single User responsible for the Asset.
- Use *Current Phase* and *Due Date* only when the Asset is a Project Phase (for example, Phase 1 through Phase 3).
- Use *At Risk*, *Relative Value* and *Relative Value Note* only after understanding Enterprise Rating.

Many Assets may be assigned a (monetary) value at Risk, but it is difficult to assign a monetary value to other areas at risk (e.g. patients, passengers, employees and children at risk). However, you may assign any of five *Relative Values* from *Very Low* to *Very High* against any Asset. The default is *Medium*.

When the system determines the Enterprise Rating of a Risk, it looks for the highest impact via *Potential Loss* or *Relative Value* combined with the Risk's Likelihood. The *Relative Value* may be included in many reports, and may be specifically selected in the Dashboard and Risk Matrix report.

Project Risks are normally coded under the project name listed in the *Initiative* column (and *Initiative* may be renamed to *Project* to be more specific).

However, projects have phases such as Design, Construction, Testing and Production. Some Risks apply to only one stage and do not need to be managed early on in the project. These Risks can be closed when that stage has passed. This can be documented by assigning a phase to an Asset, and the date the phase will start. At the moment there is no automation related to these two data items.

14.4. Asset Types

Select *Asset Types* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the Asset Type is being used on any Risk, you will not be allowed to delete it.

Asset Type	Risks	Assets		
Asset/Infrastructure	8	3	Edit	Del
Business Operations	14	4	Edit	Del
Community and Public	5	4	Edit	Del
Compliance/Governance	0	2	Edit	Del
Employees/Workplace	3	3	Edit	Del
Environment	0	0	Edit	Del
Financial	7	5	Edit	Del
Legal	1	1	Edit	Del
Political	0	1	Edit	Del
<input type="text"/>			Add	

[Print List](#) [Asset](#)

Asset Type is a higher level of classification for reporting purposes.

14.5. Departments

Select *Departments* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the Department is being used on any Risk you will not be allowed to delete it.

Department	Department Manager			
Across all Business Units		Edit	More	Del
Corporate		Edit	More	Del
Engineering		Edit	More	Del
Finance	Financial Systems Manager	Edit	More	Del
Human Resources		Edit	More	Del
Information Technology		Edit	More	Del
Internal Audit		Edit	More	Del
Manufacturing		Edit	More	Del
Occupational Health and Safety		Edit	More	Del
Office of the CEO		Edit	More	Del
Professional Services		Edit	More	Del
Program Office/Projects		Edit	More	Del
Research and Development		Edit	More	Del
Risk Management		Edit	More	Del
Sales and Marketing		Edit	More	Del
<input type="text"/>	<input type="text"/>	Add		

[Previous] Page 1 of 2 [Next]

[Print List](#) Show 15 rows per page [Change](#)

You can create an Objective for a Department by clicking on the *More* link text. The following form is displayed.

Description:	<input type="text"/>
Department Objectives:	<input type="text"/>
Department Custom 1:	<input type="text"/>
Department Custom 2:	<input type="text"/>
Department Custom 3:	<input type="text"/>
Allow this department to be viewed by all users:	<input type="checkbox"/>
Back To List	Edit



Note: A Department's Objective can be displayed in some reports. See "Reporting" on page 22 for more information.

14.6. Divisions

Select *Divisions* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the Division is being used on any Risk, you will not be allowed to delete it.

Division	Group	Division Manager			
Across all Divisions	All		Edit	More	Del
Corporate	All	Natalie FitzHugh	Edit	More	Del
Operational	All	Natalie FitzHugh	Edit	More	Del
Project	All	Natalie FitzHugh	Edit	More	Del

[Add](#)

[Print List](#)
[Division Groups](#)

Show rows per page [Change](#)

When editing Divisions you can also enter other information such as division objective. There are also three custom data items.

Description:

Division Objectives:

Division Custom 1:

Division Custom 2:

Division Custom 3:

Allow this division to be viewed by all users:

☐

[Back To List](#)
[Edit](#)

If a Division is configured so that it can be viewed by all Users, any Risk information for that Division can be viewed (but not edited) by all Users, regardless of Role Based Security.

14.7. Division Groups

Select *Division Groups* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the Division Group is being used on any Risk, you will not be allowed to delete it.

Division Group		
All	Edit	Del
Domestic	Edit	Del
International	Edit	Del

[Add](#)

[Print List](#)
[Divisions](#)

14.8. Exposure Periods

Select *Exposure Periods* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Exposure Period* is being used on any *Risk*, you will not be allowed to delete it.

Exposure Period		
Continuously	Edit	Del
Daily	Edit	Del
Frequently	Edit	Del
Infrequently	Edit	Del
Monthly	Edit	Del
Occasionally	Edit	Del
Quarterly	Edit	Del
Rarely	Edit	Del
Very Rarely	Edit	Del
Weekly	Edit	Del
<input type="text"/>		Add

[Previous] Page 1 of 2 [Next]

[Print List](#)

14.9. Function

Select *Function* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Function* is being used on any *Risk*, you will not be allowed to delete it.

Function	Function Manager	
Maintenance	Alison Heard	Edit Del
<input type="text"/>	<input type="text" value="v"/>	Add

Show rows per page [Change](#)

[Print List](#)

Enter the *Function* name and select the *Function Manager* from the drop-down list. Click *Add* to create the new *Function*.

14.10. History Types

Select *History Types* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *History Type* is being used on any *Risk*, you will not be allowed to delete it.

History Type		
Action Change	Edit	
Action Completed	Edit	
Action Created	Edit	
Action Item	Edit	Del
Action Progress	Edit	Del
Action Results	Edit	Del
Alert	Edit	
Approval	Edit	
Assumptions	Edit	Del
Cause Recorded	Edit	
<input type="text"/>		Add

[First] [Previous] Page 1 of 3 [Next] [Last]

[Print List](#)

14.11. Project

Select *Project* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Project* is being used on any Risk, you will not be allowed to delete it.

No Project records have been entered yet. Use the fields below to enter new records.

Project	Project Manager	WBS Code	Function	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Add

[Print List](#) Show rows per page [Change](#)

Enter the *Project* name, select the *Project Manager* from the drop-down list, enter a *Work Breakdown Structure Code* and select a *Function* from the drop-down list. Click *Add* to create the new *Project*.

14.12. Locations

Select *Locations* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Location* is being used on any Risk, you will not be allowed to delete it.

Location	Address	City	County	Postcode		
Across all Locations					Select	Delete
All Counties					Select	Delete
Branch Offices					Select	Delete
Head Office					Select	Delete

[Print List](#) (Report best printed in landscape.) Show rows per page [Change](#) [New Location](#)

14.13. Responsible Parties

Select *Responsible Parties* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Responsible Party* is being used on any Risk, you will not be allowed to delete it.

Responsible Party		
Contractor	Edit	Del
Electricity Supplier	Edit	Del
Federal Government	Edit	Del
Gas Supplier	Edit	Del
Insurance Broker	Edit	Del
Internal	Edit	Del
Internal - Contracts	Edit	Del
Internal - HR	Edit	Del
Internal - IT	Edit	Del
Internal - Risk Management	Edit	Del
<input type="text"/>		Add

[Previous] Page 1 of 2 [Next]

[Print List](#)

Responsible Party is used to configure an external party who is responsible for an Action or ongoing control.

14.14. Review Frequencies

Select *Review Frequencies* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Review Frequency* is being used on any Risk, you will not be allowed to delete it.

Review Frequency	Days		
4 Monthly	120	Edit	Del
6 Monthly	182	Edit	Del
Bi-Monthly	60	Edit	Del
Monthly	30	Edit	
Not Applicable	0	Edit	
Quarterly	90	Edit	
Yearly	365	Edit	
<input type="text"/>	<input type="text"/>	Add	
Print List			

Four review frequencies cannot be deleted. Do not alter these four frequencies directly in the database. Use this form to translate the name, but it do not alter their meaning or the number of days for these four because the logic in the software expects them to be Not Applicable = 0, Monthly=30, Quarterly=90, and Yearly=365 days.

If others are added, ensure the *Days* are configured. Common additions are 4-Monthly=122 and 6-Monthly=182.

It does not make sense to have a *Review Frequency* equal to or less than the *Risk Review Due Period* in System Settings, otherwise the Risk is always due or overdue.

Review Frequency does not relate to how often the Risk is monitored. It refers to how often the Risk Rating is reviewed.

14.15. Risk Events

Risk Events define the Risks which have been identified for your business. Once a Risk Event has been defined, it can be used to define new Risks and can be used to create Risk Templates.

Select *Manage*, then select *Reference Data* and select *Risk Events* from the menu. You can add or edit Risk Events. Only Risk Events which have not been used (indicated by 0 in the Risks column) can be deleted.

Risk Type: All

Event Context: All

Risk Event	Risk Type	Description	Willingness	Impact	Appetite Rating	Average Residual Rating	Average Target Rating	Risks		
Bridge Collapse	Technical Failure	Bridge Collapse	Unwilling	Major	Medium	Medium	Low	1	Select	Delete
Building Collapse	Technical Failure	Building Collapse				Medium	Medium	3	Select	Delete
Database Corruption	System Failure	Database Corruption						0	Select	Delete
Earthquake	Natural Hazard	Earthquake				Medium-High	Medium-High	2	Select	Delete
Failure of BCM Strategy	System Failure	Failure of BCM Strategy	Very Willing	Major	High			0	Select	Delete
Failure to Approve	Process Failure	Failure to Approve				Low	Low	2	Select	Delete
Failure to Sign Off	Process Failure	Failure to Sign Off						0	Select	Delete
Fire	Natural Hazard	Fire						0	Select	Delete
Flood	Natural Hazard	Flood						0	Select	Delete
Fraud	Criminal Act	Fraud				Medium	Medium	8	Select	Delete
Negligence	Human Failure	Negligence						0	Select	Delete
System ceases to operate	System Failure	System ceases to operate						0	Select	Delete
Theft	Criminal Act	Theft				Low	Low	1	Select	Delete
Tsunami	Natural Hazard	Tsunami						0	Select	Delete

Print List

Print grouped by Type

Show 15 rows per page

Change

New Risk Event

The Risk Event has a short title and a long description. To simplify the system, the Risk Event is a few words that combine the hazard with the possible event, such as:

- Bridge Collapse (the bridge is the hazard and collapse is the possible event).
- Database Corruption (the database is the hazard and corruption is the possible event).
- Fraud – subcontractor payments (fraud is the hazard and false subcontractor payments is the possible event).



Note: In the example above, the *Willingness*, *Impact*, *Appetite Rating*, *Average Residual Rating* and *Average Target Rating* columns are visible in the *Risk Events* page. These columns will not be visible if the *Risk Appetite* setting is not activated, see ["Options Tab" on page 37](#) for further information.

The screenshot shows a web form for creating a new Risk Event. The form is divided into several sections. The top section contains 'Name' and 'Type' fields, both of which are populated with 'Failure of BCM Strategy' and 'System Failure' respectively. Below this is a large 'Description' field. The middle section contains various rating and context fields, including 'Default Likelihood', 'Event Context', 'Short Name', 'Current Risk Capacity', 'Reporting Channels', 'Willingness', 'Impact', 'Risk Appetite', 'Correlation to Strategy', 'Correlation to Strategy Description', 'Default Consequence', 'Acceptable Risk Level', 'Standard', 'Custom Report Order', 'Ownership', 'Override Average Residual Rating', 'Average Residual Rating', 'Override Average Target Rating', and 'Average Target Rating'. The bottom section contains a 'Rationale' field. At the bottom of the form are buttons for 'Back To List', 'New Risk Event', and 'Edit'.

- **Name** – The name of the Risk Event which appears in the drop-down list of *Event Types* when creating a new Risk or when adding a new Risk Event to a Risk Template.
- **Type** – The Risk Type groups similar Risks together. For example, you might have a Risk Type of *Natural Hazard* which groups the Risk Events *Flood*, *Tsunami* and *Earthquake*. The Type must be associated with a Risk Event for high level reporting.
- **Description** – If required, enter a more detailed description of the Risk Event.
- **Default Likelihood** – If you define a Risk Event which has a *Likelihood* of occurring that is unlikely to vary across Projects or Divisions, then you can select a default value from the drop-down list. However, the Likelihood of a Risk often varies between Projects, Locations, and so on so this is rarely used.
- **Default Consequence** – If you define a Risk Event which has a *Consequence* of occurring that is unlikely to vary across Projects or Divisions, then you can select a default value from the drop-down list. However, the Consequence of a Risk often varies between Projects, Locations, and so on so this is rarely used.

- *Event Context* – Default values are Internal, External and Internal/External. The Event Context is displayed as the *Risk Group* on the Risk Search form. See ["Risk Events" on page 96](#) for more information on setting the Event Context for a *Risk Event*.
- *Acceptable Risk Level* – May be allocated an Acceptable Risk Level which is merely an indicator of Risk tolerance. It does not control anything but will cause a message *Risk level is not acceptable* if a Risk's residual Risk is higher than this setting, or *Acceptable risk level not set* if this value is not set.
- *Short Name* – A short name for more succinct labels in the *Chart Wizard*.
- *Standard* – If required, select the associated Standard from the drop-down list.
- *Current Risk Capacity* – Lets you select a descriptions from the drop-down list which has been configured in ["Risk Capacity" on page 102](#).
- *Custom Report Order* – Custom Report Order is used if clients prefer to use other reporting tools (e.g. Crystal Reports, Cognos) and want to control the sequence of reporting rather than alphabetic order.
- *Reporting Channels* – This is a "free-field" text area where you can enter information relevant to the Risk Event reporting channels.
- *Ownership* – Displays the risk ownership details, configured in the *Ownership and Dates* tab.
- *Willingness* – Lets you select one of the Willingness names from the drop-down list, see ["Willingness" on page 65](#) for further information.
- *Override Average Residual Rating* – With this selected you can override the Average Residual Rating for the Risk Event.
- *Impact* – Lets you select one of the descriptions from the drop-down list, see ["Impact" on page 66](#).
- *Average Residual Rating* – This drop-down list lets you choose a Residual Rating for the Risk Event.
- *Risk Appetite* – This is a "fixed field" that displays the Risk Appetite derived from the Willingness and Impact matrix, see ["Appetite Matrix" on page 66](#) for further details.
- *Override Average Target Rating* – With this check box selected you can override the Average Target Rating for the Risk Event. If the check box is not selected, the Average Target Rating can not be overridden.
- *Correlation to Strategy* – Lets you select one of the descriptions from the drop-down list that are configured in ["Correlation To Strategy" on page 102](#).
- *Average Target Rating* – The field displays the Average Target Rating for the Risk Event. You can change the Average Target Rating by selecting the Override Average Target Rating check box which will activate a drop-down menu to choose a different Average Target Rating.
- *Correlation to Strategy Description* – This is a "free-field" text area where you can enter a description of the Correlation to Strategy for the Risk Event.
- *Rationale* – This is a "free-field" text area where you can enter the Rationale for the Risk Event.
- *Edit* – When viewing a Risk Event, click the *Edit* button if you want to make changes to it.
- *Save* – After editing a Risk Event, click *Save* to save the changes you made and return to the Risk Event Viewer.
- *Cancel* – After editing a Risk Event, click *Cancel* to discard the changes you made and return to the Risk Event Viewer.
- *Back To List* – Selecting this button returns you to the Risk Event Viewer.
- *New Risk Event* – Selecting this button opens a blank Risk Event page, in Edit mode, to create a new Risk Event.

14.16. Other Classification

Risks can be assigned a *Classification*. The default *Classifications* are: *Business Continuity*, *Strategic*, *Operational* and *Opportunity*.

To edit an existing *Classification*, click the edit link text beside the *Classification*. You can then edit the name of the *Classification*.

To create a new *Classification*, enter the new *Classification* name in the text box and click the *Add* link text.

The *Classification* is displayed as *Class.* on the Risk Search form.

A Risk's *Classification* is set on the Risk form, on the *Context* tab, in the *Other Categories* section of the form.

14.17. Event Context

Select *Event Context* from the *Reference Data* menu to *Add*, *Edit* and *Delete* records. If the *Event Context* is being used on any Risk, you will not be allowed to delete it.

Event Context			
External		Edit	Del
Internal		Edit	Del
Internal/External		Edit	Del
<input type="text"/>			Add
Print List			

Risk Contexts (which may be named Risk Group in your system) are used in high level reporting, especially in the Risk List Report and Risk Action Report where Risk Context may be selected in the Sort Column or the Group By criteria.

14.18. Risk Types

Select *Risk Types* from the *Reference Data* menu to *Add*, *Edit* and *Delete* Risk Types. If the Risk Type is being used on any Risk you will not be allowed to delete it.

Risk Type	Short Name	Risks				L	C	
Criminal Act	Criminal Act	1 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
Human Failure	Human Failure	1 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
Malicious Act	Malicious Act	0 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
Natural Hazard	Natural Hazard	0 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
Process Failure	Process Failure	0 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
System Failure	System Failure	6 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
Technical Failure	Technical Failure	0 Events Factors	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Edit	Del	
<input type="text"/>								Add
Print List Risk Events								

A Risk Type is the higher level of classification for hazards and is used for reporting purposes. Each Risk Type will have a number of Risk Events.

The *L* column shows whether *Likelihood Factors* have been created.

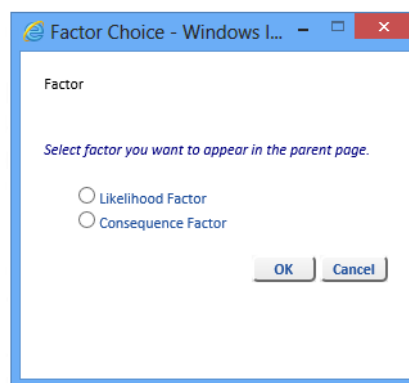
The *C* column shows whether *Consequence Factors* have been created.

14.18.1. Manually Create Likelihood And Consequence Factors

To create *Likelihood* and *Consequence* Factors manually, select the *Manage* tab, select *Reference Data* and select *Risk Types* from the menu.

Risk Type	Short Name	Risks		L	C	
Criminal Act	Criminal Act	1 Events Factors				Edit Del
Human Failure	Human Failure	1 Events Factors				Edit Del
Malicious Act	Malicious Act	0 Events Factors				Edit Del
Natural Hazard	Natural Hazard	0 Events Factors				Edit Del
Process Failure	Process Failure	0 Events Factors				Edit Del
System Failure	System Failure	6 Events Factors				Edit Del
Technical Failure	Technical Failure	0 Events Factors				Edit Del

Click the *Factors* link text next to the appropriate *Risk Type* (for example, *Criminal Act*) and select either *Likelihood Factor* or *Consequence Factor* (if you need to configure both Factors for the selected *Risk Type*, they need to be configured one at a time).



Factor

Select factor you want to appear in the parent page.

☐ Likelihood Factor
☐ Consequence Factor

OK Cancel

By default, there are no *Consequence* Factors configured.

Click the *Add Factor* button to configure the factors, for the selected Risk Type (Criminal Act in this example). Enter a name for the factor (Financial, in this example) and descriptive text for each of the ratings: *Very High*, *High*, *Medium*, *Low* and *Very Low*.

CONSEQUENCE FORMULA DETAIL ON RISK TYPE: CRIMINAL ACT

Factor	Very High (5)	High (4)	Medium (3)	Low (2)	Very Low (1)	
Financial	£1,000,000 loss	£500,000 loss	£100,000 loss	£50,000 loss	£10,000 loss	Edit Del

◀ Back To List

Add Factor

Repeat these steps to add as many other Factors as required.

Then repeat these steps for other Risk Types for which you want to create *Likelihood* and *Consequence* Factors.

14.19. Standards

Select *Standards* from the *Reference Data* menu to *Add a Standard*, *Edit* and *Delete* records. If the Standard is being used on any Risk you will not be allowed to delete it.

14.19.1. Add A Standard

Click the *Add a Standard* button to add a Standard document. Add a name for the Standard in the *Standard* field, a description, the name of the person issuing the Standard and then select a *Type* from the drop-down list. Click *Save* to save your changes, or *Cancel* to discard the changes.

14.19.2. Attach A Document To A Standard

Click on the name of the Standard. You are taken to the Document which is linked to the Standard. If no Document is linked to the Standard, you can attach a Document by clicking the *Attach Document* button. The Documents For Standards page is opened.

Click the *Browse* button to navigate to the required document. Click *Open*.

If required, enter a *Version*.

The *Created* date defaults to today. Click the calendar to select a different date.

Attached By defaults to the User who clicked the *Attach Document* button. You can change the name by selecting a different User from the drop-down list.

Enter the name of the *Author* and a *Security Class*, if required.

Select a date from the calendar for the *Revised* date, if required.

If required, enter a *Status*.

Click *Save* to save the document details or *Cancel* to discard the changes.

You are returned to the Documents For Standards page.

14.20. Timeframe

Timeframes are used on the Action *Ownership and Dates* tab.

There are four default Timeframes:

- *Existing*
- *Immediate*
- *Long-term*
- *Short-term*

These can be *Edited* or *Deleted*. However, When a Timeframe has been used, it cannot be deleted. More Timeframes can be created by clicking the *Add* link text.

14.21. Categories

Categories are used on the Risk Description tab and on the Action Description tab. To add a Category, type a Category name in the *Category Name* text box. Each Category name must be unique. Select an owner from the *Category Owner* drop-down list. Setting the *Category Owner* is optional. Click *Add* to add the Category to the list. These Categories can then be added to Risks and Actions.

CATEGORIES

Category Name	Category Owner		
Data Protection	None	Edit	Del
Financial Crime	None	Edit	Del
Information Security	None	Edit	Del
Knowledge Management	None	Edit	Del
Operational Processing	None	Edit	Del
Other	None	Edit	Del
People	None	Edit	Del
Regulatory Risk	None	Edit	Del

[Add](#)

[Print List](#)

Select *Edit* or *Delete* to edit or delete the selected Category. If the Category is being used on any Risk or Action, you will not be allowed to delete it.

14.22. Risk Capacity

Risk Capacity is a measure of the extent to which a strategy can withstand negative events without jeopardising the achievement of goals. From this page a user is able to input descriptions for the Risk Capacity, which can then be assigned to "[Risk Events](#)" on [page 96](#).

From the *Reference Data* menu, select *Risk Capacity* to add a risk capacity description.

RISK CAPACITY

No Risk Capacity records have been entered yet. Use the fields below to enter new records.

[Add](#)

[Print List](#)

Enter a name for the risk capacity and select *Add*. The name will be saved.

Click *Edit* to change the name or *Del* to remove it. To print all *Risk Capacity* data, select the *Print List* button.

14.23. Correlation To Strategy

Correlation to Strategy is a way of measuring the relationship between strategies and their dependencies. This page lets a user input *Correlation To Strategy* descriptions, which can then be assigned to "[Risk Events](#)" on [page 96](#).

From the *Reference Data* menu, select *Correlation To Strategy* to add a correlation to strategy description.

CORRELATION TO STRATEGY

No Correlation to Strategy records have been entered yet. Use the fields below to enter new records.

Name	
<input type="text"/>	Add

[Print List](#)

In the text field, enter a name for the correlation to strategy and select *Add*. The name will be saved.

Click *Edit* to change the name or *Del* to remove it. To print all the *Correlation To Strategy* data, select the *Print List* button.

15. Manage Risk Data

Select the *Manage* tab and then select *Risk Data* to open the *System Management* page. This page lists the tasks that are available to those personnel.

Select the *Manage* tab and then click *Risk Data*.

The screenshot shows the 'Risk Data' management interface. At the top, there are nine dropdown menus for filtering risks: Division, Department, Asset, Function, Project, Class, Risk Type, Event Type, Status, Location, Categories, and Owner. Below these filters, it indicates 'Number of Risks: 1' with a 'Refresh' button. A list of actions is provided, including: 'Change risks filtered above with status "Input" to "Open"', 'Activate recurring actions for risks filtered above', 'Recalculate risk values if risk matrix altered (applies to ALL risks, ignoring filter criteria above)', 'Change risks filtered above with status "Suspended" to "Open"', 'Change risks filtered above with status "Suspended" to "Cancelled"', 'Update Action Strategy field on Risk Record', 'Raise risks for expired exemptions', 'Set Financial Impact values to equivalent Consequence Table financial values', 'Generate Monthly Risk Data', and 'Convert Item IDs to Autogenerated IDs'. At the bottom, there is a section to 'Change risks filtered above with current status' with two dropdown menus and a 'Go' button.

The fields at the top of the page allow you to filter the Risks. The System Administrator can then select one of the options below, which will affect only the filtered Risks (with the exception of *Recalculate risk values if risk matrix altered*).

- *Change risks filtered above with status "Input" to "Open"* – change the status of the filtered Risks from *Input* to *Open*.
- *Activate recurring actions for risks filtered above* – the System Administrator manages activation of recurring actions. We suggest this is run monthly for all areas.
- *Recalculate risk values if risk matrix altered (applies to ALL risks, ignoring filter criteria above)* – updates the Risk matrices for all Risk (regardless of the filter selected) for the new Risk Matrix options selected on the *Change Risk Matrix* page (see ["Risk Matrix Options"](#) on page 5).
- *Change risks filtered above with status "Suspended" to "Open"* – change the status of the filtered Risks from *Suspended* to *Open*.
- *Change risks filtered above with status "Suspended" to "Cancelled"* – change the status of the filtered Risks from *Suspended* to *Cancelled*.
- *Update Action strategy field on Risk Record* – for all Active Actions associated with the Risks returned by the filter, selecting this option copies each Action's *Action Details* to the Risk's *Action Strategy* field (see *Action Strategy* in the *Risks* chapter of the *OpRiskControl Users' Guide* for more information about this field).
- *Raise risks for expired exemption* – a Risk can be created with a status of *Suspended* and, on the *Ownership and Dates* tab, you can then set a date the Risk should become active (that is, change from *Suspended* to *Open*). Selecting *Raise risks for expired exemption* checks for any *Suspended* Risks where the date has passed and changes the status to *Open*.
- *Set Financial Impact values to equivalent Consequence Table financial values* – this option takes the *Consequence Cutoff* value equivalent to the *Inherent/Assessed Consequence*

rating of the Risk(s) and populates the value in the *Financial Impact* field on the *Financial* tab of the Risk.

- *Generate Monthly Risk Data* – you need to generate monthly Risk data before you can view an up-to-date *Waterfall Chart*. Please refer to the *Charts* chapter of the OpRiskControl Users' Guide for more information on waterfall charts. When the Notification Manager is active, the *Notification Monitor* will get an email on the first day of each month as a reminder to run this job. If the Job Scheduler is active, this will be done automatically, but it is worth checking the Waterfall Chart some days into the month to confirm the job has been run automatically.
- *Convert Item IDs to Autogenerated IDs* – when the *Autogenerate Codes* option (on the *System* tab, select the *System Settings* option and then select the *General* tab) is changed from *cleared* to *selected*, click this option to change the manually created IDs to automatically generated IDs. The IDs are generated according to the values configured for *Set Risk IDs to start numbering from* and *Set Action IDs to start numbering from* which are found on the System Settings tab, on the *Setup* page. (See "[Setup Tab](#)" on page 38 for more information on these two options.) However, if a Risk was created with an Automatically generated ID which was later manually changed, this option renumbers with Risk with the original ID.
- *Change risks filtered above with current status* – from the first drop-down list, select the current status of the filtered Risks and then, from the second drop-down list, select the new Status for the filtered Risks. Click *Go* to change the filtered Risks with the selected current Status to the new Status.



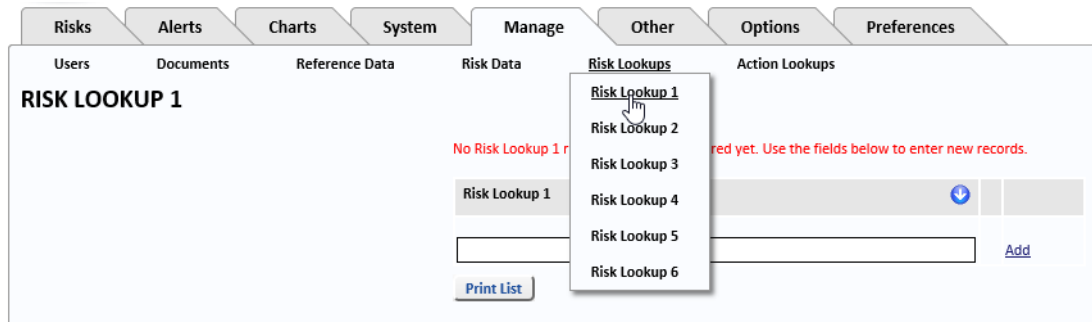
Note: If the Job Scheduler is installed and running, *Activate recurring actions for risks filtered above* and *Change risks filtered above with status "Suspended" to "Open"* will be run daily. The Job Scheduler also updates Key Risk Indicators daily.

16. Manage Lookups

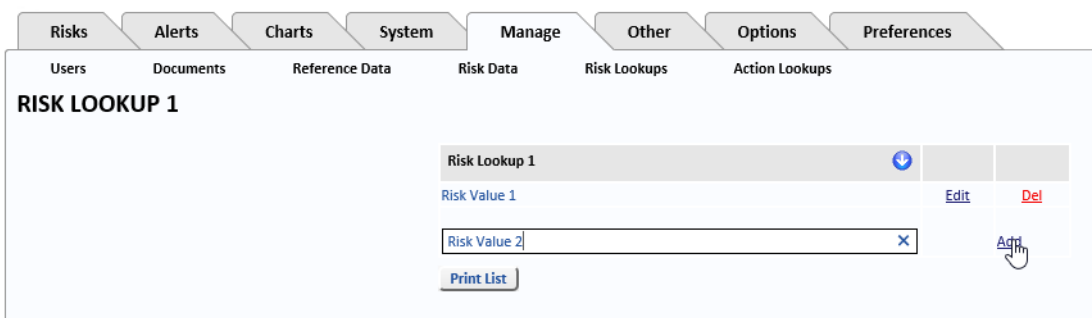
Lookups enable you to configure a list of values for each Lookup field. Users must then select a value from the drop-down list.

16.1. Risk Lookups

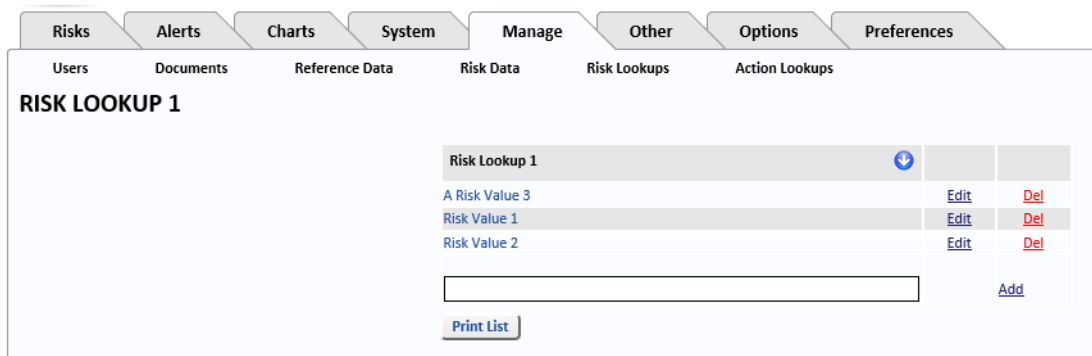
Select the *Manage* tab and then select *Risk Lookups* to display the list of Risk Lookups. Select the Risk Lookup you want to edit.



When you have selected a Lookup, you are shown the values which have already been added. To add a new value, enter the value in the text box and click *Add*.



Values are sorted alphabetically as they are added.



The values added here are available on the tabbed Risk form, on the *Custom Lookups* tab.



Note: If the *Custom Lookup* tab is not available when creating or viewing a Risk, check the appropriate options are set in both *Default Form Settings* and in *My Form Settings*.

The field names (Risk Lookup 1, Risk Lookup 2 etc.) can be renamed on the Language Translation page.



Note: Should you need to rename any fields once the system has gone live, please contact the Help desk for advice and guidance on how to do this. When renaming fields, keep a note of the original name and the new name so this documentation can still be used.

16.2. Action Lookups

Select the *Manage* tab and then select *Action Lookups* to display the list of Action Lookups. Select the Action Lookup you want to edit.

When you have selected a Lookup, you are shown the values which have already been added. To add a new value, enter the value in the text box and click *Add*.

Values are sorted alphabetically as they are added.

The screenshot shows a web interface with a top navigation bar containing tabs: Risks, Alerts, Charts, System, Manage, Other, Options, and Preferences. The 'Manage' tab is active, showing sub-tabs: Users, Documents, Reference Data, Risk Data, Risk Lookups, and Action Lookups. The 'ACTION LOOKUP 1' section is displayed, containing a table with the following data:

Action Lookup 1		
A Action Value 3	Edit	Del
Action Value 1	Edit	Del
Action Value 2	Edit	Del

Below the table is an input field and an [Add](#) button. At the bottom left is a [Print List](#) button.

The values added here are available on the *Lookup* tab of Actions associated with Risks created on the tabbed Risk form.



Note: If the *Lookup* tab is not available when creating or viewing an Action, check the appropriate options are set in both *Default Form Settings* and in *My Form Settings*.

The screenshot shows a web interface with two tabs: 'Ownership and Dates' and 'Lookup'. The 'Ownership and Dates' tab is active, showing the following fields:

- Recorded By: Alison Heard
- Date Recorded: 21/04/2015
- Action Owner: Alison Heard
- Timeframe:
- Due Date: 25/04/2015 (Overdue)
- Action Approved By: Alison Heard
- Date Approved: 21/04/2015
- Responsible Party: Internal - IT
- Percent Complete:
- Completed Date:

The 'Lookup' tab is also visible, showing the following fields:

- Action Status: Active
- Action ID: 1
- Action Code: Scheduled Maintenance
- Action Details: Nightly database backups
- Categories:
- Status Details:
- Test Result:
- Test Result History:
- Action Document:
- Action Hyperlink:
- Action Lookup 1: A Action Value 3, Action Value 1, Action Value 2
- Action Lookup 2:
- Action Lookup 3:
- Action Lookup 4:
- Action Lookup 5:
- Action Lookup 6:

At the bottom right are [Save](#) and [Cancel](#) buttons.

The field names (Action Lookup 1, Action Lookup 2 etc.) can be renamed on the Language Translation page.



Note: Should you need to rename any fields once the system has gone live, please contact the Help desk for advice and guidance on how to do this. When renaming fields, keep a note of the original name and the new name so this documentation can still be used.

17. Options

17.1. Processes

To view Processes which have been created in OpRiskControl, select the *Options* tab, select *Processes* then select the required Process from the menu. Alternatively, import a previously exported Process using the *Import a Process* option.



Note: Only Processes which were created in OpRiskControl and exported can be imported using this option.

17.2. Process Management

The *Process Management* option allows you to add a *Process*, with steps, to help Users as required. The Processes can then be accessed by clicking *Processes* on the *Options* tab.

Process Name: New Process Edit

Description:

Enter a *Process Name* and a *Description* and click *Save*.

Process Name: Save Cancel

Description:

To add Steps, click *Edit*.

Process Name: Risk Management Global Edit Export Save Cancel Delete

Description: How to log a Risk.

Sequence No.	Process Group Name
	<input type="text"/>

Add

Add a description to the *Process Group Name* and click *Add* and then click *Steps*.

No steps have been entered for this process group yet. Use the fields below to enter new records.

Seq. No.	Step Name	Description	Mandatory	Owner	Anniversary		
	Identify	First identify the Risk. Determine what the Risk affects, the location that could be affected	<input type="checkbox"/>				Add

[Back To List](#)

If required:

- select the *Mandatory* tick-box if the step is mandatory.
- select an *Owner* from the drop-down list.
- select an *Anniversary* month and day.

and then click *Add*.

Add more steps as required. A second step has been added to the above example. When a User clicks on *Processes* and selects *Risk Management*, the *Risk Management Process* just created is displayed.

17.2.1. Global Edit

The *Global Edit* button opens up a form which allows to make edit to all the Processes in Process Management.



Note: Make a backup of your database before using this facility.

In the first column, enter the old word (the word or phrase you want changed). In the second column, enter the new word (the word or phrase you want to see instead of the old word). Click *Go* beside the row you want to change. A tick indicates the changes have been made.

17.2.2. Export

A Process can be exported to create a backup. Click *Export* to export the process to a zip file. The default name is *Process-id_string.zip*, where *id_string* is a series of numbers. This zip file can be imported at a later date, see "[Processes](#)" on page 111 for more information about importing a Process.

17.2.3. Edit

To make changes to a Process, select the *Options* tab, then select *Process Management*. In the *Process Name* box, click on *New Process* to show the list of Processes and select the Process you want to edit. Click *Edit* to make changes to the selected Process or *Delete* to delete the selected Process.

To change the text in the *Process Group Name* box, select *Edit*. To change or add information to the steps, click *Steps* next to the Sequence you want to edit and then click *Edit* beside the Step you want to edit (or *Del* to delete the Step).

Click the *More* link text beside the Step and click *Edit* to change the extra information such as whether the Step is *Mandatory*, the *Anniversary* Month and day and to *Acknowledge* an Anniversary, if required. Click *Save* to save the changes. Click *Simple Mode* to hide the extra information.

17.3. Risk Templates

Select the *Options* tab, select *Risk Templates* and then select the required menu option.

Risk Templates can be created using any number of Risk Types selected from the Risk Types. Therefore, if there are a common set of Risks across a number of areas, you can create a Template of those Risks, and then automatically create those Risks for each project. It would then be the task of each project manager to discuss, rate and manage the Risks in their area using the pre-populated information.

Another example is that you could create a Risk Template for each Business Unit in a typical hospital or company, and then create the Risks (using the Risk Template) for each Business Unit. Then, all the Risk Manager needs to do is review their list of Risks, delete those that are not applicable, and add others that are.

17.3.1. Manage Templates

Select the *Options* tab, select *Risk Templates* and then select *Manage Templates* from the menu.

17.3.1.1. Create A New Template

Select *New Risk Template* from the drop-down list and then click *Edit*.

Enter a name for the new Risk Template in the text box and click *Save*.

RISK TEMPLATES

Template Name:

On the *Risk Templates* page, select a *Risk Type* and then a *Risk Event* from the drop-down lists, and click *Add* to add the selected Risk Event to the Risk Template. Continue adding Risk Events to the Risk Template until the Template is complete. Click the *Risk Event* name to open the Risk

Event. Risk Events can be edited by clicking the edit button. See ["Risk Events" on page 96](#) for more information about editing Risk Events.

The screenshot shows a web browser window titled "Risk Event - Windows Internet Explorer". The browser's address bar shows "Convert" and "Select". The main content area is a form for editing a Risk Event. The form has the following fields:

- Name:** Fraud
- Description:** Fraud
- Type:** Criminal Act
- Default likelihood:** (empty)
- Event Context:** (empty)
- Short Name:** Fraud
- Default Consequence:** (empty)
- Acceptable Risk Division:** (empty)
- Standard:** (empty)
- Custom Report Order:** 0

An **Edit** button is located at the bottom right of the form.

17.3.1.2. Edit An Existing Template

Select the Risk Template you want to edit from the drop-down list and then click *Edit*.

You can delete a Risk Event from the selected Risk Template by clicking the *Delete* link text beside the Risk Event.

To add new Risk Events, select a *Risk Type* and then a *Risk Event* from the drop-down lists, and click *Add* to add the selected Risk Event to the Risk Template. Continue adding Risk Events to the Risk Template until the Template is complete. Click the *Risk Event* name to open the Risk Event. Risk Events can be edited by clicking the edit button. See ["Standards" on page 101](#) for more information about editing Risk Events.

17.3.2. Create Risks From Templates

After you have a set of Risks as a Risk Template, you can create them in bulk for various contexts across the organisation.

Select the *Options* tab, select *Risk Templates* and then select *Create Risks From Templates* from the menu.

CREATE RISKS FROM TEMPLATES

Division	<input type="text"/>	Department	<input type="text"/>
Function	<input type="text"/>	Project	<input type="text"/>
Asset	<input type="text"/>	Location	<input type="text"/>
Contact	Alison Heard	Owner	<input type="text"/>
Review Frequency	Quarterly	Status	<input type="text"/>

Template Name: Corporate Risks

Risk Type	Risk Event	# Risks*	[Refresh]
Process Failure	Failure to approve	2	<input checked="" type="checkbox"/>
System Failure	System ceases to operate	10	<input checked="" type="checkbox"/>

* Indicates the number of risks in each Risk Event within the Division / Department / Asset / location context selected above.

Create Risks

Select the Risk Template you want to use to create the Risks from the *Template Name* drop-down list.

Risks can be created only when values have been provided for these fields:

- *Asset*
- *Location*

- *Owner*
- *Status*

Select the *Risks Events* for which you want to use to create a Risk (the *Risk Events* with a tick against them will be used to create Risks when you click the *Create Risks* button).

Click the *Create Risks* button.

Risks which were created using a Risk Template have the *Source* field set to *Template*.

18. Additional Information

18.1. Risk Locking

18.1.1. Risk Locks Enabled

Risks are not locked when they are edited unless the value for *EnableSpecialRecordLocking* in the *tblControl* (in the OpRiskControl database) is set to *True*.

When *EnableSpecialRecordLocking* is set to *True*, when a user edits a Risk, that Risk is locked, and no other users can edit that Risk until the specified number of seconds has passed. The locking period value is set by entering a value between 120 and 300 in the *RecordLockingTimeout* in the *tblControl*.

When the *RecordLockingTimeout* has expired, if another user attempts to edit the Risk, they will be allowed to make the edit and the *RecordLockingTimeout* will start for the new user.

When a user saves the Risk, or cancels the edit, within the *RecordLockingTimeout*, the lock on the Risk is removed.



Note: When either of these *tblControl* entries are edited, click *Refresh System Settings* on the *General* tab of the *System Settings* tab to make the changes take effect.

18.1.2. Risk Locks Disabled

When *EnableSpecialRecordLocking* is set to *False* or *NULL*, when a user edits a Risk, that Risk is not locked. This means, if another user edits the same Risk and saves the changes after the first person saves changes to the same Risk, the changes which were saved first are overwritten with the changes which were saved subsequently.

Index

A

Acceptable Risk Division **98**
Across All Divisions **25**
Action Codes **89**
Action Entry Form **16**
Action Frequency **90**
Action Lookups **108**
Action Type **74**
Activate Compliance Alerts **37**
Activate Control Effectiveness Matrix **37**
Activate Key Indicators **37**
Activate Processes **37**
Activate Replicate Button **37**
Activate Risk Stapling **37**
Activate Scenario Analysis **37**
Activate The Matrix Button **7**
Active Directory Import **85**
Add A Standard **101**
Admin Documents Page **87**
Alert If Existing Control Date Due **36**
Allow Asset Type **29**
Allow Classification **29**
Allow Custom Lookups
 Tabbed Action Form **28**
 Tabbed Risk Form **28**
Allow Custom Text Fields
 Tabbed Action Form **28**
 Tabbed Risk Form **28**
Allow Financial Tab **28**
Allow Other Rating Information **29**
Allow Residual Risk **29**
Allow Risk Type **29**
Allow Target Residual **29**
Also Copy Prefix To Changed Risks **22**
Alternate Grid Items **46**
Appetite Matrix **66**
Appetite Rating **67**
Appetite Rating Level **67**
Approval Divisions **74**
Ask To Include Department Objectives... **23**
Asset Types **91**
Assets **90**
Attach A Document To A Standard **101**
Autogenerate Codes **22**
Automated Notifications **30**
Automated Residual Risk Formula **36**
Automated Review Dates **36**
Automatic Action History **24**
Automatic Risk History **24**
Average Residual Rating **98**
Average Target Rating **98**

B

Bottom Left **22**

Buttons (Change Font And Colours) **47**

C

Categories

Reference Data **102**

Change Matrix **6, 70**

Change Matrix Button **7**

Change Risks Filtered Above With Current Status **106**

Class **99**

Classification **99**

Consequence **61**

Consequence Factor Setup **62**

Consequence Labels **10**

Consequences On Left Of Matrix **22**

Control Effectiveness **37, 69**

Convert Item IDs To Autogenerated IDs **106**

Correlation to Strategy **98, 102**

Correlation to Strategy Description **98**

Create Risks From Templates **114**

Culture **21**

Current Risk Capacity **98**

Custom Forms **17, 27**

Custom Report Number **98**

D

Date Due **36**

Default Action Reduction **35**

Default Consequence **97**

Default Form Settings **14**

Default Likelihood **97**

Default Status For New Risk **27**

Departments **92**

Description **97**

Design Effectiveness **37**

Display Home Tab **39**

Division Groups **93**

Divisions **93**

Due Date **36**

E

Edit Process **113**

Enterprise Rating **68**

Event Context **98, 99**

Existing Control

Overdue Existing Control May Re-assert Risk **36**

Export **112**

Exposure Periods **94**

F

Footer **46**

Function **94**

G

Generate Monthly Risk Data **106**
Global Edit **112**
Global Translator **72**
Globally Change
 Action **84**
 Risk **83**
Google Links **22**
Grid Column Headers **44**
Grid Items **45**

H

Hide Logo **22**
History Location **24**
History Types **94**
Home Page
 Select Layout **38**
Home Tab
 Display **39**

I

Impact **66, 98**
Implementation Effectiveness **37**
Import Logo **76**
Imported **79**
Incident Logging **38**
Include Risk List Report In HTML Format **22**
Inverted **23**

K

Key Control Indicator Status Type **36**
Key Indicator Notifications **34**
Key Risk Indicator Status Type **36**

L

Likelihood **61**
Likelihood On Left Of Matrix **22**
Likelihood Rating Conversion **69**
Limit Risk Access By Asset **25**
Limit Risk Access By Department **25**
Limit Risk Access By Division **25**
 Example **57**
Limit Risk Access By Location **25**
Limit User List By Division **26, 56**
Localisation **21**
Locations **95**
Lookups
 Manage **107**

M

Manage Content **75**
Manage Functions (e.g. Sub-Department) **29**
Manage Links **75**

Manage Projects **29**
Manage Tab
 Action Lookups **108**
 Documents **87**
 Reference Data **89**
 Risk Data **105**
 Risk Lookups **107**
 Users **79**
Manage Templates **113**
Menu Ribbons And Sub-Menu Items **40**
Menu Tabs **39**
Message **21**
More **113**
My Form Settings **13**

N

Name **97**
Notification Manager **30**
Notification Monitor **30**

O

Optional History **24**
Options Tab
 Risk Templates **113**
Organisation **21**
Other Classification **99**
Other Parties **95**
Overdue Existing Control May Re-assert Risk **36**
Override Average Residual Rating **98**
Override Average Target Rating **98**
Ownership **98**

P

Page Banner **44**
Page Headers **44**
Panel Content **42**
Panel Headers And Borders **41**
Panel Tabs **42**
Permission List **51**
Prefix **22**
Print List
 Users And Contacts **80**
Process Management **111**
Processes **111**
Projects **95**

R

Rating **65**
Rating Descriptions **10**
Rating Score **36**
Rationale **98**
Reassign Risks **83**
Recurring Action Reset (Days) **34**

- Refresh System Settings **47**
- Rename Consequence Labels **10**
- Reporting Channels **98**
- Reset All Search Criteria To Use "My..." Whenever Applicable **26**
- Responsible Parties **95**
- Restore Default **14**
- Restore Saved Website Appearance **47**
- Retained Risk Formula Based On **36**
- Review Frequencies **96**
- Risk Appetite **37, 98**
- Risk Capacity **102**
- Risk Locking **117**
- Risk Lookups **107**
 - Manage **107**
- Risk Status **73**
- Risk Types **99**
- Row Level Security **56**
 - Example **57**
 - Troubleshooting **59**

S

- Save Website Appearance **47**
- Set Action IDs To Start Numbering From **39**
- Set Risk IDs To Start Numbering From **39**
- Setup Compliance **33**
- Setup Deactivations **33**
- Short Name **98**
- Show Additional Enterprise Structure **27**
- Show Reports In New Window **22**
- Show Risk Matrix **22**
- Standard **98**
- Standards **101**
- Structure Filter **73**
- System Content **75**
- System Management **105**

T

- Tabbed Forms **27**
- Timeframe **101**
- Title **21, 22**
- Top Right **22**
- Triage **5**
- Type **97**

U

- Use Division Name In Risk Management Report Footer **23**
- Use Division Name In Risk Management Report Title **23**
- User Details **82**
- User Groups **85**
 - Add A User **84**
 - Create **85**
- User Import **85**
- User Roles Tab **54**
- Users And Contacts **79**

W

Welcome **1**

Welcome Message **21**

Willingness **65, 98**

Workflow Forms **27**



www.mitratesch.com

5001 Plaza on the Lake, Suite 111, Austin, TX 78746
Tel: US (512) 382-7322. Email: support@mitratesch.com

6575 West Loop South, 3rd Floor, Bellaire, TX 77401
Tel: US (888) 272-4699

460 Norristown Road, 3rd Floor, Blue Bell, PA 19422
Tel: US (610) 729-1100

430 Bath Road, Slough, Berkshire, SL1 6BB
Tel: UK +44 (0)1628 600900

1 Kingdom Street, Paddington, London, W2 6BL, UK

432 St. Kilda Road, Melbourne, Victoria 3004
Tel: Australia +61 (0)3 9521 7077

Copyright © 2004 - 2017 Mitratesch Holdings, Inc. All rights reserved.
PolicyHub is a registered trademark of Mitratesch Holdings, Inc.
All other trademarks acknowledged.