User Manual

Version: 10

GuardianERM User Manual

* * * IMPORTANT NOTE * * *

Information contained in this user 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 User Manual

Produced by InConsult Pty Ltd

ACN 100 759 984

L3, 66 King Street,
Sydney NSW 2000

PO Box R653
Royal Exchange NSW 1225

Phone: (02) 9241 1344
http://www.inconsult.com.au
http://www.GuardianERM.com

material in this publication whether or not such injury, loss or damage is in anyway due to any negligent act or omission, breach of duty or default on the part of InConsult or its employees.

Table of Contents

General Risk Management Information

Introduction to Risk Management

What is risk?

Risk arises from uncertainty. Risk can be considered as the probability of occurrence of an undesirable outcome of an event due to a hazard or threat.

Risk has three characteristics:

1. an undesirable outcome;
2. the probability or likelihood of such outcomes; and
3. the consequence of such an outcome.

How is risk measured?

Risk is measured in terms of the likelihood of it happening and the consequences if it happens.

What is risk management?

Risk management is a systematic approach to managing risks. Risks can be managed in different ways including avoiding, sharing, reducing or transferring.

There must be a balance between the cost of managing the risk and the potential loss you expect from taking the risk.

Why should you manage risks?

Ignoring or not managing the risks which apply to your business activities or processes could adversely impact on the following:

- Your financial position
- Your compliance position
- The health and safety of employees, customers, volunteers and participants
- Your reputation, credibility and status
- Public and customer confidence in your organisation
- Plant, equipment and the environment

Today's organisations involve quite complicated operations managed by different people with different attitudes towards risk taking or avoidance. Establishing a clear and consistent risk management framework increases the chance of the organisation achieving its objectives.

The GuardianERM.Net Risk Management Methodology

The GuardianERM.Net Integrated Enterprise Risk Management System is built on the principles of the GuardianERM.Net Risk Management Methodology, developed and practised by InConsult, a specialist risk management consulting firm.

The GuardianERM.Net Risk Management Methodology complies with ISO31000 and can be applied to any organisation all over the world.

Some Risk Management Background Information:

Concept of Risk

Probability Theory

Types of Risks

Risk Exposure

Comparative Risk Exposure

Risk Treatment

Establishing the context
This is the first step in the risk management process. It requires you to consider your business, the environment, stakeholders and risk evaluation criteria.

Understand your business (internal)
This is a high level view of the business. Understand your organisation, the nature and extent of the activities and processes you undertake. Consider the different types of risks that exist.

Assess the environment (external)
Review the social, economic, legal, political, competitive, technological or environmental factors that affect your business. Consider the relationships between the activity and the environment. Consider the factors which may support or impair your ability to effectively manage risks.

For example, regulatory requirements will impact your organisation. While you cannot control what the regulatory requirements are, you can control how you comply with them.

Identify stakeholders

Stakeholders could be employees, managers, volunteers, unions, regulators, customers, government, suppliers and service providers. They are individuals who may affect, or be affected by, any of your decisions on risk management.

Different stakeholders have different needs and concerns. It is essential that you consider their needs or consult with them during the risk management process.

Establish risk evaluation criteria

A set of risk evaluation criteria is used to help measure and rank risks and support decision making.

Risk Analysis

Once we have defined the context of risk, we should identify and develop a complete list of items exposed to risks and the risks which could impact the organisation, activities or business processes.

This is a very important step in risk management. If you fail to identify a potential risk, it may pose a major threat to your organisation in the future.

No risk is too small or too large to have an impact. By systematically understanding and assessing the risks an organisation is exposed to, quality decisions can be made whether to accept the risks or to act on them.

What are the sources of risk?

Risks can arise from sources either inside or outside the organisation.

Internal risks are those that are part of the organisation's activities, e.g. risk of an employee being injured. Sources of internal risks include:

- Human behaviour
- Technology and technical issues
- Occupational health and safety
- Property and equipment
- Financial activities

External risks are those which impact on the organisation or its activities, e.g. legislative change that requires pools to be fenced. Sources of external risks include:

- Legal requirements
- Political issues
- Environmental issues
- Technology and technical issues
- Financial market activities
- Natural events

What are the different types of risks?

There are many ways of classifying risks and there is no one correct way to categorise an organisation's risks. A sensible method to adopt is to define the categories of risks to be used and stick to it. Below are a few commonly used terms related to risk:

Financial Risk

Financial risks are undesirable outcomes of certain events that lead to economic losses. Financial risks may include theft, fraud, loans, membership fees, insurance costs, damages claims or penalties and fines

Physical Risk
Physical risk refers to risks that arise from certain physical attributes of an object, for example, the risk of an engine breaking down. It may include personal injuries, environmental risks and the damage to physical assets of your organisation, such as equipment and vehicles.

Moral or Ethical Risk
Moral risk involves human nature and is dependent on the character and moral standards of individuals, e.g. the risk of an employee embezzling company funds. Ethical risks involve harm to the reputation or beliefs of an individual or organisation.

Legal Risk
This refers to risks that arise from various legal obligations including judicial precedent. For example federal, state and local Government laws, regulations and standards.

Some undesirable events will attract one type of risk whilst others may attract multiple risks. For example, not complying with Sarbanes-Oxley requirements will attract a legal risk (breach of compliance requirement), a financial risk (a fine) and a reputation risk.

Other important attributes of risk

One-Sided Risk
This is also known as 'Pure Risk' and refers to the situation where there is only the possibility of loss or no loss, e.g. either your car is broken down or not.

Two-Sided Risk
Two-sided risks are also known as 'Speculative Risks' and refer to the situation where one could make a gain or a loss. The two sides are sometimes called upside and downside and are commonly encountered in business activities, e.g. making a profit or a loss. In a reasonably efficient market, the expected rate of return is directly proportional to the level of risk, that is, the higher the risk, the higher the possible reward. The concept of risk and return is well demonstrated in gambling games.

Inherent Risk

Inherent risks are risks that are naturally associated with an event **before** they are treated, e.g. car accidents and engine failure are two of the inherent risks of driving a car.

Residual Risk
Residual risks are the risks that remain after we treat the risks, e.g. we have a fuel gauge in the car to help treat the risk of running out of fuel.

What are some common methods of identifying risks?

There are several techniques that may be used to identify risk. You can use one or more of the following methods:

- Brainstorming in groups or individually
- Arrange interviews and discussions with stakeholders
- Distribute surveys and questionnaires to stakeholders
- Conduct audits and physical inspections
- Directly observe the activity or process
- Analyse specific scenarios

What are control breakdowns?

While controls are designed to reduce the risks of loss, they may not be performed or work effectively all the time. An example is 'reconciliations are not performed'.

Probability Theory

One of the fundamental characteristics of risk analysis is probability. The probability of an undesirable outcome implies a time factor which includes frequency and duration. For example, the more often you drive your car and the longer you drive every time, the more exposed you are to the risk of having an accident.

We will only examine some of the basic properties of probability here.

Certain and Uncertain Possible Outcomes
There are two basic types of possible outcomes from a certain event. The first type is where all possible outcomes are known in advance, e.g. when we toss a coin, we know for sure that the outcome can only be a head or tail (and the extremely low possibility that the coin stands on its edge).

The second type is where all the possible outcomes are not known in advance, e.g. when a person examines a payment voucher, he/she will know for sure that the voucher is either erroneous or error-free but if there is an error, he/she will not know in advance what the possible types of errors could be. Even if every character and marking on the voucher is correct, the voucher may not be genuine, it may not be related to the correct invoice, bulk purchase discount may not have been deducted, etc. In assessing risks in an organisation, we deal with this type of situation most of the time.

Certain and Uncertain Probabilities

In some situations, the probability of an outcome is known with certainty in advance. For example, in tossing a coin, we know for sure that the probability of getting a head is one half (ignoring the outcome that the coin stands on its edge).

In other situations, the probability of an outcome cannot be ascertained in advance, for example, the probability that the accounts clerk makes an incorrect ledger posting.

Random Outcomes

When we throw a 'fair' dice, the occurrence of any one outcome (one to six) is random. But if the dice is 'loaded', a systematic interference is introduced into the game and the outcome is not random any more.

In an organisation, the occurrence of an undesirable outcome (e.g. an erroneous general ledger) is rarely random because systems and procedures are introduced to direct the outcome. This type of undesirable outcome is of main interest in risk analysis as they usually indicate a weakness or flaw in the internal control system.

Mutually Exclusive Outcomes

Certain outcomes from an event are mutually exclusive. If we throw a dice, an outcome can only be one of the six possible outcomes at any one time. That is, if the outcome is three, then the probability of throwing anything else must be zero.

In an organisation, many of the possible outcomes of events are not mutually exclusive. For example, a data centre can be destroyed by fire, by flooding or both at the same time or a payment can be made to the wrong payee and for the wrong amount.

Some Basic Rules of Probabilities

1. The probability of an outcome must be between 0 and 1. When we are certain that an outcome will occur, the probability is 1. If there is no chance that an outcome will occur, the probability is 0.
2. The probability of an event is the sum of all possible outcomes, e.g. if the event of the data centre being inoperative can be caused by fire (probability = 0.02) or flooding (probability = 0.1) and assuming the 2 causes are independent of each other, then the probability that the data centre is inoperative is (0.02 + 0.1) = 0.12. It should be noted that in real life, a lot of outcomes are dependent on each other, e.g. heat from the fire could cause water pipes to burst or water can be introduced into the data centre from the fire-fighting process.
3. The sum of the probabilities of all events must be 1. That is, since the data centre can only be operative or not operative, the probability that the data centre will be either operative or not operative must equal to 1. Therefore, in the above example, the probability that the data centre is operative is (1 - 0.12) = 0.88.

Risk Exposure

To evaluate risk exposures, we have to identify what is at risk and measure how much is at risk.

To identify what is at risk is usually much easier than measuring how much is at risk. For an organisation, we should always translate losses into dollar values although at times an accurate figure may be very difficult to obtain.

For example, for a natural person, what is the appropriate unit of measure if the risk involves human life, pain and suffering, embarrassment, quality of life (just to name a few)?

The difficulty of risk analysis lies in identifying *all* possible outcomes and what is at risk.

It is sometimes difficult to quantify the risk and exposures, i.e. the probability that an undesirable outcome may occur and how much is at risk (sometimes it is difficult to identify an appropriate unit of measure, e.g. for human life).

A systematic way of analysing risk exposure:

Properties of Risk:	Threats
	Undesirable Outcomes
	Probability
	Frequency

	Duration
Risk Exposure	What is at risk How much is at risk

The Probability of loss caused by a threat = Probability of occurrence per unit time X Frequency X Duration / Total available time

In risk analysis, it is common to call this probability "likelihood".

Risk = Sum of the probability of loss caused by all threats

Consequence or Value of Risk ($) = Sum of all items at risk X Value at risk of individual items

Exposure to risk ($) = Risk (probability) X Consequence ($)

See also comparative risk exposure

Consequence of Risk

The consequence of the risk is the potential loss the organisation can suffer if things go wrong. It is NOT related to what may cause the loss. For example, a factory building may have a replacement value of $10m. The consequence to the organisation of losing the building is therefore $10m,regardless of whether the loss is caused by fire, earthquake or flooding.

When valuing the consequence, use the maximum probable loss. The risk exposure will be adjusted by the probability of the loss.

Exposure to risk ($) = Probability X Consequence ($)

Comparative Risk Exposure

If there are no cost and time constraints, we can eventually calculate quite accurately the risk exposure values of all activities of an organisation.

Two questions:

1. Do we **need** to know the absolute risk exposure value before we can bring the risk under control?

2. Is there a **simpler**, faster and effective way to measure risk exposure?

While we can spend enormous amounts of resources to measure the risks of all the thousands of business units and activities of an organisation, the value of such an exercise may not be commercially justified.

A simpler and faster way is to categorise the level of risk of the activities using comparative risk exposure measurements into a pre-determined number of categories.

GuardianERM.Net uses a 5-level rating system. That is, a risk can have a value of 1 (lowest) to 5 (highest).

A very effective method of comparative risk ranking is called the Delphi technique. Put simply, the Delphi technique groups all activities exhaustively in pairs and compares the relative risk of each pair of activities. The score for comparing each pair of activities is summed and an overall ranking obtained.

GuardianERM.Net can cater for both the absolute and comparative risk exposure measurement methods.

Risk Treatment - Hazard and Control

As risk is almost always related to undesirable outcomes, it is something that is unwanted. However, there is inherent risk in everything. While we cannot eliminate risk, we can control risks to some extent. The whole process of identifying, assessing and controlling risks is called Risk Management.
Hazards are conditions or activities that lead to an increase in risk exposure, and controls are those that lead to a reduction in risk exposure. For example, drinking alcoholic beverages is a hazard to driving as it increases the likelihood of having an accident. Having a designated non-drinking driver is a control. Having the car serviced regularly is another control as a properly maintained car has less chance of mechanical failure which is also a frequent cause of car accidents.

Other than avoiding the risk (or activities associated with the risk) or limiting the financial exposure by buying insurance, a risk can be controlled by:

1. Reducing the probability of the undesirable outcomes; or
2. Reducing the value exposed to the risk (consequence of the risk).

Threats

Threats are the causes of potential loss. For example, having a car accident is a risk of driving a car but there are many causes of car accidents. Drink driving, a punctured tyre or falling asleep at the wheel can all be some of the causes.

It should be noted that causes can be immediate or remote. A driver falling asleep at the wheel may be the immediate cause of a car accident but the remote cause may be that the driver has been partying all night before driving home.

Similarly, an error in the balance sheet may be caused by an incorrect entry in a sub-ledger but the remote cause could be inadequate training provided to the accounting staff.

A challenge of risk analysis is to identify and measure the probable causes of loss from a number of immediate and remote causes.

Identifying the threats is important both in analysing risks and in designing controls to reduce the risk exposures.

Remember, analysing risks is only a means to an end. The end is to control the risks.

Types of Control

Detective Control: A control which is designed to detect irregularities, errors or non-compliance, e.g. accounts reconciliation.

Preventive Control: A control designed to prevent something from happening, e.g. a computer log-in control to prevent unauthorised access.

Corrective Control: A control designed to correct errors or non-compliance, e.g. automatic temperature regulator to correct overheating of certain equipment.

Getting Started

GuardianERM.Net overview

GuardianERM.Net simplifies the process by taking the mystery out of risk management and through step-by-step evaluation procedures, builds a comprehensive and reliable risk management system for organisations of any size.

Using the top-down approach, an organisation is broken down into its operational components. The processes, risks and controls are evaluated at each component level. The results are rolled up using a bottom-up approach following the same path for consistent and meaningful high level executive information.

From the information collected in the evaluation process, compliance and/or audit programs can be prepared automatically. This ensures that the review programs are consistent across the organisation and over time.

Once results of the reviews are entered into GuardianERM.Net and the review program is finalised, the consolidated results for the organisation are instantly updated.

With the integrated Incident and Compliance management functions, GuardianERM.Net is one of the most powerful risk management systems available.

The workflow management system identifies tasks to be done and overdue deadlines. It is particularly useful in managing periodic compliance requirements. Alert emails will be automatically sent to desired staff members based on the workflow settings configured by the users.

Documentation including process maps, company policies, procedure manuals and legislation can be dynamically linked to GuardianERM.Net reducing time and effort searching for reference materials.

GuardianERM.Net has two primary sets of information: the expert information and the experience information.

The expert information set contains data as a result of the assessment of risks and controls of an operation.

The experience information set contains data collected periodically via compliance reviews, audits, incidents investigation and treatment. The information confirms (or

otherwise) the theoretical risk assessment and paints a true picture of the organisation's risk profile.

System Requirement

GuardianERM.Net is designed to work best with Internet Explorer v10. Other browsers are not supported and may not display information properly.

You need to have Java installed and pop-ups allowed.

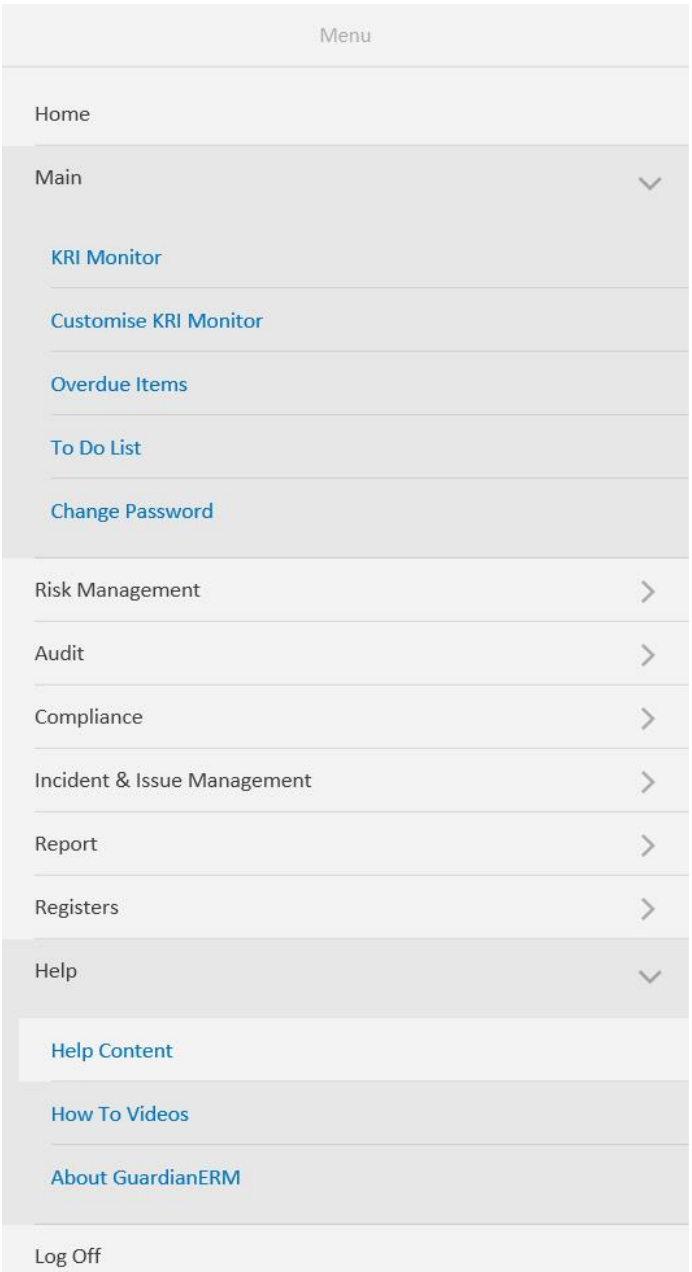
To utilise the reporting, import and export functions, Adobe Reader and Microsoft Excel must be installed on your computer.

System Navigation

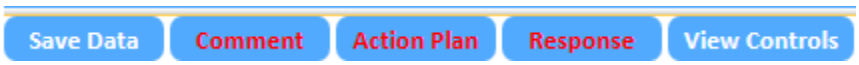
The user ID and password provides access to the system. Your user ID determines your access level and may restrict or disable certain functions. If you have difficulties with your password or access level you need to contact your system administrator.

Navigation throughout the system is by a dropdown navigation menu:

Click the 3-bar menu icon at the top left to display the menu.



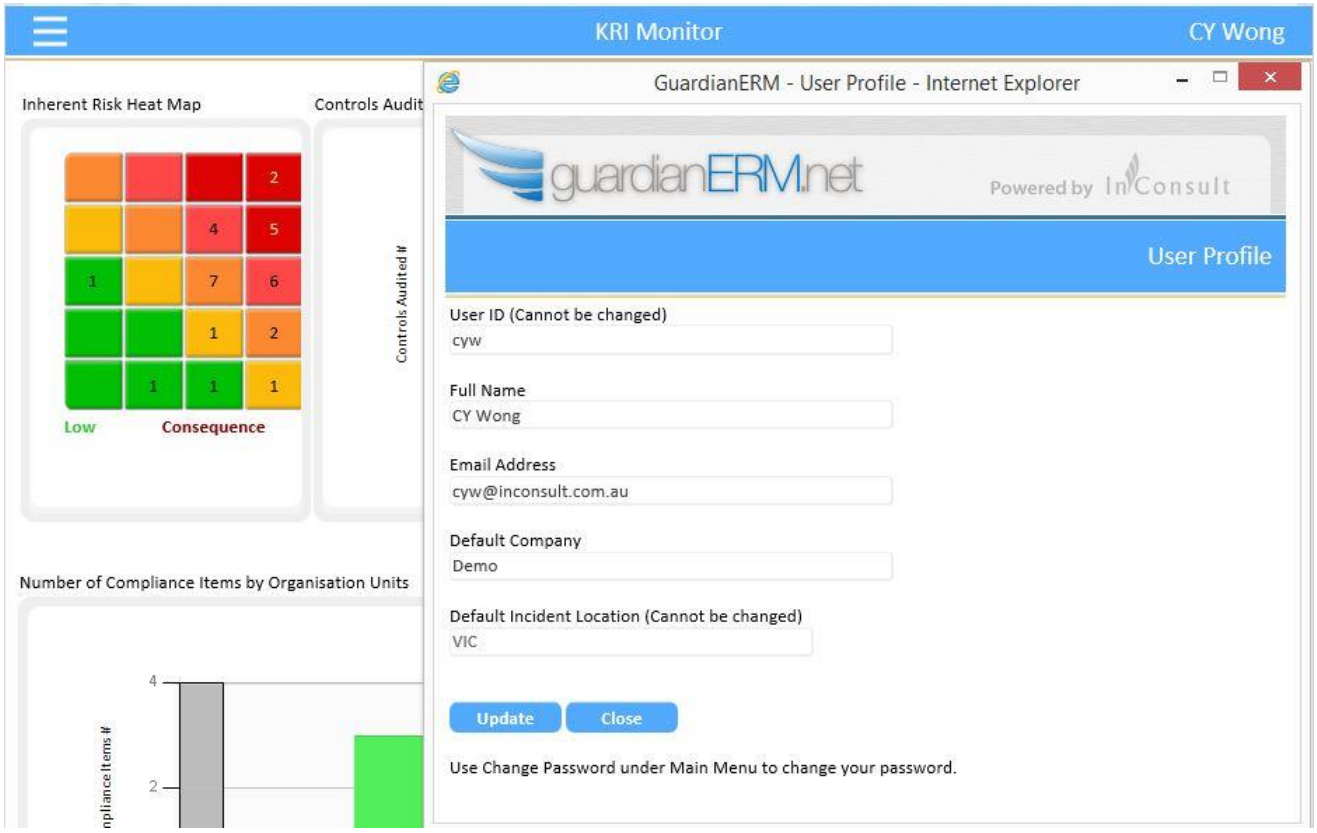
On most screens, there are also some function buttons:



If you move your mouse cursor on top of any button, a pop-up description of the function of the button will appear.

On certain screens, there is no navigation menu displayed. You must click the Exit button to return to a page where the navigation menu is displayed before you can navigate to another module or function.

If you click your user ID at the top right of the screen, you can change your user profile.



Initial Setup

For initial setup, follow these steps to set up the GuardianERM.Net system for your organisation:

1. Create an organisation chart for your organisation.
2. For each organisation unit, complete all details paying special attention to accurately rating the significance of the organisation unit in relation to the whole organisation. The Significance level is used by the system to calculate risks. If Not Available is selected, risks will not be calculated for the organisation unit.

3. For each business unit or activity on the organisation chart, identify the inherent risks.
4. For each risk identified, review the operation's processes to identify (or design) the controls that would mitigate the risk.
5. Analyse the risks and controls and rate them.
6. For each control, identify or design audit procedures that can be used to verify that the control is actually working effectively and efficiently.

Data collected is entered into the system via the Risk Evaluation module.

See also: Workflow Management

Online Help

GuardianERM.Net has an online context-sensitive help system. Click the Help button if you require assistance.

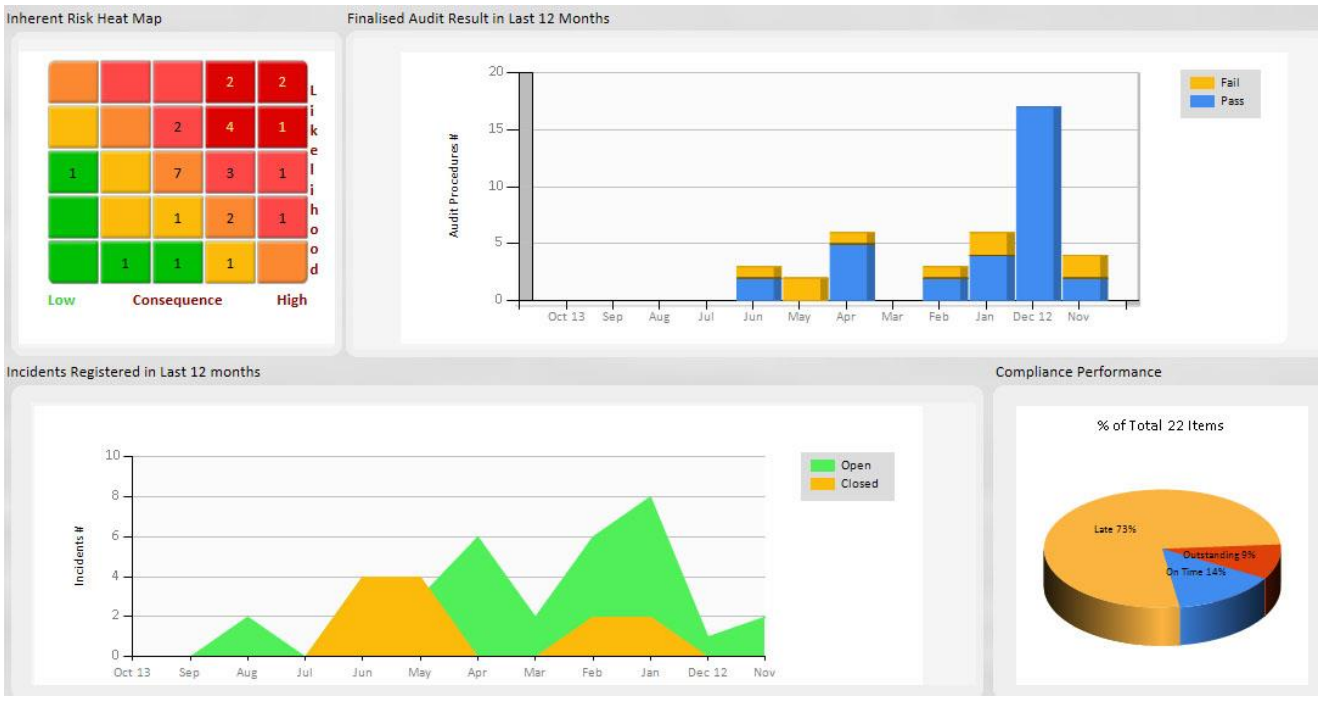
Main Menu

KRI Monitor and the System Start Up Screen

The KRI Monitor is the default start up screen for GuardianERM.net. You can customise the information displayed or show the Overdue List as the start-up screen instead. When you first use GuardianERM.net, you must customise the KRI Monitor screen. Each user has his/her own customised KRI Monitor screen.

The KRI Monitor consists of 4 user-selectable charts and an overdue action items monitor.

A typical charts layout looks like:



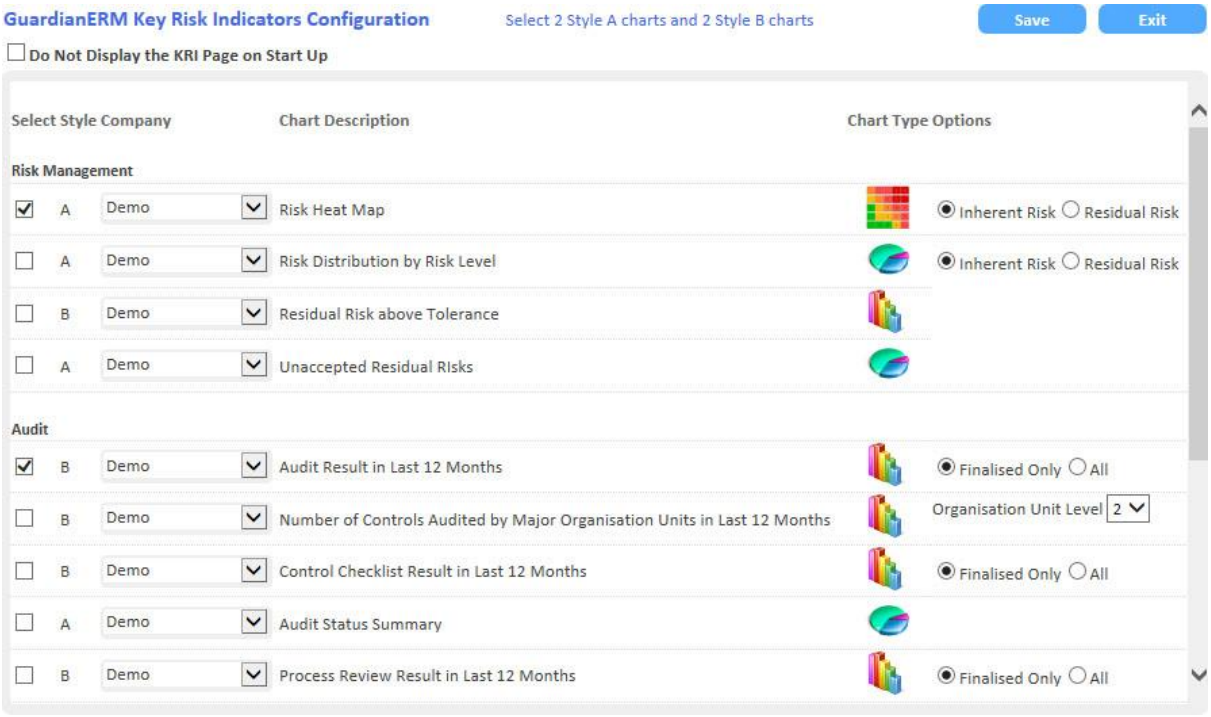
The Overdue Actions monitor is not user configurable and shows the overdue action items:

The gauge shows the percentage of overdue items compared to the total number of action items within the last 12 months. The red alert dots show the number of overdue items in each category. Where there is no overdue item, the red alert dot will not be displayed. To view the overdue items, click the desired button with the red alert dot on it.

Note: The number of overdue items shown on the Overdue Actions Monitor may not be the same as the number shown on the charts. The charts only show overdue items within the last 12 months while the Overdue Actions show all overdue items, regardless of age.

Customising the KRI Monitor Screen

To customise the KRI Monitor screen, click the Customise Screen link on top of the Overdue Actions Monitor.



You must select 4 charts, 2 from Style A and 2 from Style B.

If you do not want to have the KRI Monitor screen as your start up screen, tick the Do Not Display the KRI Page on Start Up box at the top of the customisation screen

Overdue Items

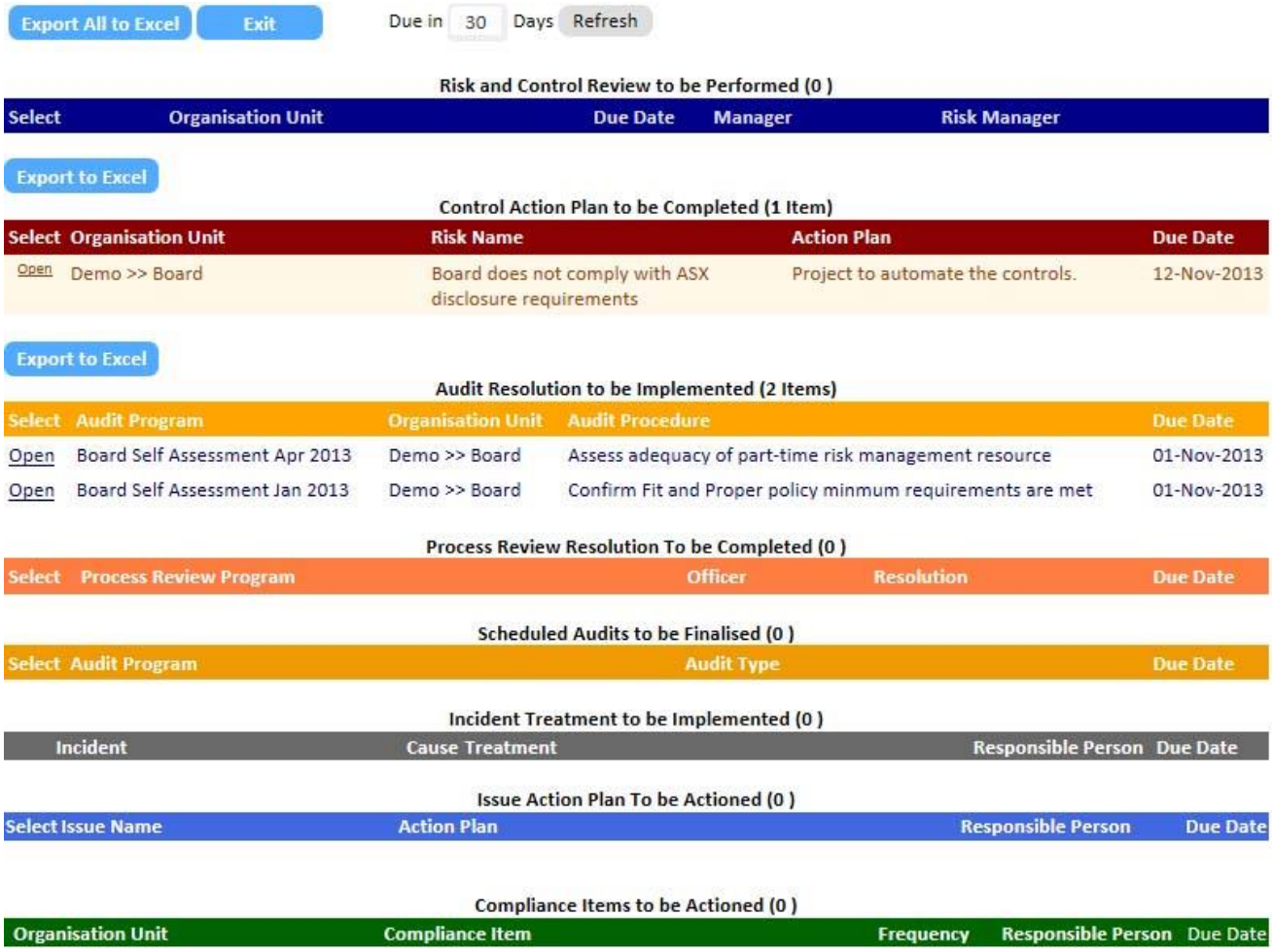
The Overdue Items List is divided into sections as below. Each section shows action items past their due date.

To action an item, click the Open link for that item.

You may export individual section or all the sections to Excel by clicking the respective Export button.

To Do List

The To Do List is divided into sections as below. Each section shows action items that will become due in the timeframe specified.



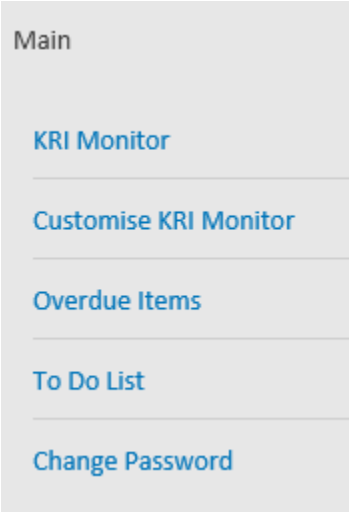
The "Due in __ Days" is defaulted to 30 days. You can change that to any other integer number and click the Refresh button.

You may export an individual section or all the sections to Excel by clicking the appropriate Export button.

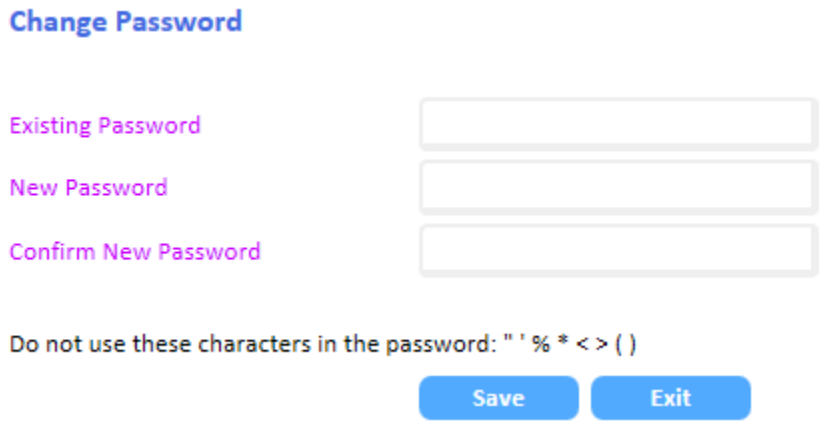
For compliance items that may be assigned to someone other than the organisation unit owner, you may choose to view only items assigned to you or all items for the organisation units you are granted access. This applies to both the Overdue and To Do lists.

Changing Your Password

You can change your password anytime by clicking Change Password under Main on the Menu:



Enter your existing password and then the new password. Enter the new password again to confirm.



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

Library

The library consists of four sets of standing information which is used for risk evaluation: Organisation Unit, Risk, Control and Audit. It also has a function to manage the uploaded external documents.

Changing System Library Data

The GuardianERM.Net system uses a number of library files to share information across the system and among the users globally. The use of library files ensures consistency within the system and to avoid duplicated data entry.

Library files are like the chart of accounts in the general ledger and once in use should not be changed. If an account is called 'Fixed Assets' and journals are posted to this account by users globally and then someone changes this account to be called 'Current Liabilities', imagine the problems and confusion this would cause.

It is strongly recommended that you create a new item rather than change an existing one unless it is to correct a typographic error or to make the description more meaningful without changing what the data represents.

Any change will affect the whole system and it is therefore recommended that only one person (with backup) has access to the library files.

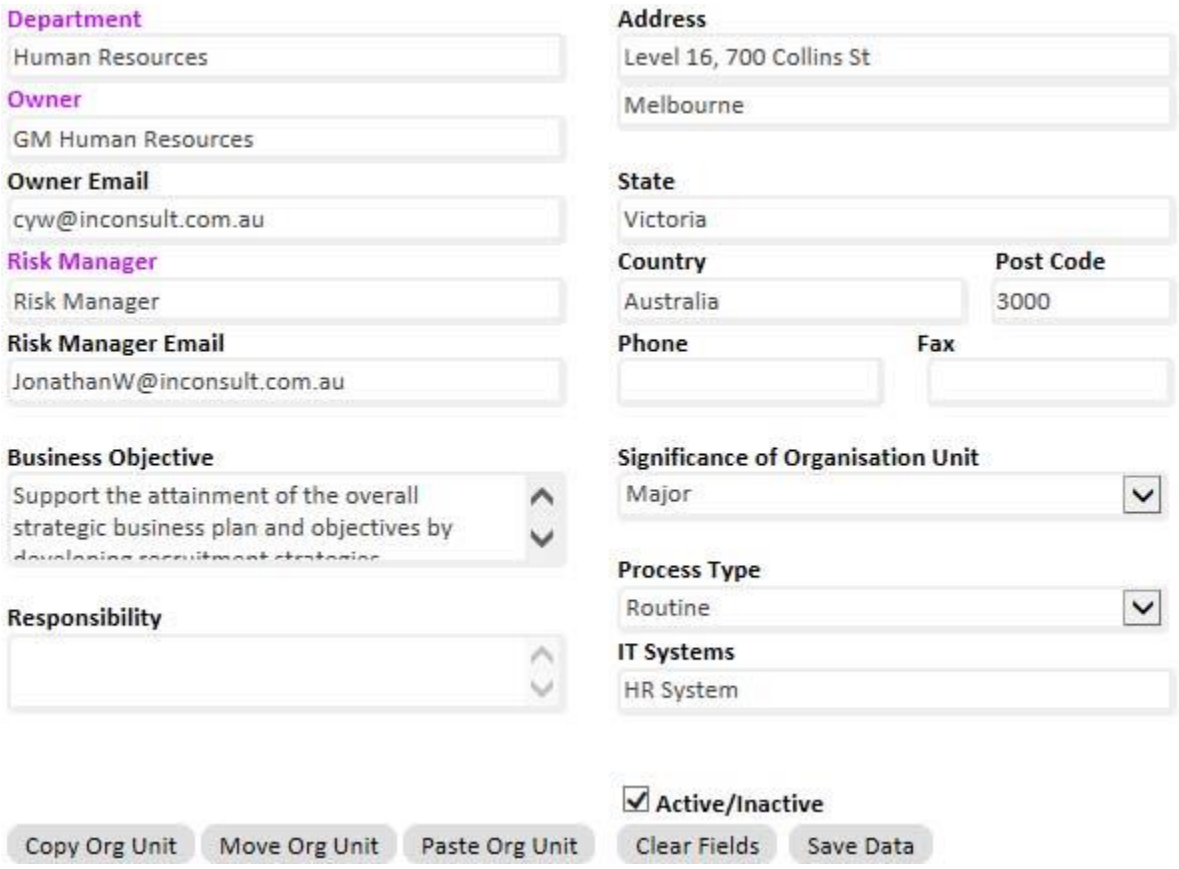
Organisation Unit Library

This function is used to create and maintain the organisation's risk management structure. The risk management structure consists of hierarchically related organisation units.

An organisation unit can be a physical object (e.g. a building or machine), a functional unit (e.g. marketing department), an activity (e.g. payment processing) or a task/milestone of a project. Before you set up the risk management structure, careful consideration should be made to the functionality of the structure in relation to your risk management and reporting functions. Although GuardianERM.Net has available various tools to change the risk management structure, once the structure is set up and the system is put into production, the risk management structure **should not be changed** unless the change is to reflect a change in the organisation (e.g. addition of a new branch office). The reason is that all 'transactions' in the system (e.g. audits, audit schedules, compliance items, attached documents or incidents) are recorded against the risk management structure. Changing the structure (e.g. moving an organisation unit from one parent unit to another) may cause confusion and loss of continuity to the information collected over time. Extreme care should be taken as the effect of changes made to the structure is generally not reversible.

A risk management structure may look like:

Select an organisation unit from the hierarchical structure and its details are shown for editing:



Data Fields:

Organisation Unit	The name of the selected organisation unit.
Owner	The person who is responsible for the organisation unit.
Risk Manager	The person in charge of the organisation unit's risk management activities.
Email	The email addresses of the Owner and the Risk Manager. This is used by the system to send notification and reminder emails.
Business Objective	The business objective of the organisation unit.
Process Type	Select the type of process from the dropdown list.
IT Systems	The main IT systems used by the organisation unit.
Significance	Select a significance level from the dropdown list.
Last Reviewed	The date the risks and controls for this organisation was reviewed and

	the user who reviewed it. These fields cannot be changed.
Address, State, Country, Post Code	The address of organisation unit.
Phone	The phone number to contact the organisation unit.
Fax	The organisation unit's fax number.

To **activate** or **deactivate** an organisation unit, check or uncheck the Active/Inactive checkbox. An organisation unit is active when the Active/Inactive checkbox is checked.

Note: When an organisation unit is deactivated, the organisation unit, all its children organisation units and all their attached risks, controls and audit procedures will not be shown in any part of the GuardianERM.Net system. However, none of the information is deleted. To retrieve the organisation unit and everything attached to it, simply activate the organisation unit again. When you deactivate an organisation unit, all its children units will be deactivated as well. However, when you activate an organisation unit, none of its children units will be activated. You need to manually activate the children units where appropriate.

To create a new company, click the New Company button and fill in the details for the company and then click the Save Data button.

Note: When a new company is created, the workflow settings will be automatically created and the settings will be the same as the first company that was created. You should check (or request the system administrator to check) the workflow settings for the new company created to make sure it is proper.

To create an organisation unit, select an organisation unit from the structure under which you want to create the new organisation unit and then click the New Organisation Unit button. Fill in the details for the organisation unit and click the Save Data button.

Important Note: When a user creates a new organisation unit, the user is the only one who has access to that organisation unit. You should determine who needs to have access to the newly created organisation unit and request the system administrator to grant the respective users the appropriate access to the organisation unit.

To copy an organisation unit, select the organisation unit and click the Copy Org Unit button. Then select the destination organisation unit you want to copy the organisation unit to and click the Paste Org Unit button.

To move an organisation unit, click the Move Org button instead of the Copy Org button.

When an organisation unit is copied or moved, the selected organisation unit, all children organisation units, risks, controls and audit procedures within the organisation unit and its children organisations will be copied and moved as well. Make sure you check the risk and control evaluations afterwards as they may not apply to the new organisation unit.

Copy, Move and Paste Organisation Units

An organisation unit, with all of its children, can be copied or moved and pasted to another parent unit, provided that the parent is not a child of the organisation unit being copied or moved. When an organisation unit (or a branch of organisation units) is copied or moved, all their attached risks, controls and audits are copied or moved as well. Please note that when you copy an organisation unit, external documents attached to the organisation unit are not copied. However, if you move an organisation unit, you will be asked if its attached documents are to be moved with it.

To copy an organisation unit, select the organisation unit and click the Copy Org Unit button. To move an organisation unit, select the organisation unit and click the Move Org Unit button. Now, select an organisation which is to be the parent unit of the organisation units you want to copy or move and then click the Paste button. You will be asked to confirm the action - at which stage you can cancel the operation.

Security Access

When a user creates an organisation unit, the user automatically is granted full access to that organisation unit. However, no other user will have any access to the organisation units created by one user. It is important that the System Administrator be requested to grant the appropriate access to other users who will require access to those organisation units.

Copying and moving organisation units is equivalent to creating new organisation units and the security access should be reviewed and modified accordingly.

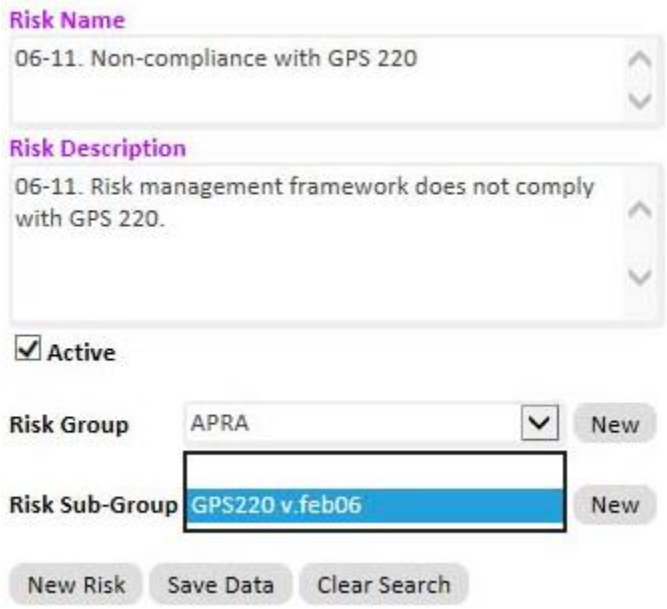
The Risk Library

The Risk Library stores all the risks identified for the organisation. If you have created more than one company, the Risk Library is shared amongst all the companies.

The Risk Library is accessed by clicking the Risk link in the Library.

Creating a New Risk

To create a new risk, click the New Risk button, enter a short name for the risk and a full description of the risk.



You may assign a Group and/or Sub-Group for the risk to categorise it for easy searching at a later stage. If the Group or Sub-group is not on the list, click the corresponding New button and enter the new group.

Click Save Data when data entry is completed.
Note: If you forget to click Save Data, the data will be lost if you exit or click on New Risk to enter another risk.

Modifying a Risk

To modify a risk, select the risk from the list, make the required changes and click the Save Data button. Once a risk has been used in Risk Evaluation, it is recommended that

you do not modify the risk except to correct typographical errors. Refer to Changing System Library Data for more information.

Finding a Risk

To find a risk quickly, you may use the Group Filters or the Search Text functions.
To use the filters, select a Group and/or Sub-Group and the list of risks will be filtered to show only the risks belong to the Group or Sub-Group.

The Search Text function will search one or more words entered in both the name and description fields.

When a risk is selected, all the organisation units using that risk will be listed.

Deactivating a Risk

To deactivate a risk, un-tick the Active button and click Save Data. Deactivated risks are not deleted and can be found by clicking the Inactive button just below the Search button. To reactivate a risk, select it from the Inactive list, tick the Active box and click Save Data.

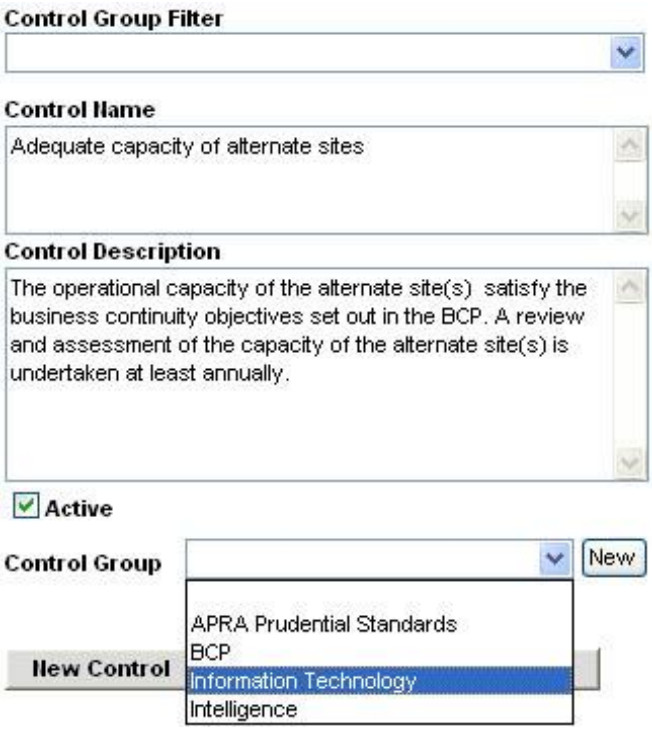
The Control Library

The Control Library stores all the controls identified for the organisation. If you have created more than one company, the control library is shared amongst all the companies.

The Control Library is accessed by clicking the Control link in the Library.

Creating a New Control

To create a new control, click the New Control button, enter a short name for the control and a full description of the control.



You may assign a group for the control to categorise it for easy searching at a later stage. If the group is not on the list, click the corresponding New button and enter the new group.

Click Save Data when data entry is completed otherwise the data will be lost.

Modifying a Control

To modify a control, select the control from the list, make the required changes and click the Save Data button. Once a control has been used in Risk Evaluation, it is recommended that you do not modify the control except to correct typographical errors. Refer to Changing System Library File Data for more information.

Finding a Control

To find a control quickly, you may use the Group Filter or the Search Text functions. To use the filters, select a group and the list of controls will be filtered to show only the controls belonging to the group.

The Search Text function will search one or more words entered in both the name and description fields.

When a control is selected, all the organisation units using that control will be listed.

Deactivating a Control

To deactivate a control, un-tick the Active button and click Save Data. Deactivated controls are not deleted and can be found by clicking the Inactive button just below the Search button. To reactivate a control, select it from the Inactive list, tick the Active box and click Save Data.

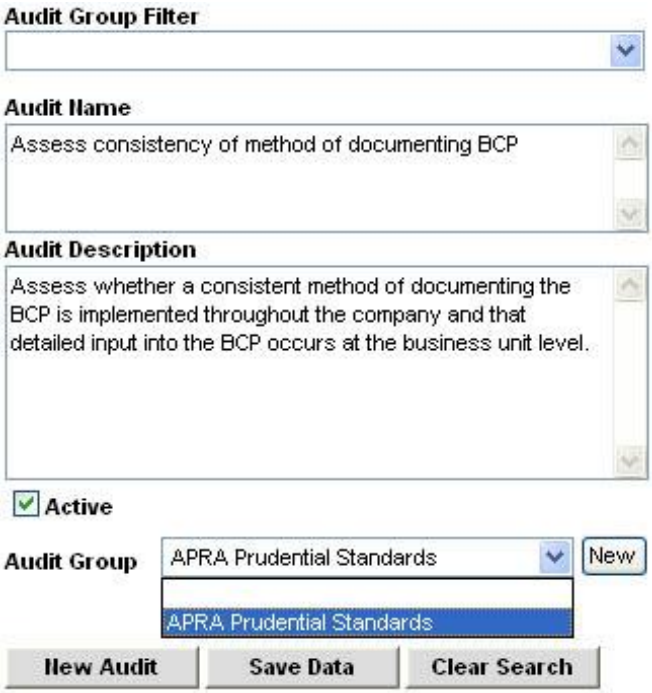
The Audit Library

The Audit Library stores all the audit procedures identified for the organisation. If you have created more than one company, the Audit Library is shared amongst all the companies.

The Audit Library is accessed by clicking the Audit link in the Library.

Creating a New Audit

To create a new audit, click the New Audit button, enter a short name for the audit and a full description of the audit.



You may assign a group for the audit to categorise it for easy searching at a later stage. If the group is not on the list, click the corresponding New button and enter the new group.

Click Save Data when data entry is completed, otherwise the data entered will be lost.

Modifying an audit

To modify an audit, select the audit from the list, make the required changes and click the Save Data button. Once an audit has been used in Risk Evaluation, it is recommended that you do not modify the audit except to correct typographical errors. Refer to Changing System Library File Data for more information.

Finding an Audit

To find an audit quickly, you may use the Group Filter or the Search Text functions. To use the filters, select a group and the list of controls will be filtered to show only the audits belonging to the group.

The Search Text function will search one or more words entered in both the name and description fields.

When an audit is selected, all the organisation units using that audit will be listed.

Deactivating an Audit

To deactivate an audit, un-tick the Active button and click Save Data. Deactivated audits are not deleted and can be found by clicking the Inactive button just below the Search button. To reactivate an audit, select it from the Inactive list, tick the Active box and click Save Data.

External Document Management

The External Document Management function allows you to view all external documents attached within the system.

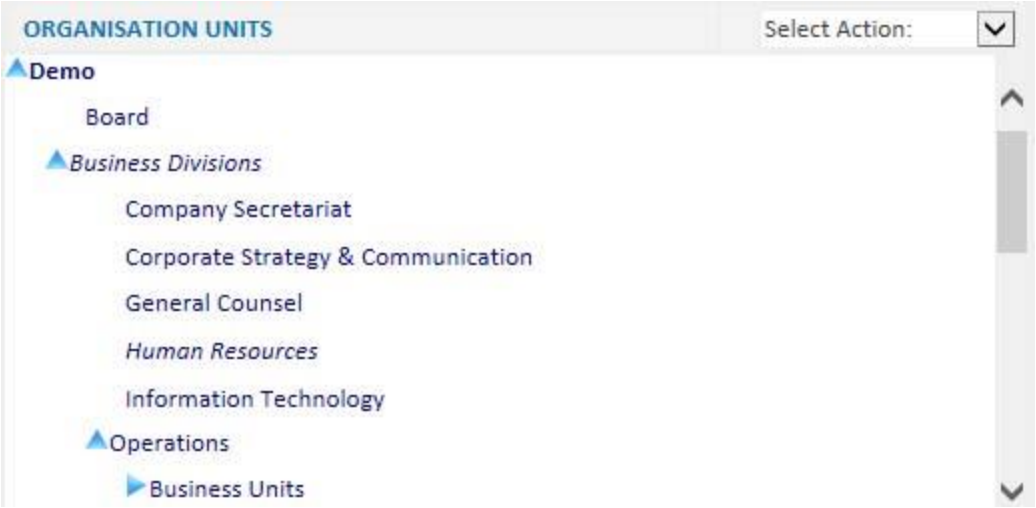
		Type	Document Name	Organisation Unit	Risk Name	Control Name	Audit Name	Audit Program	Incident	Compliance Item
Open	Delete	Audit Program	20060420.reg	Demo >> Group Executive	Breach of risk management guidelines	Organisations utilises AS/NZS 4360:1999	Confirm that the organisations utilises AS/NZS4360	Comprehensive Audit of Demo Company		
Open	Delete	Audit Program	Payment Listing	Demo >> Finance	Material misappropriation of funds	Two cheque signatories at all times	Ensure that two cheque signatories approved the payment	Comprehensive Audit of Demo Company		
Open	Delete	Control	RiskLibrary.txt	Demo >> Board	Board does not comply with ASX disclosure requirements	Each board member completes quarterly attestation				
Open	Delete	Incident	Corporate Policy.doc	Demo >> Business Divisions >> Products and Services					T0001-Gas poisoning	
Open	Delete	Incident	Photo of defective machine	Demo >> Finance					CYW005-Injury by flying object	
Open	Delete	Org Unit	Dummy BCP.doc	Demo >> OH&S						
Open	Delete	Risk	RiskLibrary.txt	Demo >> Board	Board does not comply with ASX disclosure requirements					
Open	Delete	Compliance	Dummy BCP.doc	Demo >> Business Divisions >> Company Secretariat						Quarterly APRA return

You may open a document by clicking the Open link in front of it or you may choose to delete the document from the server **permanently** by clicking the Delete link.

Note that if a document is attached to multiple items, all occurrences of the deleted document will be removed from the system.

Risk Evaluation

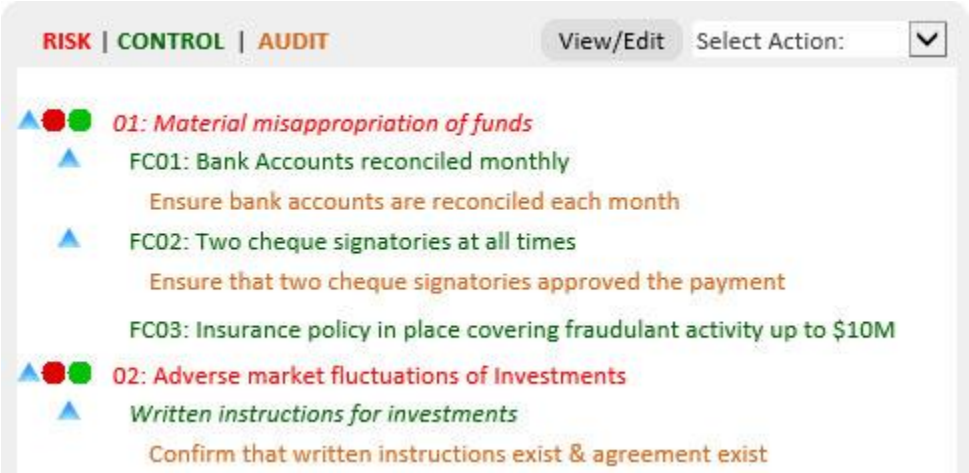
Start by selecting an organisation unit you would like to evaluate.



Once an organisation unit is selected, the risks, controls and audit procedures attached to the organisation unit, if any, will be displayed in the Risk Control Audit panel.

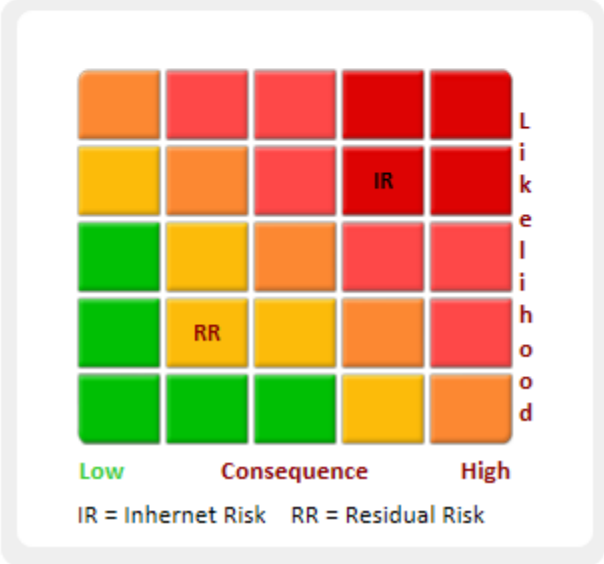
The Risk/ Control / Audit Selection Panel

The relationship between **Risk**, **Control** and **Audit Procedures** are shown in a relational tree structure and is coloured coded for easy reference.



Click a Risk, Control or Audit Procedure to view the summary evaluation result.

Tip: An item in *italics* means there are attached documents to the organisation unit, risk, control or audit.



To expand or collapse individual items on the tree, click the small arrowheads before the risk or control items.

To edit the risk, click the View/Edit button or select Edit from the Risk/Control/Audit panel Select Action dropdown list.

Attaching a Risk

Risks can only be attached to organisation units. To attach a risk to an organisation unit, select the organisation unit and select Attach Risk from the Risk Select Action dropdown list.

When the Risk Selection page appears, select a risk from the list of risks in the Risk Library.

You may use the Search or Filter functions to help you find a risk quickly.

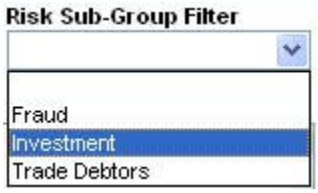
To search, type in the search text into the Search Text field and click the Search button.

To clear the search and list all risks in the library, click the Clear Search button.

If the risks have been grouped in the Risk Library, you can filter the risks according to groups and sub-groups.

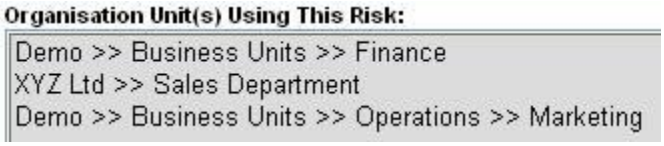
Select a group from the Risk Group Filter dropdown list:

If there are sub-groups within the group, they will be shown in the Risk Sub-Group Filter dropdown list:



To clear the filters, click the Clear Search button.

When a risk is selected, the organisation units within the system that have the risk attached will be shown:



Once a risk is selected from the list, click the Select button to attach the risk to the organisation unit.

You can cancel the attach risk operation by clicking the Cancel button.

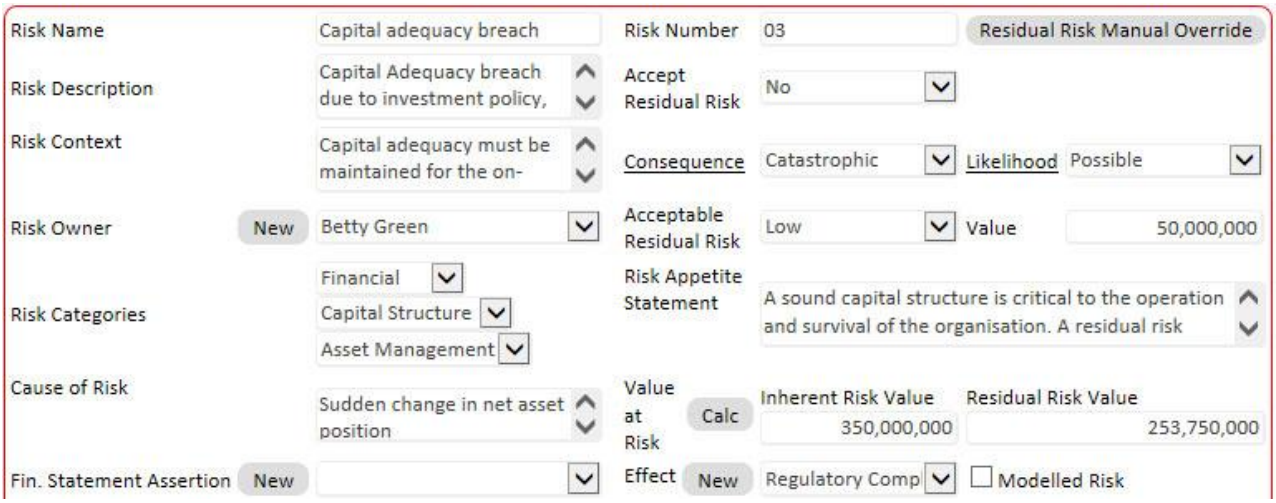
If you want to attach more than one risk, hold down the Shift or Ctrl key while selecting the risks. If you hold down the Ctrl key, clicking a risk will add that to the risks to be attached. If you hold down the Shift key, all risks between the first selected risk and the newly selected risk will be selected for attachment.

If you want to add a new risk to Risk Library and attach it, click the Quick Add button (only available if you have Library Maintenance authority), type in a new risk name and description and click the Select Risk button.

Enter Risk Information

On the Risk/Control/Audit selection panel, select the risk you want to change and select Edit from the Select Action dropdown list.
Tip: Risks are Red in colour.

Enter the appropriate data in the risk details panel:



Data fields:

- Risk Name - a short description of the risk. Cannot be changed here. See Changing Library Data
- Description of Risk - full description of the risk. Cannot be changed here. See Changing Library Data.
- Risk Context – definition of the external and internal parameters that organisations must consider when they manage risk.
- Risk Owner - the person responsible for managing the risk.
- Risk Category - Select up to three levels of risk categories for the risk. The hierarchical risk categories are set up in the Administration module by the system administrator.

- Cause of Risk - The factor or event that gives rise to the risk. More than one cause can be entered.
- Risk No: A reference number for the risk.
- Accept Residual Risk - whether the residual risk, if any, is accepted by the operation. A residual risk may be accepted by the operation based on the materiality of the consequence and offsetting influence of other controls. A reason should be given for accepting the residual risk. Click the Reason button to enter the reason. Where a residual risk is not accepted, an action plan should be entered by clicking the Action Plan button.
- Consequence - select an appropriate consequence level from the dropdown list. Click the link to open the Risk Consequence Rating Guide if one is available. A Risk Consequence Rating Guide, which is used to help users determine the consequence consistently, can be created using the Administration function.
- Likelihood - select an appropriate likelihood level from the dropdown list. Click the link to open the Likelihood Rating Guide.
- Value at Risk (Inherent Risk Value) - the dollar value of the inherent risk.
- Value at Risk (Residual Risk Value) - the monetary value of the risk after application of the implemented controls. You can let the system calculate the residual risk value by clicking the Calc button when an inherent risk value has been entered. You can calculate the value yourself using other methods and enter it manually.
- Acceptable Residual Risk (Risk Appetite) - Select an acceptable residual risk level for this risk and/or enter the monetary value of the residual risk that the organisation is willing to accept for this risk. This is a reflection of the organisation's risk appetite.
- Risk Appetite Statement - When a risk category is selected from the Risk Categories dropdown lists and if a risk category has a suggested risk appetite statement (entered via the Risk Category Maintenance function in the Administration Module), the suggested risk appetite statement will be shown. The user can modify the suggested statement to suit the nature of the specific risk. The Risk Appetite Statement should support the Acceptable Residual Risk level.
- Financial Statement Assertion: The assertion made in the financial statements that may be impacted by the risk. A new assertion can be added by clicking the New button above the dropdown list.
- Effect - a description of the effect of the risk for reporting purposes. A new effect can be added by clicking the New button next to the dropdown list.
- Comment - any notes and comments on the risk that are not captured elsewhere.

- Action Plan - an action plan can be attached to the risk. Click the button to enter the action plan. If the button label is red in colour, one or more action plan is attached.
- Response - the response strategy if the risk eventuates. If the button label is red in colour

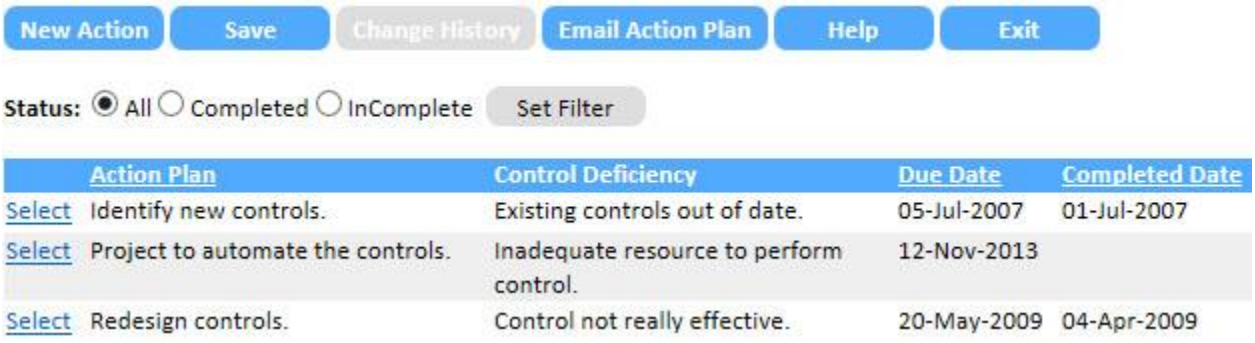
The result of the risk evaluation is summarised in real time for both the current risk and the targeted risk (if all proposed and agreed controls were implemented). Click the Current Risk or the Targeted Risk button to view the respective results.

The blue line on the Heat Map shows the Acceptable Residual Risk level, that is, acceptable if the residual risk (RR) is to the left of the blue line and unacceptable if it is to the right of the line.

Other functions

Action Plan

Click to enter an action plan. An action plan is usually required when the existing controls are not adequate and something needs to be done.



Click New Action to create a new plan or select an existing action plan from the list.

Implementation Due Date: The date the action plan is due for completion. The workflow system will track the item with reminder emails.

Implementation Date: The date the action plan is actually implemented. Entering a date here will stop the workflow system from tracking the item.

Responsible Officer: The person or office responsible for taking the action.

Control Deficiency: A description of why the action plan is needed.

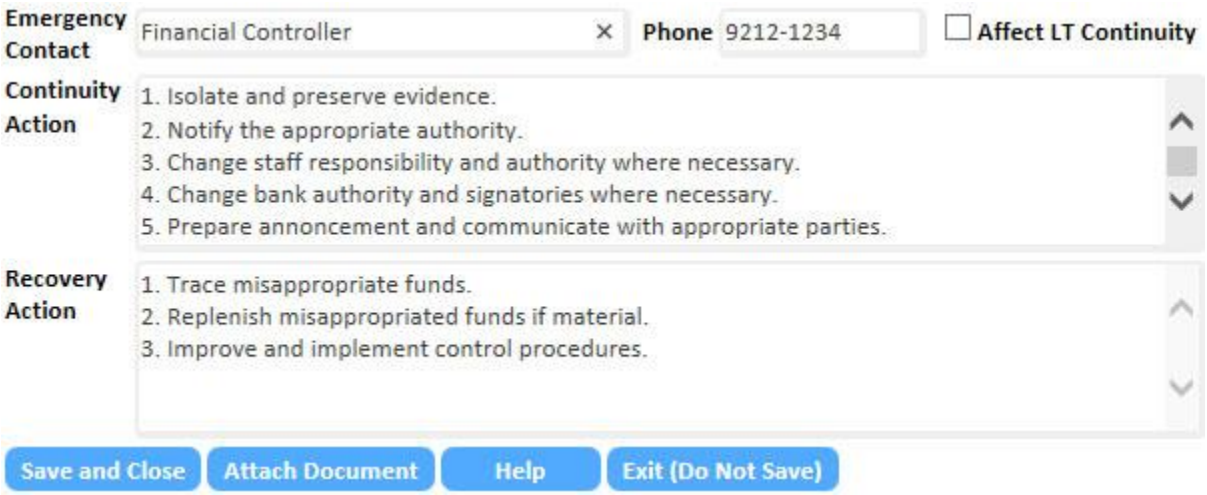
Action Plan: A description of what needs to be done.

Reason for Change: A description of the reason for updating data in the Action Plan.

A history of changes to the action plan is kept by the system. To view the history, click the Change History button. A report listing all previous versions of the action plan will be displayed in a new Internet Explorer window.

Response

Click to enter a response plan. A response plan contains information as to what needs to be done in the case the risk eventuates. If used consistently, this can form the basis of the organisation's Business Continuity and Business Recovery Plans.

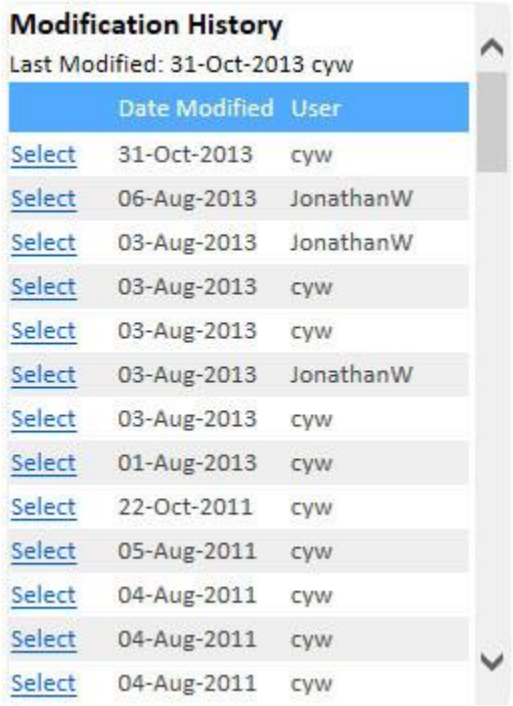


If the risk may affect the long term continuity of the organisation, tick the Affect LT Continuity box. You may attach external documents by clicking the Attach Document button.

Note: A recovery action relates to what needs to be done to restore the business to its normal status before the risk eventuated. A continuity action relates to what needs to be done to carry on the business before the recovery action is completed.

View History

All histories of risk evaluation information are kept by the system. You may view what the risk evaluation data was at a point in time by clicking the View History button:



Selecting an item from the Modification History list will show the risk evaluation data as at that particular point in time.

Clicking the risk on the Risk/Control/Audit panel will restore the system to normal operation instead of the history view.

Attaching a Control

Select a risk from the Risk/Control/Audit selection panel and click the Attach Control button. This will take you straight to the Control Library.

Select a control from the Control Listing and click the Select Control button. You may select more than one control by holding down the Ctrl or Shift key while selecting controls to be attached.

If you want to add a new control to Control Library and attach it, click the Quick Add button (only available if you have Library Maintenance authority), type in a new control name and description and click the Select Control button.

This will take you straight back to the Risk Evaluation Screen.

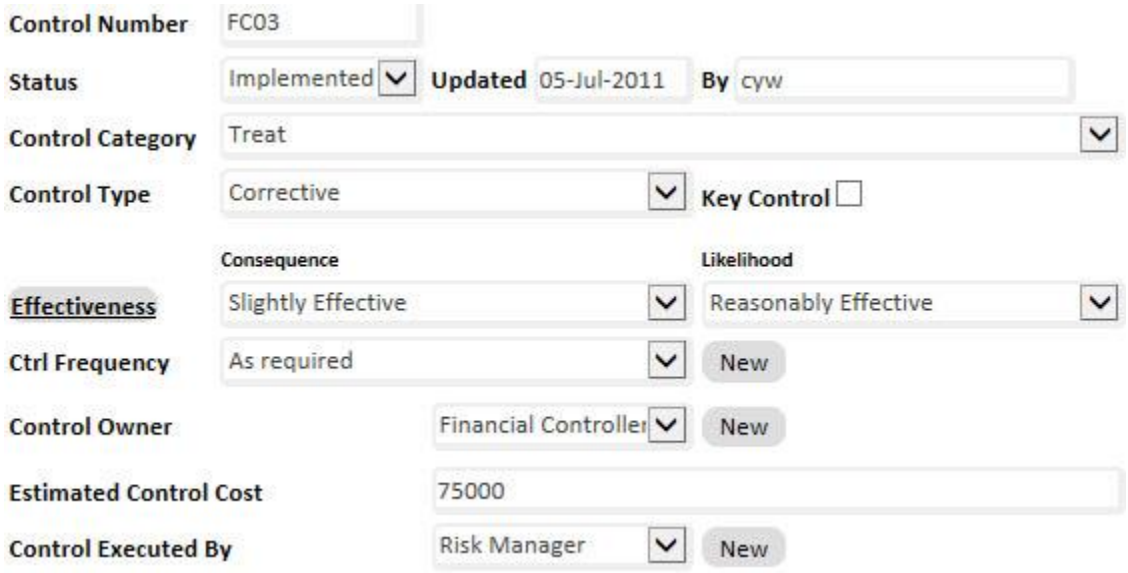
Enter Control Information

Select the control from the Risk/Control/Audit selection panel and select Edit from the Select Action dropdown list.

Tip: Controls are Green in colour.

All controls attached to the selected risk are listed and you can switch to another control by clicking the Select link.

Data Fields:



Control Name: A short name to describe the control. Cannot be changed here.

Description of Control: A full description of the control mechanism or procedure. Cannot be changed here.

Control Number: A reference number for the control (optional). The control list is sorted according to the Control Number. If not entered, the list will be sorted according the oldest added item first.

Control Status: Select the status of the control from the dropdown list. If the Status is other than 'Implemented', the inherent risk will NOT be affected by the control.

Control Status Date: The data the control status was last changed.

Status Updated By: The person who last updated the control status, cannot be modified.

Control Category: Select a control category from the dropdown list.

Control Type: Select a type of control from the dropdown list.

Key Control: Tick if it is a key control.

Control Effectiveness: Select an appropriate control effectiveness level for the risk consequence and the risk likelihood from the dropdown list.

Ctrl Frequency (Control Execution Frequency): How often is the control executed?

Control Owner: The person who has the overall responsibility for the control.

Estimated Control Cost: (Optional) The annualised cost of the control.

Control Executed By: The person responsible for executing the control.

The effectiveness of the controls for a risk is combined using a statistical algorithm weighing the consequence and likelihood of the risk and the effectiveness of the control over the consequence and likelihood of the risk for each control to arrive at the overall control level for the risk which is shown on the Risk Evaluation screen.

If the Effectiveness of Control is not Very Effective, that means there is a residual risk after the control is applied. When this happens, the system will ask whether you want to accept the residual risk. If you accept the residual risk, you will be asked to enter the reason why you accept it. If you do not accept the residual risk, you should enter an action plan to further treat the risk until it becomes acceptable.

Effectiveness of Control (Control Level)

GuardianERM.Net compares the effectiveness of control against the corresponding risks. The control level can be viewed as a number from 0 to 5 and is a measure of the effectiveness of the control as compared to the risk:

Level	Effectiveness	% Equivalent
0	Not Effective	0%
1	Slightly Effective	20%
2	Somewhat Effective	40%
3	Reasonably Effective	60%
4	Mostly Effective	80%
5	Very Effective	100%

Alternatively, you may assign a percentage effectiveness equivalent to the control level as above. For example, Level 4 means the control is effective 80% of the time.

Level 0 can be used to indicate that the control has not yet been rated.

Risk Evaluation Summary

As you enter data into the GuardianERM.Net system, the results are calculated and shown as soon as you save the data:

GuardianERM.Net uses a five-point scale, that is, items are scored from 1 to 5.

Item	Value	Score
Consequence	Not available	0
	Insignificant	1
	Minor	2
	Moderate	3
	Major	4
	Catastrophic	5
Likelihood	Not available	0
	Rare	1
	Unlikely	2
	Moderate	3
	Very Likely	4
	Almost Certain	5
Effective Control	Not Effective	0%

Slightly Effective	20%
Somewhat Effective	40%
Reasonably Effective	60%
Mostly Effective	80%
Very Effective	100%

The Effective Control is calculated using a weighted average of the effectiveness of each control against the impact and likelihood levels of the risk.

The Targeted Residual Risk shows the effect of proposed and agreed control if they were implemented.

Attach an Audit Procedure

Select a control from the Risk/Control/Risk selection panel.

Click the Attach Audit button. This will take you straight to the Audit Library.

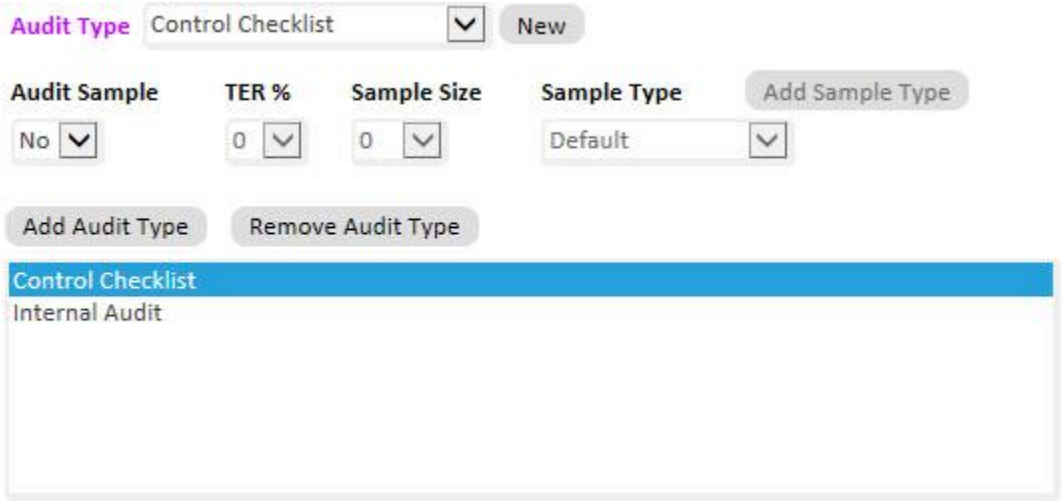
Select an audit procedure from the listing displayed and click the Select Audit button. You may select more than one audit procedure to be attached by holding down the Ctrl or Shift key while selecting audit procedures to be attached.

This will take you back to the Risk Evaluation Screen.

Enter Audit Procedure

Select an audit procedure on the Risk/Control/Audit selection panel and select Edit from the Select Action dropdown list.

Data Fields:



Audit Type: Select the type of audit from the list and click Add Audit Type to add this audit type to the audit procedure. If you want to create a new audit type click the New button next to the dropdown list. An audit procedure can be performed by different people in different types of audits, e.g. internal audit, quality audit, peer review and self- assessment. GuardianERM allows an audit procedure to have multiple audit types.
Audit Sample: Whether the audit procedure requires testing a sample of documents or transactions.

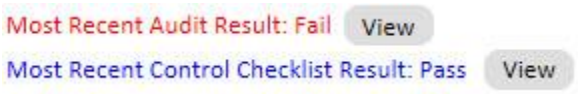
Tolerable Error Rate: When Audit Sample is 'Yes', the maximum error rate in percent that can be tolerated before the control being tested is considered to have failed. The TER is not applicable where no audit sample is used.

Sample Type: The source of the audit sample. This is used for creating separate audit work paper schedules for convenience of recording audit sample test results. For example, if you are testing payments, the sample type may be invoices or cheques.

Sample Size: The required sample size for this audit procedure. This value is copied to future audit programs created but can be modified at the audit program level.

Functions:
View History: View a history of changes for the various audit types of the audit procedure.

Save Data: Save changes to the data.
The system also displays results from the latest audit or control checklist.



Click the View button to view the details of the audit or control checklist results.

To Add an Audit Type:

1. Select an audit type from the dropdown list. If the desired audit type is not on the list, create one by clicking the New button next to the dropdown list.
2. Click the Add Audit Type button. The selected audit type will appear in the Audit Type List.
3. Click the Save button.
4. Configure the sampling details if required for the audit type.

Note:
Tolerable Error Rate – the percentage of errors allowed in the sample.
Sample size – the suggested size of the sample to test, it can be overridden in the audit function.

Sample Type – You may segregate different types of sample so they appear on different audit testing work papers. E.g. you may want to separate invoice testing where you would select a sample of invoices and reconciliations where you would select a sample of periods of reconciliations. The use of Sample Type is optional.

Detach Risk, Control or Audit Procedure

To detach a risk:

Select a risk on the Risk/Control/Audit selection panel.

Select Detach Risk from the Select Action dropdown list. You are required to provide a reason for detaching the risk.

To detach a control:

Select a control from the Risk/Control/Audit selection panel.

Select Detach Control from the Select Action dropdown list. You are required to provide a reason for detaching the control.

To detach an audit procedure:

Select an audit procedure from the Risk/Control/Audit selection panel.

Select Detach Audit from the Select Action dropdown list. You are required to provide a reason for detaching the audit.

Note
When you detach a risk – all controls and audits attached to the risk will be automatically detached as well.

When you detach a control – all audit procedures attached to the control will be automatically detached as well.

Attach, View or Remove External Documents

On the Risk Evaluation screen, select any organisation unit, risk, control or audit you want to attach external documents to and select External Document from the Selection Action dropdown list.

Note: External documents can be attached from various modules of the system. The procedure is the same.

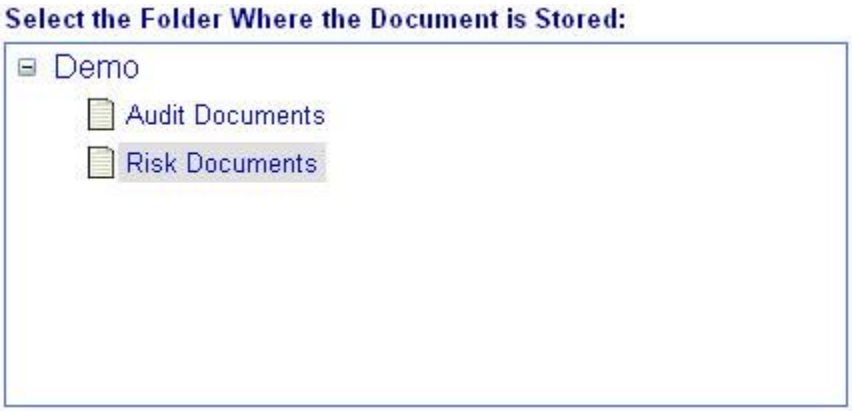
When you open the Attach Document page, the Attached Documents List shows, if any, all the documents attached.

The description of the document is shown when a document is selected. To **open the document for viewing**, click the View button. You have a choice of either saving the document to your computer or open the document. Please note that the selected document is downloaded to your computer before it is opened. A large document will take a longer time to download than a small document. Any changes made to the document can only be saved to your computer. The document on the server remains unchanged. To change the document on the server, you have to upload the changed document on your computer to the server.

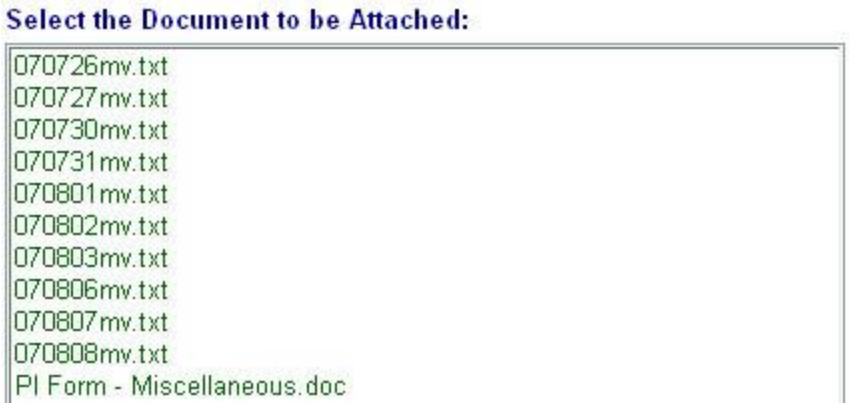
To **detach** a document, select it from the list and click the Detach button.

To **attach** a document, click the Attach button, the select document boxes will appear.

Select a folder on the server where documents are stored from the list:



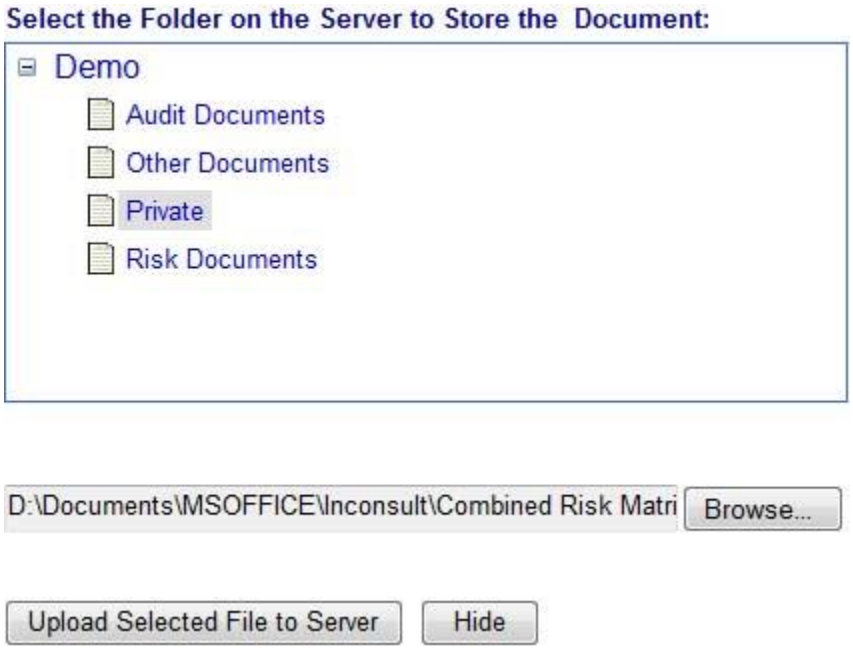
The documents that have been uploaded to the selected folder on the server will be shown:



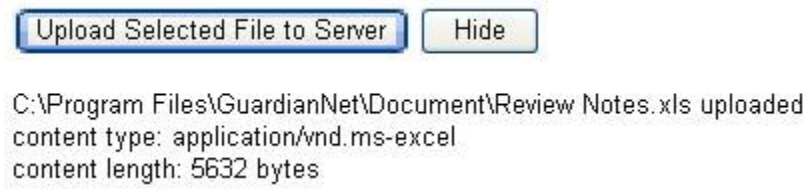
Select the file you wish to attach and click the Select button. If the document is stored on your computer and has not been uploaded to the server, you need to upload the document to the server first before it can be attached.

To **upload** a document to the server:

Click the Attach button to show the Select Document boxes then click the Upload button:



Select a folder on the server to store the document. If the **Private folder** is selected, after the document is uploaded and attached, the document will not be listed for attachment anymore. It will be shown as a document attached and users authorised to access the item the document is attached to can still open the document for viewing as usual. The Private folder is used to upload sensitive documents such that users cannot list its contents, attach a sensitive document and view it.
Click the Browse button to select the document to be uploaded on your computer.
Click the Upload Selected File to Server button to upload the document. When the upload is completed, the upload information will confirm the successful upload:



Check that the content length matches the size of the document to ensure the complete document is uploaded.

If an error message appears, the upload has not been successfully completed and you will have to try again.

To delete files that have been uploaded to the server, contact your system administrator.

Once a document is uploaded, it will be shown on the Select Document list and can be attached.

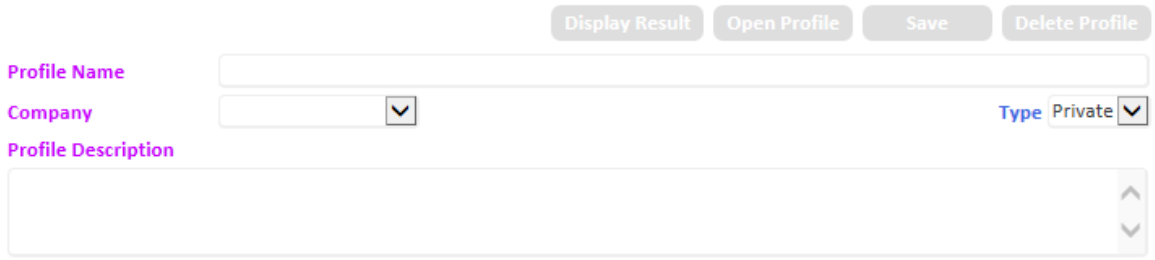
Risk Profiler

The Guardian Risk Profiler provides real time information on risks that are selected according to a user's specifications.

There are two types of risk profiles you can create:

Public - can be used or modified by any Guardian user.
Private - can only be used or modified by the person creating the profile.

To view the risks for a profile, click the Select link to select the desired profile from the list and click the Display Result button.
To create a new risk profile, click the New Profile button.



Fill in the details and click Save.

To modify an existing profile, click the Open Profile button.

A risk profile consists of three parts:

- The selection criteria;
- Organisation units; and
- Data fields to be included.

Selection Criteria:

To configure the selection criteria, select the data field, operator and criteria for risks to be included in the profile. Click the Add Field button to add another criteria. If you have more than 1 criterion, be careful with the AND and OR selection as they are not the same and will produce different results.

For example, if we are selecting balls from a box which contains large and small balls in either red or green:

Select all red OR large balls will select all red balls whether they are large or small and also all large balls whether they are red or green. The only balls not selected are the small, green balls.

Select all red AND large balls will select all red balls that are large only.

Select all red OR green balls will select all balls in the box.

Select all red AND green balls will select none as the balls are either red or green but never both.

Organisation Unit:

Tick the organisation units to be included in the profile.

Data Field to be Included:

Tick the data fields that you would like to be included and then click the left-to-right arrow  . The selected fields will be shown on the right-hand side box.
To remove a selected field, tick the field and click the right-to-left arrow.
To move a selected data field up or down (which determines the order the data field appears on the report) select a field and click the Up or Down arrow  .

You can preview what the report looks like by clicking the Preview Result button.

Click the Save Criteria button to save the profile.

Note: You do NOT have to worry about the sort order of the data as you can click the underlined header in the result display to sort the data. Sorting is not available in the preview page.

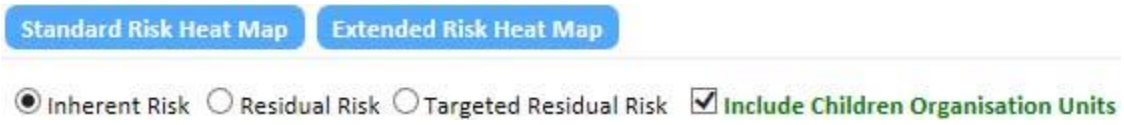
	Organisation Unit	Risk Name	Inherent Risk	Residual Risk
Select	Demo >> Business Divisions >> Operations >> Claims Management	Risk of incorrect benefit payments	5 - Extreme	3 - High
Select	Demo >> Finance	Adverse market fluctuations of investments	5 - Extreme	4 - Very High

To view the risk profile, click Display Result. Click the Select link to view details about the risk.

Risk Heat Map

The Risk Heat Map is an overview of the distribution of risks according to the risk level across an organisation. It also allows you to interactively drill down to different levels of the organisation with direct links to the evaluation details of a risk.

You can choose to view the Inherent, Residual or Targeted Residual (residual risks after all proposed and agreed controls are implemented) risks:

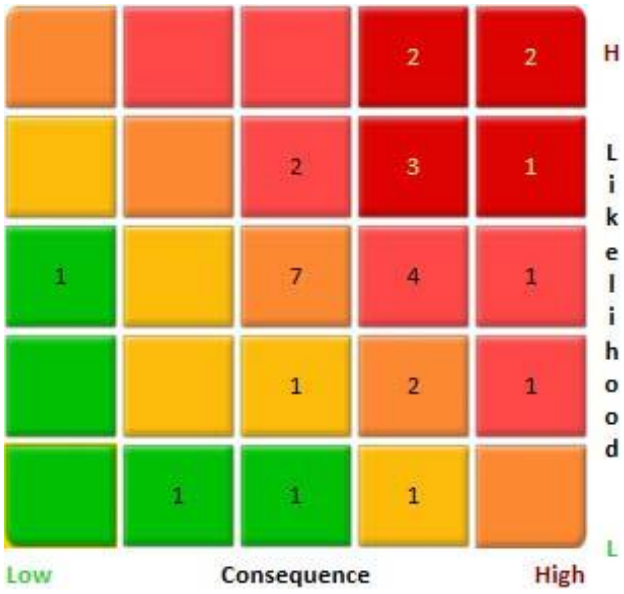


Select an organisation unit from the hierarchical organisation tree:

Note that when an organisation unit is selected, all the risks of the selected organisation unit and its children units will be **included** in the heat map unless the Include Children Organisation Units box is not ticked (which will then show only the risks attached to the selected organisation unit).

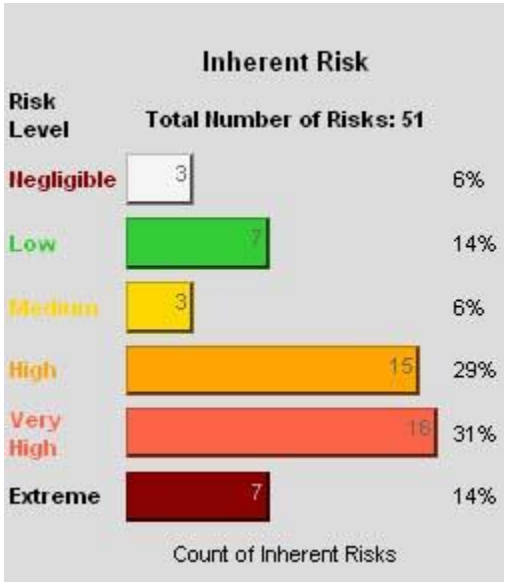
You may filter the risks by risk categories by selecting the desired risk categories from the dropdown lists:

The risk concentration map shows the number of inherent or residual risks in each level of risk consequence and likelihood:



(The consequence and Likelihood levels are expressed from one to five, one being the lowest and five being the highest)

The distribution of the risks is also summarised in the risk level map:



When a cell in the risk concentration map is clicked, the name of the risks and the organisation units they attached to are shown in the bottom panel. You may view the details of the risk evaluation by clicking the Select button:

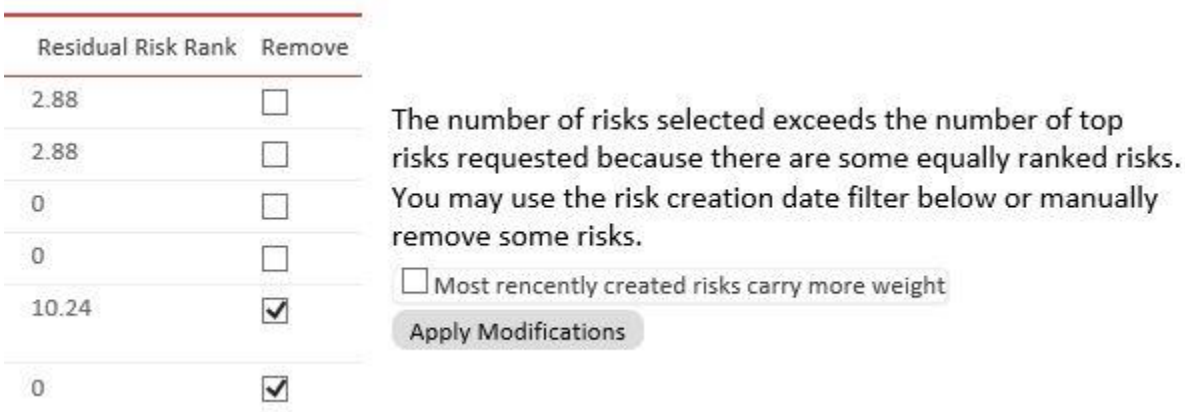
Organisation Unit: Demo. Impact: 4, Likelihood: 4 [Click the Detail Button to view detailed risk evaluation information.]

Detail	Organisation Unit	
Detail	Demo >> Group Executive	Board does not comply with ASX dis
Detail	Demo >> Business Units >> Operations >> Claims Management	Risk of incorrect benefit payments
Detail	Demo >> Business Units >> Products and Services	External Pushback - Risk of Non Acc
Detail	Demo >> Business Units >> Finance	Material misappropriation of funds

You can view the risks with high risk levels using the Top Risks filter.

Enter the number of top risks you would like to view and click the Go button.

If a number of risks have the same rating such that the system comes up with more than the desired number of top risks, you may either tick the risks you want to remove from the list or assign more weight to the more recently created risks by ticking the "Most recently created risks carry more weight" box.



Extended Risk Heat Map

The Extended Risk Heat Map provides a more in-depth and comparative analysis of risks compared to the Standard Risk Heat Map. Only risks for the selected organisation unit will be shown. Risks belonging to the children organisation units will **NOT** be shown. The numbers on the heat map are the risk numbers. If you have not entered a risk number for a risk, a GuardianERM generated number will be shown. Corresponding risk information for each of the risk numbers are shown below the heat map.

There are several views available:

- Inherent Risk - Only shows the inherent risks for the selected organisation unit.
- Residual Risk - Only shows the residual risks for the selected organisation unit.
- Inherent vs Residual Risks - Shows both the Inherent and residual risks for the selected organisation unit on the same heat map.
- Inherent Risk Date Comparison - Shows the current inherent risks and the inherent risks on or the closest date before the date specified for the selected organisation unit.
- Residual Risk Date Comparison - Shows the current residual risks and the residual risks on or the closest date before the date specified for the selected organisation unit.
- Click the Detail link for the risks listed to view the risk in the Risk Evaluation mode.

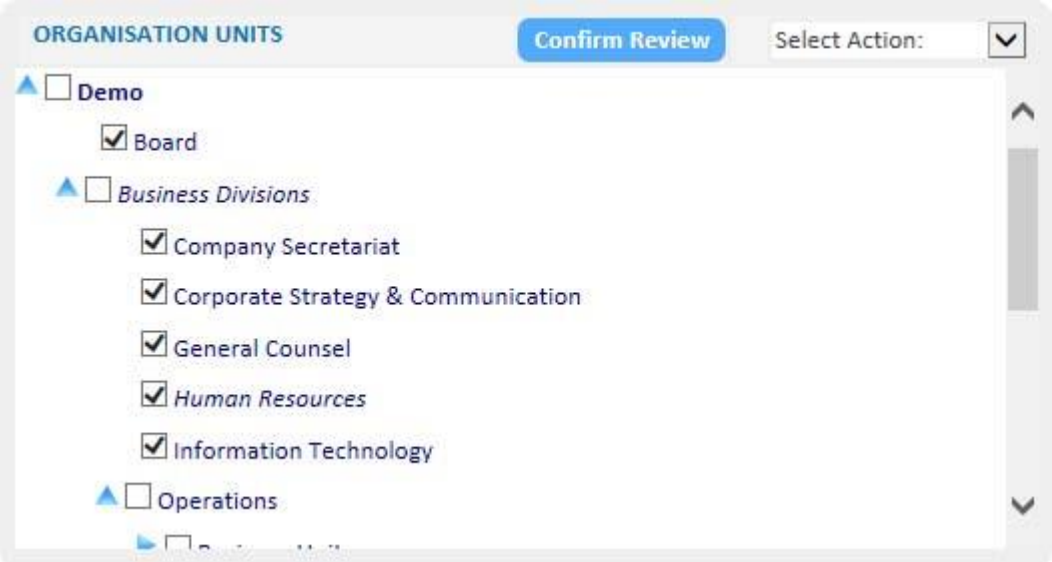
The heat map can be printed to a PDF file or exported to Excel by clicking the respective buttons.

Risk and Control Review

No matter how accurately the organisation, risk and control information is prepared, its accuracy and relevance will reduce over time.

To ensure that the risk evaluation information is up-to-date, GuardianERM.Net has a built-in risk and control review function to record the currency of the information in the system.

On the Risk Review screen (access by clicking Risk Management - Risk Review on the Main Menu), you will find that the Risk Review screen is exactly the same as the Risk Evaluation screen except for a tick box in front of each organisation unit.



To perform a risk evaluation review:

1. Select an organisation unit to be reviewed and check that all data in relation to the organisation unit is correct. Make changes where required.
2. Select a risk on the Risk/Control/Audit panel.
3. Review the data of the risk, making changes where required.
4. Select the control attached to the risk. Review and make changes where required.
5. Select the audit procedure attached to the controls and review its contents.
6. Select the next risk/control/audit procedure item on the risk tree and repeat steps 3 to 5.

7. When all the risks, controls and audits for the organisation unit have been reviewed, click the tick box in front of the organisation unit you have reviewed.
8. All children organisation units must be reviewed and ticked before the parent unit can be ticked.
9. To save the review tick boxes, click the Confirm Review button.

When you click a check box, a warning dialog box will appear to remind the user of the responsibility of signing off the review.

Note: Once a check box is ticked and the review confirmed, it cannot be 'un-ticked'. The system will reset the tick boxes automatically according to the system workflow settings or manually by the system administrator.

Tip: You can (and should) review and update information when changes are known. There is no need to wait for the system prompt. The reminder email, workflow messages, checkboxes, etc. are only there to help the organisation manage the currency and relevance of its risk management information. When you update the information in the normal course of business, you do not have to use this function (use Risk Evaluation instead).

Attestation

In organisations where evidence of discharging management responsibility in risk management is important, GuardianERM offers an attestation function in addition to the Risk and Control Review.

To use the Attestation function, you must first set up the Attestation Settings in the Administration Module.

The colour of the Attestation button shows the phase of the attestation cycle.

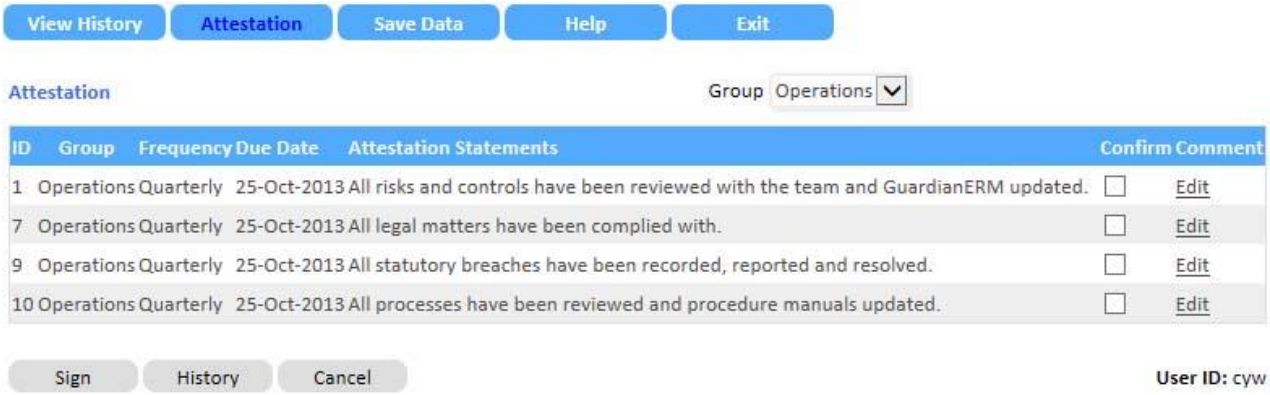
White - Attestation is not due for action. You may view the attestation statements but they cannot be completed.

Attestation Blue - Attestation is ready for completion.

Attestation Red - Attestation is overdue.

If no attestation statements have been assigned to this organisation unit, the button will not be displayed.

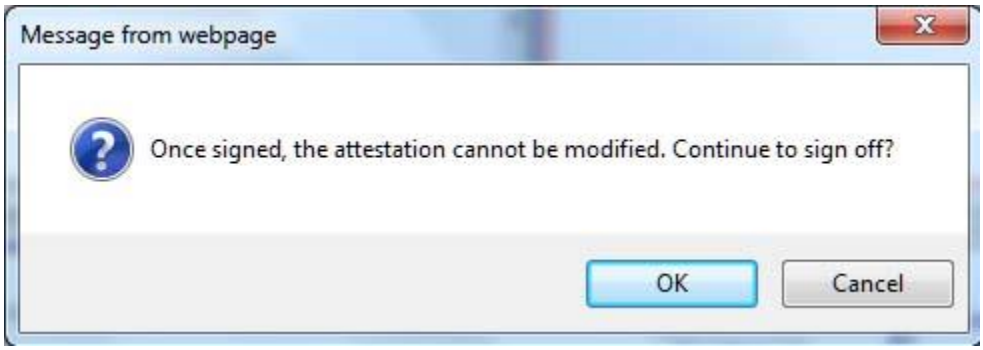
To sign off the attestation statements, click the Attestation button.
Select the Group from the dropdown list. An organisation unit may have more than one group of attestation statements to complete.



To sign off, read each statement and tick the Confirm box. If you cannot attest to the statement in accordance with the preamble, do NOT tick the confirm box.

A comment for each item can be entered by clicking the Edit link under the column Comment. If the Confirm box is not ticked, a comment is compulsory.

Click the Sign button to sign off the attestation. A message will pop up:



Click OK to sign off or Cancel to make changes. Once signed off, the attestation cannot be modified.

Click the History button to view the history of attestation for this organisation unit.

Audit

An audit in GuardianERM.Net refers to checks and confirmations that the controls as documented are actually working. It could be a formal audit, informal peer reviews, self-assessments by management or control checks by operational staff.

GuardianERM.Net has the flexibility to create and manage simple control checklists through to comprehensive internal audits with built-in audit working papers to fully documented audits on-line.

Prepare Audit Program

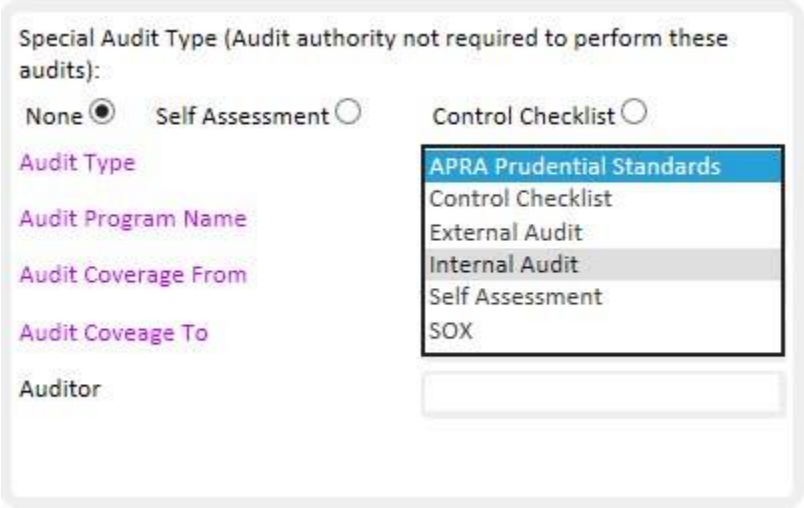
Security note: You need to have Audit Write security access to prepare an audit program except for Self-Assessment and Control Checklist (which only require Organisation Write access).

The Prepare Audit Program function is used to create an audit program. An audit program must first be prepared before an audit can be performed. An audit program is a collection of audit procedures to be performed during an audit. Usually, an audit program will cover an organisation unit, a function or a special topic of interest (e.g. review fire protection equipment of all offices, factories and warehouses globally).

To start, select the company from the dropdown list:

The Organisation Unit panel will display the organisation units for the selected company.

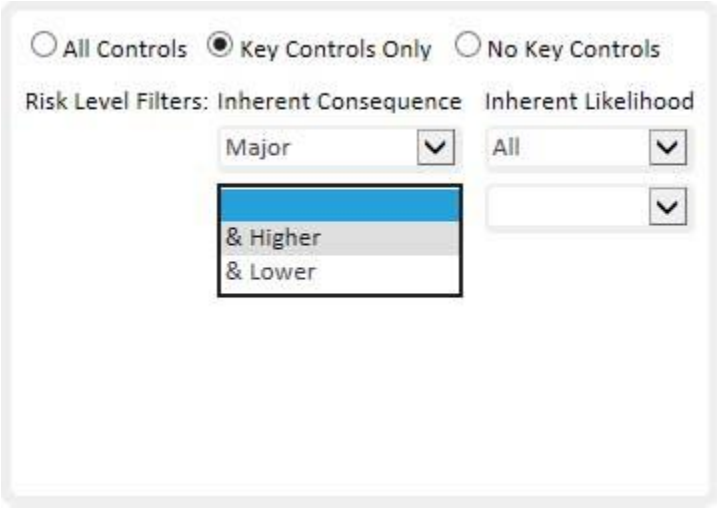
Select the type of audit. Only one type of audit can be selected for one audit program.



To prepare a special audit program, select a Special Audit Type.
These audit programs are special because they do not require a user to have auditor access level and there is a shortcut access to a Control Checklist from the main menu.

Select the organisation units to be included in the audit program.

Determine whether you want to include only the key controls, no key controls only or all controls and optionally select the risk levels:



Click the Preview button to see what the audit program includes.

Selected Audit Program Details (All Controls)

Organisation Unit	Risk	Control	Key Control	Audit Procedure	Sample	Inherent Risk
Demo >> Finance	Capital adequacy breach	Board approved investment policy in place	Yes	Review Board approved investment policy	Yes	Major
Demo >> Finance	Material misappropriation of funds	Two cheque signatories at all times	Yes	Ensure that two cheque signatories approved the payment	Yes	Catastrophic
Demo >> Finance	Material misappropriation of funds	Insurance policy in place covering fraudulant activity up to $10M	No	Confirm risk margin determined having regard to uncertainties	No	Catastrophic
Demo >> Finance	Adverse market fluctuations of Investments	Investments are reconciled each month and verified by the Finance Manager	Yes	Ensure investments are reconciled each month	Yes	Catastrophic

If you are satisfied with the audit program, complete the rest of the details for the audit program:

Audit Program Name: A unique name given to the audit program. Duplicated names will not be accepted by the system.

Audit Coverage: Enter the start and end dates of the period the audit covers. The system date is defaulted to the English format, which is day/month/year. To avoid confusion if your system is set to a different date format, e.g. USA users, use the name of the month, for example, 8-Sep-2007 or Sep-8-2007. If the American short date format 9-8-2007 is entered, the system will interpret that as 9 August 2007 instead of the intended 8 September 2007. The Financial Year of the audit coverage is the financial year of the audit end date. For example, if the audit end date is 15-Sep-2008 and the organisation's financial year starts 1-Jul, then the financial year of the audit program is 2009.

Auditor: The person in charge of the audit. Auditors can be assigned to individual audit procedures within a program in the Enter Audit Results screen.

Click the **Save** button to save the audit program.

Note: To ensure the audit program covers all controls identified, run the Controls with No Audit Procedures report to identify recently created controls where audit procedures have not been attached.

Sample Testing

In compliance audit work, sample testing is a very commonly used technique.

In compliance work, we are mainly concerned with attribute sampling, that is, we select a sample of transactions and test certain attributes for true or false. e.g. the payment authorisation procedure is being adhered to, the report has been reviewed by the General Manager before being submitted to the board. If the selected sample passed the test (i.e. the error rate is below the Tolerable Error Rate), we will conclude that the population of transactions also passes the test and that the control is working.

If the sample fails the test, it may be prudent to extend the sample size in order to obtain more evidence that the control is not working before arriving at a conclusion.

Please note that the sample testing methodology assumes that the sample is randomly selected from the population. A meaningful conclusion may not be drawn if the sample is not randomly selected.

Perform Audit

Open Audit Program

Select Perform Audit from the dropdown menu.

Select a company from the Company dropdown list.

The Audit Program List will show all audit programs prepared for the selected company for the financial year selected. Change the financial year by selecting the desired year from the dropdown list or select All to show audit programs for all financial years. Click Set Filter to apply the filter:

Audit Program List

	Audit Program	Audit Type	Status	# Procedures	Auditor-In-Charge	Year
Select	Board and Finance Audit 2013	Internal Audit	In Progress	12		2013
Select	Board Audit 2013	Internal Audit	Completed	7		2013
Select	Finance audit 2012	Internal Audit	Completed	4		2013
Select	Comprehensive Audit of Demo Company	Internal Audit	In Progress	28		2013

You have a choice to show all the details as above (slower to load) or a simplified list (faster to load) by selecting or de-selecting the Show All Details box.

☑ Show All Details

You may filter the audit program list by selecting the Audit Status and the Financial Year and click the Set Filter button (Status ticked will be shown on the list):

Audit Status : ☑ New ☑ In Progress ☑ Completed ☐ Finalised

To further filter the audit programs, the Search Text function can be used. Enter a word (or part of it) or a phrase and click the Search button and the list will only show the audit programs containing the search text. Click the Clear button to clear the search.

Finalised [ ] Search Clear

Click the Select link to select the audit program. The Audit Areas within the selected audit program will be shown:

Audit Areas for Program: Comprehensive Audit of Demo Company

Audit Area	Audit Type	Cover From	Cover To	Last Updated	Status	Auditor	# Procedures	# Failed	Fail Rate %
Board	Internal Audit	01-Jan-2013	31-Mar-2013	06-Sep-2011	In Progress	CY Wong	7	2	29
Group Executive	Internal Audit	01-Jan-2013	31-Mar-2013	06-Sep-2011	In Progress	Judy Adams	8	3	38
Finance	Internal Audit	01-Jan-2013	31-Mar-2013	06-Sep-2011	In Progress	Tony Harb	5	4	80
Human Resources	Internal Audit	01-Jan-2013	31-Mar-2013	28-Feb-2008	In Progress	CY Wong	3	0	0
Claims Management	Internal Audit	01-Jan-2013	31-Mar-2013	06-Sep-2011	In Progress	CY Wong	5	0	0

Click the **Open Audit Program** button to open the audit program.

You may change certain properties of an audit program by selecting it and then clicking the corresponding button (Finalised audit programs cannot be modified):

Change Program Name	Change the name of the selected audit program.
Change Auditor	Change the name of the auditor for the audit program. Note: The Auditor-In-Charge can be changed by clicking the Notes button.
Modify Audit Program	Add audit procedures to the audit program.
Delete Audit Program	Delete the selected audit program. Can only apply to programs with New status.
Finalise Audit Program	Finalise a completed audit program. Requires Audit Sign Off system authority. If the CompulsoryAuditReview parameter is set to True in the System Reference Table, the audit must be reviewed before it can be finalised.
Roll Forward Audit Program	Make a copy of the selected audit program and specify new audit coverage dates.
Notes	Enter or modify additional notes in relation to the audit program.

Change Audit Program Name

To change the name of a previously prepared audit program, select the audit program from the Audit Program List and click the Change Program Name button.

Enter the new audit program name in the dialog box and click Save.

Note: Finalised audit programs cannot be changed.

Change Auditor

You may change the auditor for each of the audit areas. Select an area from the Audit Area list and click the Change Auditor button.

Enter the new auditor's name and click Save. Note that a finalised audit program cannot be changed.

Deleting an Audit Program

To delete an audit program prepared previously, click Perform Audit from the Compliance & Audit menu.

Select the audit program you want to delete and click the Delete button to delete the selected program.

Note: Only audit programs with 'New' status can be deleted.

Audit Program Status

An audit program can be in four stages:

1. New – the Result field on the Compliance Audit screen is blank for all records.
2. In Progress – at least one Result field in the audit program has information entered.
3. Completed – every Result field in the audit program has information entered and all audit work paper schedules are completed.
4. Finalised – after the Audit/Risk Manager "signs off" a completed audit program.

Note:

1. Management reports are not updated until the audit program is finalised.
2. You can make a program 'New' (so you can delete it) by deleting the content of all the comment fields in the audit program.

Enter Audit Results

NOTE: Finalised audits cannot be modified. You can only enter the Resolution Implemented Date and Implementation Notes. You need Audit Write Security access to enter audit results unless the program is a Self-Assessment or a Control Checklist which requires only Organisation Write security access. A message is shown at the bottom of the screen if the audit program opened is finalised or if you are not authorised to enter data.

Audit results can be entered directly into the Enter Audit Result screen or via the Workpaper screen.

The top section of the screen shows information from the risk evaluation:

Note: If the Result is RED in colour, it means that the audit resolution has not been implemented. The Resolution Implementation Details button will be RED as well when the audit procedure is selected.

Click Select on the Audit Procedure list to select the audit procedure and details relating to the audit procedure will be displayed.

If the audit procedure requires sampling, enter the sample size tested and the number of errors found:

The error rate is calculated by the system (press the Calc button).

If the audit procedure does not require sampling, click the Pass or Fail button:

If you need to clear the Pass/Fail buttons, click the Clear button.

If you have collected audit evidence that is filed externally (not in the GuardianERM.Net system), enter a reference in the Document Reference field to identify the location of the evidence for retrieval later on. If the evidence is in electronic format and is stored in GuardianERM.Net, click the button next to the Document Reference to open the Attach Document screen.

If the audit result is Pass, a message 'Effective and efficient' is automatically entered into the Audit Result/Comment field upon saving if the field is left blank. You can overwrite the message and put in your analysis of the result and or comments. This field is 255 characters long so be brief.

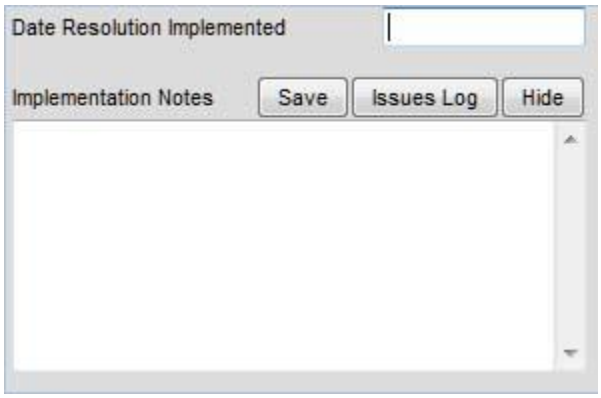
If there is anything to report, write it into the Audit Report field. You can enter unlimited text into this field. Tick the Report box will include this item in the audit report, otherwise, it will be stored in the audit program but will not appear on the audit report.

If the audit result is Fail, a message Failed will be entered in the Audit Result/Comment field upon saving if the field is left blank. You will be required to enter a resolution and a resolution due date before you can save the audit result. When the resolution is implemented, click the Details button to enter the implementation date and implementation notes (e.g. where actual control implemented is not the same as what was proposed).

You can also select a cause for the audit failure.

The selection items can be managed by clicking the Cause link. You can add, modify or delete items on the pop-up panel.

When a resolution is complex, you may use the Issues Log and link the audit to the issue by clicking the Issues Log button in the Resolution Implementation panel.



It may provide good reference if you enter a message like 'Managed in Issues Log" in the resolution field. When you click the Issues Log button and if you have already recorded an issue for this audit, the system will open the issue, otherwise, a new issue will be created.

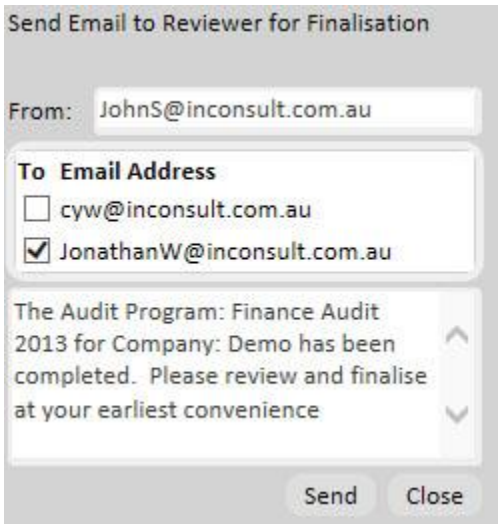
Select a Fail Alert Status to flag the seriousness of the failed control.

You may change the name of the person who performed the audit procedure.
You have two options to save the audit results:

If an audit procedure appears more than once within an audit program, e.g. attached to different controls or the same control attached to different risks or the same risk attached to different organisation units, you have the choice of saving the results for the selected audit procedure only or for all the same audit procedures attached to different

controls, risks or organisation units. Externally linked documents, however, will only be saved to the selected audit procedure, regardless of which save button is clicked. You can print the audit program or the audit report by pressing the corresponding button.

When an audit program is complete and ready to be reviewed or finalised, click the Mark Program as Completed button. You must have entered a comment in every audit procedure in the Audit Result/Comment field and all failed audits must have a resolution and resolution due date entered before the audit program can be marked as completed. After the program is marked completed, a pop-up will appear and you have the option of sending an email to the selected person with Audit Finalisation authority. When an audit result is reviewed, the Review button will display Reviewed.



Tip: When you are working on a large amount of data, e.g. a lengthy report item, saving the data regularly will help prevent loss of data in case of connectivity or other system issues.

Audit Workpaper Schedules

Audit workpaper schedules are working papers for an audit program. Their use is optional.

There are two kinds of audit workpaper schedules: the Checklist and the Sample Schedule.

The Audit Workpaper in GuardianERM.Net provides a convenient way to store your audit working papers as evidence of the audit and support for your findings, report and proposed resolutions to control weakness.

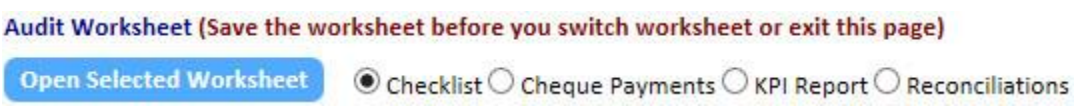
Note: Once the Audit Workpaper function is used for an audit program, the system would not allow you to enter results directly into the Enter Audit Result screen. The audit results in the work papers are automatically calculated and updated into the Enter Audit Result screen once they are saved.

The Audit Workpaper is automatically divided into different worksheets according to the Sample Type of the audit procedure.

The audit procedures that do not require sampling are called Checklist.

The audit procedures that require sampling will be named according to the sample type.

Select a worksheet from the list and click Open Selected Worksheet:



Note: Save the worksheet before closing it or selecting another worksheet. If you are working on a large worksheet, save the data regularly to prevent loss of data due to connection or other system or network problems.

See also:

Enter Checklist review result

Enter Audit Sample result

Enter Audit Checklist Results

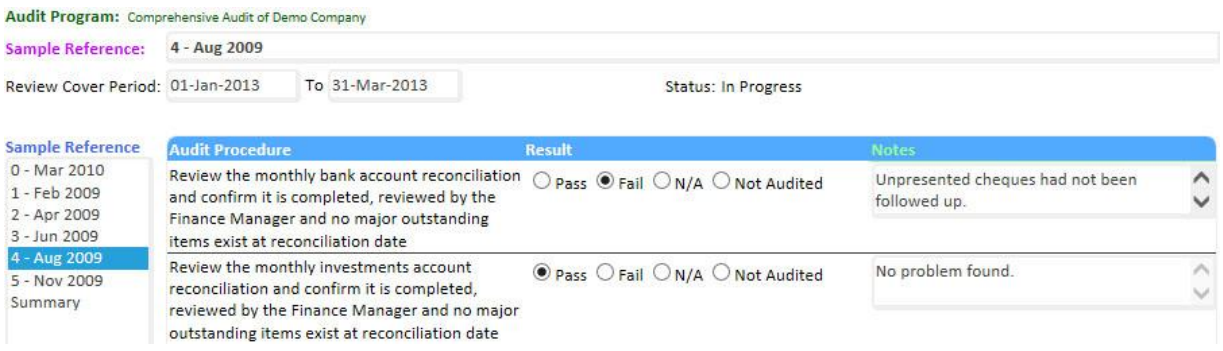
To enter results for the Audit Checklist, select Pass, Fail, Not Applicable (N/A) or Not Answered for each audit procedure. You may enter comments or notes in the Notes field.

Audit Procedure	Result	Notes
Review processes where board and management of organisations assess the particular risks associated with their activities and to appropriately monitor and manage these risks.	(•) Pass ( ) Fail ( ) N/A ( ) Not Answered	
Confirm that the organisations utilises the Australian Standard for Risk Management (AS/NZS 4360:1999) by reviewing risk management strategy, policy and procedures	( ) Pass (•) Fail ( ) N/A ( ) Not Answered	Not done.
Review evidence that the board periodically reviews and agrees risk management strategies	(•) Pass ( ) Fail ( ) N/A ( ) Not Answered	
Confirm board approval of written risk management policies by sighting a signed copy of RMP, or minutes confirming approval	(•) Pass ( ) Fail ( ) N/A ( ) Not Answered	
Sight evidence of Board re-evaluations of the organisation's tolerance for, and exposure to, risk	(•) Pass ( ) Fail ( ) N/A ( ) Not Answered	

Click the Save Worksheet button to save changes to the checklist.

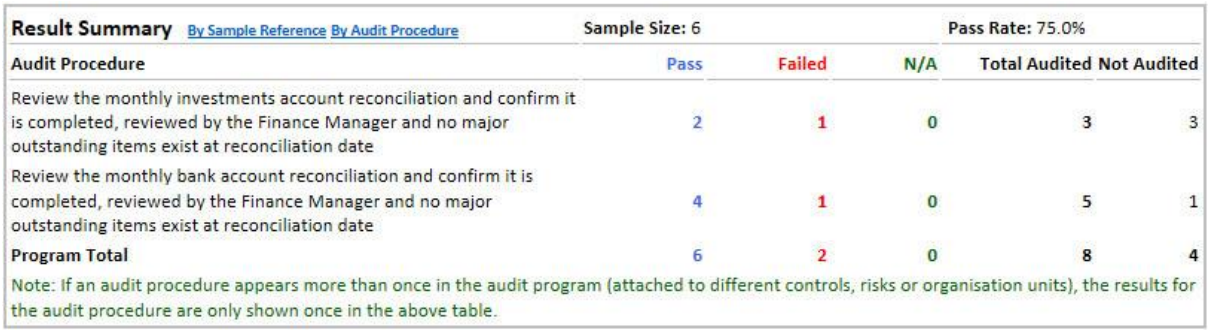
Enter Audit Sample Results

To start using the worksheet, click the New Sample button and enter a reference for the sample. Click Save to save the sample added. Repeat adding sample references for all the samples selected.



Select a sample from the Sample Reference list on the left and select the result. Add notes where appropriate. Click Save before selecting another sample.

Select Summary on the Sample Reference list to view a summary of the audit result. It looks something like this:

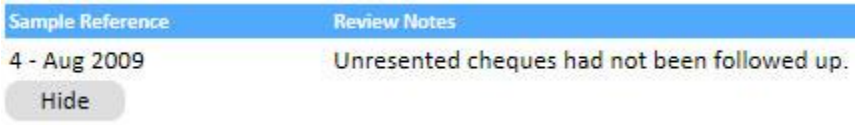


Result Summary By Sample Reference By Audit Procedure — **Sample Size:** 6 — **Pass Rate:** 75.0%

Audit Procedure	Pass	Failed	N/A	Total Audited	Not Audited
Review the monthly investments account reconciliation and confirm it is completed, reviewed by the Finance Manager and no major outstanding items exist at reconciliation date	2	1	0	3	3
Review the monthly bank account reconciliation and confirm it is completed, reviewed by the Finance Manager and no major outstanding items exist at reconciliation date	4	1	0	5	1
Program Total	6	2	0	8	4

Note: If an audit procedure appears more than once in the audit program (attached to different controls, risks or organisation units), the results for the audit procedure are only shown once in the above table.

You can view the notes for items on the Result Summary by clicking the number showing the number of items.



Sample Reference	Review Notes
4 - Aug 2009	Unresented cheques had not been followed up.

Hide

You can also toggle the view by sample reference and audit procedure by clicking the respective link.

Note: The Save button at the bottom of the screen is the same as the one at the top. It is put there for your convenience in the case where there is a lot of audit procedures to complete.

Audit Planning

Strategic Audit Planning

In the management of the Internal Audit function, a common problem facing the Internal Audit Manager is how to effectively allocate the limited internal audit resource to cover the operations of the organisation.

The Strategic Audit Planning module helps the Internal Audit Manager by systematically analysing the risks of the operations and logically allocating the internal audit resource for the various audit assignments over a three year period.

While it is not intended for GuardianERM.net to provide a final answer to the resource allocation problem, it is a good starting point in preparing a three year strategic audit plan and the audit coverage can be justified with systematic and logical data.

The Strategic Audit Planning function involves risk ranking a number of risk areas (auditable units) and allocating audit resources to the risk areas on a three year basis.

A risk area can be anything that is subject to an audit. Although not necessary, it is common to use the organisation units set up in the Risk Management module as risk areas.

There are three main functions as found on the Strategic Audit Planning menu page:

Risk Area Maintenance
Risk Factor Maintenance
Risk Area Ranking

To produce a suggested three-year strategic audit plan:

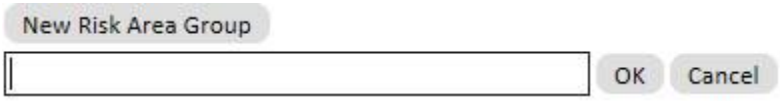
1. Establish a risk area group and add risk areas to it. You can create more than one risk area group.
2. Create a set of risk factors to be used to evaluate the risk of the risk areas in a risk area group.
3. Create a scenario; assign a risk rating for each risk factor in each risk area.
4. Risk-rank the risk areas.
5. Produce a three-year audit plan.

Risk Area Maintenance

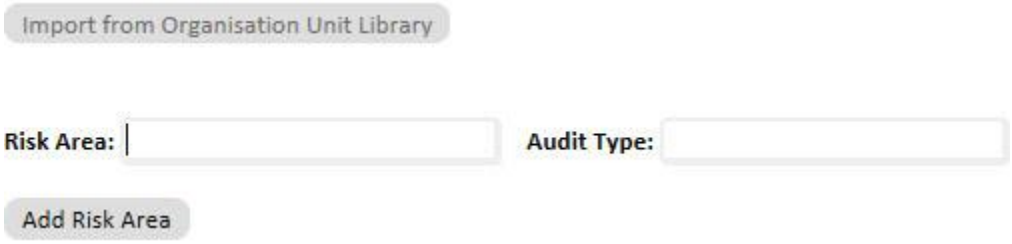
For the strategic planning module to work, you must create a number of risk areas (or auditable units) and group them under a risk area group. You can have as many risk area groups as you like.

To create a risk area group, click the New Risk Area Group button:

Enter a name for the Risk Area Group in the space provided and click OK.



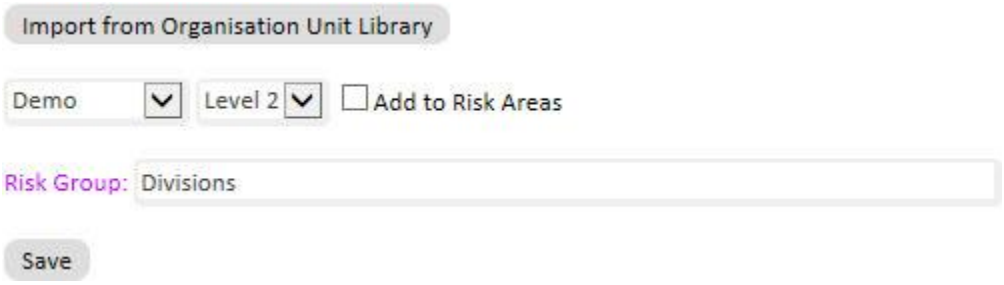
Then select the risk area group you have created by clicking it and then click the Add Risk Area button.



Enter a name for the risk area and optionally enter the type of audit that should be performed, e.g. internal control review or substantive audit. Click the Add Risk Area button to add the risk area to the selected risk area group.

Repeat the above steps to add all the risk areas for the risk area group.

If the risk areas are the same as the organisation units in the Risk Management module, you may import them by selecting a risk area group and clicking the Import from Organisation Unit Library button.



Select the company and the hierarchical level of organisation units (level 1 is the highest company level) to add to the risk area group. If you want to add the imported risk areas to the existing list, tick the Add to Risk Areas box, otherwise, the imported risk areas will overwrite any existing risk areas in the risk area group.

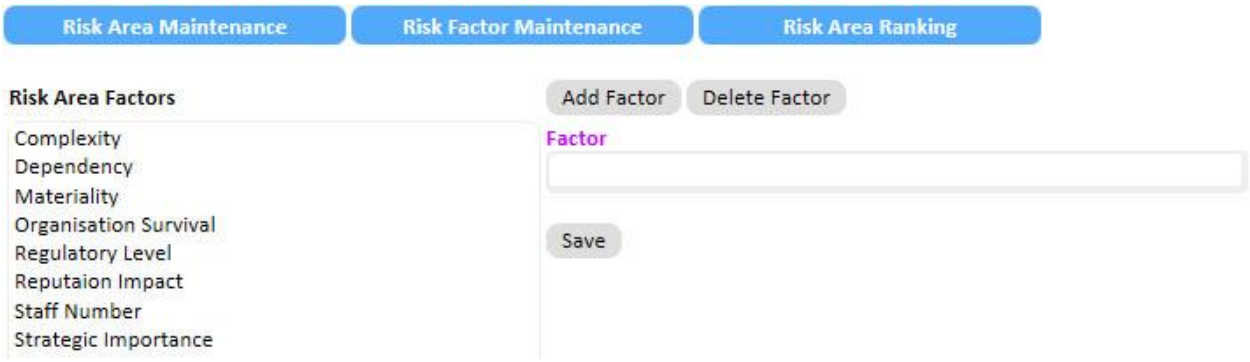
You can delete any unwanted risk area group or risk area by selecting it and then click the Delete button. Risk area groups or risk areas that have been used in a risk ranking scenario cannot be deleted. If you modify the name of a risk area, the new name will replace the old name in all previous saved Risk Ranking Scenarios.

Note: You can add as many risk area groups and as many risk areas as you like.

Risk Factor Maintenance

Risk factors are things that would affect the risk of a risk area (auditable unit) from an audit perspective. Common risk factors may include materiality, complexity of operation, level of regulatory control or strategic importance of the risk area in relation to the whole organisation.

To create a risk factor, click the Add Factor button:



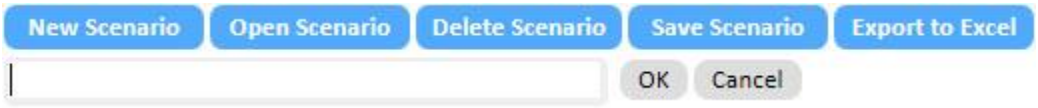
Enter a name for the risk factor and click Save.

You can modify a risk factor by selecting it or delete a risk factor by clicking the Delete Factor button. Risk factors that have been used in a risk ranking scenario cannot be deleted.

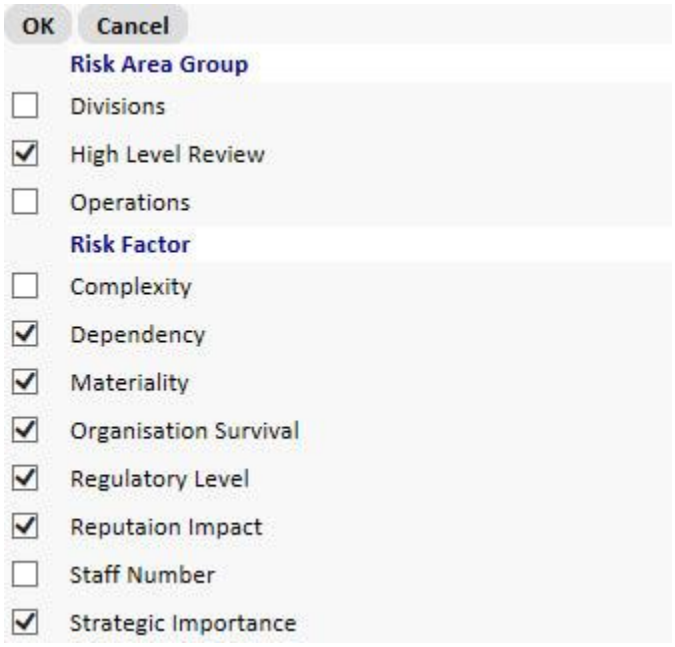
Risk Area Ranking

To perform risk area ranking, you must have already created a risk area group and a set of risk factors.

To perform risk ranking, create a scenario by clicking the New Scenario button:



Enter a name for the Scenario and click OK.
The Scenario Setup panel will appear:



On the list, select one or more Risk Area Group and the Risk Factors to be included in the rating for this scenario, and then click OK.

On the table that appears, determine the weight for each risk factor:

Scenario Setup **Total Audit Resource Available** 0 Person Hours Audit Plan

Scenario: High Risk Area Audits

Risk Areas	Risk Factors																		Risk Score
	Dependency			Materiality			Organisation Survival			Regulatory Level			Reputaion Impact			Strategic Importance			
Risk Factor Weight	1			1			1			1			1			1			
	C	L	R	C	L	R	C	L	R	C	L	R	C	L	R	C	L	R	
Board	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**6.0**
Business Divisions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**6.0**
Finance	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**6.0**
OH&S	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**6.0**

If the weight is 1 for all risk factors, it means they all rank equally. You may increase the weight for one or more risk factors by typing in a number larger than 1. You can use decimals if desired.

Now, for each risk area, rate the risk of each risk factor by determining the Consequence (C), Likelihood (L) and Past Audit Result (R). You may enter a number from 0 to 9. As the risk factors are rated by Factor Weight X Consequence X Likelihood X Past Audit Result, if any of the criteria is zero, the risk factor will be rated as zero. You may need to

establish a set of criteria to allocate a number to each cell of the table to promote consistency across the board as results will be distorted if the rating is not applied consistently across all the risk areas being ranked.

Once you have entered all the numbers, click Save Scenario and the system will risk rank the risk areas according to the data you have entered. For example:

New Scenario | Open Scenario | Delete Scenario | Save Scenario | Export to Excel

Scenario Setup | **Total Audit Resource Available** 3200 Person Hours | Audit Plan

Scenario: High Risk Area Audits

Risk Areas	Risk Factors																		Risk Score
	Dependency			Materiality			Organisation Survival			Regulatory Level			Reputaion Impact			Strategic Importance			
Risk Factor Weight	1			2			1.5			1.8			2			2.5			
	C	L	R	C	L	R	C	L	R	C	L	R	C	L	R	C	L	R	
Board	4	3	2	3	4	1	3	2	2	2	4	2	5	3	2	3	2	1	**169.8**
Business Divisions	2	3	5	3	2	4	3	2	4	3	2	4	5	3	2	3	4	1	**247.2**
Finance	2	3	4	3	1	4	4	3	4	3	3	4	3	4	3	2	2	3	**286.8**
OH&S	3	3	1	4	3	3	4	3	3	4	3	1	4	4	3	3	3	1	**275.1**

To produce a three-year audit plan, enter the total available audit resource (in person-hours) in the Total Resource Available field and click Save Scenario. Now click Audit Plan to view the three-year audit plan:

Scenario Setup | **Total Audit Resource Available** 3200 Person Hours | Risk Ranking

Scenario: High Risk Area Audits

Risk Areas	Risk Score	% Score	Resource	Year Start	Frequency	Year 1	Year 2	Year 3
Finance	286.8	29.3	938	2	Yearly	0	1,096	732
OH&S	275.1	28.1	899	1	Half-Yearly	2,208	2,104	1,404
Business Divisions	247.2	25.3	808	1	2 Yearly	992	0	631
Board	169.8	17.3	555	3	3 Yearly	0	0	433
Total	**978.9**	**100**	**3,200**			**3,200**	**3,200**	**3,200**

Select the Frequency of audits and the first year the audit will start from the dropdown lists and click Save Scenario. The system will recalculate the resource allocation plan according to your specification.

You can view the risk ranking table by clicking the Risk Ranking button.

You can export the Risk Ranking table or the Audit Plan table to Excel by clicking the Export to Excel button.

To retrieve and modify a previously prepared scenario, click the Open Scenario button and select a previously saved scenario from the list.

Audit Planner

The Audit Planner function is used to schedule dates, plan resources and calculate costs for an audit program. To use the Audit Planner, you must prepare the audit program first.

To access the Audit Planner, select Detailed Audit Plan from the menu under Audit & Compliance.

Select Audit Program for Planning

Ensure that you have selected the correct company from the dropdown list (if you have set up multiple companies in your system). To plan an audit or to edit an already planned one, click the Select link for the audit.

	Audit Program Name	Status	Start Date	End Date	Total Audit Hours
Select	Board and Finance Audit 2013	In Progress			0
Select	Board Audit 2012	Finalised			0
Select	Board Audit 2013	Completed			0
Select	Board Audit 2014	New			0
Select	Board Internal Audit H1 2014	New			0
Select	Board Self Assessment 2012	New			0
Select	Board Self Assessment Apr 2013	Finalised			0
Select	Board Self Assessment Dec 2012	Finalised			0
Select	Board Self Assessment Jan 2013	Finalised			0
Select	Board Self Assessment Nov 2012	Finalised			0
Select	CCL Executives	Finalised	01-Mar-2012	12-Aug-2012	54.5
Select	Claims Management Audit	Finalised			0
Select	Compliance Audit	In Progress	01-Jan-2008	30-Jun-2013	280
Select	Comprehensive Audit of Demo Company	In Progress	03-Feb-2008	31-Aug-2012	176

You can sort the list by clicking the Heading of the columns.

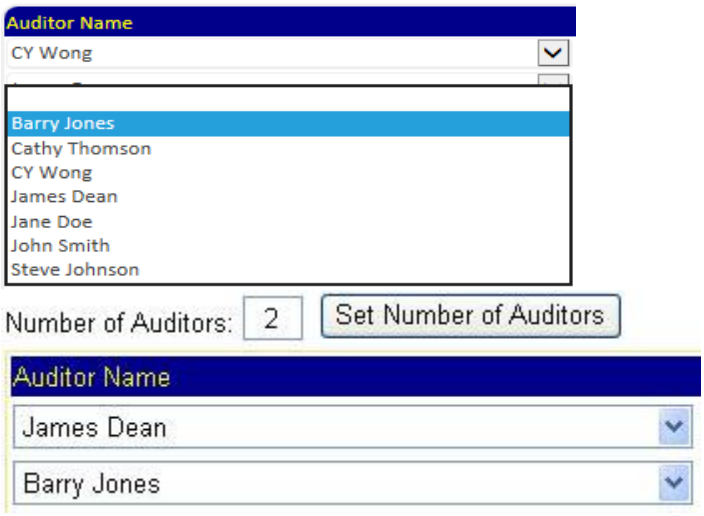
The audit programs with a Start Date, End Date and Total Audit Hours have been planned. You can view the existing plan or create a new plan by clicking the Select link.

Planning an Audit

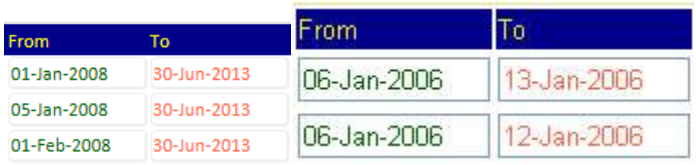
Enter the number of auditors required for the audit and click Set Number of Auditors:

Number of Auditors: 3 Set Number of Auditors

Select the auditors from the dropdown list:



Enter the From and To dates of the planned audit duration:



Click the Calculate button to calculate the number of hours between the dates entered and the time cost of the audit based on the hourly rate for each auditor selected.

Note: The system assumes Saturdays and Sundays are not working days, no public holidays and there are 8 working hours each day. If the system assumptions are not correct for the audit, the number of hours can be over-written to reflect the correct time spent. For example, if the audit duration is 2 weeks but one of the auditors assigned is a computer specialist and is estimated to perform only 10 hours of work during the two weeks.

Note: The system will only calculate the Total Hours when the field is **BLANK** so it will **not** over-write user entered data.

Enter any travel/accommodation and other costs and click Calculate to add up the total costs.

Click the Save button to save the audit plan.

Note: Once an audit is planned, if the audit is not finalised by the end date, it will be reported as outstanding on the Main Menu System Health Check.

Auditor Master File

The system keeps a record of all auditors in a master file. To access the master file, click the Auditor Maintenance button on the Schedule Audit Task screen.

To modify an existing auditor, click the Edit link for the auditor:

Auditor Name	Office Title	Hourly Rate ($)	Active	
Barry Jones	Vice President, Audit	600	Y	Edit
Cathy Thomson	Audit Director	350	Y	Edit
CY Wong	Operational Auditor	75.5	Y	Edit
James Dean	Senior Auditor	150	Y	Edit
Jane Doe	Audit Manager	200	Y	Edit
John Smith	Auditor	90	Y	Edit
Steve Johnson	Junior Auditor	40	Y	Edit

Add Auditor Exit

To remove an auditor, enter 'N' in the Active field.

Enter the required data and click the Update link to save the changes. Click Cancel to cancel the changes.

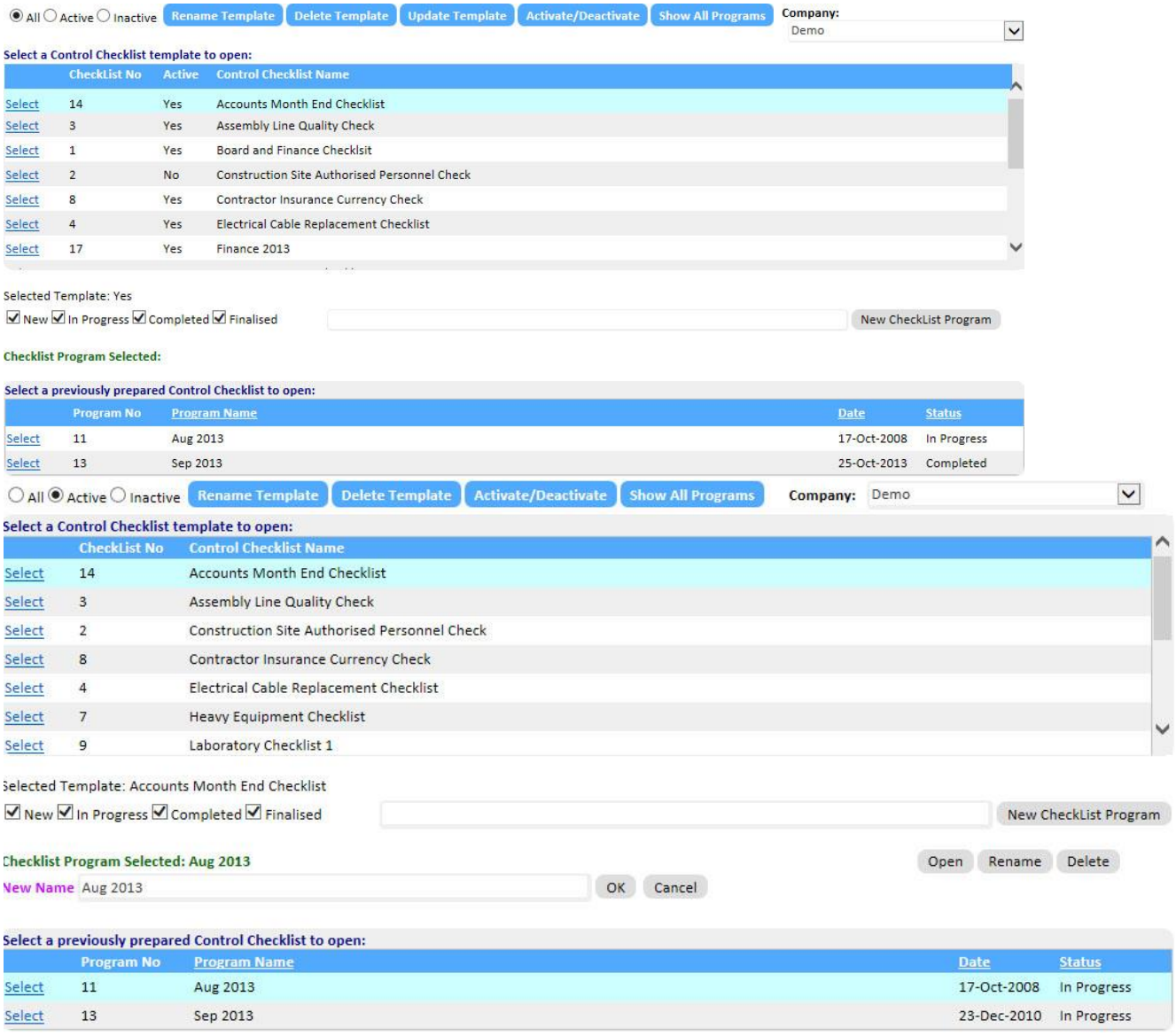
To add a new auditor, click the Add Auditor button and enter the name, title and hourly rate for the auditor.

Control Checklist

A Control Checklist is a simple questionnaire for operational staff to complete. The Control Checklist has two components: the templates and the programs. A template is a questionnaire that be used over and over. Each time the template is used, the data is stored in a checklist program. Each template can have many programs.

To prepare a Control Checklist, see prepare audit program.

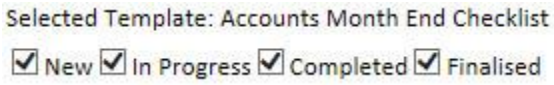
When you click Control Checklist from the Main Menu, you can select a control checklist from the list of prepared control checklist templates for the selected company. You can filter the list showing all, active or inactive ones only. You may activate or deactivate a checklist template by clicking the Activate/Deactivate button after selecting a template from the list.



You can rename or permanently delete a template by clicking the respective button.

Note: A template cannot be renamed or deleted after a checklist program has been prepared using it.

You may use the filters to filter the list if the list is long. Un-tick the status that you do not want to be included on the list.

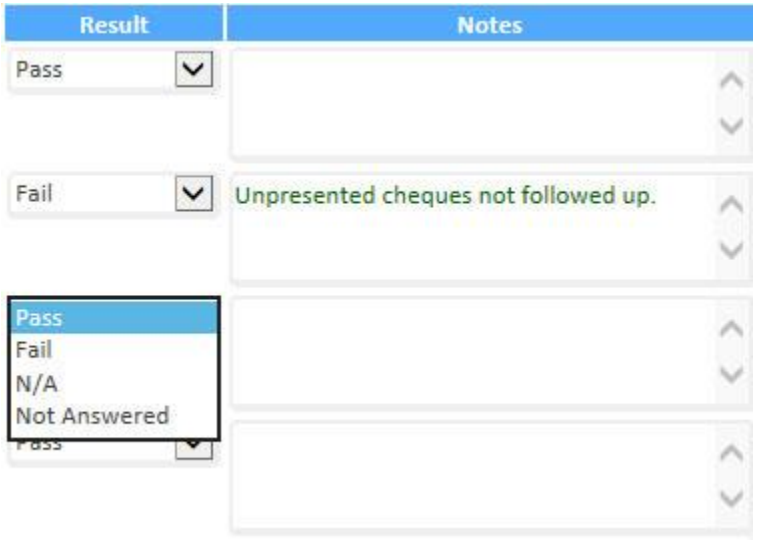


To list all the checklist programs regardless of which template was used, click the Show All Programs button.

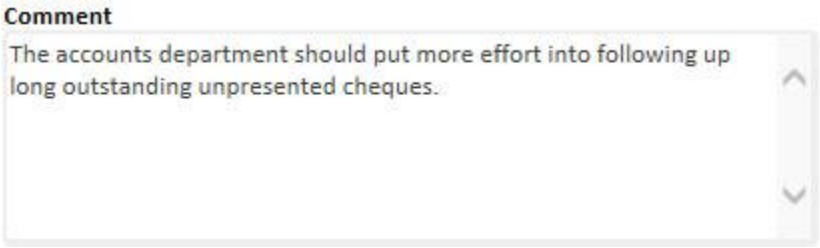
To open an existing Control Checklist Program, click the Select link next to the Program and click the Open button. You can rename a checklist program only when it has a 'New' status.

To create a new program, enter a program name in the space provided and click the New Checklist Program button next to it.

When the checklist program is opened, simply answer the questions by selecting an answer from the dropdown list.



You may also enter a note for each of the questions and a comment or conclusion at the bottom of the page.



The result of the checklist will be shown after you have saved the checklist by clicking the Save Checklist button.

Score Card	Number	Percentage
Total Number of Questions	4	100%
Pass	3	75%
Fail	1	25%
N/A	0	0%
Not Answered	0	0%

When all the questions have been answered, click Finalise Checklist to finalise the Control Checklist Program. Once finalised, the answers cannot be changed.

Update Control Checklist Template

Once a control template is prepared, you can update it with new audit procedures added in Risk Evaluation.

There are limitations to what can be modified:

1. You cannot delete any audit procedures that are already in the template.
2. Even if you have modified the audit procedure in Risk Evaluation, the existing audit procedure in a template will NOT change to the modified version,
3. The risk-based selections used when the template was first created will not be taken into consideration when updating the template.
4. Previously created control checklist programs using the updated template will NOT be changed.

A list of audit procedures that are not included in the original template is displayed:

Company	Risk Name	Inherent Risk	Residual Risk	Control Name	Key Control	Checklist Item Name
☐ Board	Breach of risk management guidelines	High	Negigible	Board and management of organisations assess risks regularly	Yes	Review processes where board and management of organisations assess risk
☑ Board	Breach of risk management guidelines	High	Negigible	Board ensures risk management control systems are established and operating effectively	No	Assess procedures of how the Board ensures risk management systems are effective
☑ Board	Breach of risk management guidelines	High	Negigible	Board questions management on risk management	No	Assess if the insurer has intentionally deviated in a material way from its RMS.
☐ Board	Breach of risk management guidelines	High	Negigible	Board questions management on risk management	No	Review evidence of Board questioning management on risk management processes
☐ Board	Breach of risk management guidelines	High	Negigible	Board regularly re-evaluates tolerance for risk	No	Sight evidence of Board re-evaluation of risk tolerance
☐ Board	Breach of risk management guidelines	High	Negigible	Board understand fully, the risks	No	Review quarterly risk management reports to ensure the board understand fully the risks

Select the audit procedures you want to include in the template by ticking the boxes in front of them.

Click the Add to Checklist button to add the selected audit procedures to the checklist template.

Note: Once added, the audit procedures cannot be removed.

Process Review

The GuardianERM Process Review is a non-risk-based audit function. It is suitable for reviewing processes according to a pre-defined checklist or questionnaire. The questions can be optionally linked to the organisation's risk structure to reinforce the risk management function.

For certain types of review, for example quality audits and compliance audits, using the Process Review function can be simpler and quicker as it does not need an established risk structure.

To use the Process Review function, you will need to create a checklist or questionnaire and then using the checklist as a template, prepare review programs and perform the review by obtaining answers to the questions.

The Process Review supports the use of samples. For example, you may use a Payment Review template to check a sample of paid invoices or use a Quality Audit template to check a sample of products or transactions.

Note: To use this function, your security profile must include Auditor or Audit Sign-Off at the company level. Please contact your administrator for further information.

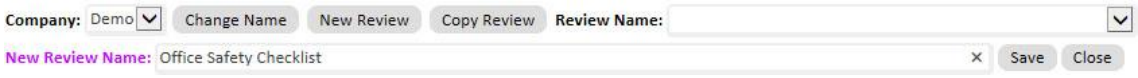
Process Review Checklist Maintenance

The Checklist Maintenance function is used to create and maintain Process Review checklists or templates. To create a checklist, you must first have some idea what the checklist would look like, what questions to ask and how the questions may be grouped to make it easier to follow and complete.

Note: To use this function, your security profile must include Auditor or Audit Sign-Off at the company level (top level). Please contact your administrator for further information.

To create a new Process Review checklist:

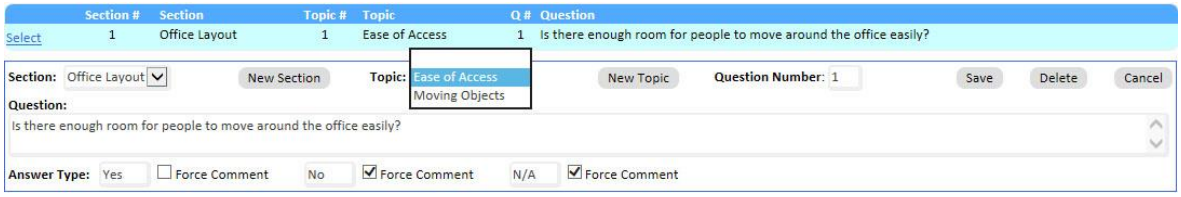
1. Select Process Review Setup from the Main Menu or the dropdown menu.
2. Select the company from the dropdown list.
3. Click the New Review button and enter a name for the Process Review checklist (Review Name) to be created.
4. Click the Save button.



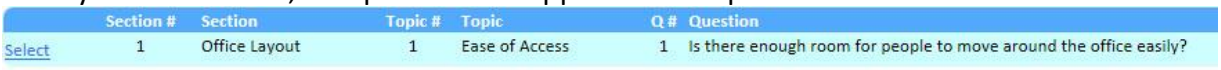
5. Click the Header References button. The Header References are fields used to described the samples selected or the reviews (if sampling is not applicable to this review) to be performed in the future based on this checklist. Typical header references are Location, Person-in-Charge, Invoice Number, etc.
6. Enter up to 7 header reference field names and click the Save button. Note: header references are optional. For example:

7. Click the Add Question button.
8. Click the New Section button to create a new section for the checklist or select an already created section from the dropdown list.
9. Click the New Topic button to create a new topic under the section just created. Note: Using Section and Topic to group questions together is optional.
10. Enter a question.
11. You can have 3 answers to each question. The default answers are Yes, No and N/A. You may change them by typing in your preferred answers but the first answer must be the positive answer, the second must be the negative answer and the third a neutral answer. This is important as this is what the system uses to rate the answers and provide a score for the review.

12. If you want to force the person answering the question to provide a comment when a certain answer is selected, tick the Force Comment box for the answer. The system automatically ticks the Force Comment for the second answer but you can change that.
13. The system automatically numbers the questions sequentially. If you want to change the default number, type your number in. It is suggested that you do not change the default question numbers at this stage. You can change the numbers after all the questions are entered.
14. Click Save when you have finished creating the question. For example:



15. Once you clicked Save, the question will appear on the question list.



16. Repeat the process from steps 7 to 14 to complete your checklist.

If you want to modify any question, click the Select link in front of the question, make the modifications and click the Save button.

You can renumber the questions, sections and topics to change the sequence of presentation of the questionnaire. To see what the questionnaire looks like, click the Preview Checklist button.

When a checklist is out-of-date or no longer in use, you can deactivate it by clicking the De-activate Review button.

To view or modify a previous prepared Process Review Checklist, select the review from the Review Name dropdown list.

Note: Once a checklist has been used in a review, the checklist cannot be changed. To update a used checklist, click the Copy Review button at the top to create a copy of the checklist, modify the copied checklist and deactivate the old one.

Perform Process Review

To perform a Process Review, you must have a Process Review checklist or template prepared first.

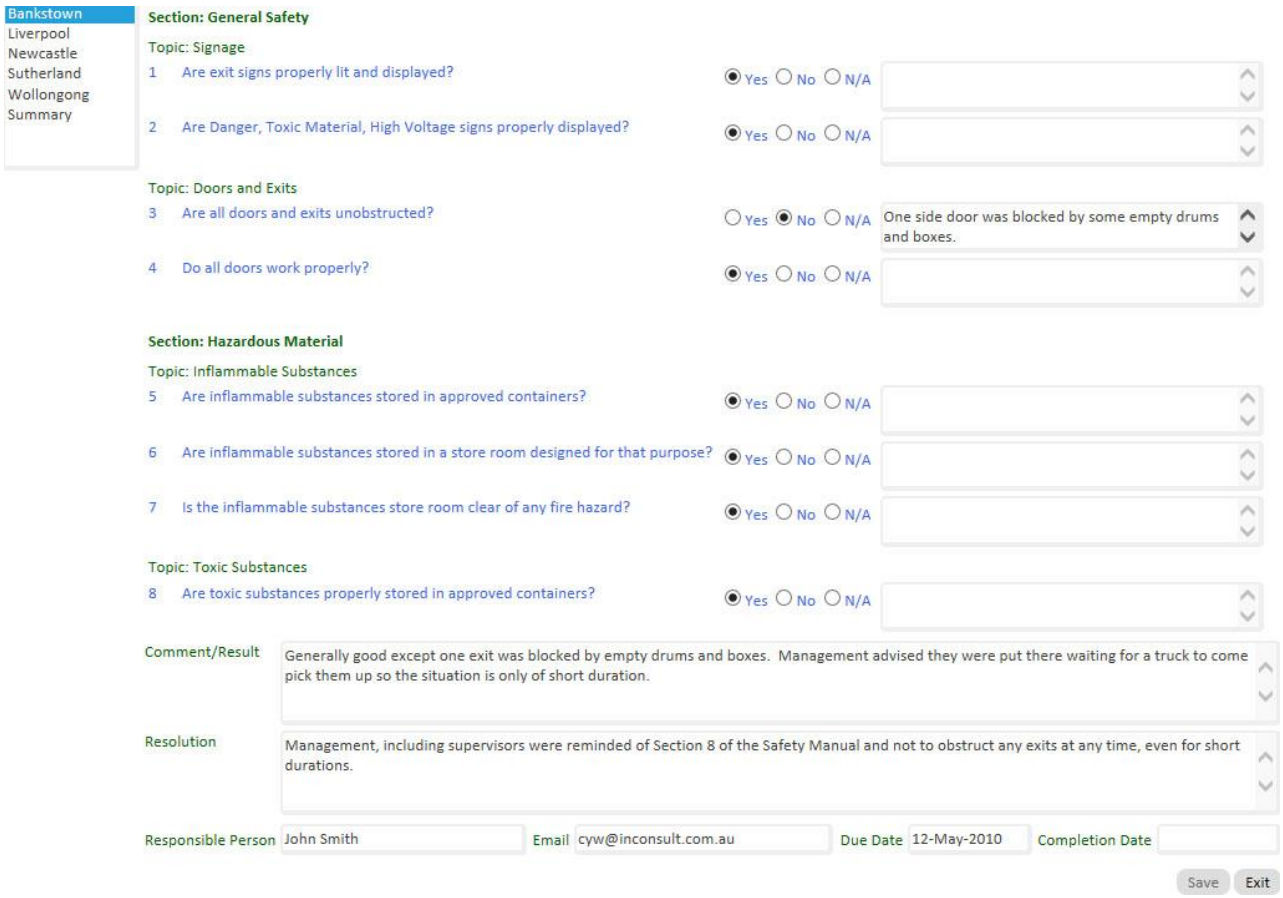
1. Select Perform Process Review from Audit & Compliance on the Main Menu or the dropdown menu.
2. Select a previously prepared Process Review Template from the list by clicking the Select link in front of the review.
3. Enter a review program name, for example NSW Workshop Safety Audit 2010 as below and click the New Review Program button.

The Review Program will be displayed. You can now see the header references and questions.

Assuming we are doing a safety review for 5 out of the 35 workshops in NSW, that is, we have a sample of 5 workshops to use the checklist on.

1. Enter a Sample Reference. In our example, say, Bankstown.
2. Complete the header references.

3. Answer the question with comments where appropriate. If you select an answer configured with the Force Comment option, then the system will prompt you to enter a comment when you save the answers.
4. Click Save to save the data. You will notice the sample reference Bankstown is now on the Sample Reference List. When more samples are added, the new samples will be added to the list as well.



5. To create another sample, say the Liverpool workshop, click the New Sample button at the top and complete the form as the previous example.

You may view the overall result of the review by clicking Summary on the Sample Reference List.

Result Summary By Sample Reference By Question **Pass Rate:** 87.2% **Rating** 0

Question	Yes	No	N/A	Blank	Total
1. Are exit signs properly lit and displayed?	5	0	0	0	5
2. Are Danger, Toxic Material, High Voltage signs properly displayed?	5	0	0	0	5
3. Are all doors and exits unobstructed?	1	4	0	0	5
4. Do all doors work properly?	4	1	0	0	5
5. Are inflammable substances stored in approved containers?	4	0	1	0	5
6. Are inflammable substances stored in a store room designed for that purpose?	5	0	0	0	5
7. Is the inflammable substances store room clear of any fire hazard?	5	0	0	0	5
8. Are toxic substances properly stored in approved containers?	5	0	0	0	5
Program Total	34	5	1	0	40

You may view the results by Sample Reference or By Question. Click the corresponding links at the top of the score card.

In the By Question view, you can click on a number on the scorecard to view the samples making up the result and any comments made on the questions:

Sample Reference	Review Notes
Bankstown	One side door was blocked by some empty drums and boxes.
Liverpool	Lots of rubbish just outside rear exit.
Newcastle	Someone parked a car right outside the rear exit and blocking it.
Wollongong	Side exit was blocked by old furnitures.

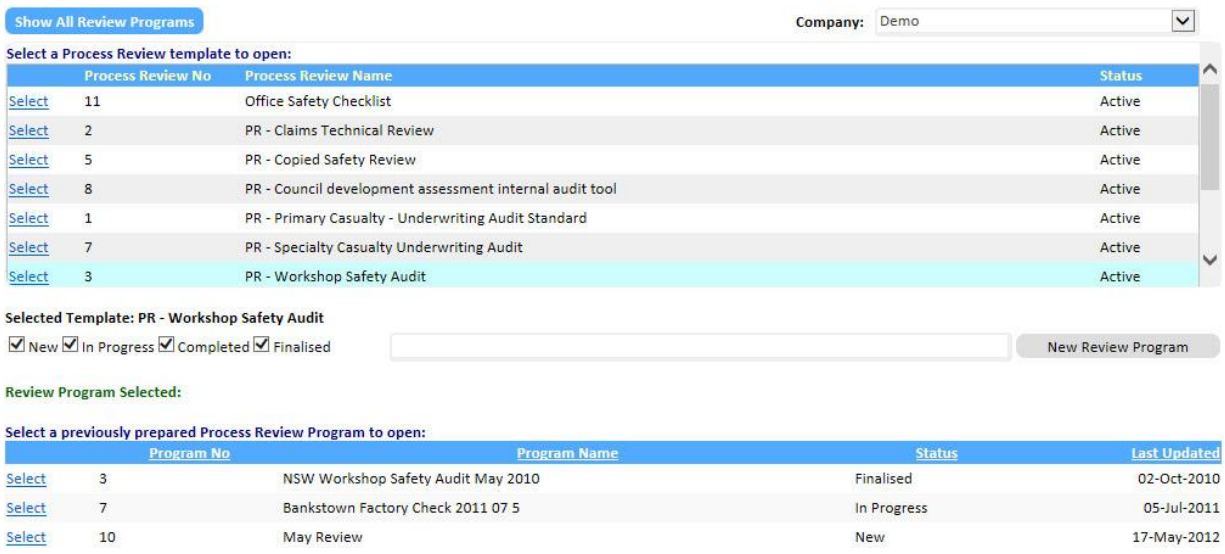
Hide

You may also complete the Review Notes and Review Report items.

Once all questions are completed, the Process Review Program can be finalised by clicking the Finalise button. A finalised program cannot be modified in any way.

To open a previously prepared Process Review Program, select Perform Review under Process Review on the Main Menu or dropdown menu.

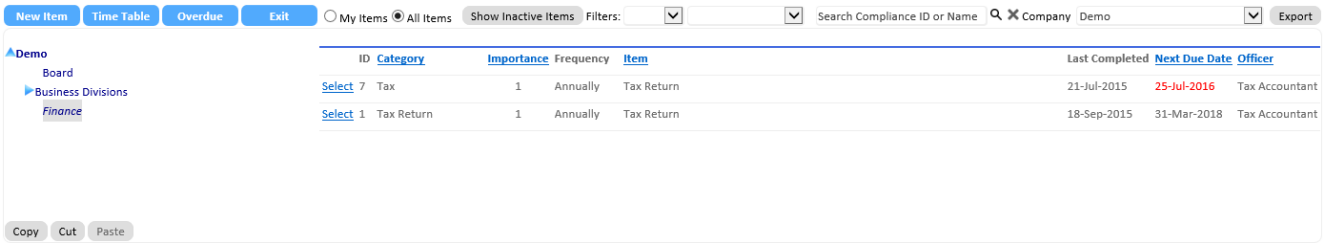
Select a Process Review template on the top list. Tick the Status filter boxes to included programs in the various stages of completion and select a review program from the bottom list. Click the Open button to open the selected Process Review Program. Note: a finalised process review program cannot be modified.



Compliance

Compliance Management

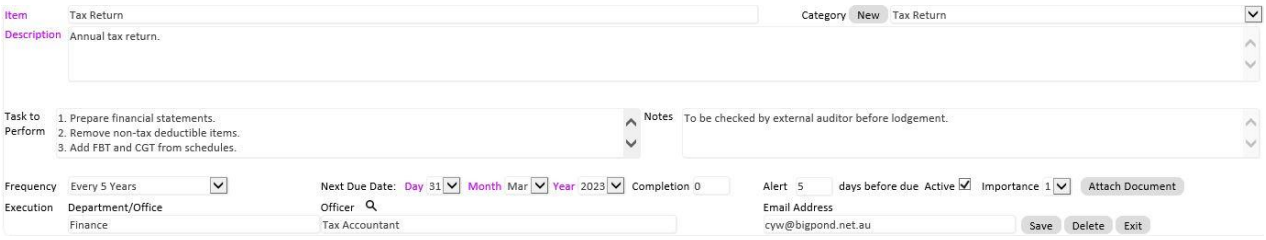
The Compliance Management function assists you in documenting the organisation's external and internal compliance requirements, especially those that require certain action to be completed periodically, for example submitting a return or report.



Select an organisation unit and a list of compliance items will be displayed (if any) for that organisation unit.

To view previously deactivated items, click the Show Inactive items button. To toggle back to the active items, click the button again.

Either click the New Item button to create a new compliance item or select a compliance item from the list to show the details:



The 'Alert Days Before Due' is used by the Workflow system to send alert emails to the selected recipients. For example, if the Alert Days Before Due is 14 days and in the Workflow Configuration, the first email was scheduled to be sent 10 days before due, then the email will be sent 24 (14+10) days before the compliance due date.

You may attach more detailed documentation in relation to the compliance item by clicking the Attach Document button.

You may deactivate the compliance item if it is not to be used any longer (or replaced by another item) by un-ticking the Active box and then Save. A deactivated item can be

activated (by ticking the Active box and Save) again any time and the completion history will remain intact.

Tip: If the frequency is *ad hoc*, you are still required to enter the next due date. Either enter 31 December 2020 or today's date and then complete the item immediately using the Timetable function. This way you won't get a reminder for the item.

To select the Executed By Officer from a list of registered users, click the search icon next to Officer. You may search the list by entering the user's ID or name.

Click the Overdue button to obtain a list of all compliance items overdue for completion for the whole organisation (regardless of which organisation unit is being selected).

Compliance items can be copied/cut and pasted to another organisation unit. For a single compliance item, select the item and click the Copy (or Cut) button:

Then select the destination organisation unit and click the Paste button.

To copy/cut all the compliance items in one organisation unit, select the organisation unit and without selecting any compliance item, click the copy or cut button. Then select the destination organisation unit and click the paste button.

Compliance Timetable

The Compliance Timetable shows the history of completion of the selected compliance item and when the compliance item is next due.

	Due Date	Date Completed	User	Notes
Select	31-Mar-2012		System	
Select	31-Mar-2011	15-Nov-2012	cyw	Done.
Select	31-Mar-2011	20-Jan-2011	System	Compliance item disabled by user cyw.
Select	31-Dec-2010	20-Jan-2011	System	Compliance item disabled by user cyw.
Select	31-Mar-2010	24-Dec-2010	cyw	Completed
Select	31-Mar-2009	24-Dec-2010	cyw	Completed

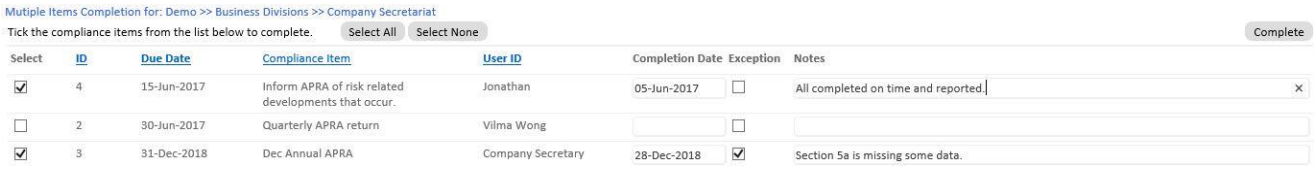
You may record completion of an item by selecting it. Note that a completed item cannot be selected.

To complete an item, enter a note (optional), either leave the default Date Completed (the current date) or enter a completion date (cannot be in the future) and click the Complete button. The system will automatically create the next due entry based on the Frequency recorded for the compliance item. Note that the system will NOT create the next due entry if the frequency is 'ad hoc'.

If you only want to insert a note without completing the item, enter the note and click the Save Notes button.

If an item is completed but there are exceptions (e.g. a form is not completely filled due to lack of information or the item submitted late), enter the exception in the Notes field and click the Complete with Exception button. The item will be completed and will be flagged Completed with Exception which can be selected in the reports.

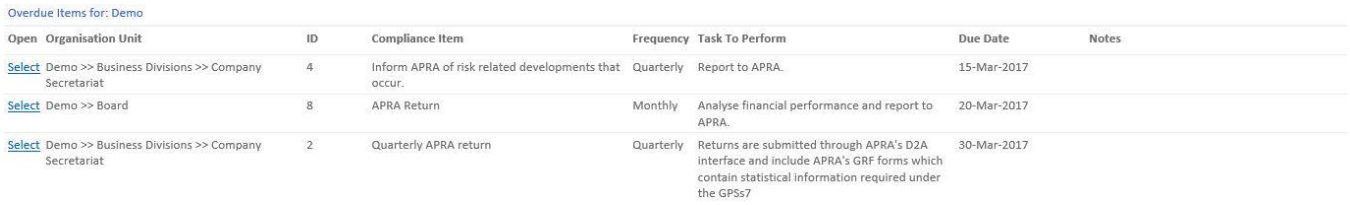
If there are multiple items to complete within the selected organisation unit and none of the items is selected, clicking the Timetable button will trigger the Multiple Items Completion function.



Select the items completed and fill in the details. Click the Complete button to complete the multiple items. You cannot enter '"Notes Only " on the multiple items completion screen.

Compliance Overdue Items

The Compliance Overdue screen lists all compliance items overdue for completion for the organisation.



Overdue Items for: Demo

Open	Organisation Unit	ID	Compliance Item	Frequency	Task To Perform	Due Date	Notes
Select	Demo >> Business Divisions >> Company Secretariat	4	Inform APRA of risk related developments that occur.	Quarterly	Report to APRA.	15-Mar-2017	
Select	Demo >> Board	8	APRA Return	Monthly	Analyse financial performance and report to APRA.	20-Mar-2017	
Select	Demo >> Business Divisions >> Company Secretariat	2	Quarterly APRA return	Quarterly	Returns are submitted through APRA's D2A interface and include APRA's GRF forms which contain statistical information required under the GPSs7	30-Mar-2017	

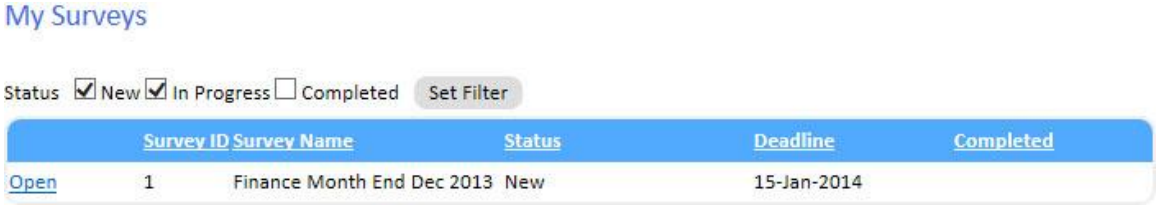
Select an item you want to complete and the system will bring you to the Compliance Timetable screen where you can complete the overdue item.

Compliance Survey

The GuardianERM.net Compliance Survey is a simple and effective self-assessment tool that consists of questionnaires prepared by the Compliance Manager (a user with Compliance Survey Management authority specified in the user access profile) and can be distributed to any GuardianERM.net user for completion. After a survey questionnaire is created, the Compliance Manager can send a notification email within GuardianERM.net to all users selected to complete the survey. A link is provided in the email and when the user clicks the link, the user will be directed to GuardianERM.net. Once logged in, the user will be directed to the questionnaire for completion.

For the User

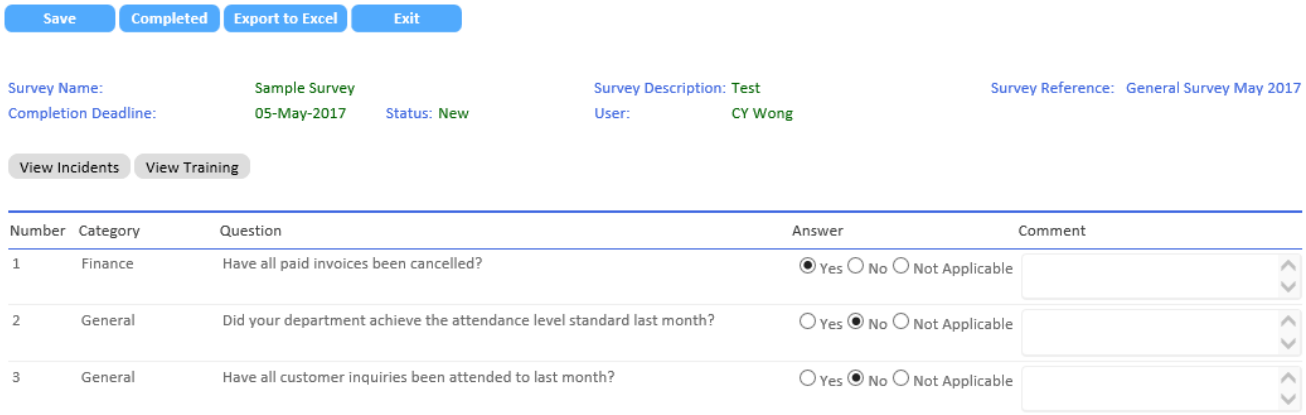
The main Compliance Survey page lists all the surveys you were invited as a participant.



You can filter the surveys by their status by ticking the appropriate boxes. Ticking all boxes and not ticking any box has the same result. To open a survey, click the Open link for the survey.

If you have received an email inviting you to participate in a compliance survey and you clicked the link in the email, you will be directed to the survey completion page after logging in.

If you want to review the incident or training register before answering related questions, click the View Incident or View Training button.



You can check the incident or training registers if the information is relevant to some questions.

If the question was set up as a 'Comment Only' question, the Yes, No and Not Answered selections will be disabled and you are only required to complete the Comment Field. Click the appropriate answer. If the answer selected is No or Not Answered, a comment is required. You can also enter a comment when the answer is Yes.

When all the questions are answered, the Completed button will be activated. Click the Completed button to complete the survey. Once a survey is completed, its answers can no longer be modified.

For the Compliance Survey Manager

To access these functions, you need the Compliance Survey Management authority. The functions available to the Compliance Manager are:

My Surveys	A list of surveys for the Compliance Manager to complete as a user. Same functionality as the Compliance Survey for Users.
All Surveys	A list of all surveys. The Compliance Manager can only complete his/her own surveys but can view the other surveys. Typically used when a user has a question about the survey.
Launch Survey	To launch a recurrent survey and invite users to complete it.
Question Maintenance	To create and modify questions, survey groups and the

	question identifier.
User Group Maintenance	An optional function to group GuardianERM registered users into user groups for faster retrieval of selected users when creating a new survey.
New Survey	To create a new survey and invite users to complete it.
Modify Survey	To modify surveys that are created but not yet completed by any user.
Roll Over to New Survey	Copy the selected survey and roll it over to a new survey.
Survey Results	View the summary and details of survey results.

You can choose to modify an active survey (one that is already launched but is still in the New status) or a recurrent survey template.

To select a survey or template for modification or roll over, tick the box for the survey and click the appropriate button at the top button bar.

To open the survey for completion or to view if you are not a participant for the survey, click the Open link for the survey.

Recurrent Survey

A recurrent survey is a survey template consisting of selected questions and each question has pre-assigned users attached to it. It can be launched and relaunched and is typically used when the same compliance survey is done periodically.

In order for the Recurrent Compliance Survey to work, the questions included in the recurrent survey must have users attached to them. Users can be added or modified by clicking the Modify Users button on the Survey Question Maintenance screen.

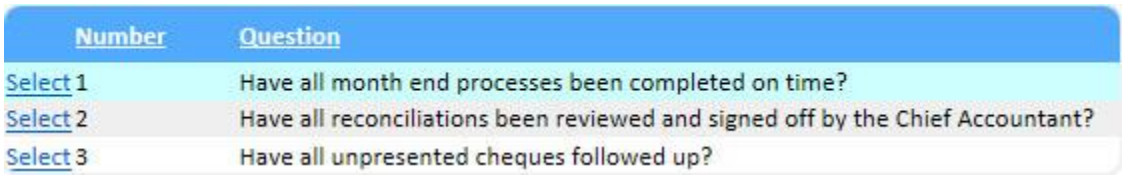
Having the survey pre-configured makes it very simple and quick to start a survey. All you need to do is to select the survey to launch, enter a deadline date if desired and click the launch button. You can optionally select to send an invitation email to the users selected to perform the survey.

Question Maintenance

To use the Compliance Survey function, you must first build a library of compliance questions to be used in future surveys. The surveys have fixed answer choices of Yes, No and Not Answered so you must phrase the questions accordingly. For example, the question "Did you go to work by bus this morning?" is a proper question but there will be no appropriate answer choice for the question "How did you get to work this morning?" A question can be set up as a comment only question where the answer choices are disabled and the user needs to enter a comment only.

If a user answers No or Not Answered, the user must enter a comment in the comment field for the question. So questions like "Did you get to work by bus this morning? If not, please specify how." are alright.

If there are any questions previously added, they will be listed:



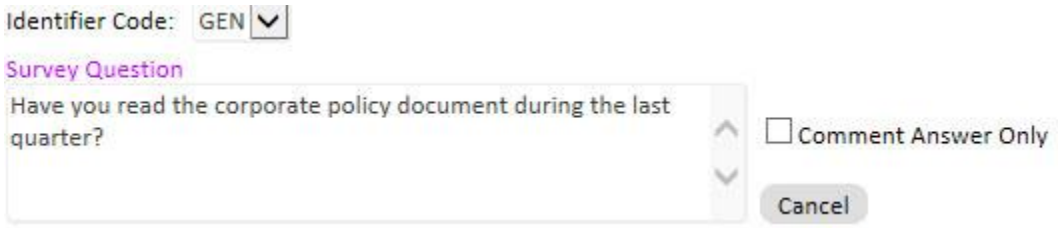
Number	Question
Select 1	Have all month end processes been completed on time?
Select 2	Have all reconciliations been reviewed and signed off by the Chief Accountant?
Select 3	Have all unpresented cheques followed up?

The list can be filtered by category or survey group by selecting the desired value from the dropdown list. You can also search for a word or phrase in a question by typing the search text in the Search text box and click Go. To clear the search, click the Clear button.

To add a new question, click the New Question button. You can select an identifier so you tell what type of question it is. The question is identified by the 3 character identifier code plus a sequential number generated by the system. The default is GEN for general questions. You can add or modify the identifiers by clicking the Edit Identifier button at the top action buttons bar.

To add a new identifier, click the Add Identifier button. To edit an existing identifier, click the Select link for the Identifier and enter a new identifier code. The identifier code must be a 3 character code. If you modify an existing identifier, all questions and those in previously created surveys using that identifier will be changed to the new identifier code but the number following the identifier code will remain the same.

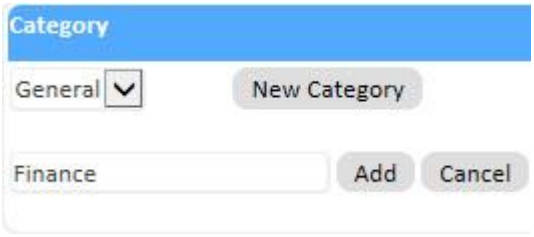
Enter the question and if the question is to be a comment only question, tick the Comment Answer Only box. Always make the question clear, concise and to the point.



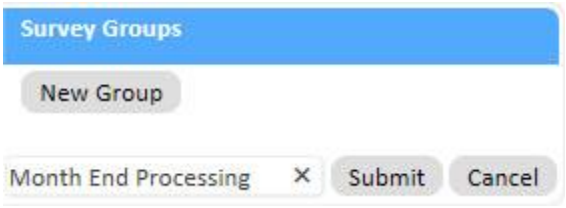
After a question is entered, you may allocate it to a category and/or survey group. Using categories and survey groups make creating surveys later on easier and is optional. If you have more than 20 questions, it is recommended that you categorise and/or group them for convenience.

A survey group is a group of related questions. When you create a survey later on, you can select a survey group and the system will retrieve all the questions belonging to the group. A question can be included in more than one survey group. You can then select either all or some of the questions in the survey group.

To create a category, click the New Category button, enter a name for the category and click Add. The new category will appear on the Category dropdown list.



To create a survey group, click the New Group button, enter a name for the survey group and click the Submit button.

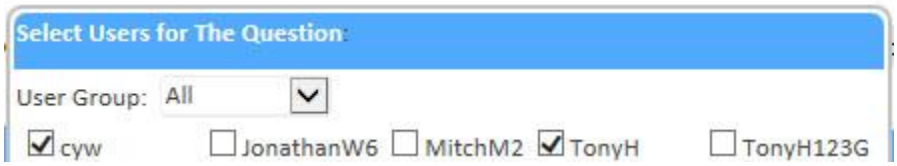


To allocate a category to a question, select the question, select the category from the dropdown lists and click the Save button at the top.

To put a question into one or more survey groups, select the question and tick the appropriate boxes in the Survey Group list.

Note: If you do not allocate a newly created category or survey group to at least one question, the category or survey group will NOT appear on the dropdown lists once you exited from the screen and get back in again. Do NOT create categories and survey groups in advance and not use them.

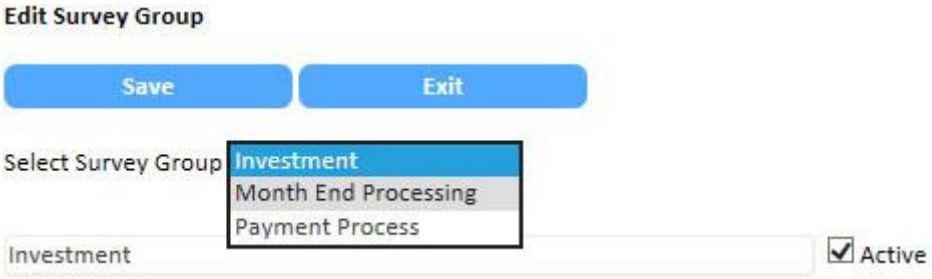
If the question is to be used in a recurrent survey, you must assign users to it. Click the Modify Users button at the top menu bar, tick the users to be included for this question and click the Save button.



To modify a question, select the question and click the Modify Question button at the top. You can change the question, the category or the survey group. Click the Save button at the top when you have finished making the changes.

To delete a question, select the question and click the Delete Question button. A deleted question will not be shown in the future when preparing a new survey but it will still be shown when viewing the results of past surveys.

If you want to change the name of the survey groups, click the Edit Survey Group button at the top.



Select the survey group you want to change and make the desired modification. You can disable a survey group by un-ticking the Active box. Once deactivated, the survey group will not be shown when creating a new survey.

User Group Maintenance

A Compliance Survey User Group is simply a group of related users for survey purposes to make it convenient to select users for a new survey. Its use is optional. Its use is recommended if you have more than 20 users that are surveyed regularly.

A list of all users registered in the GuardianERM.net system is displayed:

To create a user group, click the New Group button, enter a name for the group and click the Submit button.

Tick the users to be included in this group and then click the Save button at the top.

To modify a user group, select the group from the dropdown list and click the Modify Group button. If you want to change the name of the group, type the new name and click the Submit button. If you want to change the group members, tick or un-tick the users and click the Save button at the top.

To delete a user group, select the group from the dropdown list and click the Delete button at the top.

Note: The name No Group is a system default and cannot be changed.

Creating a New Survey

A Compliance Survey consists of users invited to complete the survey and the questions for the survey. To ensure the quality of answers, it is suggested that a survey should contain no more than 10 questions.

There are two kinds of compliance surveys you can create in GuardianERM, a recurrent survey and a one-off survey. A recurrent survey consists of selected users and questions and can be launched and re-launched. A one-off survey is one that you intend to use once only. A one-off survey can still be reused using the Roll Over function.

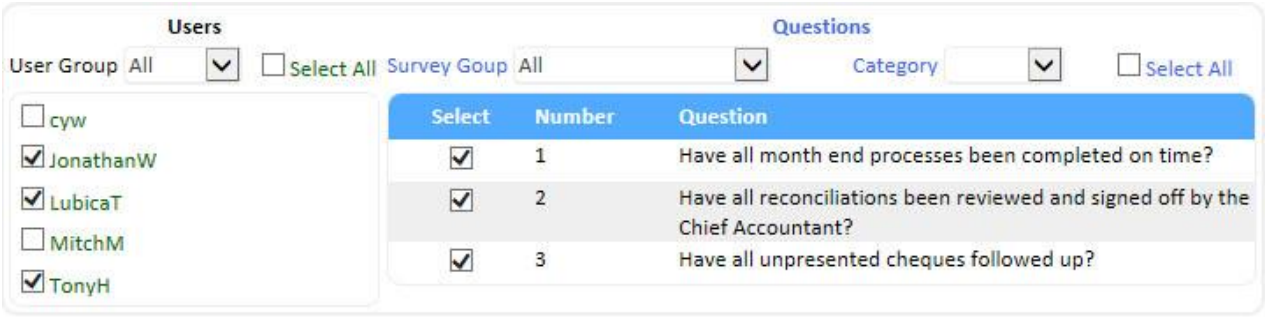
To create a One-off Survey

To create a new survey, first select the type of survey desired:

Then enter a name for the survey and a description. The description will be shown on the survey form the users will use to complete the survey and should briefly describe the purpose of the survey and special instructions to complete the survey, if any.

If required, enter a deadline date for the completion of the compliance survey.

Tick the users to be included in the survey and tick the question to be answered.



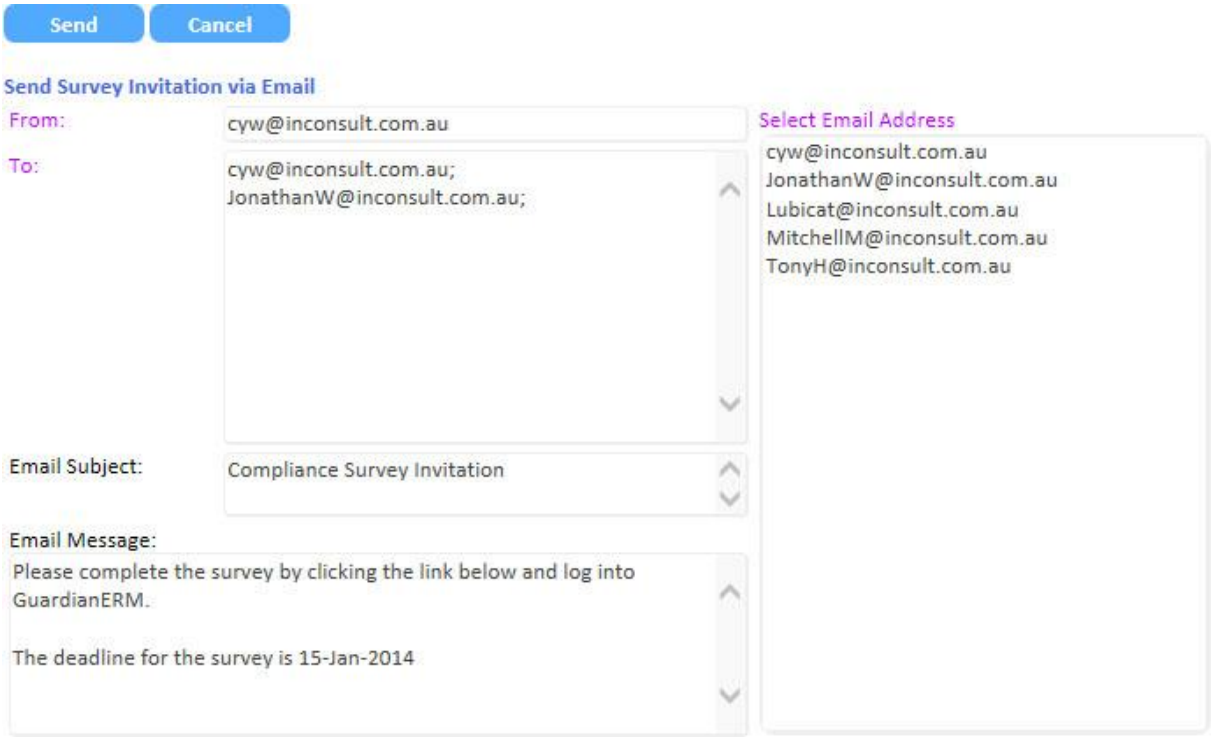
You can filter the users using the User Group dropdown list if user groups have been created.

You can filter the questions using the Survey Group and/or Category dropdown lists if they have been created.

You can click the Select All boxes to select all users or all questions on the lists. Un-ticking the Select All box will deselect all items.

Click the Save button at the top to save the compliance survey.

If you want to send an email to the selected users, click the Email button instead. The new survey will be automatically saved and an email dialogue box will pop up,



You can change any of the email fields. You can add more recipients by clicking the desired item on email address list. However, if the user is not included in the survey when it was created, the user will not see the survey after logged in.

The GuardianERM link will be inserted into the email by the system when the email is being sent.

Send the email by clicking the Send button or cancel the email by clicking the Cancel button.

If you did not send the email when creating the survey, you can always send it or resend it using the Modify Survey function.

<u>To create a Recurrent Survey</u>

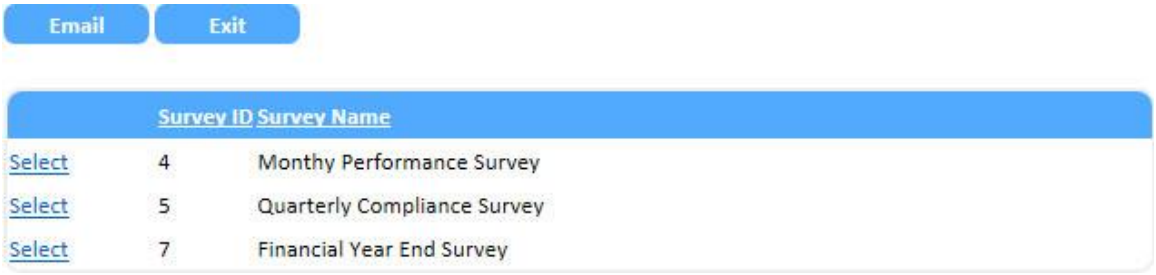
The process is the same as the one-off survey except that you must link users to each question selected for the recurrent survey. Users can be linked to questions in the Questions Maintenance function.

Select Recurrent as the Survey Type. The user selection panel will be deactivated as users are already included in the questions selected. Enter the name, description and

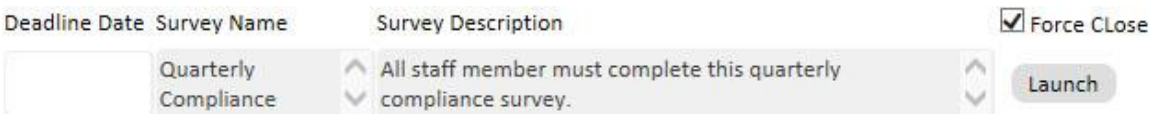
deadline date and select questions as in the one-off survey. Click Save to save the survey.

To Launch a Recurrent Survey

To launch a recurrent survey, click the Launch Survey button at the top button bar.



On the list displayed, click the Select button to launch the desired survey.



Enter a deadline date for the survey and if you would like to force close all previously launched surveys using this template, tick the Force Close box. Click the Launch button and the survey will be ready for completion immediately.

If you would like to send an email to each participant included in the survey, click the Email button. You can add or remove participants and change the subject and the message of the email. A link to the survey for the participant will be automatically appended to the email.

To Modify a Survey

To modify an existing survey that has no answer recorded, tick the Select box for the survey and then the Modify Survey button at the top. The survey must have a New status to be modified.

Status ☑ New ☑ In Progress Set Filter

Select		Survey ID	Survey Name	Survey Type	Status	Deadline	
☐	Open	7	Financial Year End Survey	Recurrent	New		Print
☐	Open	2	General Survey Jan 2014	One-off	In Progress	05-Feb-2014	Print
☐	Open	1	General Executives Survey	One-off	In Progress	15-Feb-2014	Print
☐	Open	4	Monthy Performance Survey	Recurrent	In Progress	01-Mar-2014	Print
☐	Open	3	General Survey Feb 2014	One-off	New	05-Mar-2014	Print
☐	Open	6	General Survey March 2014	One-off	In Progress	05-Apr-2014	Print

You can change the details of the survey the same way you create a new survey. If you want to delete the survey permanently, click the Delete button.

On the survey questionnaire page presented to the user, the identifier is not shown, instead a sequential question number, that is, 1, 2, 3 and so on is shown. The questions are numbered in the order they appear on the Create New Survey screen by default. These question numbers can be re-ordered using the Modify Survey function.

Select	Identifier	Number	Question
☑	FIN1	7	Was last month's month end process completed on time?
☑	GEN1	6	Have you read the corporate policy document during the last quarter?
☑	GEN2	3	Did your department achieve the attendance level standard last month?
☑	GEN3	2	Have all customer inquiries been attended to last month?
☑	GEN4	4	Describe the general staff morale.
☑	GEN5	1	Please comment on the last customer survey results.
☑	SLS1	5	Did you attend the Trade Practices Act training session last year?

To Modify a Recurrent Survey Template

To modify a recurrent survey template, select Recurrent Survey Template on the Compliance Survey main screen:

Recurrent Survey Templates

Survey Type: ○ Active Surveys ◉ Recurrent Survey Templates

Select	Survey ID	Survey Name
☐	7	Financial Year End Compliance Survey

Select the desired template to modify and click the Modify Survey button at the top button bar.

Compliance Survey Roll Over

To simplify the process of creating recurring surveys, GuardianERM provides a Compliance Survey Roll Over function.

Select a compliance survey from the list and click the Roll Over to New Survey button. The selected survey details will be displayed. You can modify any data the same way as creating a new compliance survey.

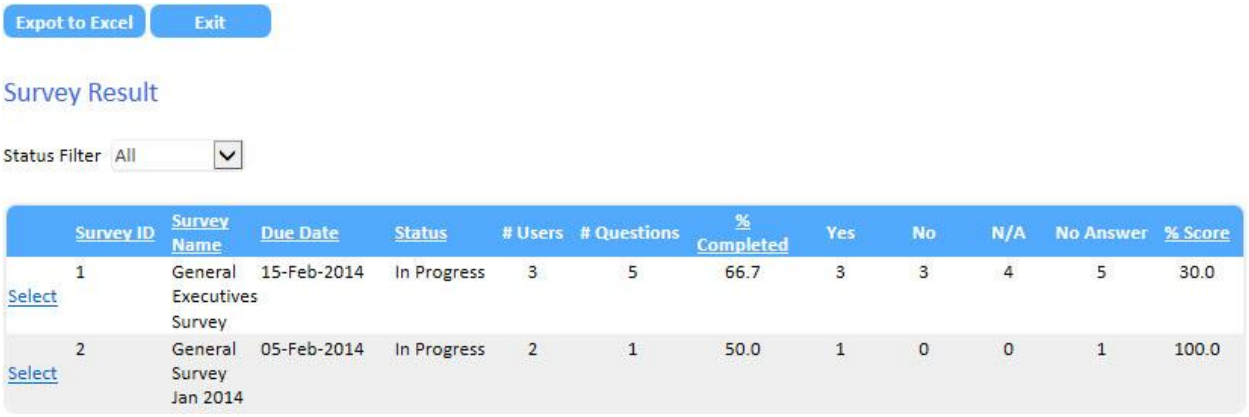
You should change the name and deadline date for the new survey.

Click the Save or Email button at the top to complete the roll over.

Survey Results

You can view the compliance survey results in summary or detailed formats.

The Results page starts with a list of all surveys recorded in the system.



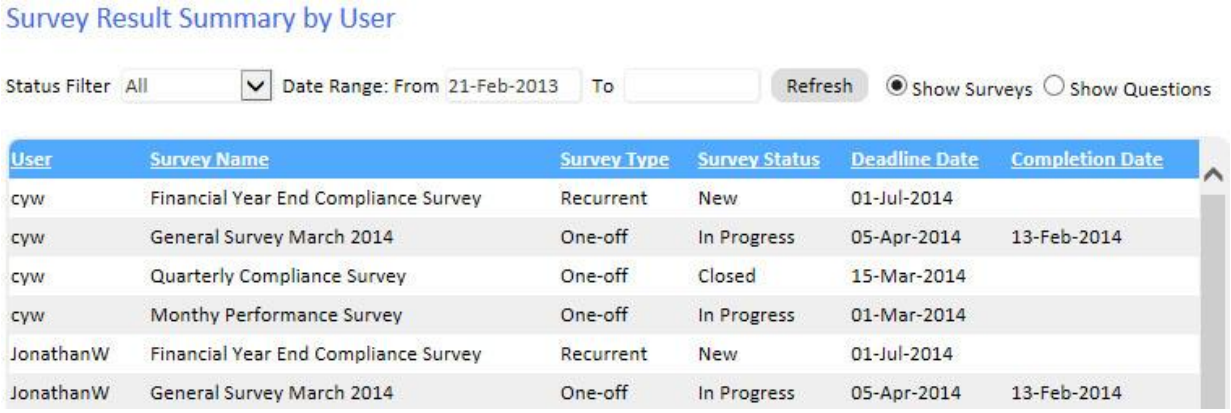
	Survey ID	Survey Name	Due Date	Status	# Users	# Questions	% Completed	Yes	No	N/A	No Answer	% Score
Select	1	General Executives Survey	15-Feb-2014	In Progress	3	5	66.7	3	3	4	5	30.0
Select	2	General Survey Jan 2014	05-Feb-2014	In Progress	2	1	50.0	1	0	0	1	100.0

You can filter the list by the survey status by selecting the desired status.

The list can be exported to Excel by clicking the Export to Excel button.

To view the results of a survey, click the Select button on the list.

If you prefer to view the results by user, click the By User button at the top.



User	Survey Name	Survey Type	Survey Status	Deadline Date	Completion Date
cyw	Financial Year End Compliance Survey	Recurrent	New	01-Jul-2014	
cyw	General Survey March 2014	One-off	In Progress	05-Apr-2014	13-Feb-2014
cyw	Quarterly Compliance Survey	One-off	Closed	15-Mar-2014	
cyw	Monthy Performance Survey	One-off	In Progress	01-Mar-2014	
JonathanW	Financial Year End Compliance Survey	Recurrent	New	01-Jul-2014	
JonathanW	General Survey March 2014	One-off	In Progress	05-Apr-2014	13-Feb-2014

You can also view the result by user by question. Select the Show Questions button at the top right-hand corner and select the users you wish to include in the report. The results can be filtered by the Survey Status or a date range. The date used is the deadline date of the survey.

Summary Survey Results

The summary page lists all the questions in the selected survey and the answers for each participant in the survey.

	Identifier	Question	JonathanW	MitchM	TonyH
Select	GEN1	Have you read the corporate policy document during the last quarter?	No	Yes	
Select	GEN2	Did your department achieve the attendance level standard last month?	Yes	No	
Select	GEN3	Have all customer inquiries been attended to last month?	Yes	No	
Select	GEN4	Describe the general staff morale.	NA	NA	
Select	GEN5	Please comment on the last customer survey results.	NA	NA	

To view the detailed answers with comments, click the Select button in front of a question.

You can also view the summary result by user. Click the By User button.

Survey Name: General Executives Survey

○ By Question ◉ By User

	UserID	GEN1	GEN2	GEN3	GEN4	GEN5
Select	JonathanW	No	Yes	Yes	NA	NA
Select	MitchM	Yes	No	No	NA	NA
Select	TonyH					

To view the detailed answers, click the Select button in front of a user.

Detailed Survey Results

If you have selected By Question, the Survey Result Detail screen will show the participants (users) of the survey and their answers and comments for the selected question.

Survey Name: General Executives Survey

◉ By Question ○ By User

Question: GEN3 - Have all customer inquiries been attended to last month?

UserID	Answer	Comment	Deadline	Completion
JonathanW	Yes		15-Feb-2014	
MitchM	No	Backlog in customer service due to abnormally high sick leave.	15-Feb-2014	09-Jan-2014
TonyH			15-Feb-2014	

If you have selected By User, you will see the result details for all the questions answered by the selected user.

Survey Name: General Executives Survey

○ By Question ◉ By User

User: MitchM

Identifier	Question	Answer	Comment	Deadline	Completion
GEN1	Have you read the corporate policy document during the last quarter?	Yes	Every monthly staff meeting.	15-Feb-2014	09-Jan-2014
GEN2	Did your department achieve the attendance level standard last month?	No	Only 63%.	15-Feb-2014	09-Jan-2014
GEN3	Have all customer inquiries been attended to last month?	No	Backlog in customer service due to abnormally high sick leave.	15-Feb-2014	09-Jan-2014
GEN4	Describe the general staff morale.	NA	Fair. Excessive sick leave caused lots of backlog and overtime.	15-Feb-2014	09-Jan-2014
GEN5	Please comment on the last customer survey results.	NA	Only 72% satisfied, lots of complaints on late responses.	15-Feb-2014	09-Jan-2014

Incident Management

Risk management involves, to a large extent, the management of probabilities. No matter how good your risk management system is, some events will end up with an undesirable outcome, or your business objectives not being achieved.

In risk management, it is important that these actual outcomes be recorded and analysed as they may provide valuable information in relation to ineffectiveness or breakdown of controls. GuardianERM.Net provides a root cause analysis platform so that incidents can be analysed logically to identify the root cause of the issue and the proper treatment designed instead of producing often damaging knee-jerk reactions. On the Incident Register screen, you may search for a particular incident or filter the list.

Access to incidents is restricted. If you cannot see incidents that you think you should be able to, please contact your system administrator to have the access authority granted.

Incident Management Module Security

As incident data may contain sensitive or personal information, GuardianERM.Net has the following security measures in place:

- A user with Incident Management authority and read (or write) access to an organisation unit to which an incident is attached, the user will have unrestricted access to the incident.

- A user with Incident Management authority can also reopen a closed incident if the incident was closed within the last 7 days.

- A user with Incident Management authority can access the Incident Code Maintenance page to add, modify or delete items on dropdown lists.

- A user with Incident Management authority can access the Incident Code Maintenance page and restrict certain data fields to be modifiable by users with Incident Management authority only. This restriction will override all otherwise unrestricted access.

- A user **without** Incident Management authority but has write access to an organisation unit, the user has unrestricted access to all incidents attached to that organisation unit.

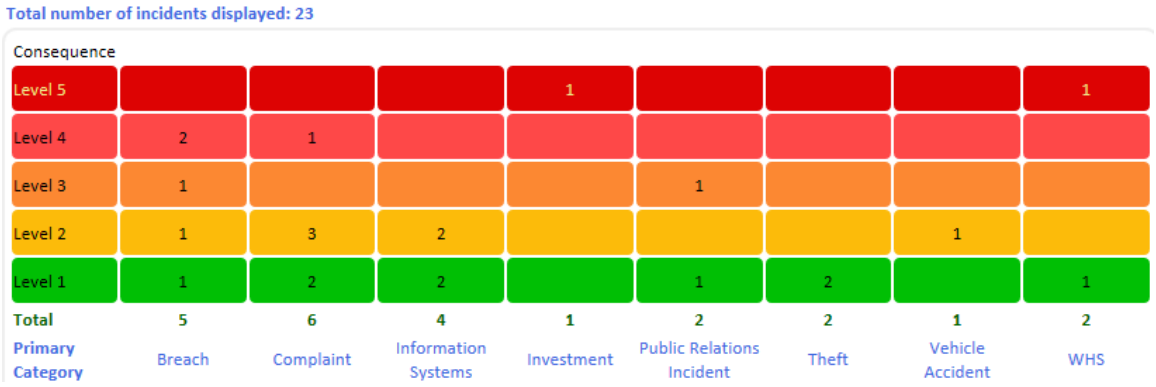
- A user has unrestricted access to incidents the user originally created.

Note: "Unrestricted Access" by users other than those with Incident Management authority is still restricted by data field restriction if implemented. To implement data field restriction, the system administration has to set the system parameter "IncidentRestrictEdit" to True and a user with Incident Management authority specifies the fields to be restricted on the Incident Code Maintenance page under Restricted Fields.

The Incident Register

By default, the Incident Register shows all the incidents the user is authorised to access. Select **Incidents for Default Organisation Unit** at the top of the screen to view incidents attached to the user's default incident organisation unit. Users with Incident Management authority will see all registered incidents and as such has no Default Organisation Unit selection.

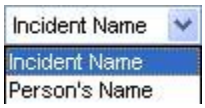
The Incident Register has a summary table showing the distribution of incidents across the primary categories and the consequence levels. As the consequence levels can be different for different categories and user definable, the summary table shows Levels 1 to 5 (1 being the lowest and 5 the highest). You can click a cell on the table to show the incidents for the category and consequence level.



You can filter the list by status using the Status Filter:

or filter by Incident Category:

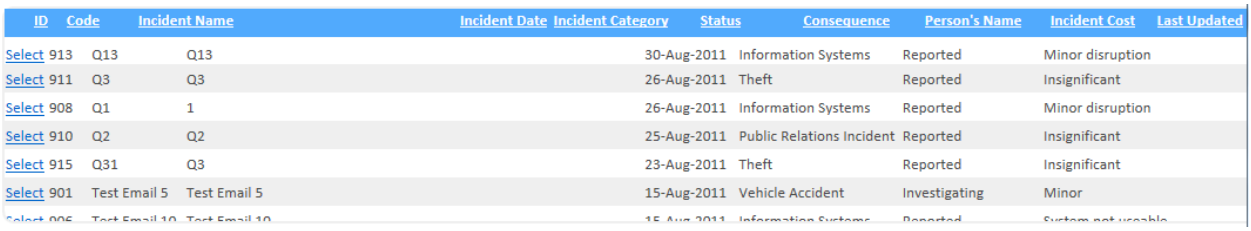
To search for incidents, select whether you want to search by incident name or by the name of a person (if it is an OH&S related incident):



Enter the search text, which can be part of the full name in the search text field and click the Search button.

To clear the search, click the Clear button.

You can also sort the list by clicking the heading of each column.



ID	Code	Incident Name	Incident Date	Incident Category	Status	Consequence	Person's Name	Incident Cost	Last Updated
Select 913	Q13	Q13	30-Aug-2011	Information Systems	Reported	Minor disruption			
Select 911	Q3	Q3	26-Aug-2011	Theft	Reported	Insignificant			
Select 908	Q1	1	26-Aug-2011	Information Systems	Reported	Minor disruption			
Select 910	Q2	Q2	25-Aug-2011	Public Relations Incident	Reported	Insignificant			
Select 915	Q31	Q3	23-Aug-2011	Theft	Reported	Insignificant			
Select 901	Test Email 5	Test Email 5	15-Aug-2011	Vehicle Accident	Investigating	Minor			

Recording an Incident

An incident should be recorded as soon as practical and the Incident Register updated when more information becomes available. When a new incident is saved, an automatic notification email will be sent to recipients on the Incident functional group. See Email List (in the Administration Manual or online help) for details. To turn off the automatic email notification, change the System Reference setting for IncidentNotifyEmail to False.

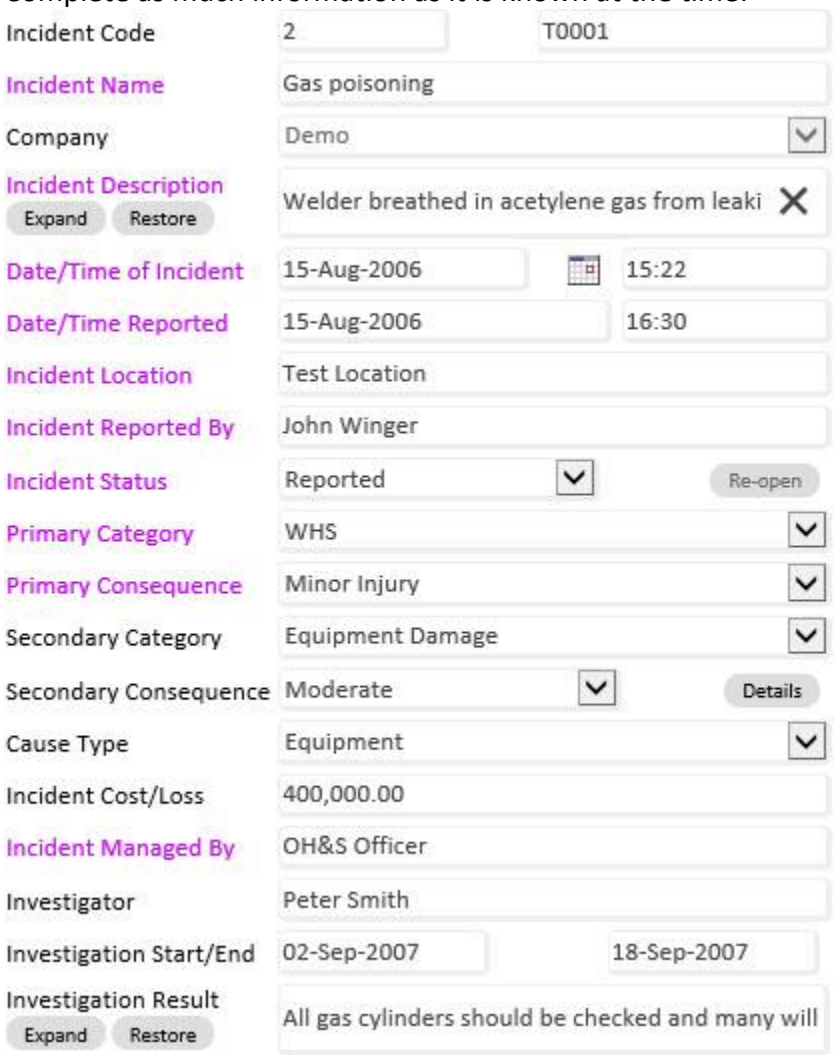
To record an incident, select Incident Register on the Main Menu or the dropdown menu.

Click the New Incident button.

You can also open an existing Incident file to view or edit. The list of incidents can be filtered by their status: All, Open or Closed. The list can be sorted by clicking the column heading, Code, Incident or Date. The date is sorted in descending order, that is, the latest date will appear at the top.

To edit an existing incident, click the Select link on the list of Incidents.

Complete as much information as it is known at the time:



Most of the data fields are self-explanatory.

Incident Code	A user-assigned code to identify the incident. The number in front is a system-generated Incident ID and cannot be changed.
Incident Name	A short name to identify the incident.
Company	Select the company the incident related to.
Incident Description	A detailed description of the incident.
Date of Incident	The recommended date format is dd-mm-yyyy.
Time of Incident	24-hour time format, e.g. 3:20 PM should be entered as 15:20.
Secondary Category	If an incident falls into two major categories, like a car accident involving both vehicle damage and injury, use the main category for the more important one and select another category as the secondary category. Additional data entry forms can be accessed by clicking the Details button next to the Secondary Consequence dropdown list.
Consequences	The first field is for the main category and the second one for the secondary category.
Cause Type	Select a cause to categorise the cause of the incident.
Incident Cost/Loss	The total cost and loss value of the incident, including both categories where applicable.

If WHS is selected from the Category dropdown list, an Injury/Illness form needs to be completed.

Click the Save button to save the incident and any additional forms that are displayed. Optionally, to link an incident to an organisation unit, risk and/or control, click the Link Incident button near the top of the screen.

Note: You can view the causes and treatment of an injury/illness incident by clicking the Treatment Plan button:

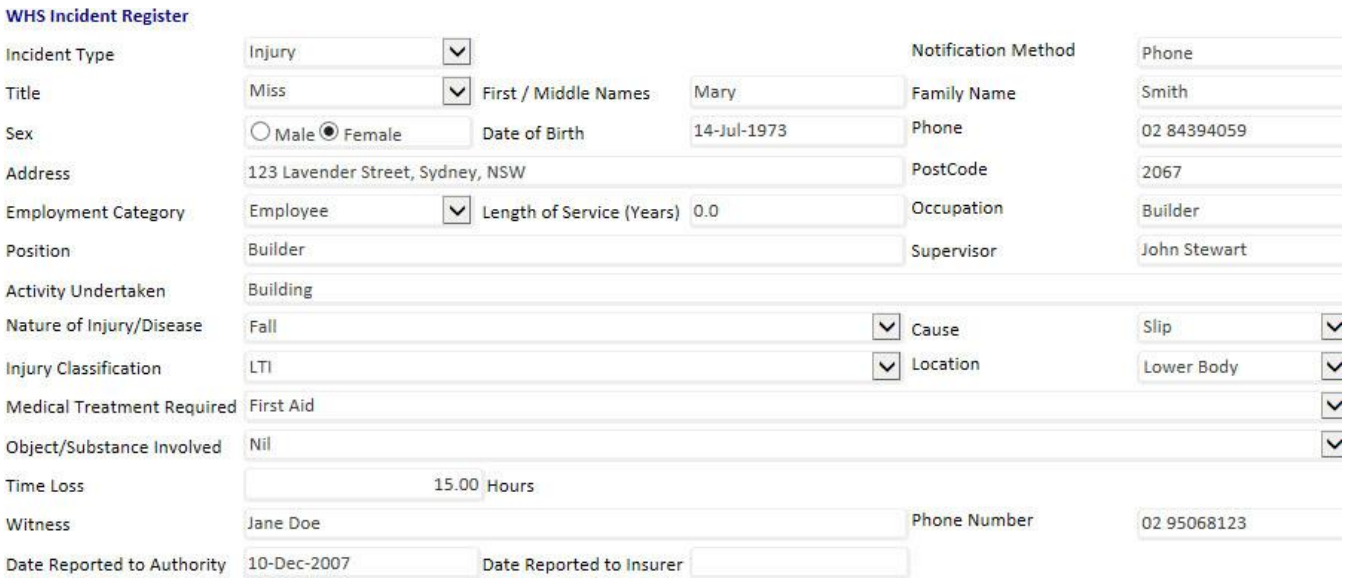
Cause	Treatment Details	Due Date	Completed Date
Wet floor	Dry the floor	02-Sep-2007	Nil
Leaking pipe	Fix the leak	03-Sep-2007	30-Aug-2007
Inadequate maintenance	Review maintenance process.	15-Sep-2007	Nil
Pipe very old	Replace pipes.	19-Dec-2007	30-Aug-2007
Janitor off sick	Nil	30-Dec-2007	30-Aug-2007
Worker was drunk	Counsel worker on company's policy of no drinking at work.	04-Sep-2007	30-Aug-2007

Note: You can send the selected Incident Report by email to the owner and risk manager of the selected organisation unit by clicking the Email button. You can change the recipients, email subject and add an email message on the pop-up dialog box.

Incident – Work Health and Safety

If an incident is an injury or illness (involving human beings), Work Health and Safety legislations in Australia and many countries in the world require an Injury/Illness report be prepared and submitted to the relevant government department.

If the Incident Category is WHS, a WHS form will be displayed after the incident is saved:

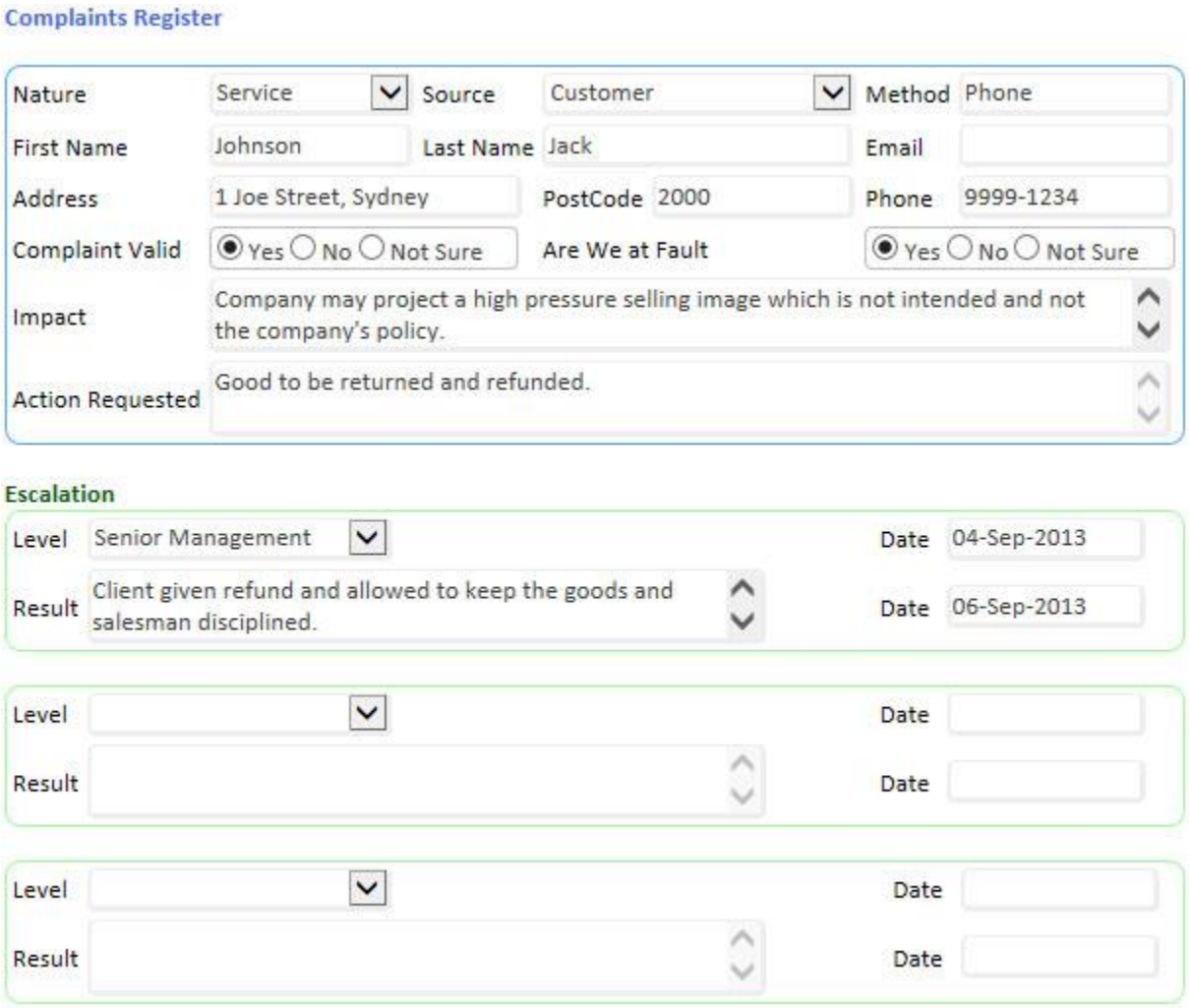


Complete all known information at the time and update the data when more information becomes known.

Click the Save button to save the Injury/Illness form.

Incident – Complaints

If the Incident Category selected is Complaint, a Complaint form will be displayed after the incident is saved:



Complete all known information at the time and update the data when more information become known.

Click the Save button to save the form.

Incident – Breach

If the Incident Category selected is Breach, a Breach form will be displayed after the incident is saved:

Complete all known information at the time and update the data when more information become known.

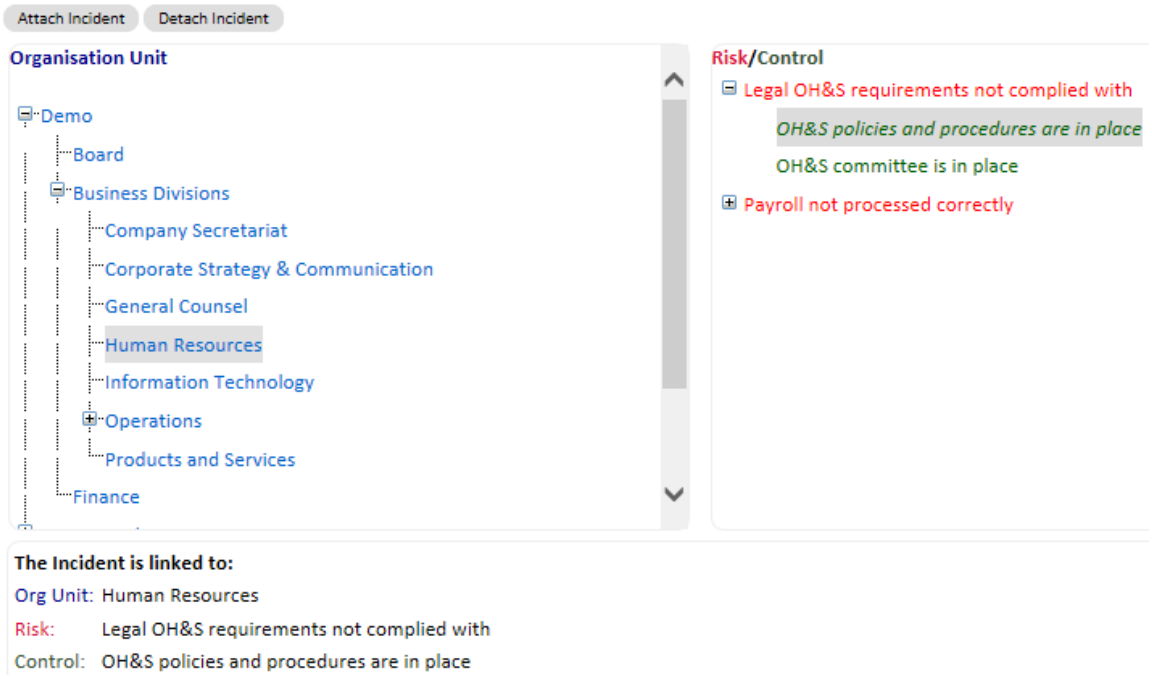
Click the Save button to save the form.

Attaching Incident to Risk Management Structure

While it is optional to attach an incident to the risk management structure, to provide information to the business managers about possible control weakness as reflected in an incident, it is recommended that incidents are linked to the Risk Management Structure where possible.

After recording the details of an incident, click the Link Incident button.

After selecting an organisation unit, if the unit has risks and/or controls attached, they will be displayed in the Risk/Control panel:



After selecting an organisation unit, a risk or a control, click the Attach Incident button. The items in the risk management structure the incident is attached to will be displayed at the bottom section.

Root Cause Analysis and Treatment

In the management of incidents, a very important task is to find out why the incident happened and what can be done to lessen the impact and to prevent it from happening again.

In a lot of cases, organisations tend to produce knee-jerk reactions to incidents. For example, after a fraud is uncovered, the payment system is made so restrictive that it hinders the proper functioning of the organisation.

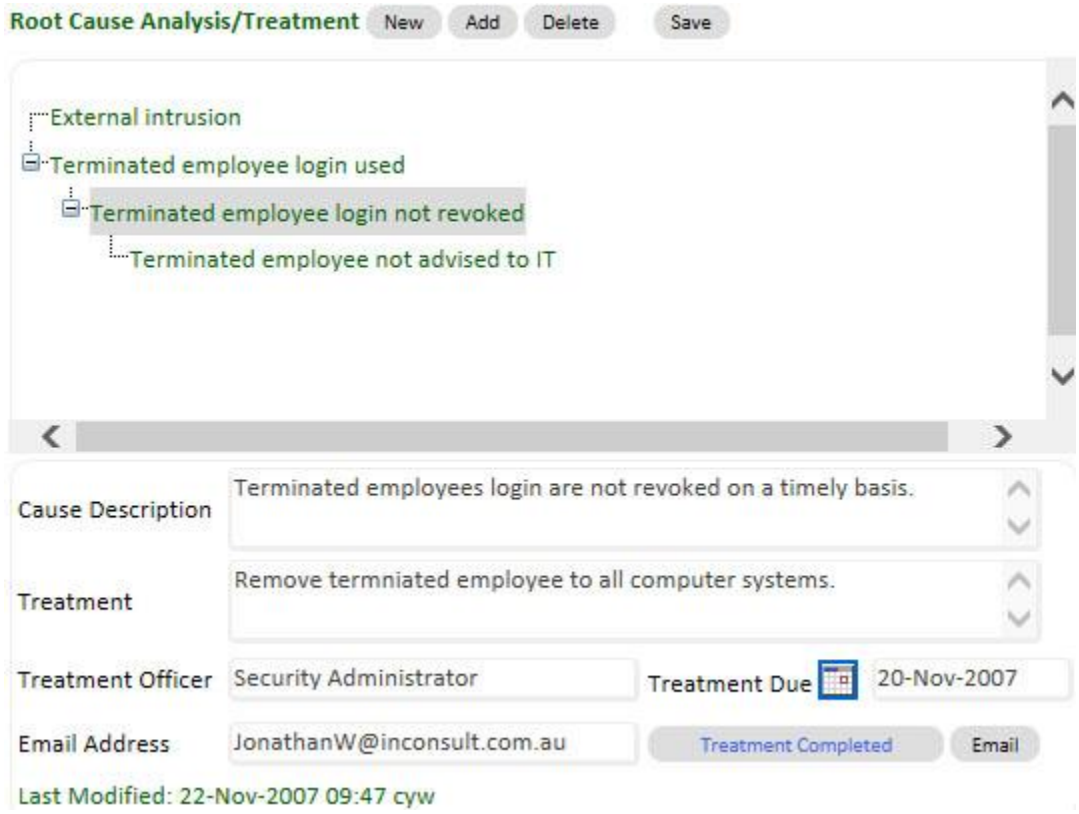
GuardianERM.Net provides the framework to perform a Root Cause analysis of the incident which will lead to more appropriate treatments for the root cause of the problem.

To start the Root Cause analysis, on the Incident Register screen, after creating or selecting an incident, click Cause & Treatment and then click the New button next to Root Cause Analysis/Treatment:

Enter a short name and a detailed description of the most immediate or direct cause of the incident. Click Add Cause to create the new cause.

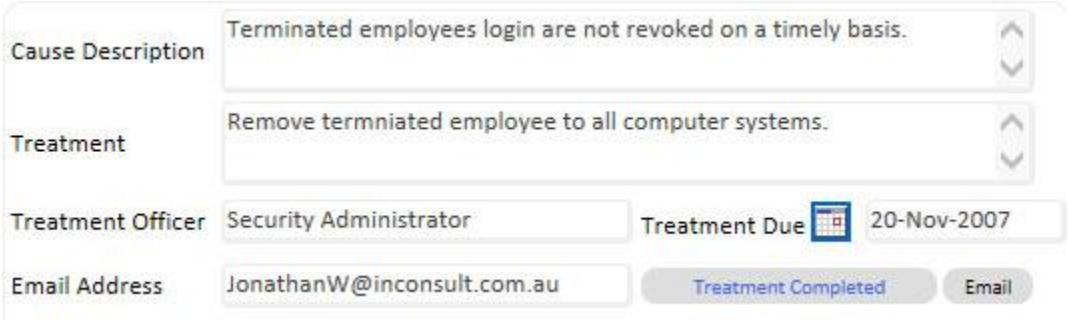
If you want to create another immediate cause, click the New button again.

If you can identify a cause which is the cause of the immediate cause, click the Add button and enter a name and description of the cause:



By repeatedly tracing the immediate cause to the eventual root cause, a relational tree of causes can be established (as the above diagram).

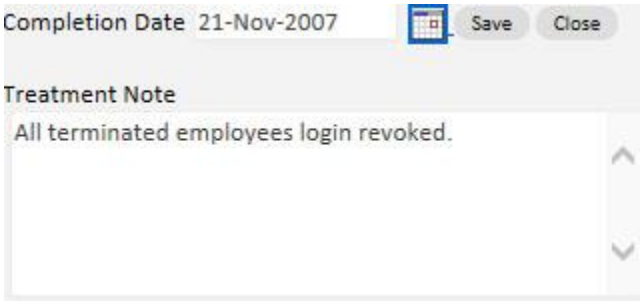
To add treatments to any of the causes, select the cause and enter the details:



If the treatment has not been performed, leave the Treatment Date blank for now and enter the date later when the treatment is implemented.

The treatment plan can be emailed by clicking the Email button. You may change or add recipients (separated by semi-colons ;) and change any data on the email before sending.

To complete the treatment, click the Treatment Completed button and enter the details and click the Save button:



Incident Code Maintenance

The selections on the dropdown lists in the Incident Management module (Incidents and Issues) are user created, except for the incident categories WHS, Breach, Complaint and Client Challenging Behaviour.

To create or modify the selections, the user must have Incident Management authority.

Click the link where you want to create or modify selections. A list of selections (if any) will be displayed.

If you would like to use the Express Incident Registration form as the default new incident registration form instead of the full Incident Registration form for all users, tick the Use Express Incident Registration Form box. If the box is not ticked, the system will default to the full Incident Registration screen.

Click the Add New Item button to create a new selection.

Click the Edit or Delete link for an item to modify or delete. An item that has been used in any incident cannot be modified or deleted.

The ID is system generated and cannot be modified.

Note: If an item has been used in an Incident or Issue, the item cannot be modified or deleted.

To restrict modifications to certain fields or functions, use the Restricted Fields link. Contact GuardianERM Support to obtain the proper field or function names.

Certain compulsory fields can be made not compulsory by un-ticking the field names using the Compulsory Fields configuration function.

Certain data fields can be disabled by ticking the field names using the Disabled Fields configuration function. Disabled fields are not shown on the Incident Details screen.

Issues Log

The Issues Log can be used to record issues identified outside of the normal risk evaluation, audit or incident management processes. The Issues Log is accessed from the Main Menu or the top menu bar:

	ID	Issue Name	Organisation Unit	Location	Department	Process	Date Raised	Status	Source	Importance
Select	3	Internal Audit Identified Security Issue	Demo - Board				06-Sep-2011	Investigating	Audit	1 - Low
Select	4	Pending interest rate increase may impact loan volume	Demo - Finance				16-May-2012	Recommendation Implemented	Issues Log	0 - Recommendation
Select	1	Possible Large Foreign Exchange Loss	Demo - Finance	Sydney	Finance	Investment	01-Sep-2011	Recommendation Implemented	Audit	0 - Recommendation

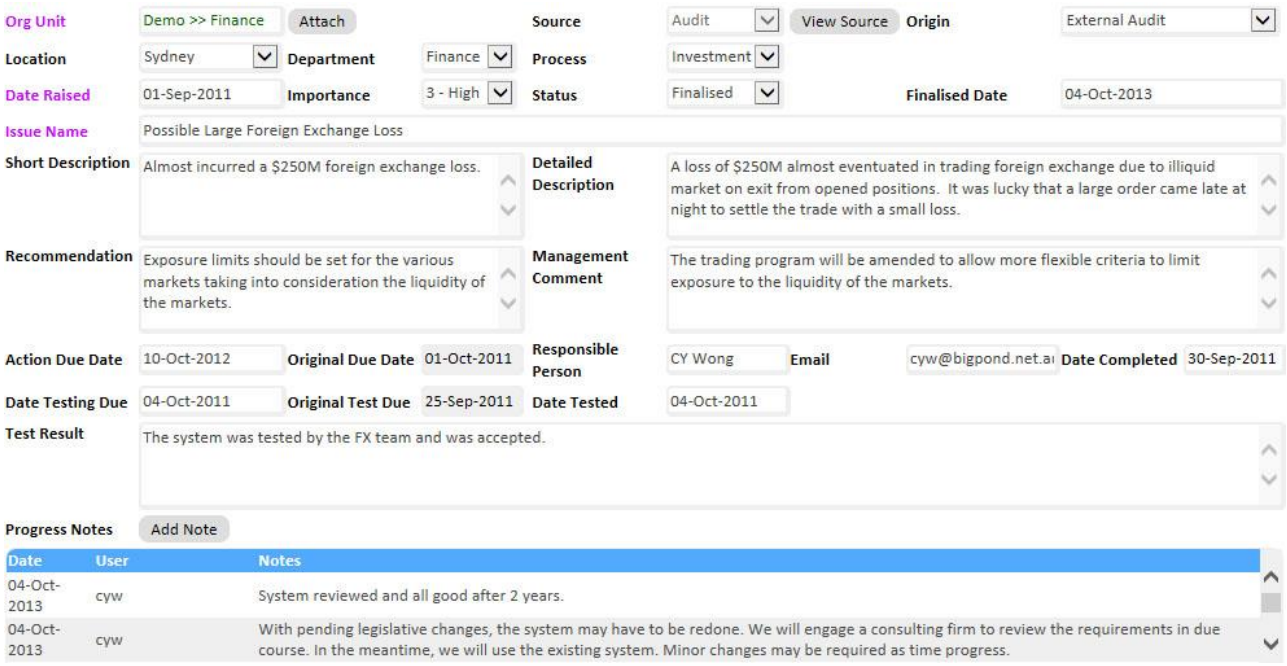
The Issues Log can be filtered by Company, Source and Status. The log can be sorted by clicking on the heading.

The Issues Log is linked to the audit module where audit identified issues can be expanded and managed using the Issues Log.

To view an issue, click the Select link.

Issue Details

The Issue Details screen will look something like this:

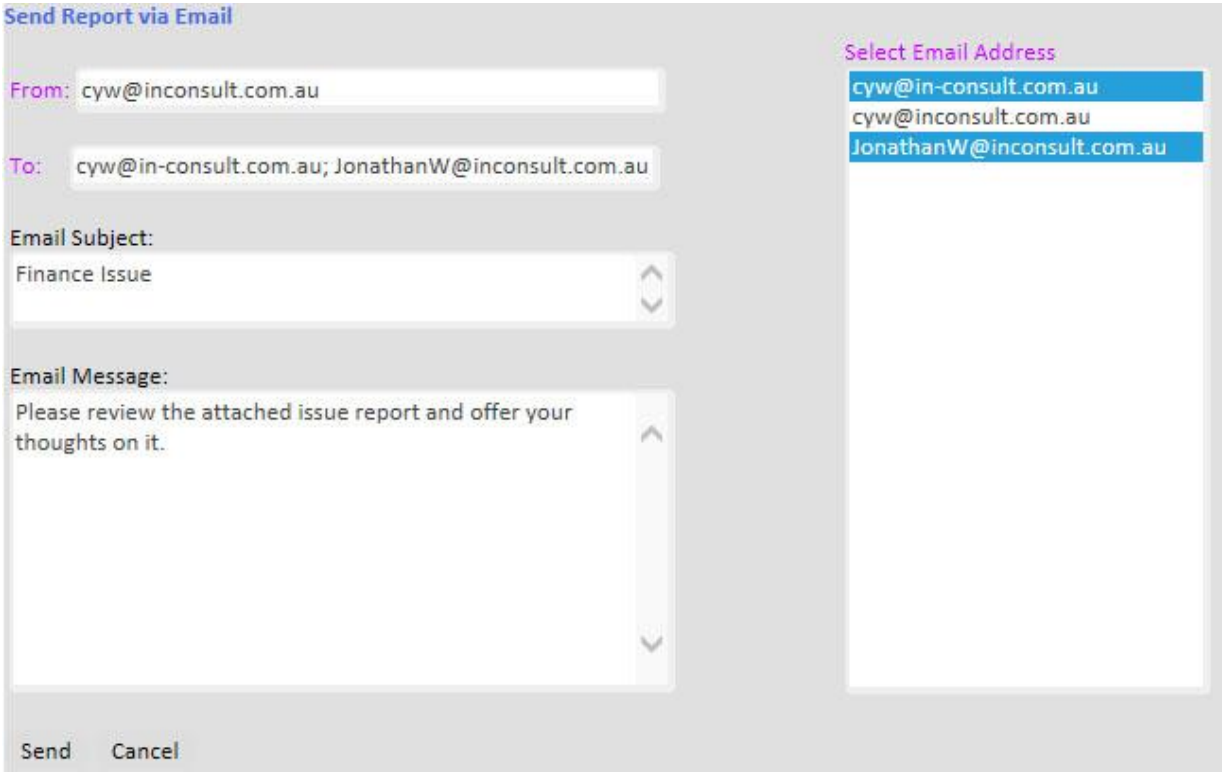


Data Field	Explanation
ID	A system-generated identification number for the issue. Cannot be changed by the user.
Source	Defaulted to Issues Log. If the issue was created in the Audit Module, the source will be Audit. The source cannot be changed by the user.
Org Unit	Click the Attach button to attach the issue to an organisation unit.
Origin	(Optional) How the issue originated, e.g. external audit, internal review.
Location	(Optional) A location the issue applied to.
Department	(Optional) A department the issue applied to.
Process	(Optional) A process the issue applied to.
Importance	The levels can be changed under System References in the Administration Module. Can only be changed by an Administrator.
Status	Select the appropriate status from the dropdown list. Once an issue is finalised, the data cannot be changed any more.

The other data fields are self-explanatory.

If you email the report, the default recipient is the Responsible Person's email address. You may change that or add other recipients separated by semi-colons (;). You can also select email addresses from the list on the right. For multiple selections, hold down the Ctrl key and click the desired email addresses.

The issue report will be attached to the email automatically. It may be more meaningful to the recipients if an appropriate Subject and Message is entered.



The bottom of the email will automatically include a link to GuardianERM. After the user logged onto the system, the system will automatically direct the user to the issue.

Reports

Guardian Reports

GuardianERM.Net has two powerful reporting functions, Guardian Reports and User Reports.

Guardian reports are pre-defined reports with many configuration options to tailor the report to the user's needs. User reports allow the user to define custom reports.

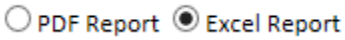
Guardian Reports:

The Guardian Reports function is opened in a new window such that you can review the reports while working online at the same time. It is particularly useful when you are working on exception reports as you can verify or correct problems online based on information obtained from the reports.

Applying various filters to selected areas of the risk management structure, the reporting function allows you to produce reports from complete listings of data to highlighting issues of special interest. The flexibility of preview the report online, printing hard copies or exporting to Microsoft Excel for further analysis adds to the functionality of the reports.

Note: You must allow pop-up in your Internet Explorer setting for GuardianERM.Net. Otherwise the reporting function will not work.

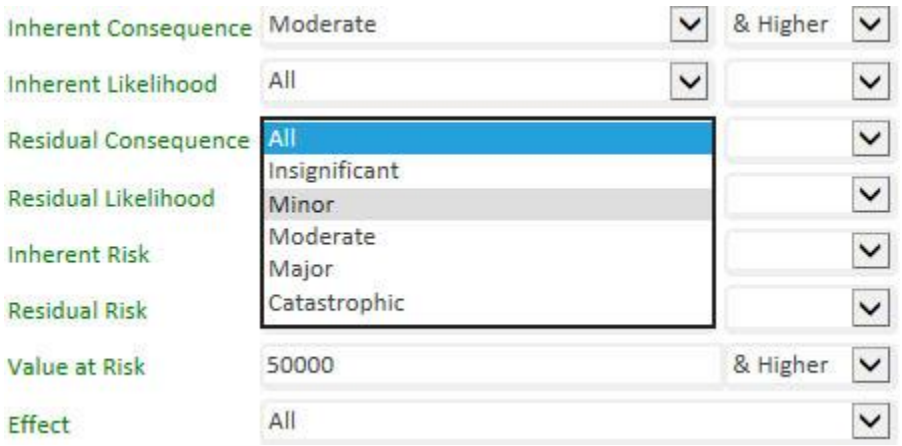
To start using the reports, select the type of report you like, PDF Report or Excel Report:



Select the desired report from the list:

Select the organisation unit(s) to be included in the report:

Select the filters, if any, to customise the report:



Some reports can be sorted in the order specified. Select a field to sort on and select whether you want the report to be sorted in ascending or descending order.

Most reports are preceded by one or more cover pages detailing what parameters and filters were selected to be included in the report. You can supress printing of the cover page(s) by ticking the No Cover page box at the top next to the Preview button.

Click the View Report button to view the report online. The report will be displayed in Portable Document Format (pdf). You need to have Adobe Reader installed on your computer to view the report.

If your selection results in no data being included in the report, a message will be displayed:

Use the Adobe Reader commands to save, print or email the report.

Excel Report

An Excel Report contains the raw data of the report in a format ready to be exported as Excel data to be downloaded to your computer and view with Microsoft Excel. You need to have Microsoft Excel installed on your computer.

An Excel Report looks like this:

Open in Excel | Help | Exit

Risk Listing

Location	Significance	RiskNo	RiskName	RiskDesc	Consequence	Likelihood	Effect	InherentRisk	ResidualRisk
Demo >> Finance	Significant	01 [M]	Material misappropriation of funds	Material misappropriation of funds either from claims, cash or investments	Catastrophic	Very Likely	Operational	Extreme	Low
Demo >> Finance	Significant	02	Adverse market fluctuations of Investments	Adverse market fluctuations of Investments	Catastrophic	Almost Certain	Operational	Extreme	Very High

To download the data, click the Open in Excel button. You will be prompted to Open or Save the data file. If you click Save, the data will be saved in your selected folder and you can open the file in Excel later. If you click Open, the file will be downloaded to your default download folder and Excel will start automatically showing the downloaded data.

User Reports

Users can create reports from scratch using the interactive User Reports function. The report is presented in a tabular format and can be downloaded to Excel for further customisation and printing.

Design User Reports

To be able to create or modify user reports, you need a special authority called Report Design. Check with your GuardianERM.Net system administrator if you have no access to the Design Reports function.

You can create reports and customise it to your specific needs using this function. Report definitions are saved and can be run any time in the future. However, be aware that this function is quite complex and the processing logic may not be the same as what you expect and you may end up with a report showing you incorrect data. In general, do not be over-enthusiastic when creating a report, especially in the beginning, and always verify the designed report using data on the online screens and the Guardian Reports, where available. Make your reports more manageable by including less data fields with fewer filter conditions to satisfy specific needs.

The GuardianERM security sanctions also apply to the reports. For example, if you have created a public report including an organisation unit where a user running the report has no read access, the user running the report will not see data for that organisation unit even if it was included in the design.

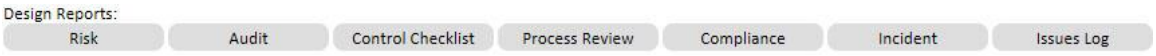
To allow a user to design a report, the user's security profile must include the User Report Design authority.

To modify an existing report, select the report you want to modify from the dropdown list. The modification procedures are the same as the Create a User Report.

To create a User Report

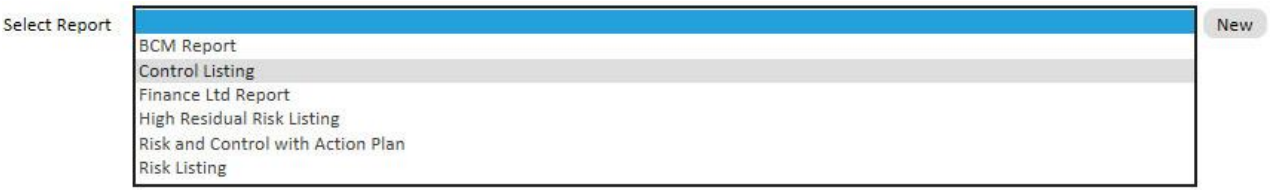
Click the Design Reports button on the GuardianERM.Net User Reporting System screen:

Select the report category by clicking the appropriate button:



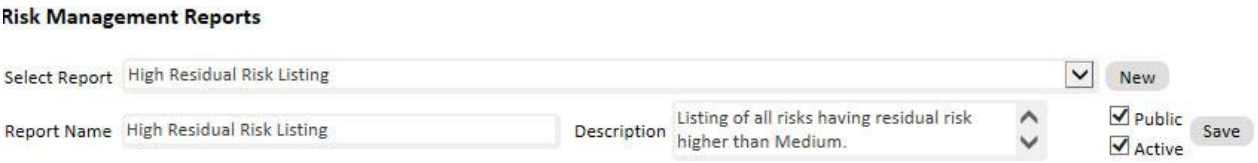
If you have multiple companies set up in your Organisation Units Library, select the company for the report from the Company dropdown list at the top of the page.

Click the 'New' button to start a new report:



Enter a name and an optional description for the report. Make sure the Active box is ticked and if you want all users to be able to run this report, tick the Public box. If the box is blank, only you, the creator of the report, can run the report. Click the Save button to save the report heading.

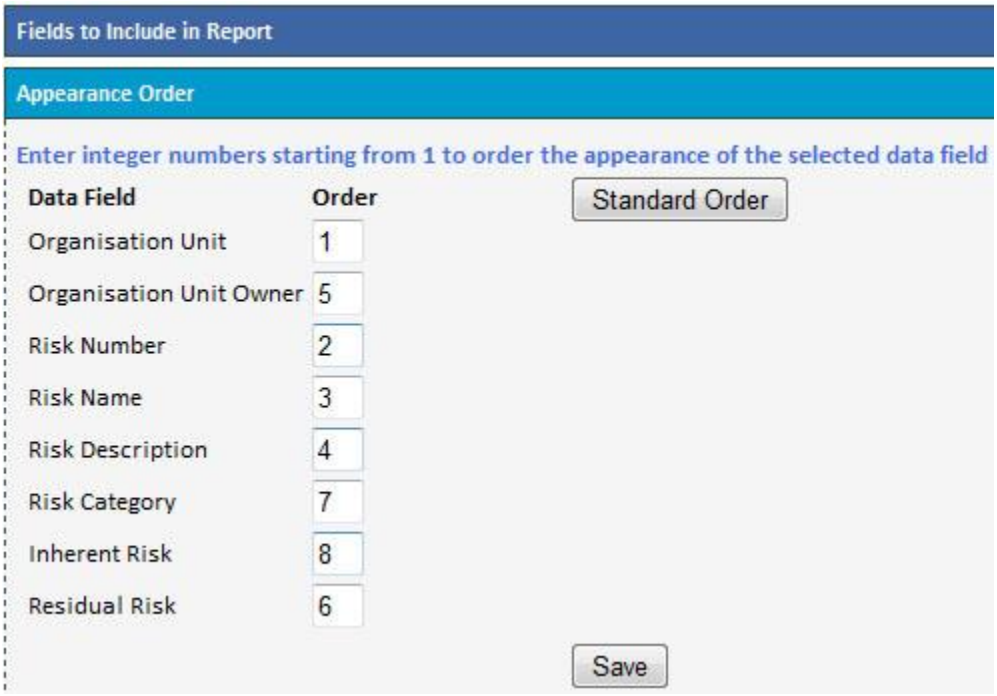
Note: If a report is made inactive (the Active box is not ticked), it will not be accessible any more.



From the Fields to Include in Report panel that appears, tick the data fields you want to include on the report

There is a limit of 15 data fields you can include in one report.

Once you have selected all the fields you want, click the Next button at the bottom to configure the appearance sequence of the selected data fields:



Enter integer numbers in the Order fields to denote which field comes before or after another field. In the above example, the report will show the data columns in this order:

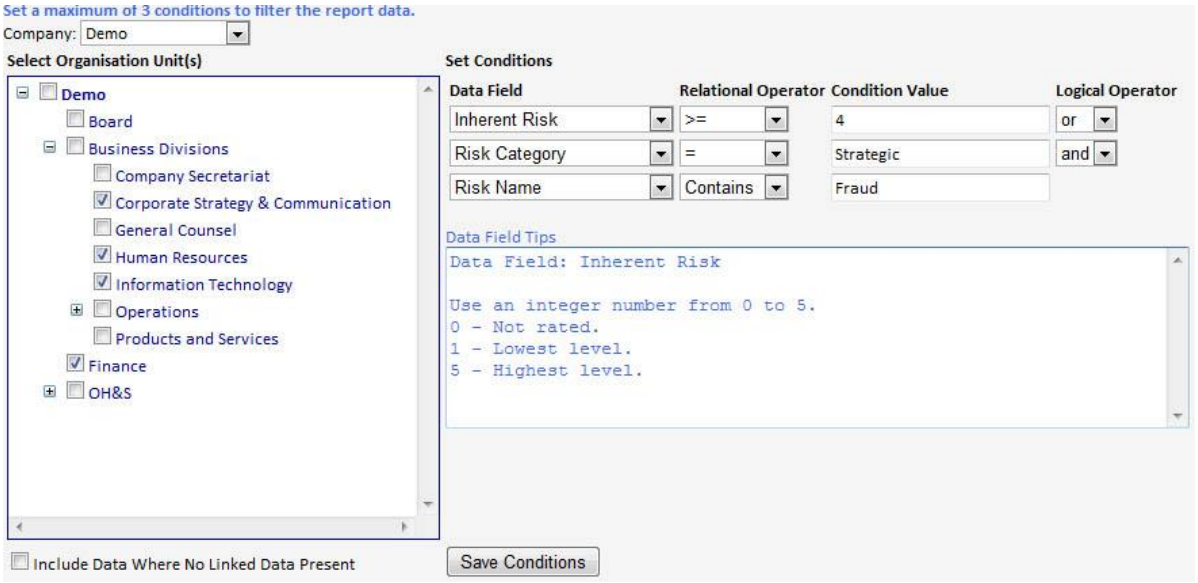
Organisation Unit
Risk Number
Risk Name
Risk Description
Organisation Unit Owner
Residual Risk
Risk Category
Inherent Risk

If you duplicate a number or have a number missing in the sequence, an error message will appear when you click Save prompting you to correct the error.

You can click the Standard Order button to re-order the fields to the default sequence. Click the Save button to continue onto configuring the report filters.

Note: If you are modifying an existing report and have changed the data field selections, the appearance order will be out of sequence. Either click the Standard Order to arrange the data fields using the default order or enter the sequence numbers manually.

Configuring the report filters:



When a data field selection is changed, the Data Field Tips box will show, where applicable, the type of data that is stored for that data field.

1. Select the organisation units you want to include in the report (where the report contains organisation units).
2. Select the data field from the dropdown list you want to apply a conditional filter to.
3. Select a relational operator from the dropdown list.
4. Enter the value in the Condition Value field.
5. Select the logical operator (and/or) from the dropdown list. This operator logically links the conditions together if you have more than one condition specified.
6. Click the Save Conditions button to save the filters and continue onto setting the sort order of the report.

Note: The logical operator is critical in determining what data is being selected for the report. Incorrect use will produce erroneous data. In the above example, only the risks that have a category of Strategic and a residual risk of 4 or above will be selected. If you use Or instead of And, then all risks with Strategic category regardless of the residual risk level and all risks with a residual risk level 4 or above regardless of what category they belong to will be selected.

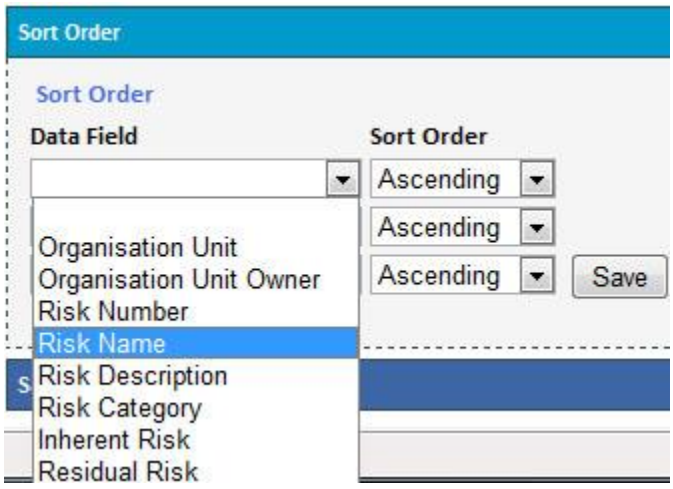
If you want to list all the data selected in a data field category whether there is data in data fields in categories to the right of the first selected category, tick the Include Data Where No Linked Data Present box. In the above example, if the box is ticked, then all organisation units selected will be listed on the report whether they have risks with residual risk level 4 or above. It is best to experiment with this to get the report you desire.

Note: Depending on the design of the report, ticking the Include Data Where No Linked Data Present box can produce a very large report and the report may take a long time to run.

Note: To remove a filter, clear the Condition Value text box and click Save.

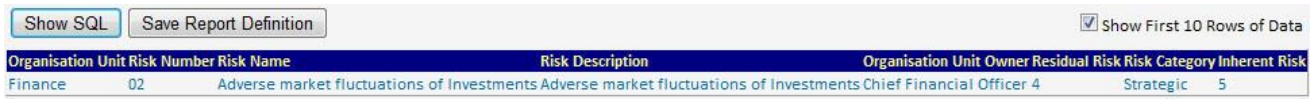
Tip: If the filed tips are not helpful enough and you do not know what value to use for the Condition Value field, do not use any filters and take a look at the sample report to see what kind of data is stored for the field.

You can now define the sort order of the rows contained in the report:



Select the first data field by which to sort the report rows and select either Ascending or Descending order.

Click the Save button when finished and a sample report will be shown:



Click the Save Report Definition button to save the report and now the report is ready to be run.

Note:

1. The production report is not exactly the same as the sample report as the sample report contains raw data which will be converted when the production report is run.

2. The sample report is useful to identify the condition value when setting the filters, e.g. Inherent Risk is an integer number instead of the Low, Medium text description that you see on the risk evaluation screen.

3. You can show more rows of the sample report by un-ticking the Show First 10 Rows of Data box. For large reports this may take a long time to run.

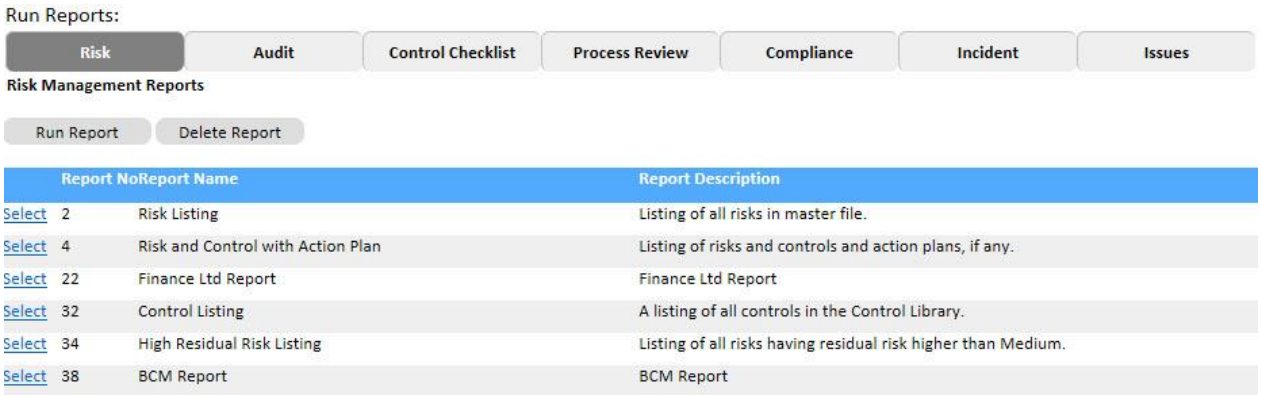
4. You can view the SQL (Structured Query Language) program that you have generated for debugging purposes by clicking the Show SQL button.

5. Once the definition is saved, you can go back to any previous sections and make changes by clicking the blue section Heading bar, e.g. Appearance Order or Sort Order.

Run User Reports

You can run all reports that were created by yourself and reports that are categorised as 'Public'.

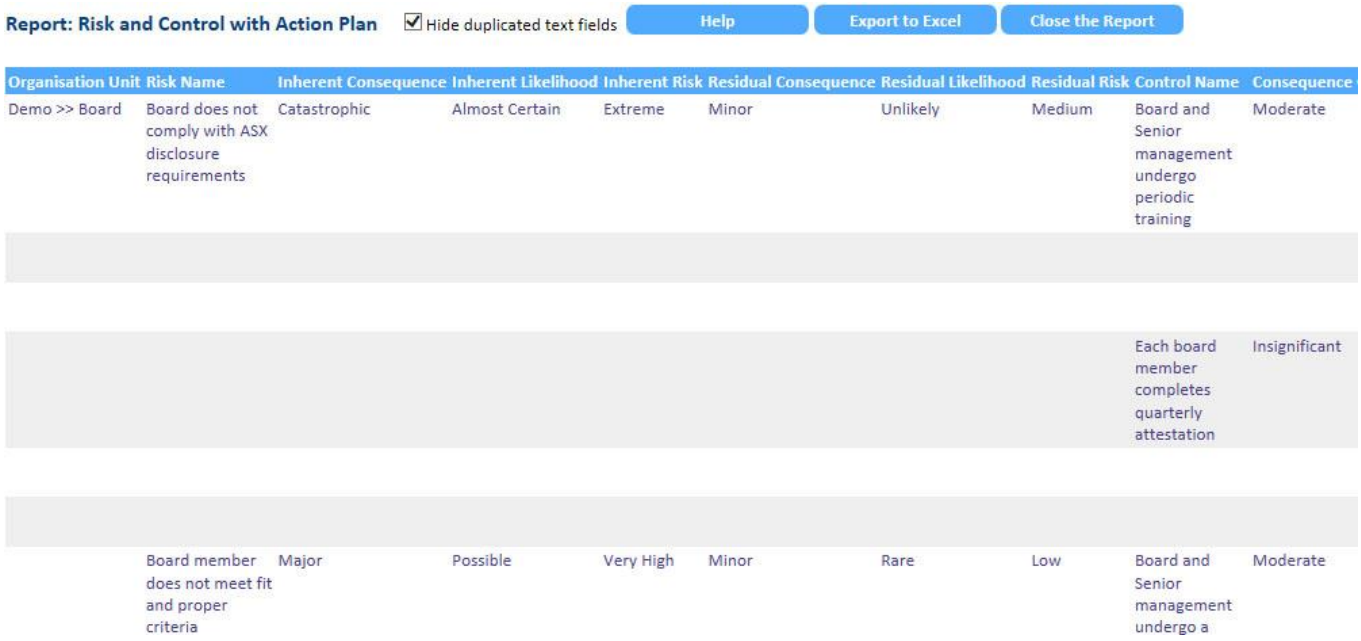
To run a report, first select a report category tab. Once a tab is selected, the available reports will be listed.



Click the Select link for the desired report and click Run Report.

On the report heading, click Export to Excel to download the report to your computer and your computer will automatically start Excel (you must have Excel installed on your computer) and load the data.

On a report where there are consecutive rows with the same data in certain cells, you can hide the duplicated data in the consecutive rows by ticking the 'Hide duplicated text fields' box.



Report: Risk and Control with Action Plan ☑ Hide duplicated text fields [Help] [Export to Excel] [Close the Report]

Organisation Unit	Risk Name	Inherent Consequence	Inherent Likelihood	Inherent Risk	Residual Consequence	Residual Likelihood	Residual Risk	Control Name	Consequence
Demo >> Board	Board does not comply with ASX disclosure requirements	Catastrophic	Almost Certain	Extreme	Minor	Unlikely	Medium	Board and Senior management undergo periodic training	Moderate
								Each board member completes quarterly attestation	Insignificant
	Board member does not meet fit and proper criteria	Major	Possible	Very High	Minor	Rare	Low	Board and Senior management undergo a	Moderate

Depending on the design of the report and its sort order, this function may not always produce the result you desired. If this is the case, do NOT hide the duplicated fields, download the report to Excel and make the modifications in Excel.

Registers

To further support an organisation's compliance obligations, GuardianERM has some registers and the ability for users to create any register they want. The system comes standard with a Training and an Archive Register as well.

Training Register

As proper training is paramount to mitigating risks, it is important for organisations to keep tracking of staff training to ensure that staff members are well trained to perform their jobs and counteract in times of adversity.

The training register is available to all. A user can only access his/her own training register. However, a user can record training for other users. The owner of an organisation as set up in the user's security profile can access all training records for that organisation unit. A person with Training Manager authority (set up in the security profile) can access all training records. Organisation unit owners and training managers can filter the list using the User Search function by typing in all or part of a user name and click the search icon. Click the X icon to clear the search.

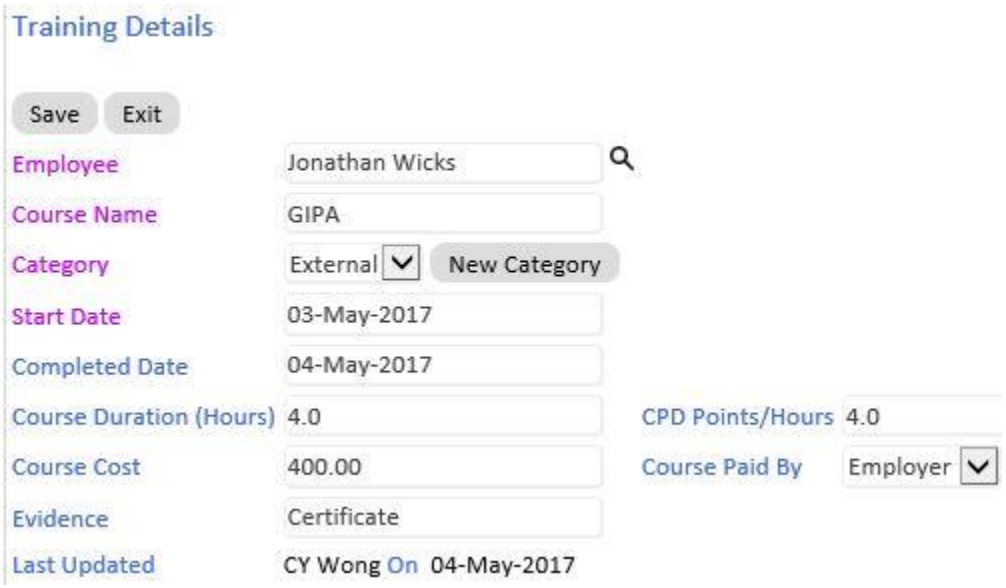
The training register shows the training records for the current month by default. You can change the month by clicking the Month field or click the View All Months button to view all the records.

To modify a training record, click the Modify link for that record.

To add a new training record, click the Add Training Record button at the top.

Training Records

Enter data as indicated. To create a new category, click the New Category button and enter the new category. Click Add to add the category.

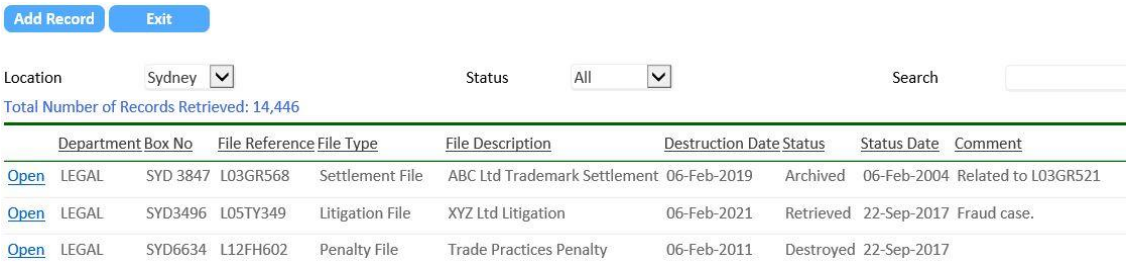


Click Save when the form is completed.

Archive Register

Archiving is a mundane but important function of any organisation. The GuardianERM Archive Register is designed to centralise the recording of archived documents so they can be tracked any time.

When a user accesses the Archive Register, the register will be shown:

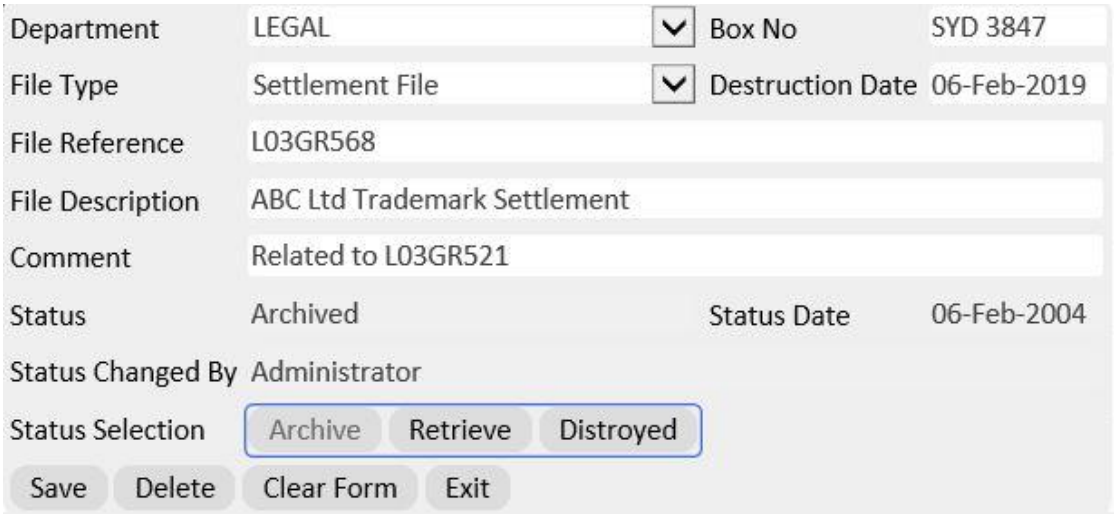


The register can be filtered by Location and Status using the dropdown list filters at the top. You can type some text and click the Search icon to search the register. GuardianERM will automatically search the Box No, File Reference and File Description fields and display only the records containing the search text entered in these fields. Click the Clear Search icon (next to the search icon) to clear the search.

To create a new archive record, click the Add Record button on the top left.

To access a record, click the corresponding Open link on the register.

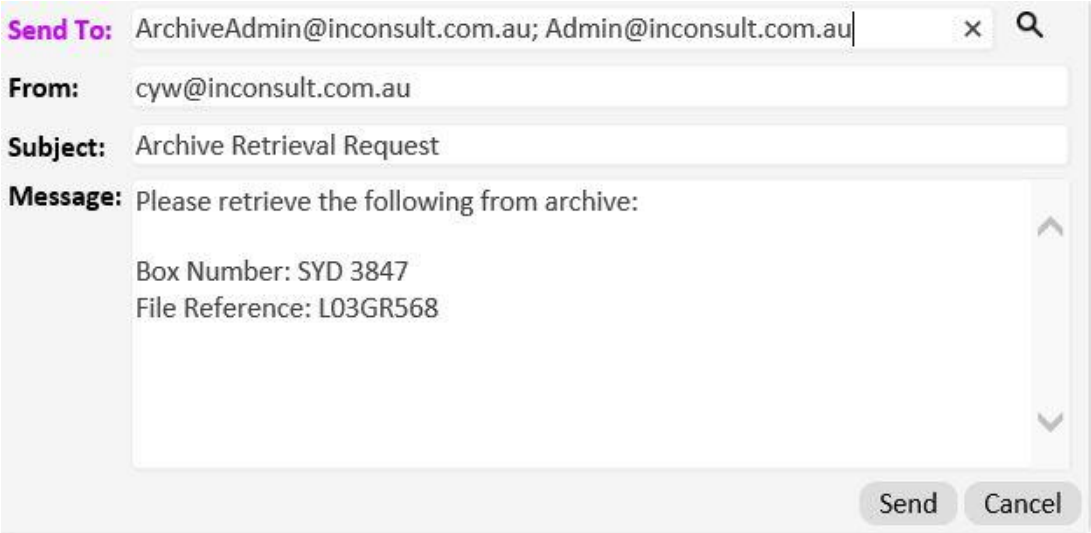
A pop-up dialog box will be shown:



You may modify the data as required or select a Status action by clicking one of the three Status Selection buttons, Archive, Retrieve and Destroyed.

When the Archive or Destroyed button is clicked, the Status information will be changed. Click Save to save the data,

When the Retrieve button is clicked, an email dialogue box will appear:



The email recipient is defaulted to the email address set up in the Archive Register Configuration in the Administration module. You may change it or add more email addresses separated by semi-colons (;) as shown above. You may change all fields on the email form. Click Send to send the email and automatically save the archive record details or click Cancel if you do not want to send the email.

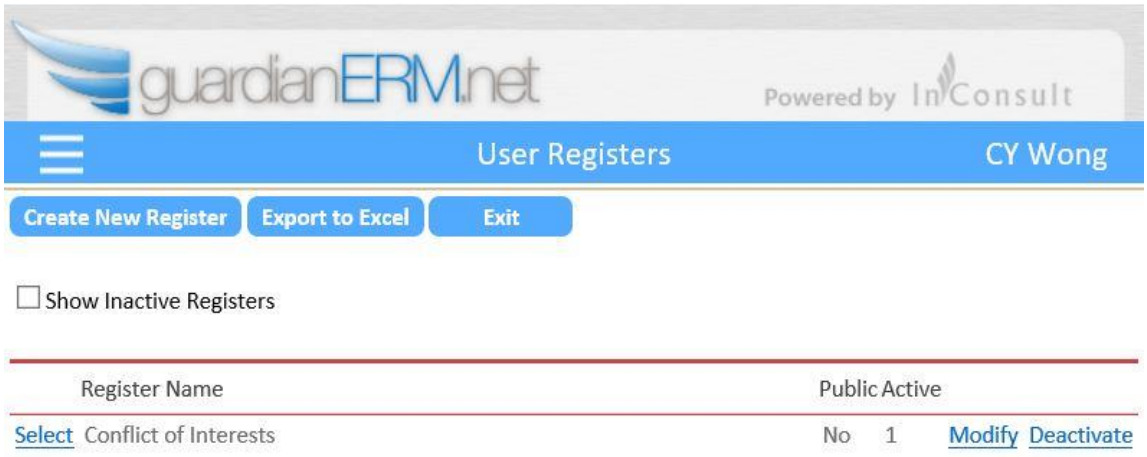
Note: If you do not send the email, you will have to click the Save button to save any changes made to the archive record.

User Registers

In GuardianERM, users can create registers to record items and activities to support their risk management and compliance obligations. Some popular registers include Gift and Hospitality, Conflict of Interests, Contractors and Assets.

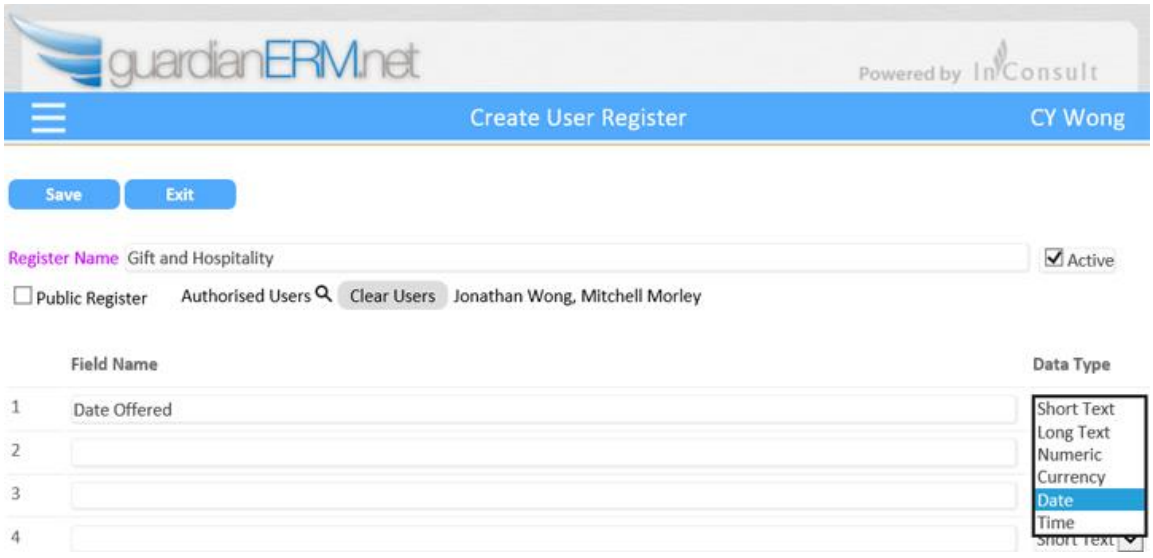
To create a register, the user need to have User Registers Manager authority granted by the System Administrator. The User Registers Manager authority allows a user unrestricted access to all user registers.

When a user access the User Registers, a list of registers the user has access to will be displayed.



To create a new register, click the Create New Register button.

- Enter a name for the new register.
- Either make the register Public (all users have access to it) or assign users by clicking the Search User icon next to Authorised Users and select users from the list.
- Enter (up to 20) field names for the register and for each field select the data type. There is no restriction in size for text fields, the Short Text and Long Text selections only affect how the text is being displayed.
- Click Save when finished.

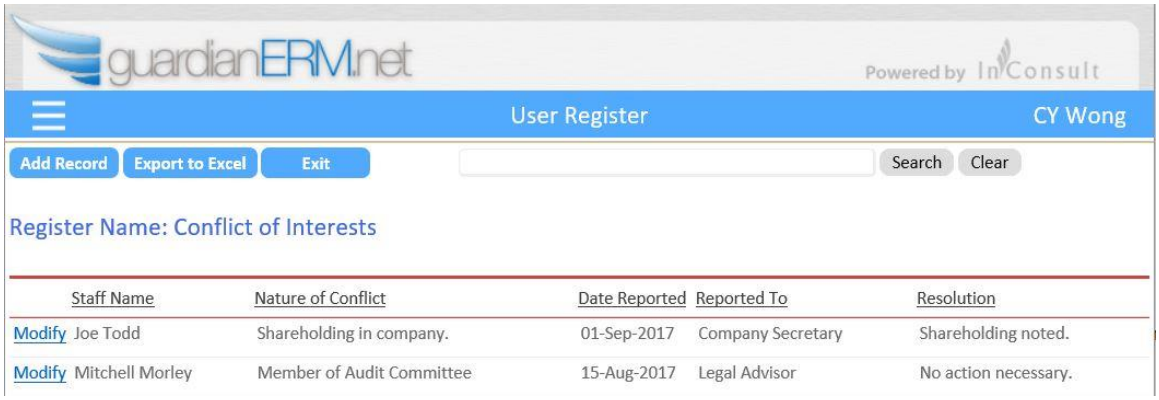


Once saved, a User Register Manager can modify the field names BEFORE the register is being used. Once users have entered data into the register, the field names can no longer be changed.

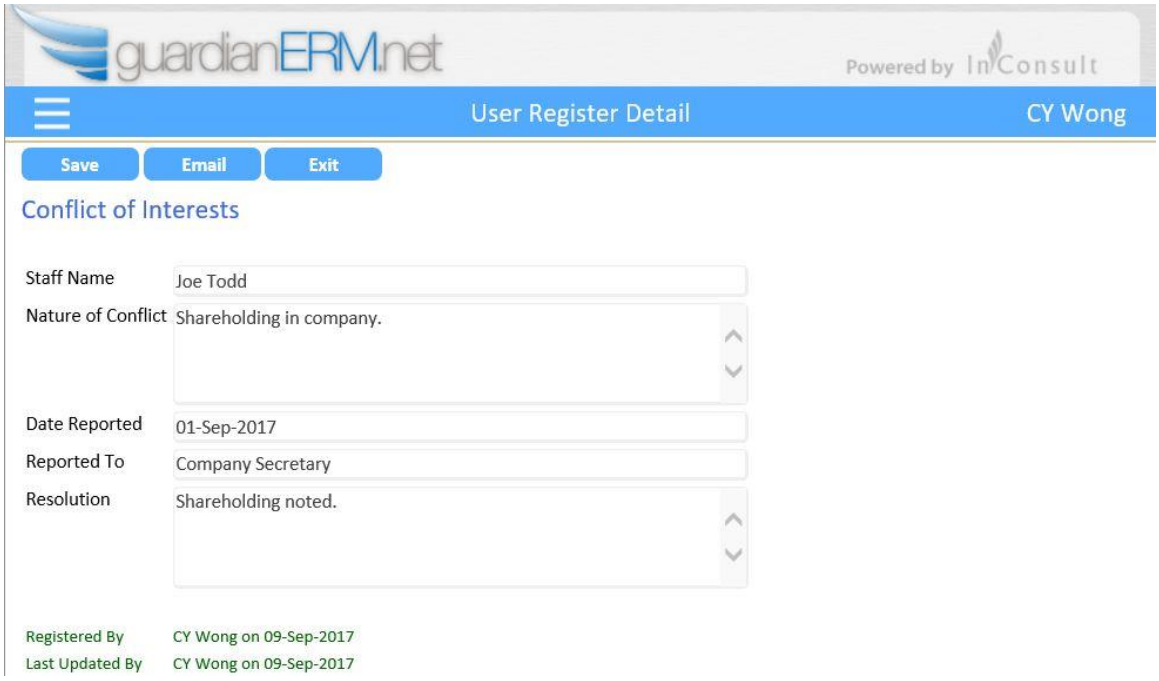
To modify the register, on the User Registers page click Modify corresponding to the register you wish to modify.

To deactivate a register so it will not accept any further data, click the Deactivate link. All historical data remains in the register after it is deactivated.

To access a register and enter data, click the Select link corresponding to the desired register.



To modify a record, click Modify corresponding to the records listed.
To add a record, click the Add Record button at the top.



Enter or modify data as required, click Save when finished.