

ERM Made Easy

You've done the hard yards, now put Guardian to work

Implementing an effective enterprise risk management (ERM), compliance and audit framework can be time consuming, resource hungry and expensive.

When you think about it, risk management is about having effective controls over your risks in order to reduce the threats to an acceptable level...within your risk appetite. Whilst the concept of internal control has been around for a long time, the major challenge now is that effective governance and internal control systems are law for some organisations! Therefore, you need to be more diligent by documenting processes, continually evaluating risks, assessing controls, auditing controls and regularly monitoring your progress.

When all the hard work is over, using ERM technology to make life a little easier makes sense because next year, it will all happen again.

Guardian is a fully integrated ERM System designed to help you take control of your ERM, compliance and audit assurance program. It helps break down silos between departments by allowing them to share risks and controls. Auditors can also share audit procedures. This helps to reduce duplication of effort and maximises the efficiency of your ERM program.

12 ways Guardian makes ERM easier

1. You can set up your own ERM structure

Because each organisation is different, the way you manage risk may also be different. Guardian lets you set up your own risk structure, risk register, alert frequency and even risk ratings. This means that Guardian can speak your language and support your ERM and compliance framework.

2. You have multi-view capabilities by process or financial account

People look at risks in different ways. Organisations typically analyse risks by process and assess the financial impact or assertion. Guardian has multi-view capabilities to allow users to view risks and controls by processes or by financial accounts.

3. Guardian has workflow alerts to escalate issues

The major challenge facing organisations when implementing ERM is that people often have other more important things to do besides helping manage risk. Guardian comes with workflow capabilities that can be integrated with your email system to help people focus on risk management tasks also. Guardian will email risk owners when risk reviews and action plans are due. It will also email auditors when audits and audit report resolution items are due.

4. All your risks documented and analyzed in one system

Guardian is designed to allow users to share risks, controls and audit procedures. This means that all risks are in one place and you don't need to re-enter data. Simply attach and analyse risks relevant to each area. Users can also assess the likelihood, impact, sources and type of risk.

5. You can identify, attach and assess controls to risks

To minimise risk exposure, risks must be controlled. Guardian allows users to select the controls that help to reduce each risk. Users can assess the effectiveness of controls, frequency and other important factors. Guardian tracks the inherent risk before controls and any residual risk after controls. Where there is a residual risk remaining, users must develop an action plan to address the residual risk.

6. Develop action plans to fix control weaknesses

Good risk management requires that control weaknesses be addressed. Where controls are deficient, users can develop an action plan in Guardian and set a due date for completion. Users can track the action to completion and are reminded by email when overdue. In addition, where there is a residual risk remaining, users must develop an action plan to address the residual risk.

7. Guardian is a central document repository

Guardian allows users to attach documents like process maps, process narratives, policies and procedures to organisation units, risks, controls and audit procedures. This helps you take complete control of your documentation and overtime, all key control documents can be linked to Guardian to form a central document repository. Guardian can also be integrated with MS Sharepoint for optimum document management control.

8. Guardian enables on-line attestations

Periodically attesting that risks and controls have been reviewed and that internal controls are effective and efficient is the heart and soul of a governance program. Guardian allows users to periodically attest on-line. No paper, no hassle. In one glance, a CEO, CFO or CRO can see who has attested and who hasn't.

9. Auditors can plan and perform all audits in Guardian

One way to identify control weaknesses is to conduct an audit of controls. Guardian allows auditors to complete all their audit procedures in Guardian. Auditors can also view the risks and controls. All work papers, including checklists and sample testing schedules, are produced and completed in Guardian. For a paperless audit, Auditors can also attach electronic documents to the audit results.

10. Track audit issues and control weaknesses to completion

Control weaknesses identified during audits are recorded in Guardian, along with recommended resolutions and due dates. This ensures that internal control weaknesses are recorded and fixed in a timely manner. Control weaknesses not addressed on time are escalated via email alerts.

11. Guardian has powerful and flexible reporting capabilities

Because Guardian is an integrated database, data can be transformed into powerful information for management reporting, issues tracking and monitoring. Reports can be exported in various MS Office and Adobe formats.

12. You can track all incidents & issues to completion

Guardian also has a incident and issues register to record actual incidents and issues and allow you to monitor them to completion. You can also link the incident to an organisation unit or risk.

What you will need

For a typical multi-user installation, you will need the following.

End Users: Networked personal computer Pentium 3 or above with minimum 50M hard disk space, Microsoft Windows 2000 or XP, Microsoft DotNet Framework, the appropriate software and drivers for the SQL database server selected, Microsoft Internet Explorer 5 or above and Microsoft Outlook Express (or other SMTP email clients).

Servers: Windows 2000 server or above, Microsoft SQL2000 database server, Windows Terminal Services or Citrix (if remote access required).

Infrastructure: Local Area Network for the central office and broad band internet/intranet or leased line connection between remote offices and the central server (if required).