Driving information risk down to an acceptable level, using FIRM and Citicus ONE

Why manage information risk down?

Good corporate governance demands sound processes for managing risk. But there's no single method for managing all risks and few, if any, organisations have a sound method of managing **information risk** – one of the biggest and fastest growing areas of risk around.

Because information risk is not well understood or managed, on average a business-critical information resource:

- suffers an information incident almost every working day (average of 225 incidents a year)
- has a 58% chance of experiencing a major incident over the course of a year.

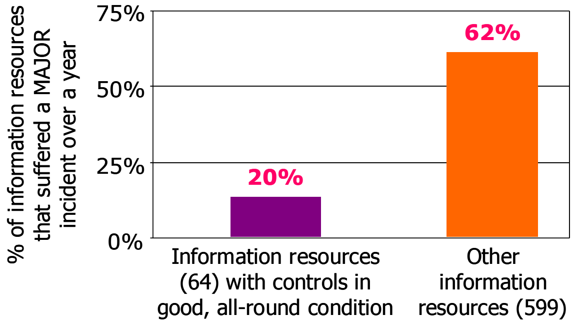
These figures are not plucked out of the air. They emerged from rigorous analysis of the world's largest source of hard fact on the chances of business critical systems 'going wrong' - the Information Security Forum's biennial information security status survey.

While most incidents have minor impact, some can have very serious consequences; and the cumulative effect of such incidents significantly erodes profits and makes enterprises under perform.

This may seem obvious. What is not so apparent is that these unwanted effects are largely avoidable.

This is no mere assertion – there is a clear correlation between the status of controls and the likelihood of a major incident, as shown below.

Probability of experiencing MAJOR incidents



Source: Citicus analysis of some 149,000 incidents affecting 663 information resources 'on the ground' covered by the Information Security Forum's 2000-02 information security status survey.

By getting controls in good shape, your organisation can not only reduce the information risk it faces: it can save substantially - since as well as reducing the chance of suffering major incidents, good controls cut the number of minor incidents suffered day-to-day, and the inefficiencies that go with them.

Thus the benefits of driving risk down are substantial.

So what's stopping businesses from doing so? The answer is **behaviour**: to drive risk down you've got to **motivate and equip people** to do it.

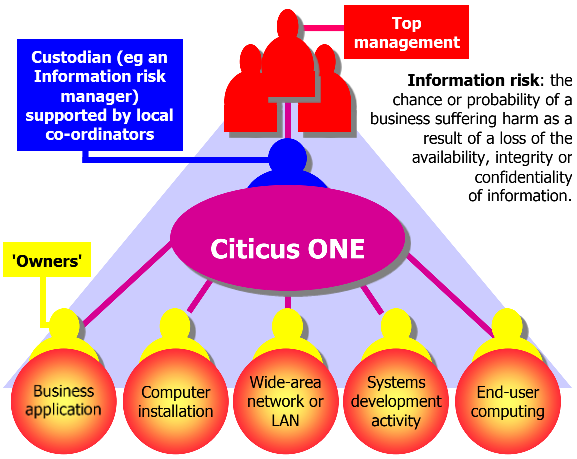
That's where **Citicus ONE** comes in.

The power of Citicus ONE

Citicus ONE's power stems from the rigorous methodology that it employs for measuring and managing information risk. This is called **FIRM**.

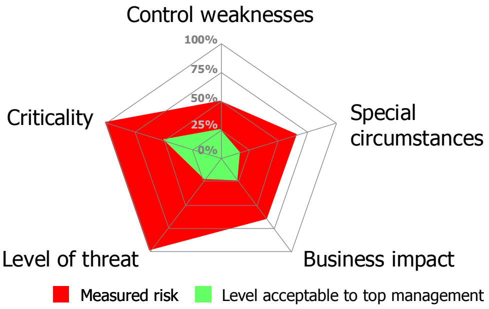
FIRM was developed by Citicus's co-founders for, and in conjunction with, the Information Security Forum. Based on rigorous research, it employs carefully designed scorecards and other forms to collect key facts about the level of risk posed by individual business applications, computer installations, networks and systems development activities.

As shown below, these facts are drawn together and used to provide succinct, business-oriented results to top management, 'owners' of individual systems and specialist practitioners charged with helping keep risk under control.



Information risk: the chance or probability of a business suffering harm as a result of a loss of the availability, integrity or confidentiality of information.

A key feature of **Citicus ONE** is its ability to **measure** the factors that determine or indicate the level of information risk. This quantitative approach enables actual risk to be contrasted with the level deemed acceptable by top management, in the form of easily understood risk charts.



The purpose of **Citicus ONE** is not to measure risk for its own sake but to help people drive risk down.

This purpose is manifested in the **two-phase constructive risk management process** supported by **Citicus ONE**. Further details are provided overleaf.

Support for the core components of **FIRM**

Citicus ONE automates all the core components of the ISF's published **FIRM** methodology. Specifically, it:

- **supports the entire FIRM constructive monitoring process** i.e. all steps in its 'dry run' and 'for real' phases
- **quantifies risk in line with the published methodology** using easy-to-fill-in scorecards and incident forms and presenting five-point risk charts automatically
- **recognises and supports all FIRM roles** i.e. information risk manager, local co-ordinators, 'owners', internal audit, top management and other decision-makers
- **provides high-level results** designed to gain the attention of decision-makers.

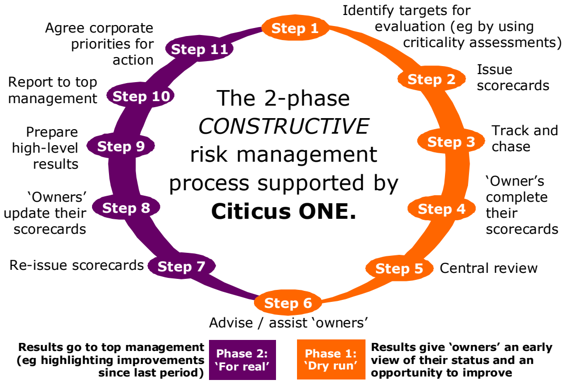
Additional capabilities

Citicus ONE provides extensive functionality over and above that set out in the **FIRM** methodology. This takes it to a higher plane. For example:

- **Criticality assessments**, which can be completed by an 'owner' in minutes, yielding a Criticality status report that highlights the need for protection and recommends whether full evaluation is warranted.
- Succinct **Individual risk status reports**, produced as soon as a scorecard is submitted.
- **Guidance on driving down risk**, produced automatically for individual 'owners'.
- **Comments schedule**, which keeps track of key points made when evaluating risk (these are often highly informative and tend to highlight areas where action is needed).
- **Document uploads** enable evaluators to maintain a full record of each evaluation.
- **Action plans**, maintained at information resource, enterprise and intermediate levels.
- **One-click access to completion aids** such as harm reference tables and controls/threats checklists, which ensure business-oriented, objective and consistent evaluations.
- **Standards of practice** - including the **ISF SoGP, ISO 27001, PCI, COBIT** - which may be selected and customised to meet your needs, or you can enter your own in-house standards.
- **Criticality league tables** rank information resources according to their importance to the enterprise. Such risk inventories provide a factual base for prioritising evaluations.
- **Dependency risk maps**™, which highlight the risk status of groups of related systems.
- **E-mail integrated workflow** automating the risk management lifecycle.
- **Data exports and integration aids**, enable you to get full value from **Citicus ONE** and deploy it efficiently.

A *constructive* risk management process

The risk management process supported by **Citicus ONE** is specifically designed to help people succeed in driving down risk in key areas.



Results go to top management (eg highlighting improvements since last period)

Results give 'owners' an early view of their status and an opportunity to improve

Targeting evaluations with minimal effort

Citicus ONE enables you to decide what to evaluate, with minimal effort. The preliminary screening process entails asking 'owners' of information resources to fill in **Criticality assessments**. These can be completed in minutes.

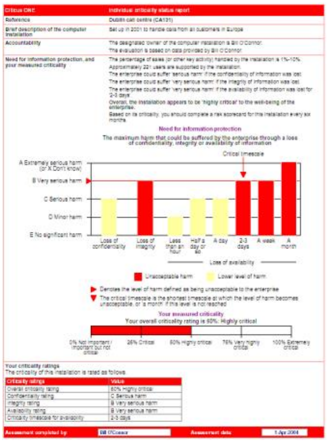
Each yields a succinct **Criticality status report** - written in plain language - which tells the 'owner' concerned whether a full evaluation is needed or not.

An 'owner' can obtain a **Criticality status report** in minutes.

It highlights:

- the level of protection required by his or her system
- its criticality, evaluated in business terms.

It also advises whether a full risk evaluation is needed or not.



Citicus ONE	Individual criticality status report
Reference	Dublin call centre (CA131)
Brief description of the computer installation	Set up in 2001 to handle calls from all customers in Europe
Accountability	The designated 'owner' of the computer installation is Bill O'Connor. The evaluation is based on data provided by Bill O'Connor.
Need for information protection, and your measured criticality	The percentage of sales (or other key activity) handled by the installation is 1%-10%. Approximately 221 users are supported by the installation. The enterprise could suffer 'serious harm' if the confidentiality of information was lost. The enterprise could suffer 'very serious harm' if the integrity of information was lost. The enterprise could suffer 'very serious harm' if the availability of information was lost for '2-3 days'. Overall, the installation appears to be 'highly critical' to the well-being of the enterprise. Based on its criticality, you should complete a risk scorecard for this installation every six months.

Need for information protection

The maximum harm that could be suffered by the enterprise through a loss of confidentiality, integrity or availability of information

▶ Denotes the level of harm defined as being unacceptable to the enterprise

▼ The critical timescale is the shortest timescale at which the level of harm becomes unacceptable, or 'a month' if this level is not reached

Your measured criticality

Your overall criticality rating is 60%: Highly critical

Your criticality ratings

The criticality of this installation is rated as follows:

Criticality ratings	Value
Overall criticality rating	60% Highly critical
Confidentiality rating	C Serious harm
Integrity rating	B Very serious harm
Availability rating	B Very serious harm
Criticality timescale for availability	2-3 days

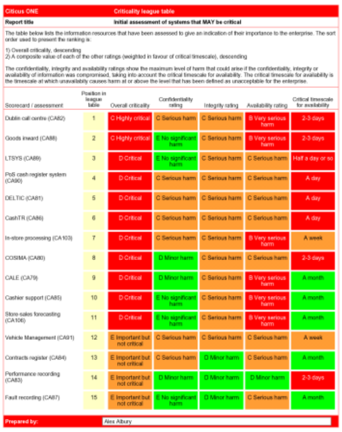
Assessment completed by: Bill O'Connor Assessment date: 1 Apr 2004

Once assessed, information resources can be ranked in a **Criticality 'league table'** that highlights their relative importance to the enterprise. The ranking will help determine where full evaluation is warranted.

Criticality league tables highlight systems which warrant full evaluation.

Their content can be sorted to bring together other categories of system.

For example, those with particularly demanding confidentiality requirements, or those with very short timescales for recovery.



Citicus ONE	Criticality league table
Report title	Initial assessment of systems that MAY be critical

The table below lists the information resources that have been assessed to give an indication of their importance to the enterprise. The sort order used to present the ranking is:

1) Overall criticality, descending
2) A composite value of each of the other ratings (weighted in favour of critical timescale), descending

The confidentiality, integrity and availability ratings show the maximum level of harm that could arise if the confidentiality, integrity or availability of information was compromised, taking into account the critical timescale for availability. The critical timescale for availability is the timescale at which unavailability causes harm at or above the level that has been defined as unacceptable for the enterprise.

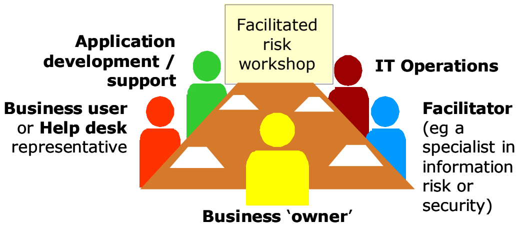
Scorecard / assessment	Position in league table	Overall criticality	Confidentiality rating	Integrity rating	Availability rating	Critical timescale for availability
Dublin call centre (CA82)	1	C Highly critical	C Serious harm	C Serious harm	B Very serious harm	2-3 days
Goods inward (CA88)	2	C Highly critical	E No significant harm	C Serious harm	B Very serious harm	2-3 days
LTSYS (CA89)	3	D Critical	E No significant harm	C Serious harm	C Serious harm	Half a day or so
PoS cash register system (CA90)	4	D Critical	C Serious harm	C Serious harm	C Serious harm	A day
DELTIC (CA81)	5	D Critical	C Serious harm	C Serious harm	C Serious harm	A day
CashTR (CA86)	6	D Critical	C Serious harm	C Serious harm	C Serious harm	A day
In-store processing (CA103)	7	D Critical	C Serious harm	C Serious harm	B Very serious harm	A week
COSIMA (CA80)	8	D Critical	D Minor harm	C Serious harm	C Serious harm	2-3 days
CALE (CA79)	9	D Critical	D Minor harm	C Serious harm	B Very serious harm	A month
Cashier support (CA85)	10	D Critical	E No significant harm	C Serious harm	B Very serious harm	A month
Store sales forecasting (CA106)	11	D Critical	E No significant harm	C Serious harm	B Very serious harm	A month
Vehicle Management (CA91)	12	E Important but not critical	C Serious harm	C Serious harm	C Serious harm	A week
Contracts register (CA84)	13	E Important but not critical	C Serious harm	D Minor harm	C Serious harm	A month
Performance recording (CA83)	14	E Important but not critical	D Minor harm	D Minor harm	D Minor harm	2-3 days
Fault recording (CA87)	15	E Important but not critical	E No significant harm	D Minor harm	C Serious harm	A month

Prepared by: Alex Albury

Full evaluations of information risk

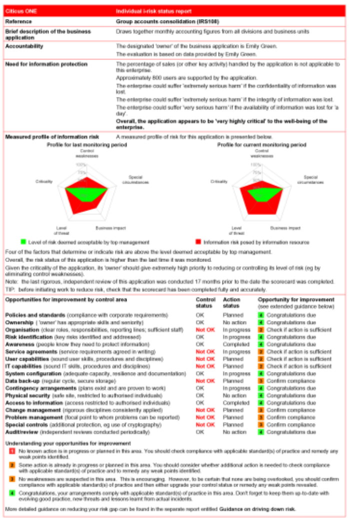
Citicus ONE presents scorecards backed up by powerful completion aids. These enable full evaluations of risk to be carried out efficiently in a consistent, business-oriented manner. First-time evaluations are best completed collectively at a 3-hour facilitated risk workshop, as illustrated below.

The facilitator uses **Citicus ONE** to walk-through completion of a scorecard (showing the applicable harm reference table and standard of practice when necessary), and to keep track of completers' comments.


Facilitated risk workshop
Application development / support
IT Operations
Business user or Help desk representative
Facilitator (eg a specialist in information risk or security)
Business 'owner'

Scorecards can subsequently be updated in minutes, as control improvements are made.

Immediately a scorecard is submitted, **Citicus ONE** presents a succinct **Individual risk status report** that a business 'owner' can take in 'at a glance'.



Citicus ONE	Individual i-risk status report
Reference	**Group accounts consolidation (IRS108)**
Brief description of the business application	Draws together monthly accounting figures from all divisions and business units
Accountability	The designated 'owner' of the business application is Emily Green. The evaluation is based on data provided by Emily Green.
Need for information protection	The percentage of sales (or other key activity) handled by the application is not applicable to this enterprise. Approximately 800 users are supported by the application. The enterprise could suffer 'extremely serious harm' if the confidentiality of information was lost. The enterprise could suffer 'extremely serious harm' if the integrity of information was lost. The enterprise could suffer 'very serious harm' if the availability of information was lost for 'a day'. **Overall, the application appears to be 'very highly critical' to the well-being of the enterprise.**
Measured profile of information risk	A measured profile of risk for this application is presented below.

🟩 Level of risk deemed acceptable by top management 🟥 Information risk posed by information resource

Four of the factors that determine or indicate risk are above the level deemed acceptable by top management.

Overall, the risk status of this application is higher than the last time it was monitored.

Given the criticality of the application, its 'owner' should give extremely high priority to reducing or controlling its level of risk (eg by eliminating control weaknesses).

Note: the last rigorous, independent review of this application was conducted 17 months prior to the date the scorecard was completed.

TIP: before initiating work to reduce risk, check that the scorecard has been completed fully and accurately.

Opportunities for improvement by control area	**Control status**	**Action status**	**Opportunity for improvement** (see extended guidance below)
Policies and standards (compliance with corporate requirements)	OK	Planned	4 Congratulations due
Ownership ('owner' has appropriate skills and seniority)	OK	No action	4 Congratulations due
Organisation (clear roles, responsibilities, reporting lines; sufficient staff)	Not OK	In progress	2 Check if action is sufficient
Risk identification (key risks identified and addressed)	OK	In progress	4 Congratulations due
Awareness (people know they need to protect information)	OK	Completed	4 Congratulations due
Service agreements (service requirements agreed in writing)	Not OK	In progress	2 Check if action is sufficient
User capabilities (sound user skills, procedures and disciplines)	Not OK	Planned	2 Check if action is sufficient
IT capabilities (sound IT skills, procedures and disciplines)	Not OK	Planned	2 Check if action is sufficient
System configuration (adequate capacity, resilience and documentation)	OK	In progress	4 Congratulations due
Data back-up (regular cycle, secure storage)	Not OK	Planned	3 Confirm compliance
Contingency arrangements (plans exist and are proven to work)	OK	In progress	4 Congratulations due
Physical security (safe site, restricted to authorised individuals)	OK	No action	4 Congratulations due
Access to information (access restricted to authorised individuals)	OK	Completed	4 Congratulations due
Change management (rigorous disciplines consistently applied)	Not OK	Planned	3 Confirm compliance
Problem management (focal point to whom problems can be reported)	Not OK	Planned	3 Confirm compliance
Special controls (additional protection, eg use of cryptography)	Not OK	Planned	3 Confirm compliance
Audit/review (independent reviews conducted periodically)	OK	No action	4 Congratulations due

Understanding your opportunities for improvement

1 No known action is in progress or planned in this area. You should check compliance with applicable standard(s) of practice and remedy any weak points identified.

2 Some action is already in progress or planned in this area. You should consider whether additional action is needed to check compliance with applicable standard(s) of practice and to remedy any weak points identified.

3 No weaknesses are suspected in this area. This is encouraging. However, to be certain that none are being overlooked, you should confirm compliance with applicable standard(s) of practice and then either upgrade your control status or remedy any weak points revealed.

4 Congratulations, your arrangements comply with applicable standard(s) of practice in this area. Don't forget to keep them up-to-date with evolving good practice, new threats and lessons learnt from actual incidents.

More detailed guidance on reducing your risk gap can be found in the separate report entitled **Guidance on driving down risk.**

Risk charts for current and previous period highlight changes in risk over time

Need for improvement in particular control areas highlighted, with clear priorities for action

Consolidated results for decision-makers

Citicus ONE's powerful analysis capabilities enable you to combine such individual results into fact-rich, high-level results for decision-makers. **Information risk 'league tables'**, for example, highlight your areas of greatest risk - and successes in driving risk down.

Top 10 information resources in information risk league table

Information resource	Risk ranking	Criticality	Control weaknesses	Special circumstances	Level of threat	Business impact
SecurNet (IRS10)	1	100%	82%	86%	100%	100%
New York data centre (IRS89)	2	100%	76%	100%	50%	25%
European data centre (IRS100)	3	75%	100%	57%	100%	50%
Group treasury mgt (IRS102)	4	75%	100%	43%	100%	75%
Global e-mail (IRS133)	5	75%	100%	71%	100%	50%
Accounts consolidation (IRS29)	6	75%	94%	71%	100%	25%
E-banking (IRS127)	7	75%	94%	86%	75%	50%
London data centre (IRS108)	8	75%	94%	71%	100%	50%
Group-wide WAN (IRS2)	9	75%	94%	86%	100%	75%
Billing system (IRS112)	10	75%	88%	71%	75%	25%

Bottom 10 information resources in information risk league table

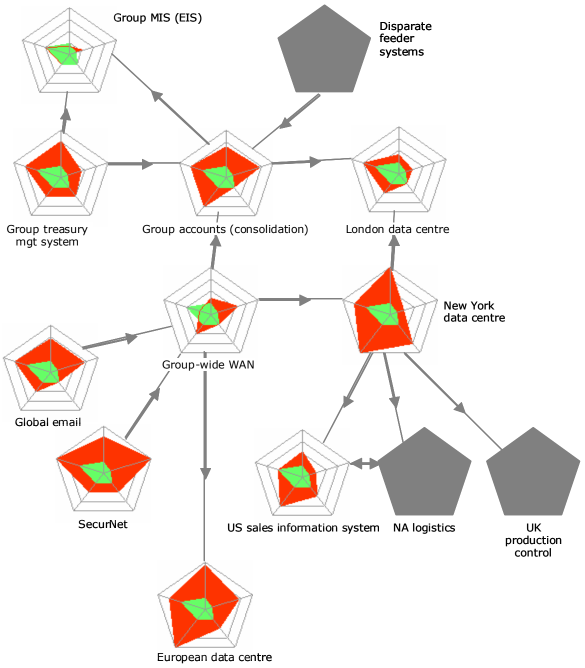
Group EIS (IRS50)	154	25%	12%	86%	50%	25%
Payroll (IRS46)	155	25%	6%	43%	50%	25%
DELTIC (IRS24)	156	25%	0%	29%	50%	0%
UK sales information (IRS57)	157	25%	0%	0%	50%	25%
CashTR (IRS42)	158	0%	100%	29%	75%	25%
Vehicle management (IRS34)	159	0%	82%	43%	100%	25%
Fault recording (IRS93)	160	0%	65%	14%	50%	0%
Performance recording (IRS15)	161	0%	59%	29%	100%	50%
Contracts register (IRS104)	162	0%	47%	57%	50%	0%
Expense claims (IRS88)	163	0%	24%	14%	100%	25%

The **financial impact of incidents** is also assessed (for incidents judged sufficiently serious to warrant it).

This enables the 'cost of insecurity' to be presented in meaningful, business terms.

	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 of tangible assets)	**$11,524,500**	**$960,375**
*Value of **staff-time lost** through incidents*	*$60,800*	*$12,200*

In today's increasingly interconnected world, the risk status of individual systems needs to be looked at in context. Thus, high-level **Dependency risk maps** enable system 'owners', IT staff and other decision-makers to look at how the risk posed by one system affects others in the chain, as illustrated below.



Infrastructure 'owners' can use these diagrams to gain a better understanding of the security needs of the applications they support; application 'owners' can use them to see if others are likely to let them down; security staff and auditors can use them to identify 'pinch points' and to plan reviews; and they are also helpful when setting recovery priorities in business continuity plans.

Together, **Citicus ONE**'s graphical results, easy-to-deploy fact-gathering tools and completion aids take inconsistency and expense out of risk management. In their place, you gain a helpful, efficient and constructive process that will fully equip you to manage information risk successfully enterprise-wide.

Contact www.citicus.com for details of our extensive support services, customer testimonials and prices.

For further information

If you are interested in learning more about Citicus Limited or our flagship product **Citicus ONE**, you are welcome to contact Citicus Limited as follows:

Direct contact

Simon Oxley, Managing director
E-mail: simon.oxley@citicus.com
Tel: +44 (0)1729 825 555

Sian Alcock, Director
E-mail: sian.alcock@citicus.com
Tel: +44 (0)20 7866 8116.

Head office

Citicus Limited
71-75 Shelton Street
Covent Garden
London WC2H 9JQ
United Kingdom.
E-mail: info@citicus.com
Web: www.citicus.com
Tel: +44 (0)20 3126 4999.