TECHWORLD
The infrastructure & network knowledge centre

Citicus ONE risk management software

Web-based risk assessment software that tells you which bits of your infrastructure you should worry about.

by David Cartwright, Techworld

List Price:	Starts at around £3,000 for the low-end, entry-level system. Typical installations are between £20,000 and £40,000
Made by:	Citicus
Pros:	The system's simplicity is reflected by the 2-day training course that is all most clients' information risk managers require. Brings procedural risk management out of the stratosphere and into the real world for the average business.
Cons:	The financial investment in the software is just part of the task – a sizeable amount of people time will also be required.
Buying advice:	Alongside the software purchase, it's a good idea to add the 2-day training course for the information risk managers in order to get the best value from the system. Given the raft of concepts involved in risk management, it's a compliment to the standard of the system that you only need a couple of days' training.

Citicus ONE is an information risk management assessment and monitoring tool which allows organisations to automate the process of investigating and managing the business risks associated with a company's information systems. It is a Web-based system written with ASP on top of an SQL Server back end that the customer can host internally or purchase as an externally hosted service.

The basis of Citicus ONE is the FIRM (Fundamental Information Risk Management) methodology devised by the Information Security Forum . FIRM is a mechanism that leads an organisation through the process of gathering data about its perceived information risks, categorising them sensibly and comparing the results with the management's view of acceptable risk levels. It's an iterative process, the idea being that between iterations, issues will be solved and the actual risks will gradually reduce until they are within the management-defined maxima.

Before we get started, it's important to bear in mind that Citicus ONE doesn't magically figure out the risks posed by the various information systems in your organisation. That is, it's not the kind of package that scans your network for software-level vulnerabilities. The assessment of risk is done by the people in the organisation; Citicus ONE is the workflow and collation tool that takes the information that the people have gathered and transforms it into a comprehensive analysis of the risks you face.

User types
There are three basic type of user in Citicus ONE. At the centre is the information risk manager – the person who's co-ordinating the assessment exercise, and who is the main driver of the system. The information risk manager delegates the responsibility of assessing the various risks down to the individuals who are responsible for looking after the various information systems in the organisation – the information "owners".

Each of the information owners is provided with a two-page "scorecard" to complete for each of the information systems he or she is responsible for. This may be a paper scorecard, but it's more convenient to get them to use the Web-based one that Citicus ONE provides; the content of the scorecard is based on the ISF's FIRM methodology, the idea being that although it's brief, the questions it's asking are the pertinent ones. Along with the usual personal details and summary information, the scorecard is split into five main categories of risk:

- Criticality: Assessing the harm that the business could suffer as a result of a problem.
- Threat levels: Quantification of actual occurrences of problems in the past.
- Business impact: Did previous problems cause real financial loss, or just minor irritation?
- Control weaknesses: Assessing the quality of procedures and processes.
- "Special circumstances": stuff that doesn't fit the other categories, such as immature technologies and accessibility by outside parties.

It's worth mentioning that instead of using the whole scorecard, there's a "mini-scorecard" that incorporates just the criticality-related section of the evaluation, and not the other four subject areas. It seems Citicus's customers value this area most highly, and have asked to be able to set this area aside for special treatment.

Although the scorecard completion and collation process relies on tickboxes and relatively simplistic "allocate a score from A to E" concepts, each question allows the respondent to add a free text comment as well.

Telling porkies

Our immediate reaction to this idea of scorecards was: "What if the information owner tells fibs to protect himself?". There are three safeguards that help prevent this. First, the scorecard completion screens use cross-checks that will catch out the blatant fibbers (so if you've said in one section that you've never had an independent review of a system, it'll complain if you later tick an "item was subject to independent scrutiny" box later on). Second, there are a number of different status types for each scorecard, and so the person co-ordinating the exercise can dictate that each card needs to be "signed off" by a second individual before it becomes valid. Finally, and perhaps most importantly, because many organisations' information systems are such that it's not realistic to expect an individual to complete a scorecard for a particular system on his or her own, Citicus provides a standard agenda for group workshops.

When the Citicus ONE system is initially implemented, it's recommended that a "dry run" is done before the first real iteration of the system. Most organisations have some fairly fundamental issues that will skew the results completely, and the dry run allows you to spot these and sort them out before the first proper iteration.

Instant reporting

Once completed scorecards have begun to appear in the system, the results start to fall out immediately because the package can begin to analyse what it sees straight away. Alongside the information that's coming in via the scorecards, the package can be told of the management's opinion of the acceptable risk levels in each of the various categories, and as soon as some results start to come in, the package graphs the reality against the management view in a pentagonal graph (sounds weird, but they're very easy to understand and you get an excellent overview of the problem). The reports produced by the system give a combination of graphical and textual descriptions of the various issues, and the graphs show the current iteration's results alongside the previous iteration's, so that you can see whether things are improving or (heaven forbid) worsening in any given area. Because many information systems depend on others for their reliability, it's also possible for the various information owners to specify the parts of the business that their systems depend on, and the risk assessment for each system will include details about the external entities it depends on.

The levels of complexity of reports vary from top-level overviews (for management) which include reports at the "top ten problems" or "financial cost" level, down to detailed analyses (incidents by type, or by system, for instance) which are more useful for the people at the coalface tasked with eradicating the risks. Citicus ONE also produces "action plans", which summarise the issues for each system and lay out in simple terms what needs to be done to improve matters. Report generation is entirely interactive via the Web GUI, incidentally, though output to PDF is also supported for off-line reporting.

Customisation

Because risk management isn't a one-size-fits-all concept, the last thing we should mention is that the various parameters of the system can be configured to fit each company's size and shape. So although certain elements (such as the questions the scorecards ask) are fixed because they're based on the ISF methodology, you can switch to a different methodology if you so desire (the system knows about both the ISF's published approach and both the 1999 and 2002 flavours of BS7799/ISO17799). You can also modify (for instance) the definitions of what constitutes each level of harm (company A might class a billion-dollar loss as major harm, for example, while company B might decide that £100,000 is in fact pretty major).

Citicus ONE isn't a product that you install and forget. Instead, it is merely a tool that significantly eases the task of analysing and evaluating the information-related risks of your company. To get the most of the system, an organisation needs to plan properly and do a proper job of defining the organisational structure and the various systems and people that are to be involved in the exercise. Indeed, Citicus estimates that a typical customer would take about six months to get through the first cycle, and then a further two to three months for subsequent cycles (and, of course, from iteration two onwards you start to see where improvements have taken effect).

Summary

The benefit of this system is that it understands the risk assessment methodologies (both ISF and BS/ISO ones) and handles the drudgery of implementation for you – which leaves you to deal with the actual issues instead of spending hours managing the process. The scorecard system is simple to use, and the package schedules all aspects of scorecard completion and data collation; the reporting tools are also straightforward for both information system owners and upper management, and the fact that data can be reported upon in real time is a huge benefit. What particularly impressed us is the sheer usefulness and readability of the system output; it's cleverly laid out, and the graphing systems give excellent overview information. Although this is the type of package you'd expect to find in huge organisations such as banks, we believe that Citicus has done a sufficiently good job, at a sensible enough price, to make it relevant to even moderate-sized SMEs who want to understand the potential business impact of their information systems.