

Web-based risk management

Citicus ONE

Supplier Citicus Limited
Price from \$10,000; hosted service from \$8,000 per year
Contact www.citicus.com

Citicus ONE is a service to help your senior management to understand the risks they face. This is an on-going risk management exercise, rather than a one-off assessment, so you can use the software to produce periodic reports that graphically demonstrate the necessity of funding security efforts.

The methodology used is FIRM (fundamental information risk management). It has been developed by the Information Security Forum and is based on many years of research.

So how does it work? First, you have to establish an inventory of your critical information systems. The software then generates an 'information risk scorecard' for each of the identified systems, a two-page questionnaire that collects data about the risk status of a system. This can be completed online and Citicus ONE will automatically generate an email providing the owner of each with a hyperlink to their specific scorecard.

The scorecard can be completed by the owner of the system, but Citicus recommends that they are completed by your information security staff during short workshops, with representation from business users, systems administrators, help desk representatives and IT operations.

While your team is completing a scorecard they can also use a series of supporting aids, such as harm-reference tables, that are used to quantify the impact of potential or actual incidents. The scorecard covers a range of risk factors, such as criticality to the business, the status of security controls and the type and impact of incidents that have been experienced.

The workshop can also be used to put together an action plan, so you can tackle any identified weak-



nesses in security controls or investigate the root cause of incidents. The ability to track and maintain your action plan online makes the whole process very easy.

Once a scorecard is completed an information risk status report is generated, displaying the risk profile graphically and providing guidance on how to tackle the identified risks.

Once the first series of scorecards has been completed, information resources can be ranked according to their importance to the company, and the level of risk they pose. A schedule can be defined to review and update each of the scorecards at regular intervals.

At each subsequent workshop, an updated scorecard is filled out, using the baseline data from the most recent scorecard. It takes into account all new information, such as the results of the completed action plan. An updated report is generated showing the trend in risk in graphical form. This process can be repeated as many times as wished, until the desired risk and security status is achieved.

It is worth noting that second or subsequent scorecard can either be started from scratch or bring forward data from a previously completed scorecard. The original scorecard and the new one will be saved in the system so that a historic record of risk management activity is maintained. Finally, the scorecards, which form the basis of the reports described below, are summarised and are ready to be presented to all levels of management. Senior managers can then use the reports in order to prioritise security projects together with

other projects.

Various reports are delivered. The individual resource status report includes a brief description of the resource, its owner and its need for protection, two five-point graphs depicting its risk profile before and after improvements, and a section that highlights opportunities for improvements.

Another report gives guidance on driving down risk using five key indicators: criticality to the company; control of weakness using 17 control areas; special circumstances that apply; the level of threat measured by the number of incidents, and the business impact of harm caused to the company.

You will also receive a table depicting the risk ranking of all the individual resources (there may be hundreds of them) using these five key indicators. The chart can be sorted to suit and is colour-coded to make for easy reading, in order to see and understand the organisation's resources, and determine just where and when to apply security measures.

A further report describes the dependencies between different information systems and the impact of these on risk.

Other information resources include a brief incident assessment, and a high-level risk status report showing the risk status and profiles for the five information systems posing the greatest risk to the company, and a brief summary of improvements since the last report.

The software can run without the help of Citicus, but they encourage companies to have an employee trained as a facilitator in the methodology and the software.



Citicus usually assist with the initial scorecard workshop and provide backup on the second workshop. You can then either pass it over to your own facilitator for the rest of the workshops, or let Citicus facilitate workshops on your behalf.

Training and or facilitation can be provided globally, but Citicus also has a network of partners, including PricewaterhouseCoopers, who are fully trained in the product and methodology.

By Richard O'Connor

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

FOR The software can be installed on a corporate intranet web server. In addition customers can choose the option of having Citicus host the service.

AGAINST Nothing.

VERDICT This product can help you take a big step in defining, prioritising, and allocating your security resources and in documenting their real value to the company.

Contact details:



Citicus Limited

Holborn Gate
 330 High Holborn
 London WC1V 7QT

Web: www.citicus.com
 Email: info@citicus.com
 Tel: +44 (0)20 7203 8405