Written by Ian Charlesworth, July 2004

TA000607RMT

Operations

Butler Group Subscription Services

Risk Management

TECHNOLOGY AUDIT

Citicus

Citicus ONE

Abstract *Citicus ONE is an information risk management solution designed to provide the organisation with a framework for measuring and managing exposure to risk caused by the loss of the confidentiality, integrity, or availability of information. In practical terms, this pertains to the information stored, processed, and distributed via IT systems in addition to that recorded on paper and held in people's heads. Citicus ONE is the technological embodiment of the Information Security Forum's Fundamental Information Risk Management (FIRM) methodology, and delivers via a Web-based interface, a series of scorecards geared to collecting information about an organisation's information risk portfolio. The great strength of Citicus ONE is that it not only measures information risk, but allows the organisation to build a solid business case for remedial action, such as that required to achieve compliance. On the downside the solution lacks Activity Based Costing (ABC) and business process awareness.*

KEY FINDINGS

✓	Allows compliance to be achieved as part of a wider risk management strategy.	✓	Embeds best-practice risk management disciplines.
✓	Generates action plans for prioritising remedial work.	✓	Isolates cost of insecurity/non-compliance.
✗	Does not directly map into business processes.	✗	Does not incorporate ABC.

Key: ✓ Product Strength ✗ Product Weakness *i* Point of Information

LOOK AHEAD

The next release of the product, slated for delivery Q3 2004/Q1 2005, is expected to support enhanced monitoring of compliance with regulatory regimes such as Sarbanes-Oxley, the ability to conduct risk assessments for business processes, and cost analysis of risk remediation activity.

FUNCTIONALITY

Risk management, in general terms, has hurtled up the corporate agenda of late. The principal drivers are a culture of increasingly aggressive litigation and the forceful impact of increased regulations. As a consequence, many market sectors find themselves heavily regulated and bound by certain working practices and responsibilities. Even sectors that have been only lighted impacted previously are having to wrestle with the implications of the new Companies Bill, Freedom of Information, Electronic Communications, Digital Rights Management, Sarbanes-Oxley, Data Protection, and Human Rights Acts, etc.

However, compliance is only part of the picture. Many businesses fall into the mistake of believing that if they are compliant, they are safe. This is like thinking that just because your motorcar has passed its emissions test, it is entirely safe to drive! Compliance considerations need to be embedded into the wider considerations of risk management, of which there are three principal areas:

- Market risk – incorporating currency, exchange rates, interest rates, etc.
- Financial risk – which is centred on managing earnings and expenditure uncertainties.
- Operational risk – includes information risk, theft, fraud, and loss of employees/assets.

Information risk is therefore an element of operational risk, but interestingly, it also helps when it comes to the management of market and financial risk.

When we look specifically at information risk, clearly IT assets form the main part of the consideration, either directly as a result of failure or lack of availability, or indirectly with regards to how individuals interface with the systems and resources, which includes both intentional (hacking, viruses, etc.) and unintentional (errors) issues.

Not only is there a whole range of issues to consider with regards to information risk, but isolating responsibilities can be incredibly complex. Take, for example, the risk associated with a mission-critical application going down. The issue/risk could lie with any of the following:

- Application vendor.
- Hardware (database) vendor.
- Network vendor(s).
- IT department.
- End-users.

Citicus ONE delivers a rigorous framework to help the organisation identify and manage information risk, isolating weaknesses, and helping the organisation co-ordinate efforts to provide appropriate remedial action. The key point to remember being that in almost every case, the costs associated with implementing information risk management will be dwarfed by the costs of not doing so. Typical costs include outages (both the direct cost to the business from lack of availability and the costs associated with bringing the system back online), human error, poor policy implementation, and lack of contingency arrangements.

Product Analysis

Citicus has identified four key ways in which its solution adds value to the business – these are:

- Helping to bring down the 'cost of insecurity' over time by reducing the number of incidents experienced in IT systems.
- Reducing the likelihood of a major incident by identifying high-risk systems and enabling a structured approach to risk reduction.
- Enabling organisations to demonstrate best practice in information risk management and IT governance.
- Assisting organisations to achieve compliance objectives (eg BS7799/ISO 17799, Sarbanes-Oxley, Basel II, etc).

Butler Group has long evangelised about the need to view compliance and general IT governance not as a cost centre, but as an opportunity to improve working practices, offsetting the cost of compliance with real, hard long-term benefits. Citicus ONE engenders exactly this kind of approach, for which we feel it has to be commended.

Citicus ONE is built on the Information Security Forum's FIRM methodology. This is embedded in the form of a series of structured scorecards and assessments that need to be completed for each 'information resource'. The methodology is geared to isolate weaknesses and issues that expose the business to unacceptable levels of risk. The tool is designed to be operated by business users, as they tend to have a better understanding of the impact of risk.

Citicus ONE includes the following components or elements:

- Criticality assessments that measure the importance to the business of individual information resources in a consistent and objective way.
- Information risk scorecards that provide a rigorous 5-factor evaluation of the risk posed by individual information resources (covering business criticality, control weaknesses, level of threat, impact of actual incidents, and particular special circumstances that influence risk).
- Individual risk status reports that outline to the 'owner' of information resources the nature and magnitude of risk and guidance on how to drive it down.
- A risk management cycle that allows risk to be monitored and managed over time.
- Dependency risk maps™ that allow the relationships between information resources to be recorded and displayed from a risk perspective.
- Management reporting that allows the results of individual risk evaluations to be consolidated to provide an overview of the risk status of the organisation.
- In-built and customisable standards of practice (e.g. ISO17799/BS7799) that allow the extent of compliance with specific standards to be measured and tracked.
- Action plans that allow risk remediation activity to be recorded and tracked over time.
- Incident reporting that allows consistent, objective data to be recorded about incidents affecting information systems.

As mentioned, Citicus encourages customers to find information system 'owners', whose task it will be to complete the associated scorecards. The underlying FIRM methodology is based on statistical analysis of the actual drivers of information risk in over a thousand business-critical systems in large end-user organisations. Thus, Citicus ONE allows organisations to adopt best-practice information risk management disciplines, thereby optimising associated expenditure.

For example, using Citicus ONE, organisations may find that they are over-investing in availability of non-critical information systems, yet failing to properly address basic end-user training for their most important systems.

Whilst Citicus ONE provides a mechanism for measuring and predicting the costs of 'incidents', it does not currently incorporate ABC concepts to allow remedial action to be based on the cost of achieving acceptable risk levels.

Product Operation

When faced with conducting an audit on their information systems, many organisations would struggle to know exactly where to start, such is their number and complexity. In order to address this issue Citicus has developed a Criticality Assessment. This is used as a first-pass to help the business identify the particular scenarios and systems that present the most risk and thus present the greatest threat. The result of this process is a Criticality League Table of the kind shown below:

Scorecard/Assessment	Position in League Table	Overall Criticality	Confidentiality Rating	Integrity Rating	Availability Rating	Critical Timescale for Availability
Dublin Call Centre (CA131)	1	C – Highly Critical	C – Serious Harm	B – Very Serious Harm	B – Very Serious Harm	2-3 Days
Goods Inward (CA88)	2	C – Highly Critical	E – No Significant Harm	C – Serious Harm	B – Very Serious Harm	2-3 Days
In-store Processing (CA103)	3	D – Critical	C – Serious Harm	C – Serious Harm	B – Very Serious Harm	A Week
CALE (CA79)	4	D – Critical	D – Minor Harm	C – Serious Harm	B – Very Serious Harm	A Month
Cashier Support (CA85)	5	D – Critical	E – No Significant Harm	C – Serious Harm	B – Very Serious Harm	A Month
Store-sales Forecasting (CA106)	6	D – Critical	E – No Significant Harm	C – Serious Harm	B – Very Serious Harm	A Month
PoS Cash Register System (CA90)	7	E – Important but not Critical	C – Serious Harm	C – Serious Harm	C – Serious Harm	A Month
Vehicle Management (CA91)	8	E – Important but not Critical	C – Serious Harm	C – Serious Harm	C – Serious Harm	A Month

Figure 1 – Criticality League Table

The use of Criticality Assessments allows the organisation to prioritise more detailed analyses of particular systems. As previously mentioned, it is the task of the system 'owner' to gather appropriate information to complete the actual information risk scorecards. Whilst there may be occasions where this is done as a solitary exercise, Citicus recommends that owners coordinate workshops in order to collate information from a range of sources.

Part of this process is the collection of information on known incidents. This looks at the frequency and impact of historic incidents relating to the particular system. Incidents can range from lack of availability to human error (i.e. include both hard and soft factors). This information is then used to gauge the potential risk of future incidents. Citicus Information Risk scorecards are designed to be easy to complete and to capture an appropriate level of detail without becoming an unnecessarily onerous process. Comments can be appended to the scorecard, detailing the rationale for a particular response or rating. We feel this is particularly important for shielding the business from the impact of the inevitable change in owner over time.

The FIRM methodology is based on five key risk factors, and embeds best practice principals such as those required for ISO17799/BS7799. However, the scorecards are customisable, allowing company policy or other elements of regulation to be easily embedded. Citicus claims to be evaluating the potential for providing regulatory templates on top of the Citicus ONE platform in order to make this process even easier. Butler Group believes that such an approach would be welcomed by the market.

Once the information has been collected, Citicus ONE provides both the owner and top level management with a wealth of information, in the form of series of reports, charts, and views. This pertains not only to the individual systems, but also to the organisation's whole portfolio of information risk.

For example, Risk Charts (as shown below) are produced for each system, showing the current level of information risk exposure vis-à-vis what is felt to be acceptable.

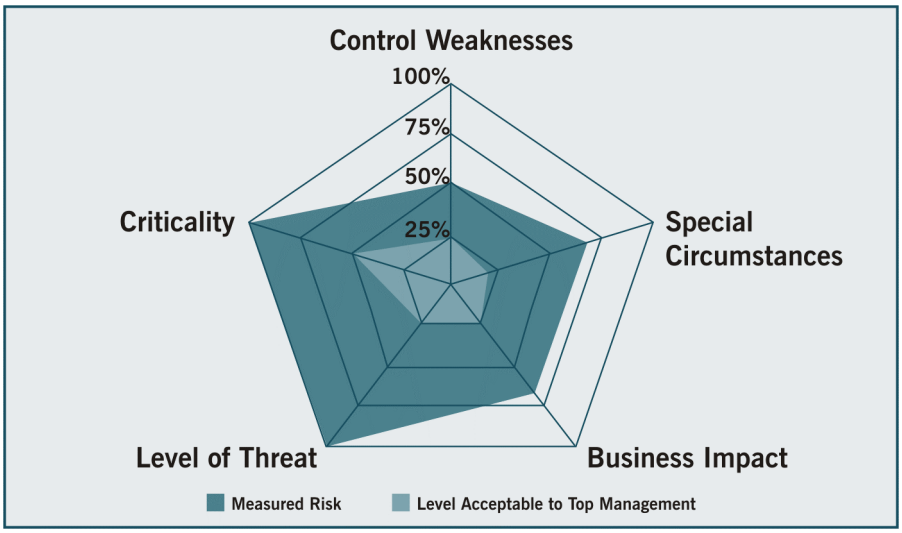

Figure 2: A Citicus ONE Risk Chart

When assessments have been undertaken for a range of systems, individual Risk Charts can then be joined and combined in a dependency risk map. This shows, in a graphical manner, the interdependencies that exist between systems and the levels of information risk that are shared.

Perhaps of greatest impact are the reports that quantify the cost of insecurity, as shown below:

	Financial Impact of Incidents	
Nature of Financial Impact	Overall ($)	Average ($)
Loss of income	5,795,000	482,920
Unforeseen costs	10,845,000	903,750
Reduction in profit (10% of loss of income plus unforeseen costs)	11,424,500	952,040
Loss of Value of tangible assets	100,000	8,330
Reduction in value of the business (reduction in profit plus loss of value tangible assets)	11,524,500	960,375
Value of staff-time lost through incidents	*60,800*	*12,200*

Figure 3: Analysis of Incidents

Such reports assimilate all the costs associated with incidents. This kind of information, quite simply, should stir even the most frugal of CIOs or CFOs into action!

In order to close-the-loop and drive positive change, Citicus ONE provides the organisation with action plans. These are designed to break the challenge of bringing information risk in-line with expectations/requirements into a series of logical, actionable steps. All of these reports and analyses can be combined in a single PDF report, designed for review by senior management.

Beneath the surface, Citicus ONE provides the necessary workflow and tracking capabilities to ensure work allocated to owners is completed on schedule. In this regard, we feel the solution would benefit from automatic alerts and full scheduling functionality. Being entirely Web-based, assessments and updates can be sent simply as a URL within an e-mail (via LDAP integration).

Product Emphasis

Citicus ONE is the only automated software incarnation of the Information Security Forum's FIRM methodology. As such, it provides organisations with the necessary framework for undertaking an analysis of information risk across all enterprise systems, quantifying the magnitude of the risk presented, and putting into place the necessary corrective action plan.

Citicus ONE is the only automated software incarnation of the Information Security Forum's FIRM methodology.

The Web-based solution contains the requisite administrative and customisation features to ensure that that information risk can be properly managed over time.

▶ DEPLOYMENT

Deployment and use of Citicus ONE will be dependant on the organisation's existing view towards risk management and the scale of initiatives made. For example, larger, more progressive organisations are likely to have a dedicated information security officer, who will clearly use the product to assist in the role. Other businesses may have a more splintered approach, driven by local regulations or departmental champions.

Being entirely Web-based means that Citicus ONE can be deployed cost-effectively on both a small and large scale. Physical installation is dramatically simplified through a Wizard, however, basic Windows 2000/SQL Server skills may be needed. Citicus claims typical installation times in the region of half a day. Configuration time depends on the scale of the implementation and the extent of local customisation required.

A modular approach to deployment can also be taken, using a criticality assessment to identify and prioritise information resources as targets for risk management. These can naturally be followed by full risk assessments.

Administration of registered users can either be carried out locally within Citicus ONE or remotely within an enterprise directory (via LDAP).

In terms of training, Citicus provides a two- or three-day on-site training course covering both the FIRM methodology and the Citicus ONE software. This typically includes a 'live' risk management workshop of an example system.

The required software environment for Citicus ONE is as follows:

- Windows 2000/2003 server.
- Internet Information Services (IIS).
- SQL Server.
- Client access requires a standard Web browser (Internet Explorer or Netscape Navigator).

However, Citicus also provides a hosted service via the Internet as an alternative to an in-house installation. This should prove to be particularly attractive to the SME sector and can also be used for undertaking pilot studies.

▶ PRODUCT STRATEGY

As a small company looking to exploit its doubtless differentiators, Citicus needs to pay particularly close attention to its product and marketing strategy. The company has experienced early success in a range of markets, particularly those that are heavily regulated, such as telecommunications and financial services.

Citicus is keen to point out that the FIRM methodology is equally applicable to small businesses as it is large multinational enterprises with hundreds of thousands of employees. The largest existing deployment of Citicus ONE supports in the range of 1000 users within a large enterprise. As previously mentioned, the hosted option supported by Citicus is particularly attractive to smaller businesses that may lack the technical resources and skills to deploy and manage the solution internally.

From a marketing perspective, the recent high profile nature of compliance and IT governance plays straight into Citicus' hands and has resulted in significant media interest and exposure.

Citicus ONE is sold both directly by Citicus and increasingly through the company's network of implementation partners which includes PwC and EPI-USE as well as other local partners.

Licensing is based on the number of 'information resources' that are the subject of the risk management process. Licensing is tiered to allow (relatively low-cost) first-cut criticality assessments to be licensed separately from full risk evaluations. Licenses for in-house installation include the first 12 months of maintenance. For the hosted option, an annual service charge is levied, based on the number of 'information resources' under management.

Project values for a typical installation range from £10,000 to £100,000, split 80% licence cost, 20% training/consulting. Annual maintenance and support is charged at 18% of the licence cost. This includes all product software releases, telephone/Web support and benchmarking data.

▶ COMPANY PROFILE

Citicus is a small software company headquartered in London, UK. The company was founded in 2000 by three key individuals with the specific intention of providing an automated software solution for the FIRM methodology. The founders, Marco Kapp, Sian Alcock, and Simon Oxley, had all been previously involved in risk management projects at the Information Security Forum, the body responsible for developing FIRM. The relationship with the Information Security Forum remains extremely important to Citicus, to the extent that an IPR agreement has been put in place giving Citicus worldwide exclusive license to sell software solutions based on FIRM, with an appropriate percentage of sales revenues being directed back to the Forum.

Initial funding for Citicus and the research and development of Citicus ONE came from 15 major organisations (all members of the ISF) paying for licences in advance. Citicus spent its first 18 months developing the initial release of the Citicus ONE software product. The next year was spent assisting launch partners and other early adopters to build successful risk management implementations.

Citicus currently employs five permanent members of staff, and augments this number with contractors on an as-and-when basis. Employee growth in the range of 50% is expected over the next 12 months. Given its size and limited resources, is it vital for Citicus to develop a strong channel strategy, aggressively seeking out new partnerships and OEM opportunities. Nevertheless, Citicus has been able to attract some 'big name' customers over a range of markets (both geographical and vertical). Key customers include:

- Tesco.
- Standard Chartered.
- Standard Bank of South Africa.
- Xerox.
- Orange.
- NCR.
- Stora Enso.
- UK police forces.

▶ SUMMARY

The market for solutions that assist organisations with their attempts to address manage risk in its many guises is growing rapidly. The market is starting to come round to the fact that risk management does not just apply to specialised market sectors and that compliance and IT governance initiatives need to be couched in a consistent framework, not tackled on a case-by-case basis. Information risk is an important element of operational risk and therefore needs to be closely monitored. Citicus ONE delivers a rigorous framework to help the organisation identify and manage information risk, isolating weaknesses, and helping the organisation coordinate efforts to provide appropriate remedial action. The key point to remember being that in almost every case, the costs associated with implementing information risk management will be dwarfed by the costs of not doing so.

▶ CONTACT DETAILS

Citicus Limited
Holborn Gate
330 High Holborn
London
WC1V 7QT
UK

Tel: +44 (0)20 7203 8405
Fax: +44 (0)20 7203 8409

Email: info@citicus.com

www.citicus.com