Administration Manual

GuardianERM Administration Manual

*** * * IMPORTANT NOTE * * ***

Information contained in this administration manual is propriety information that is the intellectual property of InConsult Pty Ltd.
All GuardianERM.Net users must comply with the license terms and conditions available from your GuardianERM.Net Co-ordinator.

* * * * * * * *

GuardianERM.Net Administration Manual

Produced by
InConsult Pty Ltd

ACN 100 759 984

L3, 66 King Street,
Sydney NSW 2000

PO Box R653
Royal Exchange NSW 1225

Ph: (02) 9241 1344
www.inconsult.com.au

GuardianERM Administration Manual

Table of Contents

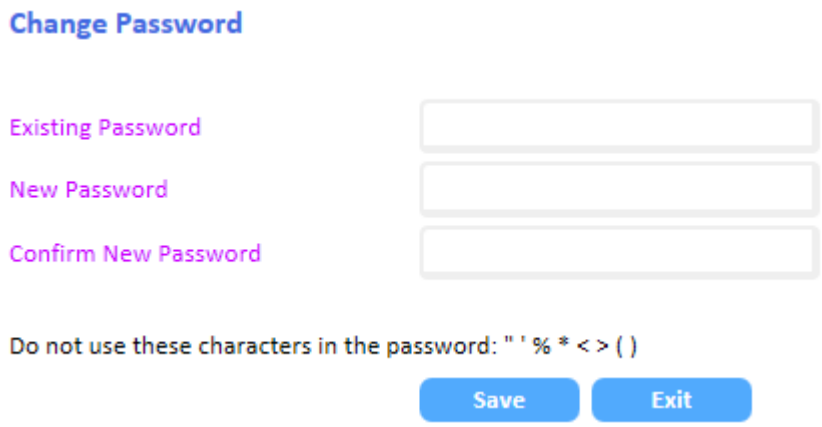
System Administration

The system administration functions are accessible by the system administrators only. A system administrator is one whose user name begins with Admin (e.g. AdminJohn, Admin123).

Change Password

You can change your password anytime by clicking on your User Name (Administrator) on the Main Menu:

Enter your existing password and then the new password. Enter the new password again to confirm. A password must be at least 5 alpha-numeric characters in length and cannot contain some characters as specified. Your system administrator may set certain password rules that must be complied with when entering a password.

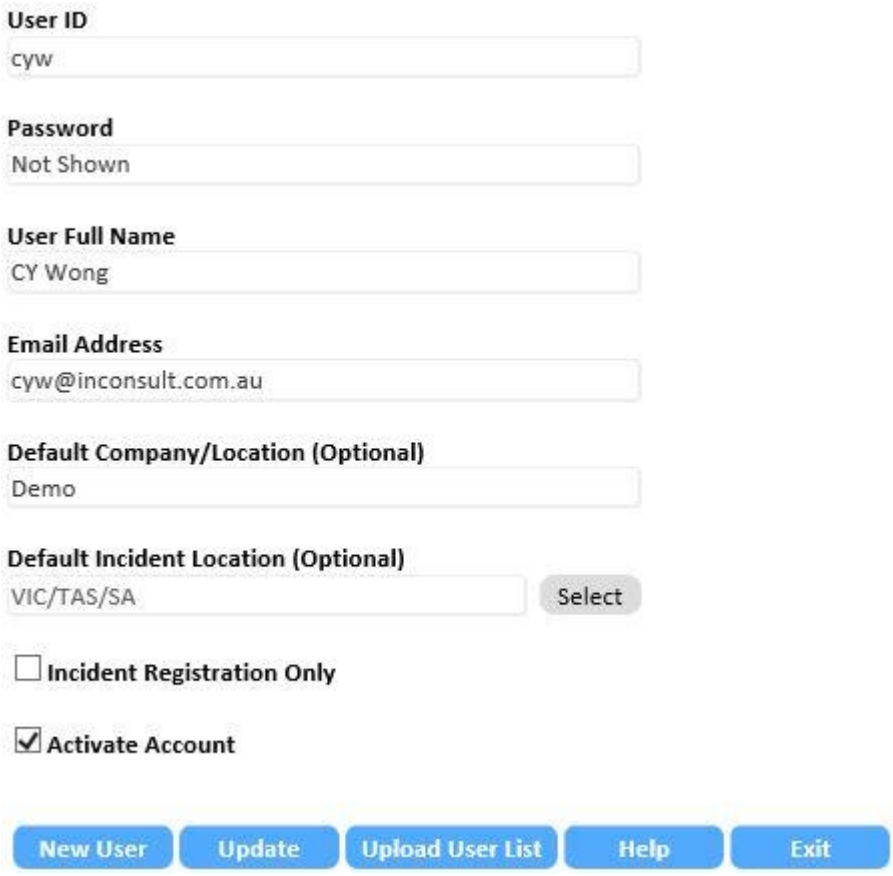


Click the Save button to save your new password. Your new password will be active next time you log in.

User Management

This function is used to create new users, deactivate existing users and reset a user's password.

To create a new user, click the New User button:



Enter the user ID (no space and no apostrophe symbol allowed) and a password for the user (minimum 5 characters). You may also enter the optional Email Address and Location fields. Tick the Activate Account box and click Update. The initial password is set to be expired already and if the system password rules are enforced, the user must change the password upon login.

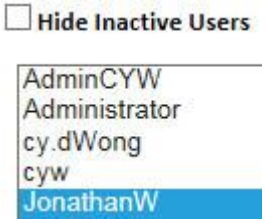
The User Full Name and Email Address fields are compulsory.

The Location field can be used to set the default company for the user if there are more than one company set up in the system. Otherwise, it is for identification purpose only. See note below.

If you want the system to automatically attach a default organisation unit to a new incident created by the user, click the Select button next to the Default Incident Location field and select an organisation unit from the pop-up organisation tree. Click Set Org Unit to attach or click Remove Org Unit to detach.

If the user is only allowed to register incidents with no authority to do anything else, tick the Incident Registration Only box. Users with this access level will not be shown on the User Access Control screen and hence cannot be granted with any additional access privilege.

To deactivate an existing user, select the user from the list:



Remove the tick from the Activate Account box by clicking it and click the Update button.

To change a user password, select the user from the list, enter a new password for the user and click the Update button.

Note: If you have set up multiple companies in your system, enter the name of company that you most frequently use in the Location field and the system will default to this company for the user whenever there is a dropdown list to select a company. Different users can have a different default company each.

Upload User List

When setting up the system for the first time, you may create users by uploading a list of users instead of creating them one by one. This is particularly useful when you have a large number of users and the data is available in an electronic format like Excel.

The User List must be an ASCII text file with data fields separated by commas without any header or footer rows. The fields must be in the following order:

User ID - maximum length 50 characters. No apostrophe allowed.

Password - minimum 5 alpha-numeric characters and is case sensitive.

Location (Optional) - maximum 100 characters.

Email Address - maximum 50 characters.

User Name - full name of user, maximum 50 characters.

Is the user an Incident Registration Only user? - Use 1 if Yes or 0 if no.

Note: If you leave an optional field blank, you must still put in the comma. Do not put a full stop (or anything) at the end of the line.

For example:

cyw, pasSwoRd, Head Office, cyw@inconsult.com.au, CY Wong, 0

cyw, pasSwoRD,, cyw@inconsult.com.au, CY Wong,1

Note: The data in the text file must be validated by the Administrator first as GuardianERM.net does not validate the data. The system will throw an error and the upload aborted if a user name is duplicated, a user field is blank or symbols that cannot be processed are encountered in the file.

GuardianERM Administration Manual

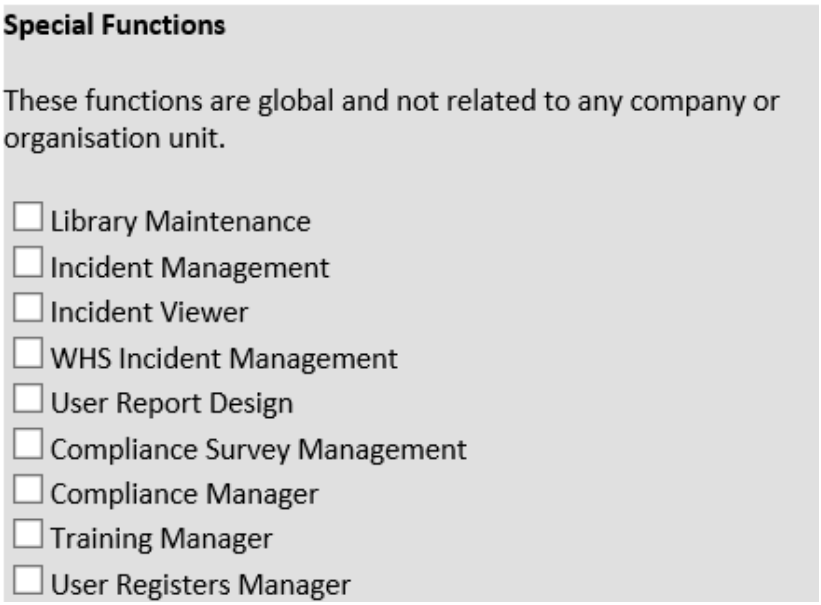
User Access Control

When a user is first created, by default the user has no access to any resource in the system. To grant access to the user, use the User Access Control function.

Select a company and then a user from the lists:

The selected company's structure as set up in GuardianERM.Net will be displayed:

To grant the user access to an organisation unit, click the organisation unit from the list (do NOT click the tick box) and tick the appropriate Access Level boxes:



Access Level	Allowed Functions
Organisation Read	Read access to the selected organisation unit's risk, control and audit details, generates reports, view audit programs and view incidents for the organisation unit.
Organisation Write	Allows creation and modifications (write access) to the organisation unit's risk and control details, create and modify incidents for the organisation unit.
Audit Write	Create and modify audit procedures in the Risk Evaluation module. Prepare, plan and execute audit programs.
Audit Sign-Off	Audit Write access plus finalise completed audit programs and create and modify auditor details in the Audit Planning module.
Special Functions These functions are applied globally regardless of company or organisation unit.	
Library Maintenance	Create and modify data stored in the library.
Incident Management	View and modify all incidents recorded in the system. If a user does not have this access, the user can only view or access incidents created by the user or if the incident is attached to an organisation unit where the user has Organisation Write access.
Incident Viewer	View all incidents recorded in the system for the selected company but cannot modify any data. Read Access to the Company (highest) level organisation unit must be granted to this type of user. This authority is mutually exclusive with the Incident Management and WHS Incident Management authorities..
WHS Incident Management	View and modify all incidents with WHS as the primary category. This authority is mutually exclusive with Incident

	Management and Incident Viewer authorities.
User Report Design	Allows the user to create and modify user report definitions.
Compliance Survey Management	Allows the user to manage the Compliance Survey functions.
Compliance Manager	Allows the user to add or modify compliance data. Users without this authority can still complete compliance items.
Training Manager	Allows the user to access all training records.
User Registers Manager	Create user registers and have access to all user registers.

Once the Access Level is applied the relevant tick boxes will be ticked by the system.

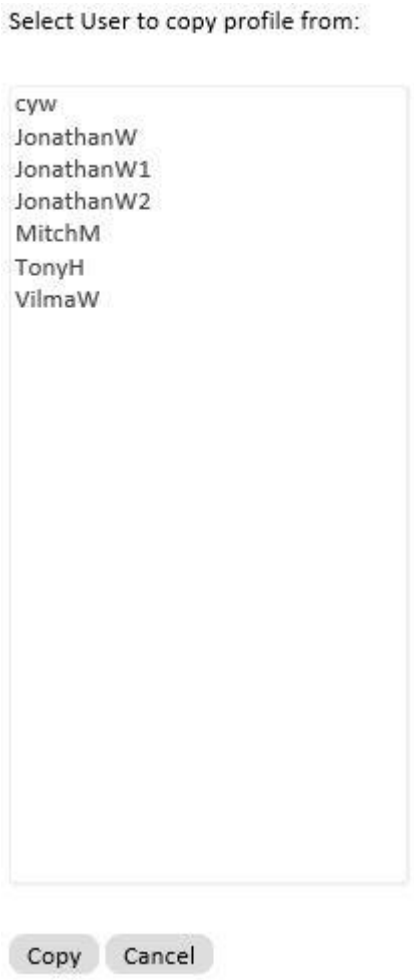
Note: Ticking and un-ticking the organisation boxes manually does not affect the user's access.

If an organisation unit has children units and the same access level is to be applied to all children units, click the Children to Inherit Access button. You **must** save the access level for the organisation unit before clicking the Children to Inherit Access button.

To change the access level of any organisation unit, click the organisation unit (not the tick box), change the access level and click the Save button.

If multiple companies are set up in the system and a user is allowed to access more than one company, the access level for the user must be set for each company individually.

If you want to set a user's profile based on another user's profile, select the user whose profile you want to set and click the Copy Profile button.



Select the user profile you want to copy from and click the Copy button.

System Parameters

The system parameters are constant values used by the system. As these parameters affect the proper functioning of the system, please contact InConsult before making any changes.

Risk Rating Configuration

GuardianERM.Net allows an installation to change its global risk rating configuration. The configuration is global and affects all risks in the installation.

Risk Heat Map Configuration

The risk levels in the Risk Heat Map can be configured to suit the organisation's reporting requirements.

When a risk is evaluated, GuardianERM.Net produces a risk rating according to the Consequence and Likelihood selected. A residual risk and targeted residual risk are also calculated after applying the effectiveness of the implemented and proposed/agreed controls.

The risk rating is in a five-point scale (i.e. from 1 to 5). There is actually a sixth level which is Negligible when the risk rating falls below 1.

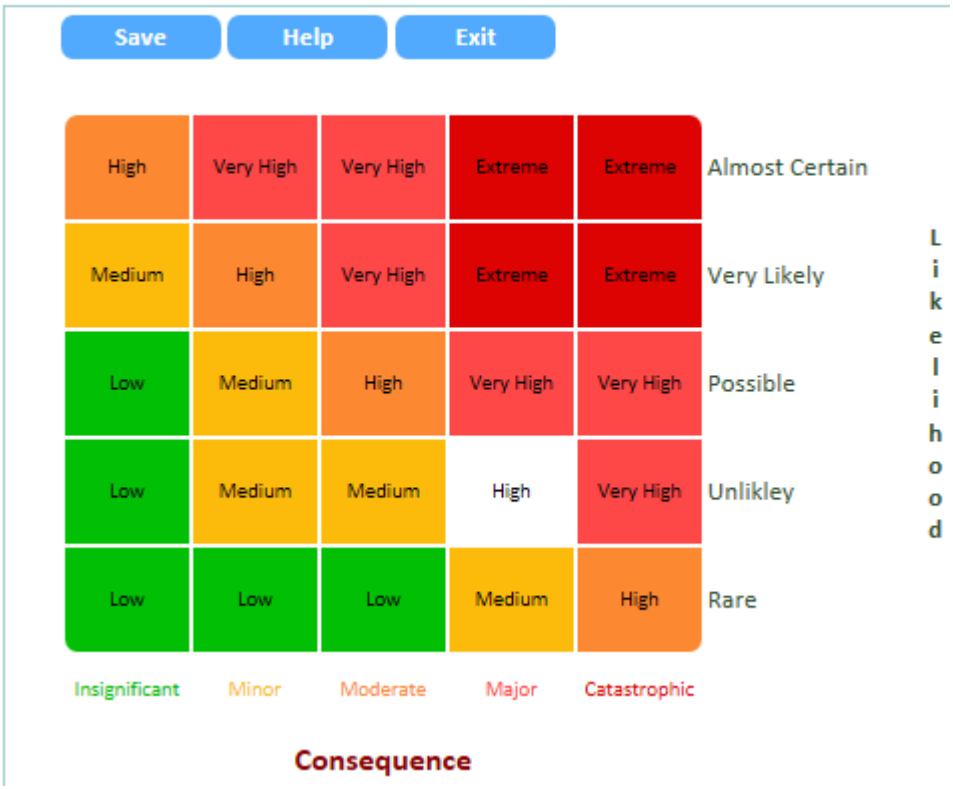
There are two things you can configure here:

1. The risk rating scale, that is, the level that you consider high risk or low risk.
2. The definition or description of the risk level.

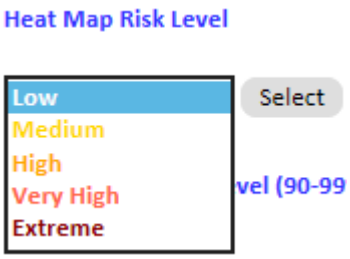
Risk Rating Scale:

This risk heat map is displayed with the current configuration. If this is the first time the risk rating is configured, it will display the default values. To change the risk rating scale, select a cell you want to change the risk level (the cell will turn white in colour):

Risk Heat Map Configuration



Select a risk level from the Heat Map Risk Level dropdown list and click the Select button.



The risk level of selected cell on the risk heat map will be changed.

When all the cells have been configured, click the Save button.

Maximum Control Level

In risk evaluation, where there is more than one control attached to a risk, the system will aggregate the effectiveness of the controls to arrive at the residual risk. When the effective control is over a certain threshold (default 90%), the system will consider the residual risk to be negligible, meaning there is no need to further improve the controls to reduce the inherent risk. This threshold can be configured by entering a number between 90 and 99%.

Maximum Control Level (90-99%) 95 %

Risk Level Definition

The Risk Level Definition table shows the long and short (up to 4 characters) descriptions of each risk level:

Risk Level Definition

Risk Level	Long Description	Short Description
<1	Negligible	Neg
1	Low	Low
2	Medium	Med
3	High	High
4	Very High	V Hi
5	Extreme	Ext

To change any of the description, click the cell and make the change.

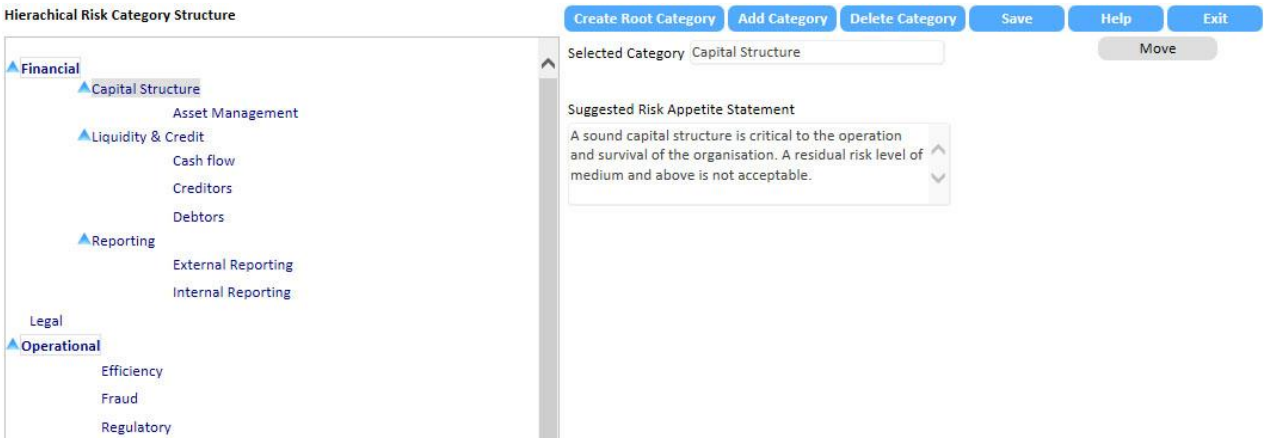
When all changes have been made, click the Save button.

Note: Once the data is saved, the heat map and the dropdown list will reflect the changes instantly. GuardianERM.Net will also re-calculate all the risks in the system to reflect the changes. It is highly recommended that no user is updating the system while this function is being performed.

Risk Category Maintenance

GuardianERM.net supports a three-level hierarchical risk category structure in the Risk Evaluation module. Its use is optional.

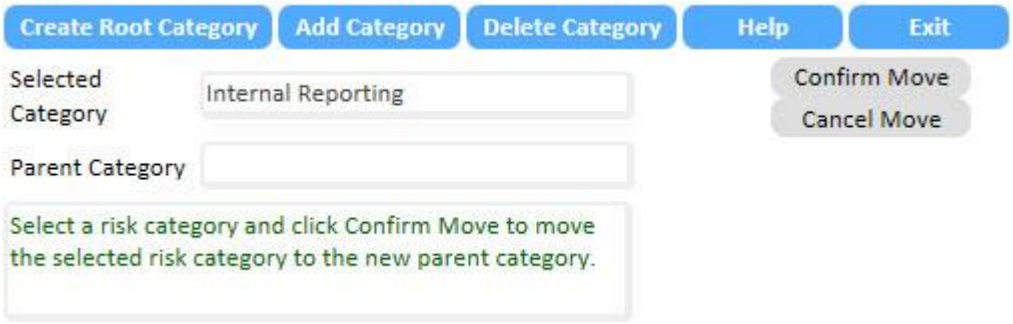
At a minimum, top level risk categories (root categories) must be set up.
To create a top level risk category, click the Create Root Category button and enter the risk category in the text box below. Click the OK button when finished.



To add a risk category underneath an existing category, select the category and click the Add Category button.

You can optionally add a Suggested Risk Appetite Statement to a category. Select a Category, enter the suggested risk appetite statement and click the Save button.

To move a category to another parent category, select the category to be moved and click the Move button.



Then select the new parent category and click the Confirm Move button. Note that the Risk Category hierarchical tree will turn red in the Move mode.

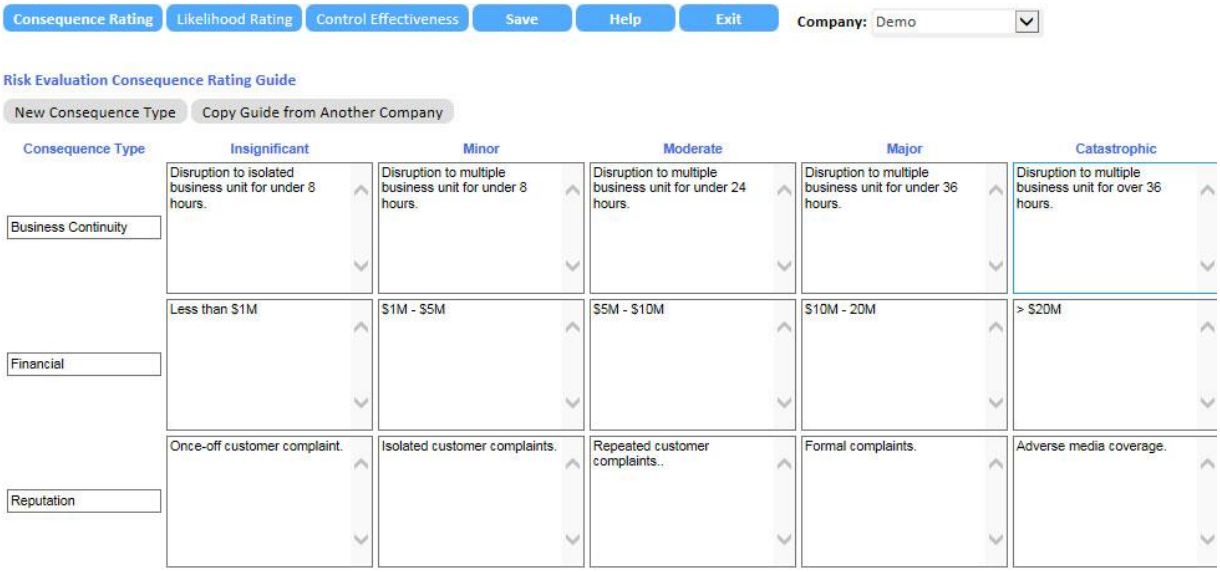
To delete a risk category (and its children categories, if any), select the category and click the delete button. Note that a risk category that has been used in the Risk Evaluation module cannot be deleted.

Risk Rating Guide

A risk rating guide is a table showing the organisation's definition of the various consequence and likelihood categories. A different set of rating guide can be prepared for each company within the organisation (if multiple companies are set up).

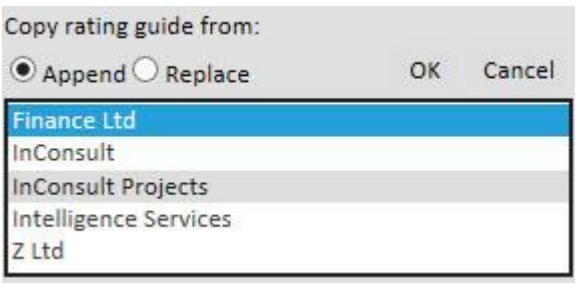
To prepare or modify a risk rating guide, select Risk Rating Guide from the Administration Main Menu.

Select the company the rating guide relates to using the dropdown list and then select the Consequence, Likelihood or Control Effectiveness Rating Guide by clicking the respective button at the top of the screen.



To add a new consequence type, click the New Consequence Type button and enter a name for the consequence type and click OK. Enter descriptions for each risk level and click Save.

You may copy the rating guide from another company by clicking the Copy Guide from Another Company button:



Select the company that has the rating guide you would like to copy to the currently-selected company. The copy function will only copy the rating guide you are currently viewing. If you are viewing the Likelihood Rating Guide, then only the Likelihood Rating Guide will be copied. You may select whether you want to append the rating guide to the current one or replace the current guide with the one from the other company. If you select Replace, then all existing data related to the currently selected rating guide will be erased. Click OK to make the copy.
The Likelihood and Control Effectiveness Rating Guides are prepared in the same way.

Note: Be careful when changing the rating guides as there may have been risks rated according to the existing definitions. If a definition is changed or new ones added, all existing risks should be re-evaluated to ensure consistency.

Workflow Settings

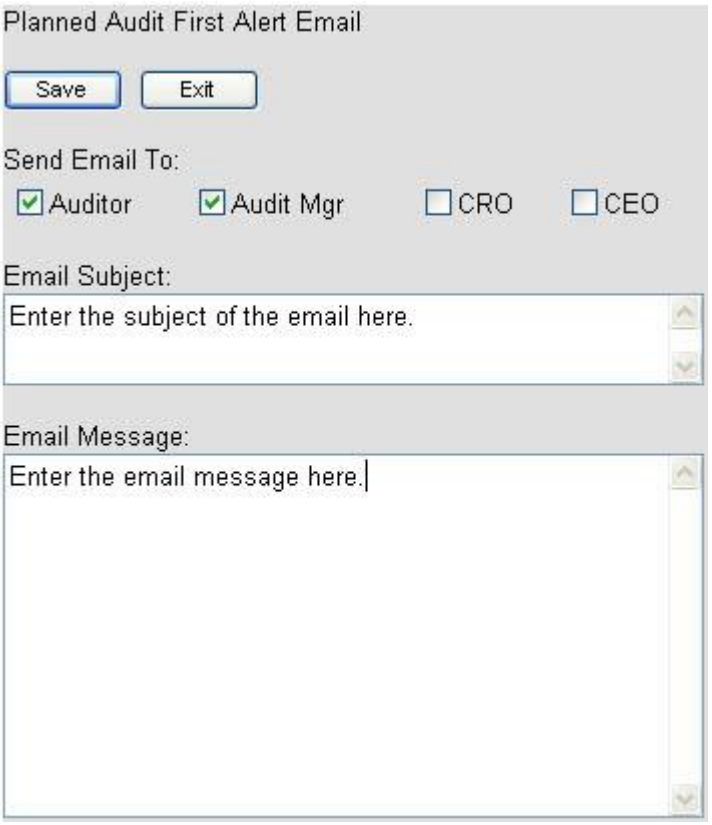
This function is used to configure the optional workflow module to automatically reset the Risk and Control Review and to send reminder emails for action items. Select a company to configure from the dropdown list.

Item	Function
Scheduled Audit Alert	Send emails to selected recipients for audit programs that are planned in the system.
Control Action Plan Alert	Send emails to selected recipients for control action plans entered in the Risk and Control Evaluation module.
Audit Resolution Alert	Send emails to selected recipients for resolutions recorded in audit programs.
Incident Treatment Alert	Send emails to selected recipients for treatments entered in the Incident Management module.
Compliance Alert	Send emails to selected recipients for compliance items recorded in the Compliance Management module.
Risk and Control Review	Send emails to selected recipients for outstanding risk and control reviews.
Risk and Control Review Tick Boxes Reset	Select the frequency of resetting the Risk and Control Review tick boxes and send emails to selected recipients advising them of the reset.
Validate Email Address	Validates all email addresses entered into system and sends an email to the system administrator reporting missing email addresses and possible incorrect email addresses.
Daily Email Confirmation	Automatically sends an email to the system administrator daily confirming that the workflow service is functioning properly.

To turn on or off a function, click the On or Off button:

Select the timeframe and whether it is before or after the due date recorded in the system for the item. If the timeframe is blank, the email will not be sent. You may configure up to 3 alerts for each item in the system.

To configure the email, click the Email Configuration button  .



Select the email recipients and enter the email subject and message. Click Save to save the data entered.

Email Recipient	**Source of Data**
Auditor	Email address of auditor-in-charge in the Audit Planning module.
Audit Manager	Email address of audit manager in the Audit Planning module.
Execution Officer	Email address of the execution officer in the Compliance Management module.
Organisation Unit Manager	Email address of organisation unit owner in the Organisation Unit Library.
Risk Manager	Email address of organisation unit risk manager in the Organisation Unit Library.
CRO	Email address of the risk manager of the company level organisation unit (top level of each company) in the Organisation Unit Library.
CEO	Email address of the owner of the company level organisation unit (top level of each company) in the Organisation Unit Library.

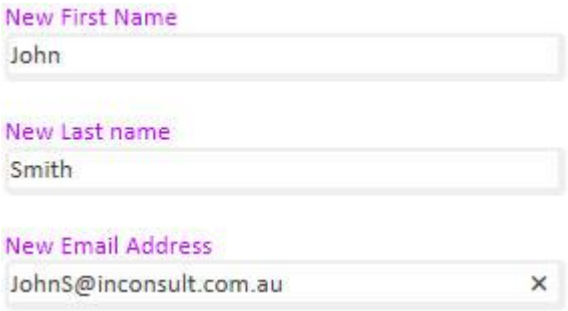
Change User Globally

This function is used to change an existing user's name and email address to new ones. The names will be changed in the organisation unit owner and risk manager names and their email addresses, the risk owner, the control owner and control executed by name and the compliance task executed by name and email fields. This can be useful when a staff member is replaced by another.

This change is not reversible so use it with care.

To change a user, select the user from the list.

Enter the first name, last name and email address of the person to replace the selected one and click the Replace button.



Attestation Settings

The Attestation Settings must be configured before the Attestation function can be used. The Attestation Settings is an administration function and can only be accessed by an Administrator using the Administration Module.

Setting up the Attestation Settings is a two-step process:

1. Create (or modify) attestation statements.
2. Link the attestation statements to organisation units.

You may also create Attestation Groups with selected attestation statements so you can apply them to various operations in your organisation.

Create (or modify) Attestation Statements:

Click the Attestation Statement button at the top of the screen.

The Attestation Statements screen will be displayed:

New Statement

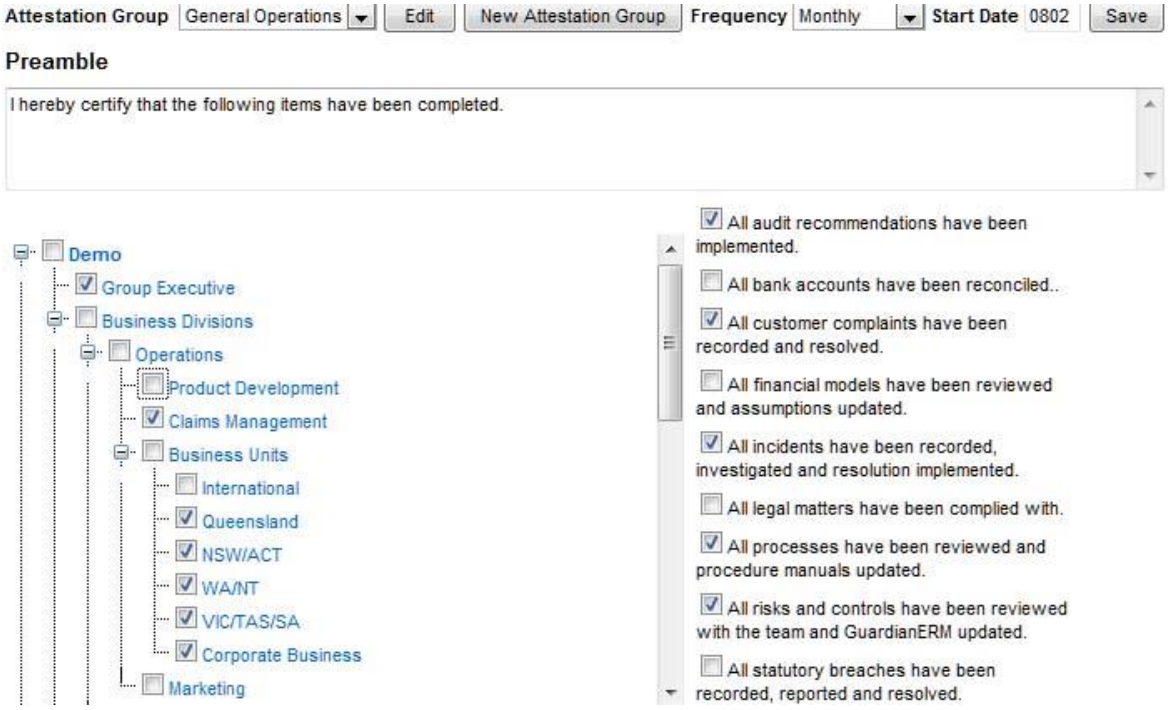
	ID	Attestation Statement	Active
Select	1	All risks and controls have been reviewed with the team and GuardianERM updated.	Yes
Select	2	All financial models have been reviewed and assumptions updated.	Yes
Select	3	All bank accounts have been reconciled..	Yes
Select	4	All sub-ledgers have been reconciled to the general ledger.	Yes
Select	5	All incidents have been recorded, investigated and resolution implemented.	Yes
Select	6	All audit recommendations have been implemented.	Yes
Select	7	All legal matters have been complied with.	Yes
Select	8	All customer complaints have been recorded and resolved.	Yes
Select	9	All statutory breaches have been recorded, reported and resolved.	Yes
Select	10	All processes have been reviewed and procedure manuals updated.	Yes

All existing statements (if any) will be listed. To modify a statement, click the Select link and type in the attestation statement. To create a new attestation statement, click the New Statement button. Tick (or un-tick) the Active box as appropriate (an inactive statement will not be shown to the users). Click Save Change to save the attestation statement.

Note: Set up all the attestation statements for the whole organisation first. You will then select the appropriate ones to link to each organisation unit.

Link Attestation Statements to Organisation Units:

If the Attestation Statements screen is shown, click the Attestation Groups button at the top of the screen.



If there are Attestation Groups already set up, select the appropriate one from the dropdown list. Click New Attestation Group to create a new group. You may edit the group name by clicking the Edit button.

Select a frequency for the attestation and enter the date the system will start to prompt the attestation in MMDD format (eg. 0630 for June 30) in the Start Date field.

In the Preamble field, enter a preamble for the Attestation Statement. This will be shown to the users.

On the Organisation Unit panel to the left, tick the organisation units that will be included in this group.

On the Attestation Statements panel to the right, select the Attestation Statements that will apply to this group.

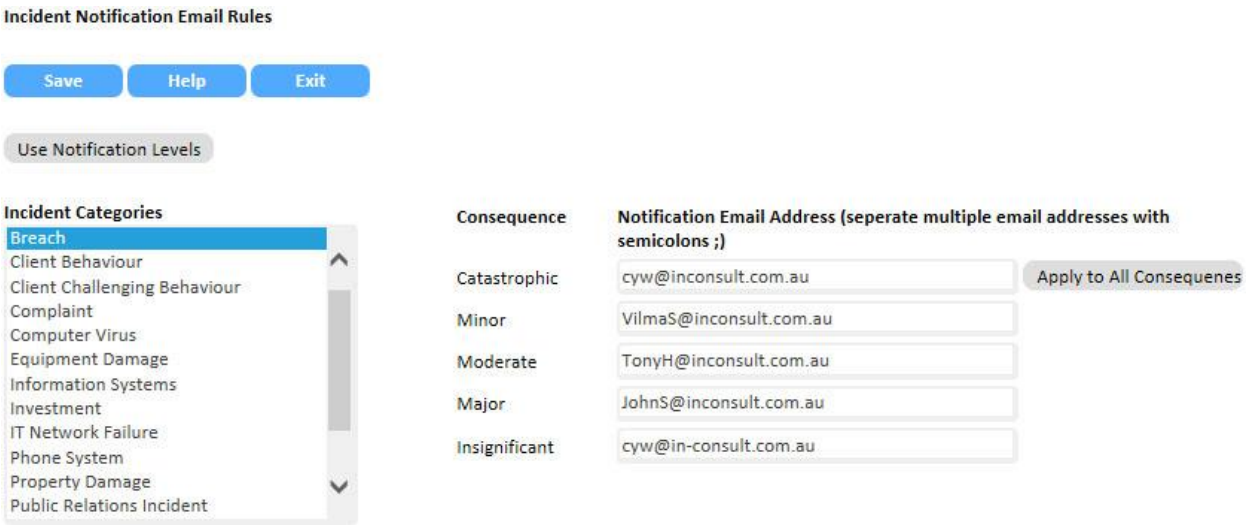
Click Save to save the Attestation Group setting.

Note: If all organisation units will be attesting to the same statements, you do not have to create an Attestation Group. Simply leave the Attestation Group dropdown list blank.

Incident Notification Rules

When a new incident is first saved, a notification email will be sent to the recipients as per the Incident Notification Rules. The rules include both the main and secondary incident categories and their consequence rating. You can specify email addresses for each incident category and its consequences or you can use the email addresses in the Organisation Unit Library and assign a notification level to each category and consequence or both.

Specifying email addresses:

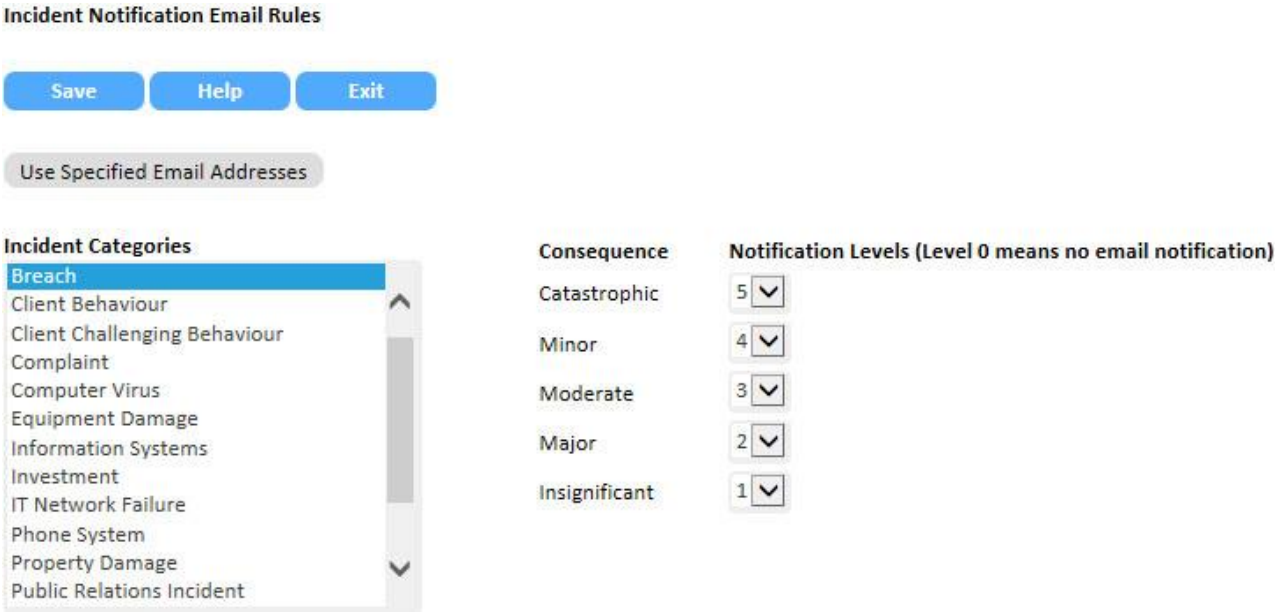


1. Select an incident category from the list displayed.
2. Enter email addresses for each of the consequence levels.
3. If multiple emails are required, separate them with a semicolon (;).
4. Click Save to save the data.

If you want to have the same email addresses for all the categories, select All Categories from the list. If you have specified non-standard consequences in the System Reference Table and there are more than 5 consequence levels in any category, you will need to select the category afterwards and add the email addresses for the additional consequences.
If you want to have the same email address for all the consequences, enter the email address for the first consequence and then click the Apply to All Consequences button.
Note: The consequence ratings for each category can be modified in the System Reference table. If no modifications are made, the default values will be used.

Use notification level:

Click the Use Notification Levels button.



Select an incident category from the list on the left.

For each consequence level, select a notification level.

Notification Level 0 means no email will be send. Level 1 means the notification email will be sent to the default organisation unit owner the incident is attached to.

The organisation unit owner email address is entered in the Organisation Unit Library.

Level 2 means that the notification email will be sent to the organisation unit owner as in Level 1 and the owner of the parent organisation unit will also receive the email. If you specify a number larger than the number of parent organisation units, the email will stop at the highest level organisation unit.

You can specify up to a maximum of 5 notification levels.

If the set up resulted in one email address receiving the same email more than once, the duplicated email(s) will not be sent so the recipient will only receive one email notification.

Archiving Incidents

As the number of incidents increases over time, you may find that loading the Incident Register and navigating through the various incidents take a long time. The Archive Incident function is used to move old and closed incidents to an offline file to improve the performance of the online Incident Register.

Archiving

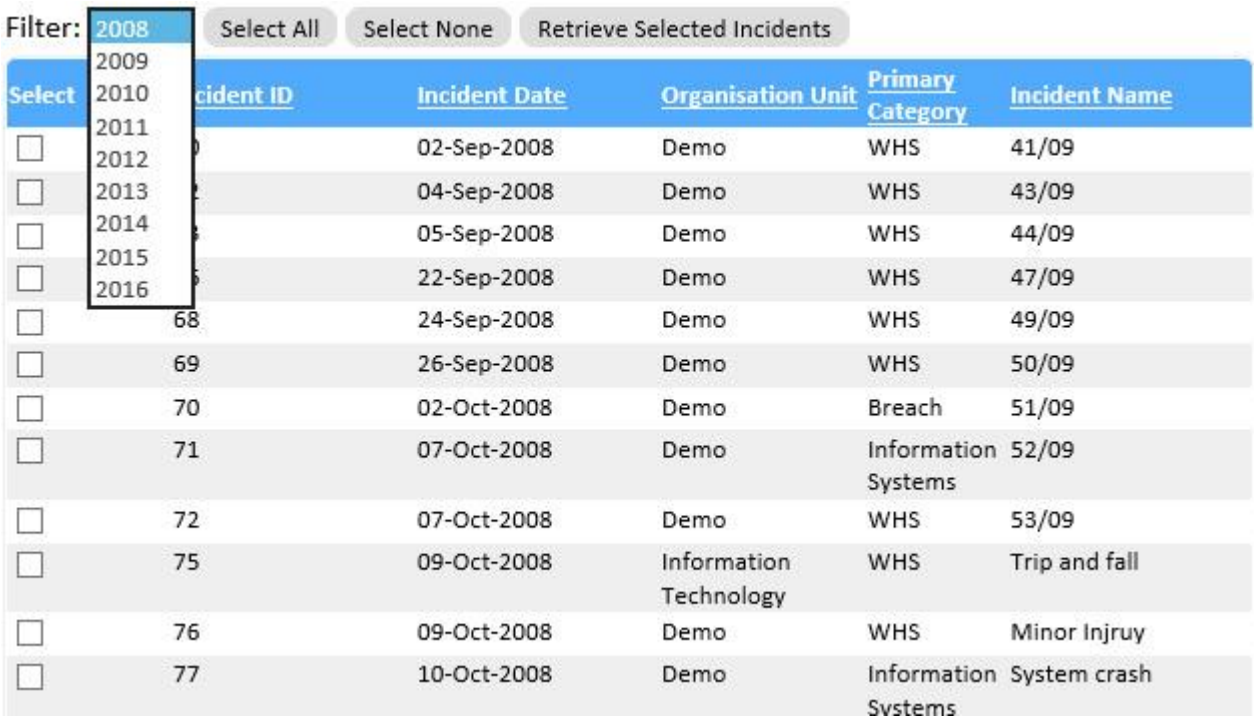
To archive closed incidents, click the Archive button. To retrieve one or more archived incidents, click the Retrieval button.

To archive closed incidents, select a year from the dropdown list. All closed incidents with an incident date falling into the selected year and the years prior to that will be archived. The history of changes, supplementary data forms (eg. WHS, Breach forms), cause and treatment and notes data will all be archived,

Note: Depending on the number of incidents you have in the system, the archiving process may take a few seconds to a few minutes. Do NOT disrupt the process by clicking something else on the screen or closing the browser. When the archiving is completed, a success message will be displayed. If an error message appears, copy the message and paste it in an email to GuardianERM@inconsult.com.au and we will investigate into that.

Retrieval

To retrieve one or more archived incidents, click the Retrieval button. A list of previously archived incidents will be displayed for the year (the incidents occurred or the incident date) selected.



Select	cident ID	Incident Date	Organisation Unit	Primary Category	Incident Name
☐		02-Sep-2008	Demo	WHS	41/09
☐		04-Sep-2008	Demo	WHS	43/09
☐		05-Sep-2008	Demo	WHS	44/09
☐		22-Sep-2008	Demo	WHS	47/09
☐	68	24-Sep-2008	Demo	WHS	49/09
☐	69	26-Sep-2008	Demo	WHS	50/09
☐	70	02-Oct-2008	Demo	Breach	51/09
☐	71	07-Oct-2008	Demo	Information Systems	52/09
☐	72	07-Oct-2008	Demo	WHS	53/09
☐	75	09-Oct-2008	Information Technology	WHS	Trip and fall
☐	76	09-Oct-2008	Demo	WHS	Minor Injruy
☐	77	10-Oct-2008	Demo	Information Systems	System crash

Tick the box for the incidents you want to retrieve and click the Retrieve Selected Incidents button. Depends on the number of incidents selected, the retrieval process may take a while to perform so be patient.

Once retrieved, the incidents will be in the current Incident Register and can be accessed just like any other incidents. However, the retrieved incidents will remain closed and you have to select the All or Closed incidents on the Incident Register to view them.

System Password Rules

By default, the system password rules are turned off. To turn it on and configure the rules, select System Password Rules from the Main Menu in the Administration Module. You have to log in as an administrator to access this function.

All changes will be activated the next time a user changes his/her password. For the "Number of Days Password is Valid For" setting, when the rules are turned on, all users have the same number of days entered to change their passwords.

The system administrator's password will never expire, regardless of the settings.

Without the password rules, when a user changes his/her password, the new password must be at least 5 characters in length and there cannot be any 3 consecutive characters that are in the old password. For example, replacing yellow with lower will not be accepted because 'low' is contained in yellow.

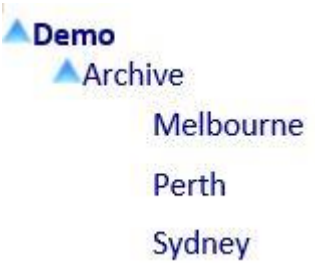
When an administrator creates a new user or resets an existing user's password, the password rules, except the default minimum 5 characters rule, do not apply. However, the new password will have expired already and the user must change the password upon login.

Note: The following special characters cannot be used for a password:
" ' % * ( ) < >

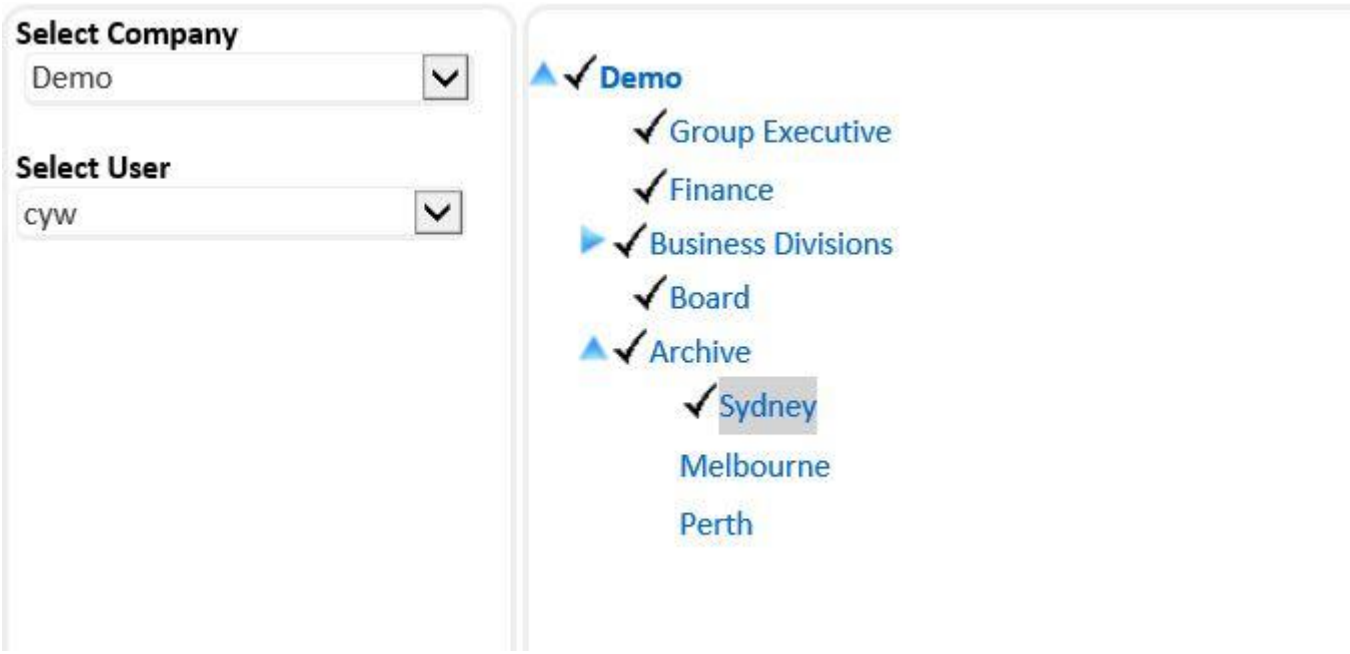
Archive Register Configuration

By default the Archive Register is NOT activated. To activate the Archive Register, log in as an adminstrator and select System Parameters. Add a new parameter called ArchiveRegister with value True.

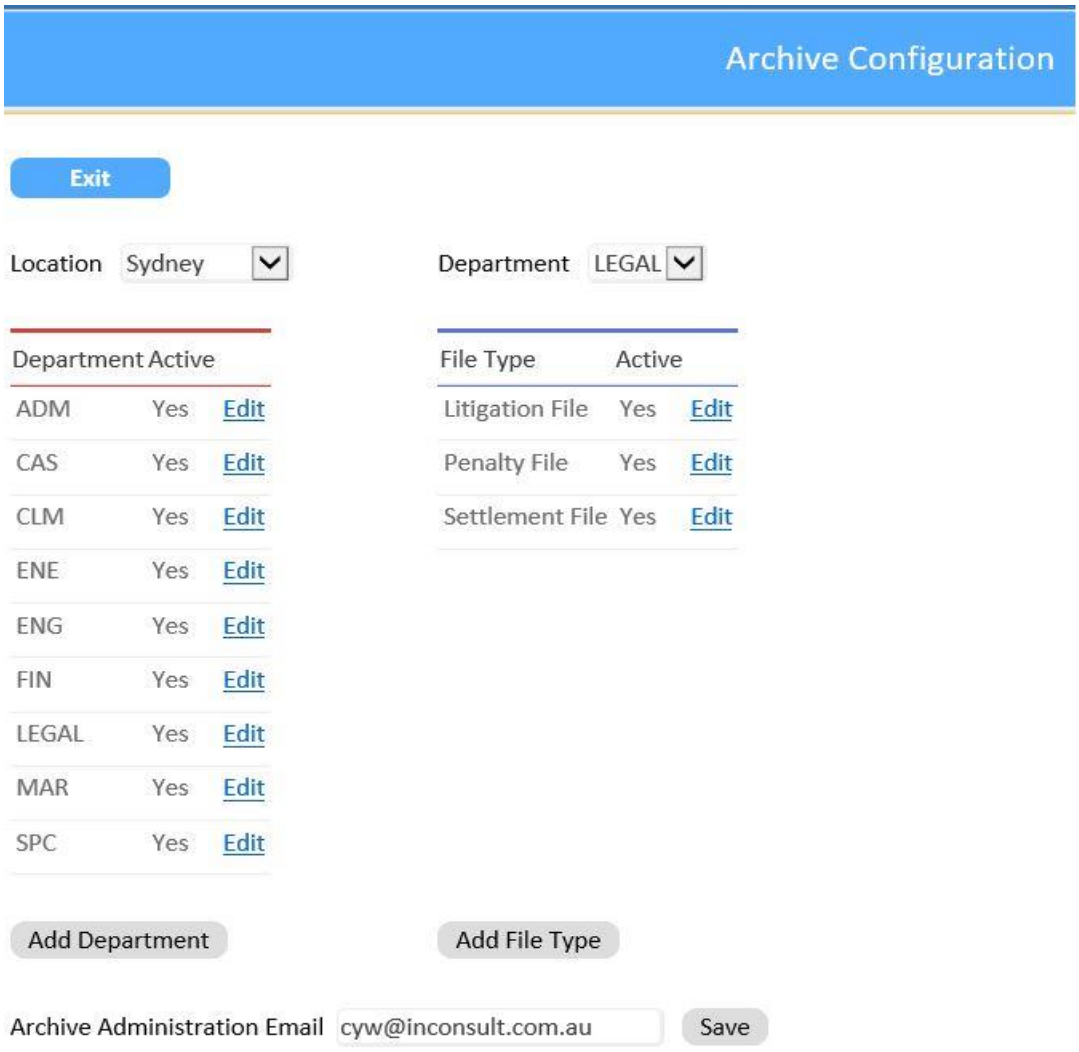
To use the Archive Register, you must first create an organisation unit in the Organisation Unit Library called Archive as a child of the top level organisation unit and then locations (or branches of your organisation) under it, like this:



Then in the Administration module, the administrator has to grant Organisation Read access to the users to access the achive records of each location.



In the Administration module, select Archive Register Configuration.



Select a location from the Location dropdown list.

Click the Add Department button and enter the Department then click Save. Repeat the process until you have set up all the departments.

Select a department that you have created from the Department dropdown list. Click the Add File Type button and enter an apporpriate File Type. Repeat the process until you have created all the appropriate file types for the selected department.

Select the next department from the Department dropdown list and repeat the above process to create file types for the department. Repeat the process until you have created all the appropriate file types for all the departments.

If there are more than one location, select the next location from the Location dropdown list and repeat the above processes to create the departments and file types for each location.

Enter an email address in the Achive Administration Email field. This is the default email address to send the automated archive retrieval request email for the selected location. Each location can have a different email address.

The setup is now completed and the Archive Register can be used.