



# Managing information risk –an automated approach

**ISACA/IRM joint meeting, York, 28 April 2004**

**Simon Oxley**  
**Managing Director**  
**Citibus Limited, London**  
[www.citibus.com](http://www.citibus.com)



# About Citicus Limited

- Started in November 2000 to automate the Information Security Forum's **FIRM** (Fundamental Information Risk Management) methodology
- Secured exclusive, worldwide right to sell **FIRM** automation - reflecting Citicus representatives' lead role in its development - and have a continuing relationship with the ISF
- Provide **Citicus One** - the world's foremost tool for driving down information risk (ie the business risk posed by mission-critical, IT-based information systems)
- Provide clients with the training and support needed to implement **FIRM** using **Citicus ONE**, either directly or via Implementation Partners

## Selected customers



## Partners



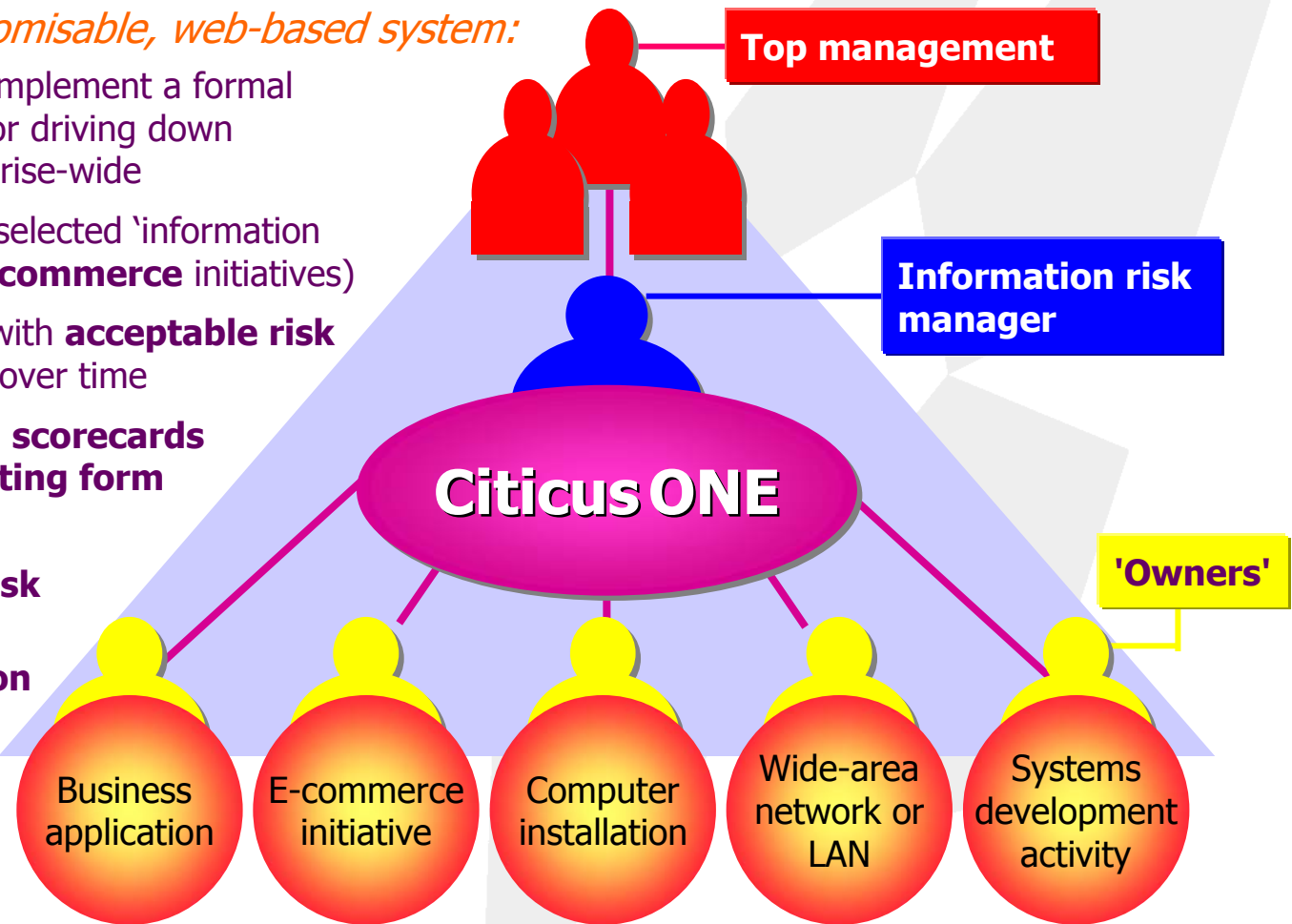
## Recognition



# Driving information risk down using Citicus ONE

*Citicus ONE is a customisable, web-based system:*

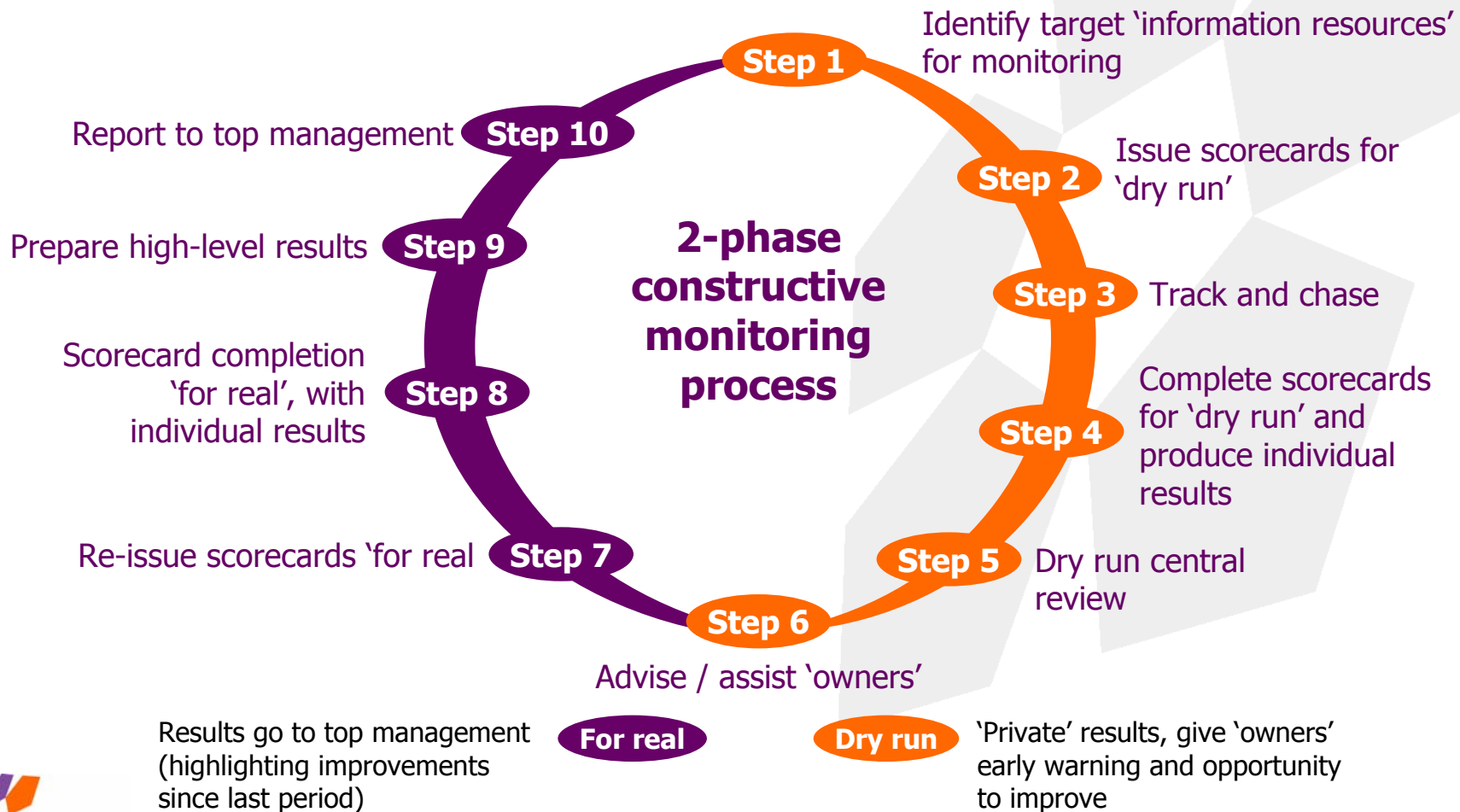
- developed to help you implement a formal methodology (**FIRM**) for driving down 'information risk' enterprise-wide
- monitors risk posed by selected 'information resources' (including **e-commerce** initiatives)
- compares **actual risk** with **acceptable risk** and highlights changes over time
- captures risk data using **scorecards** and an **incident reporting form**
- for each 'owner':
  - produces a 2-page **risk status report**
  - provides **guidance on driving down risk**
  - helps identify and track **remedial actions**
- produces:
  - **high-level risk status report**
  - **risk league tables - including external comparisons**
  - **incident lists and incident statistics**



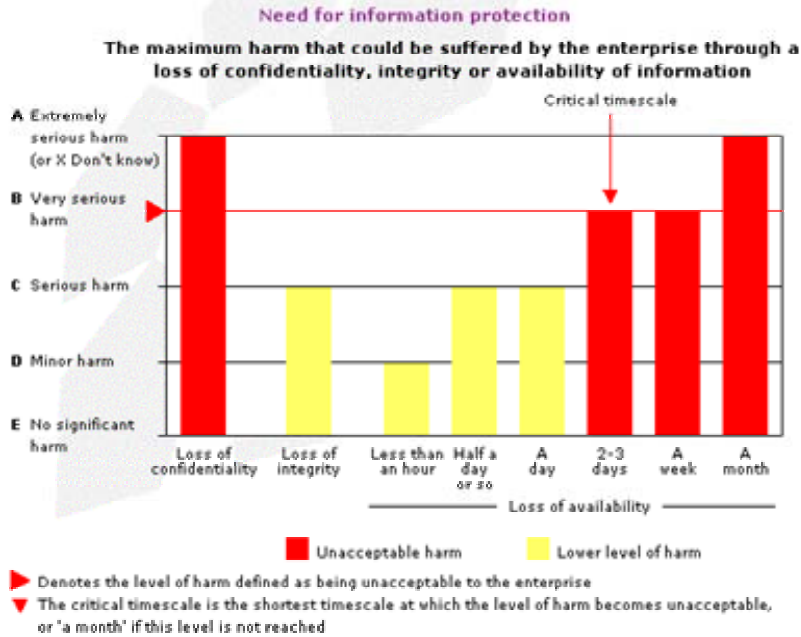
The **FIRM** methodology is published by the Information Security Forum, London.

# Citicus ONE creates a virtuous circle to drive information risk down

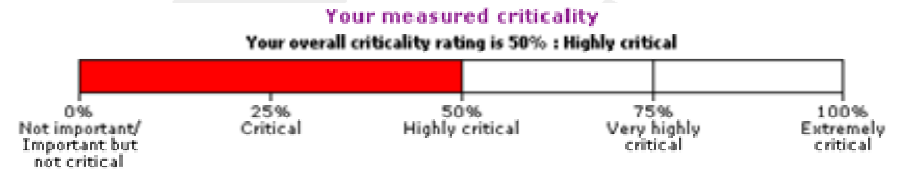
*The system supports a **2-phase, constructive monitoring process** - designed NOT to beat people up but to encourage success in driving risk down*



# A mini-scorecard supports first-cut criticality assessments



Criticality can be assessed for individual information resources



Criticality league tables can be produced covering a large number of information resources



Scorecard / assessment	Position in league table	Overall criticality	Confidentiality rating	Integrity rating	Availability rating	Critical timescale for availability
Billing system (IRS21)	1	B Very highly critical	C Serious harm	C Serious harm	A Extremely serious harm	A day
e-banking application (IRS17)	2	B Very highly critical	B Very serious harm	B Very serious harm	B Very serious harm	A day
London data centre (IRS2)	3	B Very highly critical	C Serious harm	C Serious harm	B Very serious harm	A day
Logistics system (IRS1)	4	C Highly critical	D Minor harm	D Minor harm	A Extremely serious harm	2-3 days
e-procurement initiative (ERS40)	5	C Highly critical	A Extremely serious harm	A Extremely serious harm	C Serious harm	Less than an hour



# Citicus ONE's scorecard measures i-risk realistically

*The scorecard embodies a rigorous, understanding of what drives information risk up and down*

- Statistically identified as key
- ⊗ Key for business purposes

● **Criticality:** identifies the harm that could be caused by a worst-case incident – the higher the level, the greater the need for protection

● **Vulnerability: a) Status of arrangements:** identifies weak control areas - the more there are, the greater the likelihood of incidents

● **Vulnerability: b) Special circumstances:** identifies which apply – where they do, the likelihood of incidents increases

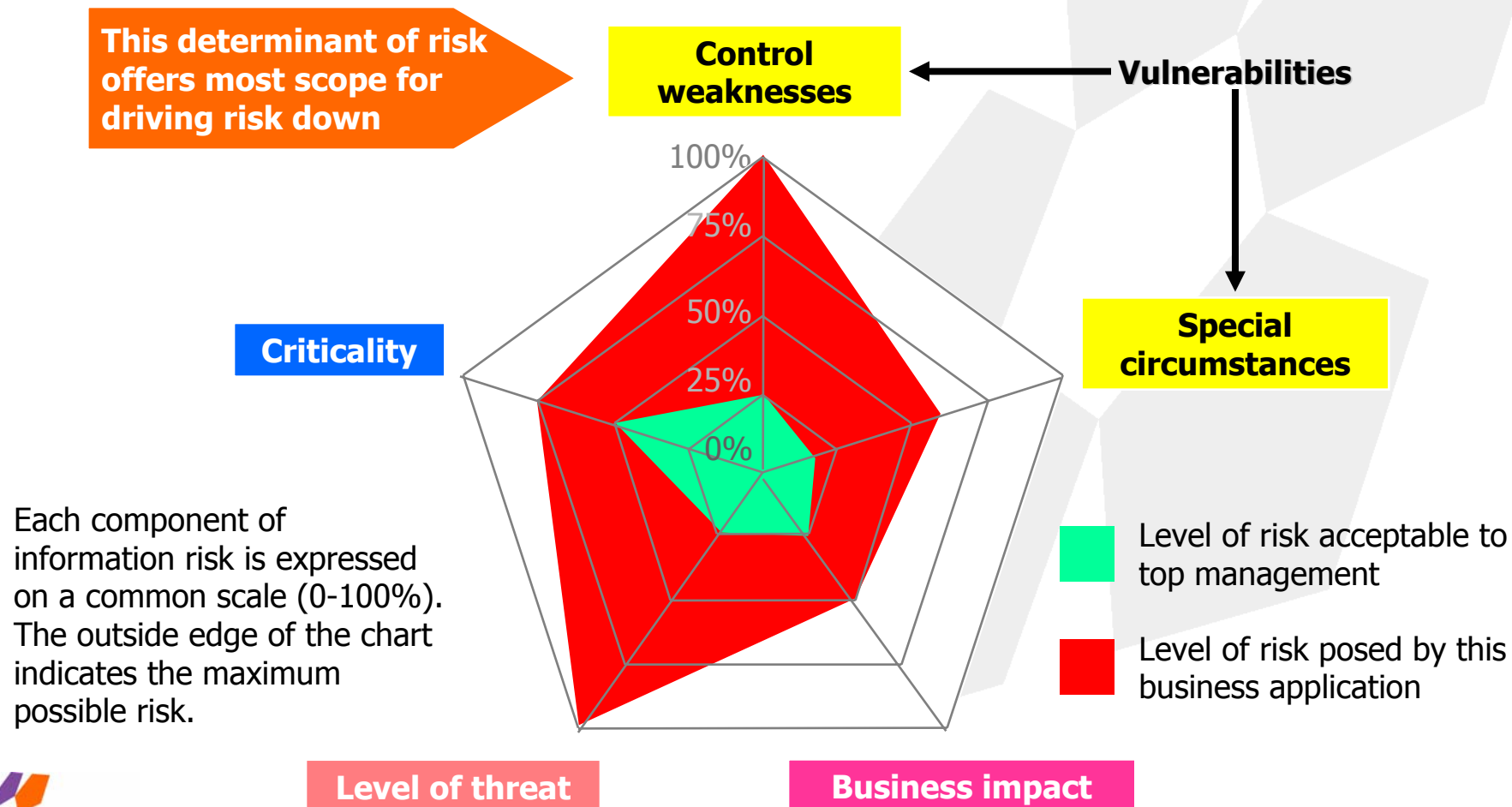
● **Level of threat:** identifies the number of incidents experienced – the more there are, the greater the likelihood of major incidents occurring (also provides a cross-check on control weaknesses)

⊗ **Business impact:** identifies the nature and level of harm caused by incidents - this shows incidents are a 'clear and present danger', enables discussion in business terms, and can trigger fuller incident reporting



# How Citicus ONE depicts risk for an individual application

*Risk charts produced by the system highlight where risk is at an unacceptable level and encourage **action to drive risk down***



# Providing 'owners' with proper management information on risk

*Page 1 enables an 'owner' to take in his or her risk status 'at a glance'*

Citicus ONE Individual i-risk status report																																																																									
Reference	Group accounts (consolidation) (RIS62)																																																																								
Brief description of the business application	Draws together monthly accounting figures from all divisions and business units application																																																																								
Accountability	The designated 'owner' of the business application is Emily Green. The evaluation is based on data provided by Marco Kapp.																																																																								
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. <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>Profile for last monitoring period</p> </div> <div style="text-align: center;"> <p>Profile for current monitoring period</p> </div> </div> <p>Level of risk deemed acceptable by top management (green) Information risk posed by information resource (red)</p> <p>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 lower 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).</p> <p>Note: the last rigorous, independent review of this application was conducted 8 months prior to the date the scorecard was completed. T.I.P. before initiating work to reduce risk, check that the scorecard has been completed fully and accurately.</p>																																																																								
Opportunities for improvement by control area	<table border="1"> <thead> <tr> <th>Control area</th> <th>Control status</th> <th>Action status</th> <th>Opportunity for improvement (see extended guidance below)</th> </tr> </thead> <tbody> <tr> <td>Policies and standards (compliance with corporate requirements)</td> <td>Not OK</td> <td>Planned</td> <td>1. Confirm compliance</td> </tr> <tr> <td>Ownership ('owner' has appropriate skills and seniority)</td> <td>OK</td> <td>No action</td> <td>2. Congratulate those involved</td> </tr> <tr> <td>Organisation (clear roles, responsibilities, reporting lines, sufficient staff)</td> <td>Not OK</td> <td>In progress</td> <td>3. Check if action is sufficient</td> </tr> <tr> <td>Risk identification (key risks identified and addressed)</td> <td>OK</td> <td>In progress</td> <td>4. Congratulate those involved</td> </tr> <tr> <td>Awareness (people know they need to protect information)</td> <td>OK</td> <td>Completed</td> <td>4. Congratulate those involved</td> </tr> <tr> <td>Service agreements (service requirements agreed in writing)</td> <td>Not OK</td> <td>In progress</td> <td>2. Check if action is sufficient</td> </tr> <tr> <td>User capabilities (password skills, procedures and disciplines)</td> <td>Not OK</td> <td>Planned</td> <td>2. Check if action is sufficient</td> </tr> <tr> <td>IT capabilities (hardware skills, procedures and disciplines)</td> <td>Not OK</td> <td>Planned</td> <td>2. Confirm compliance</td> </tr> <tr> <td>System configuration (adequate capacity, resilience and documentation)</td> <td>Not OK</td> <td>In progress</td> <td>2. Check if action is sufficient</td> </tr> <tr> <td>Data back-up (regular cycle, secure storage)</td> <td>Not OK</td> <td>Planned</td> <td>2. Confirm compliance</td> </tr> <tr> <td>Contingency arrangements (plans exist and are proven to work)</td> <td>Not OK</td> <td>In progress</td> <td>2. Check if action is sufficient</td> </tr> <tr> <td>Physical security (safe site, restricted to authorised individuals)</td> <td>OK</td> <td>No action</td> <td>4. Congratulate those involved</td> </tr> <tr> <td>Access to information (access restricted to authorised individuals)</td> <td>OK</td> <td>Completed</td> <td>4. Congratulate those involved</td> </tr> <tr> <td>Change management (rigorous disciplines consistently applied)</td> <td>Not OK</td> <td>Planned</td> <td>2. Confirm compliance</td> </tr> <tr> <td>Problem management (local point to whom problems can be reported)</td> <td>Not OK</td> <td>Planned</td> <td>2. Confirm compliance</td> </tr> <tr> <td>Special controls (additional protection, eg use of cryptography)</td> <td>Not OK</td> <td>Planned</td> <td>2. Confirm compliance</td> </tr> <tr> <td>Audit review (independent reviews conducted periodically)</td> <td>OK</td> <td>No action</td> <td>4. Congratulate those involved</td> </tr> </tbody> </table> <p>Understanding your opportunities for improvement</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> </ol> <p>More detailed guidance on reducing your risk pp can be found in the separate report entitled 'Guidance on driving down risk'.</p>	Control area	Control status	Action status	Opportunity for improvement (see extended guidance below)	Policies and standards (compliance with corporate requirements)	Not OK	Planned	1. Confirm compliance	Ownership ('owner' has appropriate skills and seniority)	OK	No action	2. Congratulate those involved	Organisation (clear roles, responsibilities, reporting lines, sufficient staff)	Not OK	In progress	3. Check if action is sufficient	Risk identification (key risks identified and addressed)	OK	In progress	4. Congratulate those involved	Awareness (people know they need to protect information)	OK	Completed	4. Congratulate those involved	Service agreements (service requirements agreed in writing)	Not OK	In progress	2. Check if action is sufficient	User capabilities (password skills, procedures and disciplines)	Not OK	Planned	2. Check if action is sufficient	IT capabilities (hardware skills, procedures and disciplines)	Not OK	Planned	2. Confirm compliance	System configuration (adequate capacity, resilience and documentation)	Not OK	In progress	2. Check if action is sufficient	Data back-up (regular cycle, secure storage)	Not OK	Planned	2. Confirm compliance	Contingency arrangements (plans exist and are proven to work)	Not OK	In progress	2. Check if action is sufficient	Physical security (safe site, restricted to authorised individuals)	OK	No action	4. Congratulate those involved	Access to information (access restricted to authorised individuals)	OK	Completed	4. Congratulate those involved	Change management (rigorous disciplines consistently applied)	Not OK	Planned	2. Confirm compliance	Problem management (local point to whom problems can be reported)	Not OK	Planned	2. Confirm compliance	Special controls (additional protection, eg use of cryptography)	Not OK	Planned	2. Confirm compliance	Audit review (independent reviews conducted periodically)	OK	No action	4. Congratulate those involved
Control area	Control status	Action status	Opportunity for improvement (see extended guidance below)																																																																						
Policies and standards (compliance with corporate requirements)	Not OK	Planned	1. Confirm compliance																																																																						
Ownership ('owner' has appropriate skills and seniority)	OK	No action	2. Congratulate those involved																																																																						
Organisation (clear roles, responsibilities, reporting lines, sufficient staff)	Not OK	In progress	3. Check if action is sufficient																																																																						
Risk identification (key risks identified and addressed)	OK	In progress	4. Congratulate those involved																																																																						
Awareness (people know they need to protect information)	OK	Completed	4. Congratulate those involved																																																																						
Service agreements (service requirements agreed in writing)	Not OK	In progress	2. Check if action is sufficient																																																																						
User capabilities (password skills, procedures and disciplines)	Not OK	Planned	2. Check if action is sufficient																																																																						
IT capabilities (hardware skills, procedures and disciplines)	Not OK	Planned	2. Confirm compliance																																																																						
System configuration (adequate capacity, resilience and documentation)	Not OK	In progress	2. Check if action is sufficient																																																																						
Data back-up (regular cycle, secure storage)	Not OK	Planned	2. Confirm compliance																																																																						
Contingency arrangements (plans exist and are proven to work)	Not OK	In progress	2. Check if action is sufficient																																																																						
Physical security (safe site, restricted to authorised individuals)	OK	No action	4. Congratulate those involved																																																																						
Access to information (access restricted to authorised individuals)	OK	Completed	4. Congratulate those involved																																																																						
Change management (rigorous disciplines consistently applied)	Not OK	Planned	2. Confirm compliance																																																																						
Problem management (local point to whom problems can be reported)	Not OK	Planned	2. Confirm compliance																																																																						
Special controls (additional protection, eg use of cryptography)	Not OK	Planned	2. Confirm compliance																																																																						
Audit review (independent reviews conducted periodically)	OK	No action	4. Congratulate those involved																																																																						

**Title:** identifies the information resource

**Responsibility:** identifies the 'owner' of the information resource, and who completed the scorecard

**Need for information protection:** describes how important it is to protect confidentiality, integrity and availability, and how critical the information resource is to the organisation

**Measured risk profile:** risk charts show measured risk this period (red) and last period (orange), compared to what is acceptable (green); along with a punchy commentary

**Opportunity for improvement:** highlights and prioritises opportunities for further action in control areas categorised as **Not OK** (ie those rated 'C' or below on the scorecard)

# Providing 'owners' with further information on risk

Page 2 explains each risk rating and highlights what we call 'dependency risk'

Citicus ONE		Individual risk status report		
<b>Contributions to risk profile</b>				
The table below shows your rating for each of the 5 components of risk plotted on the risk chart. The risk rating is shown as both a descriptive rating and its percentage of the maximum possible value (0-100%).				
Component of risk	Risk rating for this monitoring period	Equivalent value for risk chart		
Criticality	Very highly critical	75%		
Control weaknesses	11 control weaknesses apply	65%		
Special circumstances	5 special circumstances apply	71%		
Level of threat	51-100 incidents a year	75%		
Business impact	Minor harm	25%		
<b>Dependencies</b>				
The table below lists related information resources, the nature of the relationship and their risk status as measured on the date last monitored.				
Related information resource	Nature of relationship	Commentary	Risk status as data last monitored	Date last monitored
Group treasury mgmt system	Group treasury mgmt system supports Group accounts (consolidation)	Feeds + runs on same server		5-Feb-2003
London data centre	London data centre supports Group accounts (consolidation)	Runs our server		5-Apr-2002
Group-wide WAN	Group-wide WAN supports Group accounts (consolidation)	Carrier for feeds		5-Feb-2003
Disparate feeder systems	Disparate feeder systems supports Group accounts (consolidation)	Format and quality of feeds vary	Not Monitored	-
Group MIS (LIS)	Group MIS (LIS) is supported by Group accounts (consolidation)	MIS for top level executives		5-Feb-2003
Report completed by: Marco Kopp		Assessment date: 31-Jan-2003		

**Contribution to your risk profile:** a plain language interpretation of the numeric ratings that drive the red area of the risk chart

**Risk status of dependent information resources:** one risk chart for each system that the owner's information resource supports, and further risk charts showing the risk status of those it relies on (eg corporate WAN, European data centre, feeder application).

# Mapping 'dependency risk'

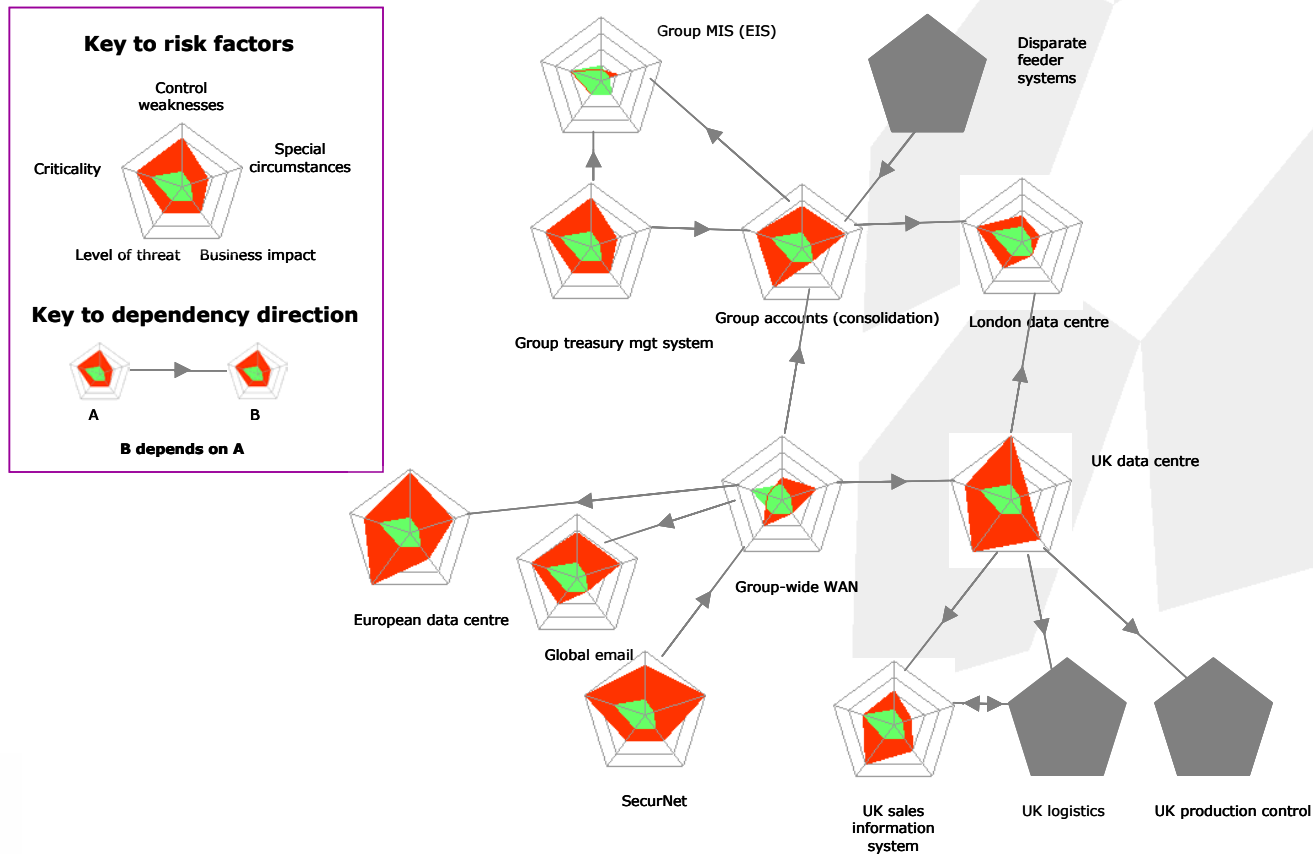
*Citicus ONE R1.3 allows you to plot dependency risk maps for your critical information resources.*

Citicus ONE

Basic version

## Dependency map

Reference: ABC enterprise dependencies



# A Citicus ONE league table shows where the key risks lie

*Citicus ONE ranks information resources in descending order of risk*

## Top 10 entries

	Rank	Criticality	Control weaknesses	Special circumstances	Level of threat	Business impact
Communications network C14	1	100%	76%	86%	50%	25%
Database C25	2	75%	100%	57%	100%	50%
Business application C97	2	75%	100%	57%	100%	50%
Computer installation C1	4	75%	100%	29%	100%	75%
Computer installation C2	5	75%	94%	71%	100%	50%
Communications network C126	6	75%	94%	86%	75%	50%
Database C134	7	75%	94%	71%	100%	25%
Communications network C67	8	75%	88%	57%	100%	100%
Computer installation C59	9	75%	88%	71%	75%	25%
Development activity C81	10	75%	82%	100%	100%	75%

Colour codes indicate the danger posed by each component of risk:

High
Med
Low

*You can control colour and sorting... and you can introduce external ratings for comparison*

## Bottom 10 entries

Database C8	136	25%	6%	43%	50%	25%
Business application C43	137	25%	0%	29%	50%	0%
Business application C116	138	25%	0%	0%	50%	25%
Database C22	139	0%	100%	29%	75%	25%
Business application C144	140	0%	82%	43%	100%	25%
Communications network C36	141	0%	65%	14%	50%	0%
Business application C111	142	0%	59%	29%	100%	50%
Computer installation C120	143	0%	47%	57%	50%	0%
Communications network C10	144	0%	41%	14%	100%	25%
Communications network C117	145	0%	24%	14%	100%	25%



## Sample **Citicus ONE** financial impact table

*Citicus ONE enables you to quantify the 'cost of insecurity', using data from individual incident assessments*

The 'cost of insecurity'	
Nature of impact	Calculated amount
Loss of sales income	\$66,400,000
Unforeseen costs	\$26,800,000
<b>Total reduction in profit</b>	<b>\$33,430,000</b>
Loss of tangible assets	\$1,100,000
<b>Total reduction in the value of the business</b>	<b>\$34,500,00</b>
<b>Average reduction in profit per individual reported incident</b>	<b>\$328,000</b>

The above figures are based on the financial impact of 102 incidents, of which 71 caused 'serious harm' or worse. The full financial impact of these incidents is not known, and the figures above do not include the impact of large numbers of minor incidents. Thus the total impact of incidents is likely to be much greater.

*You can also see the impact of incidents on **TIME** (ie the number and cost of staff hours lost through incidents)*

Collecting financial data like this:

- is practical
- provides business-oriented figures that top management want to know
- enables you to monitor trends over time in a business-oriented manner
- helps justify expenditure on staff and other improvements

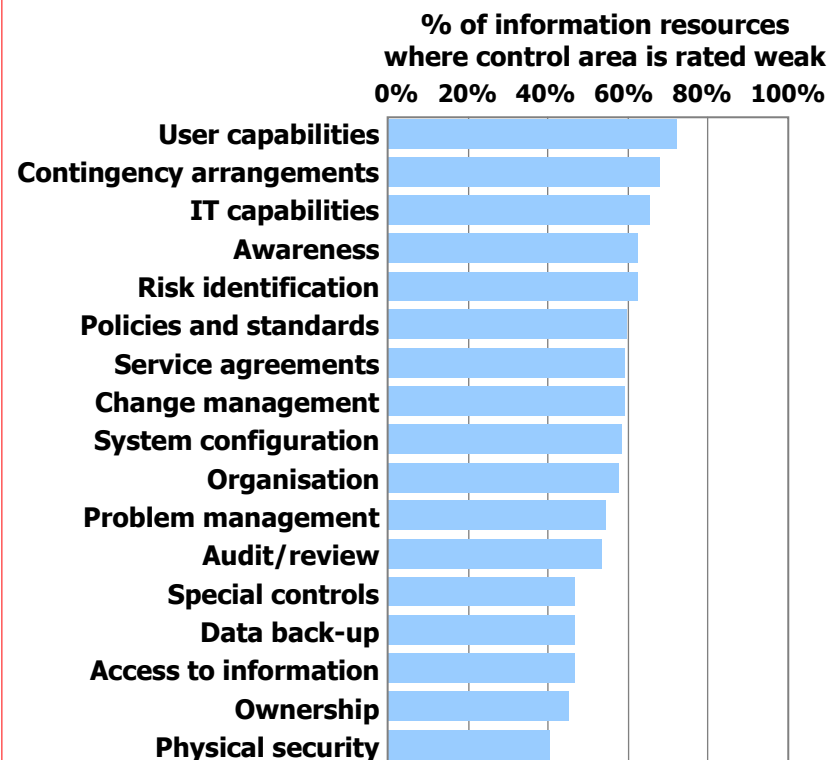
# Samples of other **Citicus ONE** aids for decision-making

*Citicus ONE provides the facts you need to devise and prioritise your risk reduction programmes (eg enhanced contingency arrangements)*

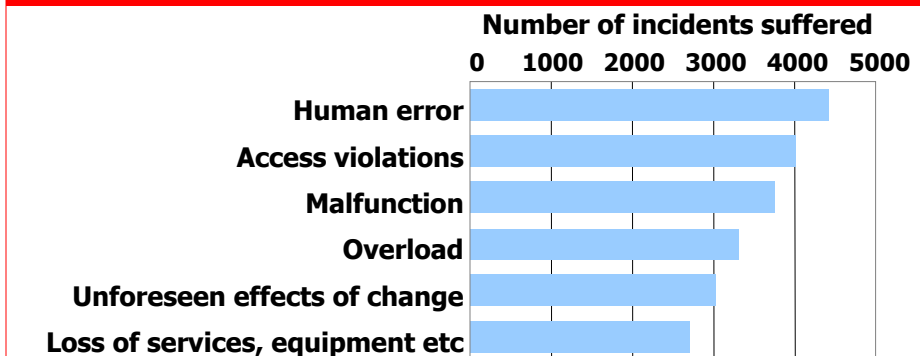
**Citicus ONE** will help you identify:

- the most common control weaknesses
- the most common types of incident
- the costs of incidents
- the root causes of incidents
- successful solutions others can apply

## Control weaknesses affecting our business-critical systems



## Type of incident affecting our business-critical systems



*Implementing **Citicus ONE** will equip you to manage a key risk down*

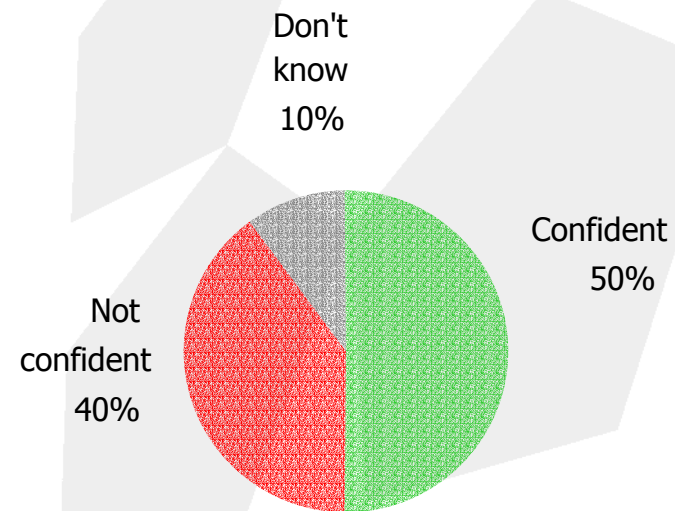
## Citicus ONE also provides incident lists and statistics

### *Incident lists show major incidents, ranked by impact*

- Nimda Virus
- Main computer room flooded
- Breach of licensing arrangements
- Loss of captured signatures on system
- Web site compromised
- Failure of hardware component caused system outage
- Customer accessed another customer's data
- Code Red Virus
- Confidential customer information obtained from website
- Wrong temporary configuration caused serious delays
- File with payments went from acceptance into live environment

### *Incident statistics reveal:*

- key features of incidents
- their business impact
- action taken to reduce them
- Confidence that remedial action will prevent repeat incidents





# Citicus ONE

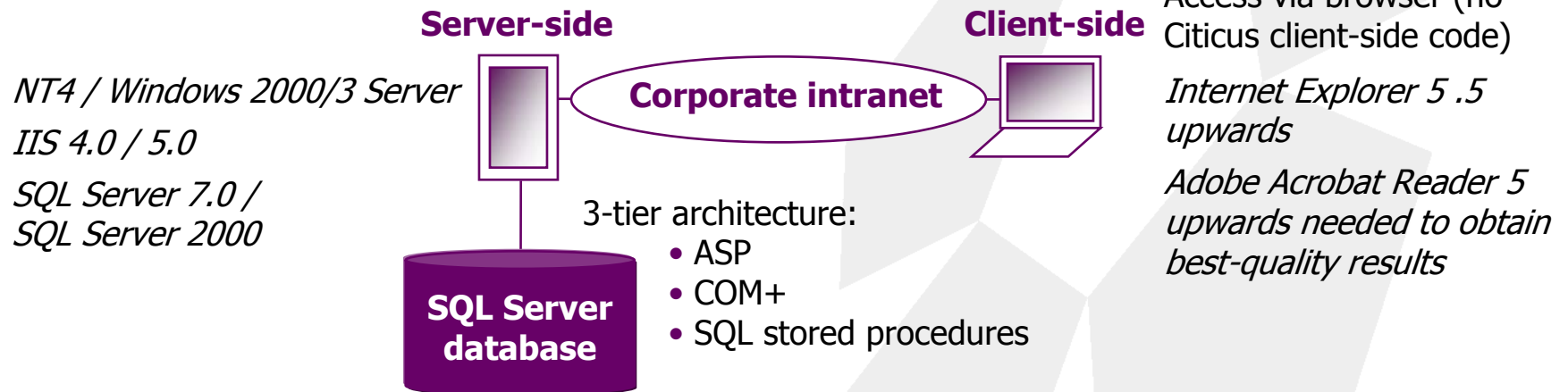
## Release 1.3



# Technical overview of Citicus ONE

## *Citicus ONE is optimised for:*

- **ease of installation:** automated install at server-side; no client-side software to install
- **ease of use:** minimises burden on owners
- **adaptability:** it facilitates customisation (eg incorporation of your standard of practice) and can support enterprises of all sizes/shapes



## *The design provides:*

- **a sound architecture:** data-driven, scalable design, use of mainstream technology
- **flexible deployment:** single, multi-server or laptop implementation, hosted service
- **selectable levels of security:** you choose how much protection to provide
- **scope for future integration** eg with corporate incident reporting, e-mail, 'internal publishing' and access control mechanisms (eg LDAP)

# Three main deployment options

*Option 1 offers an easy way of getting started  
(eg trials, pilots, limited roll-outs)*

In-house implementations		
1. Citicus-hosted service	2. Multi-user installation	3. Travelling installation
<b>Citicus ONE</b> runs on Citicus server(s) with access by users over the Internet via SSL	<b>Citicus ONE</b> runs on your server(s) with access by users via your corporate Intranet	<b>Citicus ONE</b> runs on a laptop: <ul style="list-style-type: none"> <li>• server-side and client side on same machine</li> <li>• no network connection required</li> </ul>

*Option 3 is ideal for carrying out mini-workshops' or other facilitated evaluations*

*Option 2 enables wider roll-out*



## Summarising the core capabilities of the **Citicus ONE** software

---

### Workflow management

Allows you to manage the **FIRM monitoring cycle**, eg issuing scorecards and assessments by email, monitoring completion, chasing delayed responses

### Fact gathering

Allows the on-line completion of **scorecards, criticality & incident assessments** with **help** and **supporting aids** one-click away

### Action planning

Allows owners of information resources to **define and track actions** that will drive down risk

### Results production

Allows the production of high-impact and useful results for individual owners and senior management in **PDF** format

### Customisation

Allows you to tailor **FIRM** to your own requirements eg **enterprise structure, standards of practice, acceptable levels of risk, definitions of harm**

### On-line Help

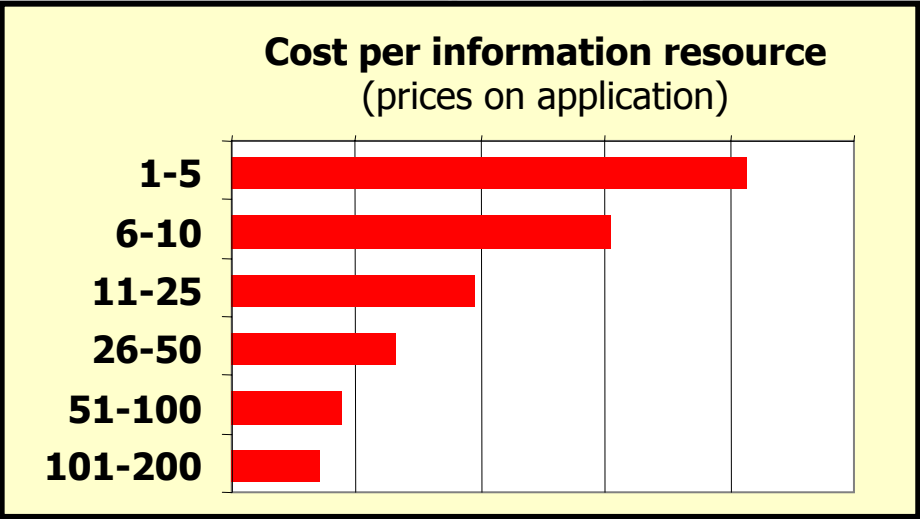
Provides comprehensive documentation on the **FIRM** methodology and the extensions provided by **Citicus ONE**

# Citicus ONE is priced to encourage wide deployment

*Four pricing options:*

	<b>In-house installation</b>	
<b>Citicus-hosted service</b>	<b>Multi-user implementation</b>	<b>Travelling installation</b>
<b>Annual service charge</b> , which includes upgrades, bug fixes and support	<b>One-time licence fee</b> , includes 1st year upgrades, bug fixes and support	Per laptop: <b>one-time licence fee</b> , or <b>fee per project</b>

*The more information resources you monitor, the lower the cost per information resource*



## We can help you deploy **Citicus ONE** successfully

---

**EDUCATION &  
TRAINING**

**PROJECT  
PLANNING**

**ASSISTED  
EVALUATIONS**

**DEVELOPMENT  
OF KEY AIDS**

**RESPONSIVE  
DEVELOPMENT**

**HOT-LINE  
SUPPORT**



# Implementing **Citicus ONE**: the cost / benefits

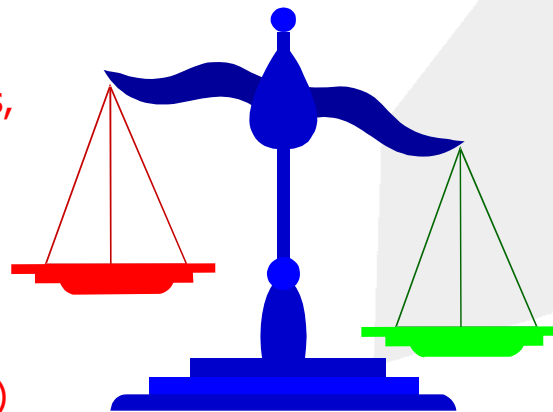
The big benefit is that **Citicus ONE** will help you drive down risk:

- Key area of risk properly understood
- Attention focused on information resources posing greatest risk, and weaknesses most commonly in need of improvement
- Owners equipped and motivated to drive risk down to a level defined as acceptable
- Measurable reduction in:
  - The number of information incidents your enterprise suffers
  - The chance of your enterprise suffering a major incident
  - Your enterprise's annual 'cost of insecurity'

## Costs

Budget for software access, maintenance and support

Running the process (half-time job for a programme manager, plus time required of local co-ordinators and 'owners')



## Business benefits

Demonstrable savings and efficiency gains that improve the bottom line

Improvement in corporate governance

Knowing you've got a grip on a key area of risk

# Supplementary information

---

The remaining slides provide further information about the following topics:

- what is 'information risk', exactly?
- other key terms (arrangement, control, incident, information resource)
- the **FIRM** methodology
- how we work
- our relationship with the Information Security Forum
- examples of the key statistics that underpin what we do.

# What is 'information risk', exactly

---

*Probability of suffering harm*

*Nature and level of harm*

Information risk is the **chance or possibility** of **harm** being caused to a business as a result of a loss of the **confidentiality, integrity or availability** of **information**

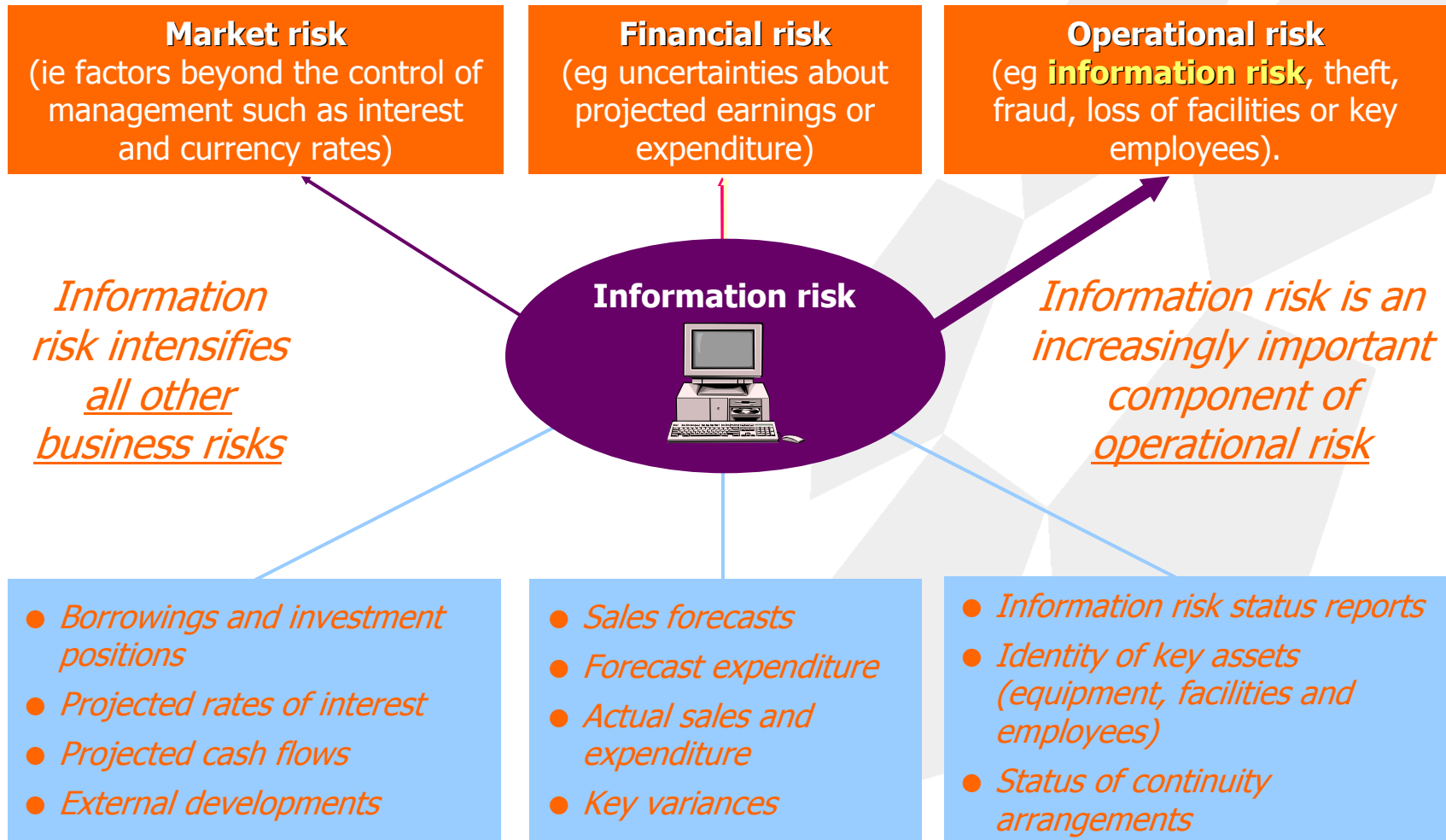
*The 3 key properties of information to be protected*

*Exists in varying forms:*

- held in people's heads
- communicated face-to-face
- recorded in deeds and other securities
- entered into, stored, processed, transmitted and presented via IT

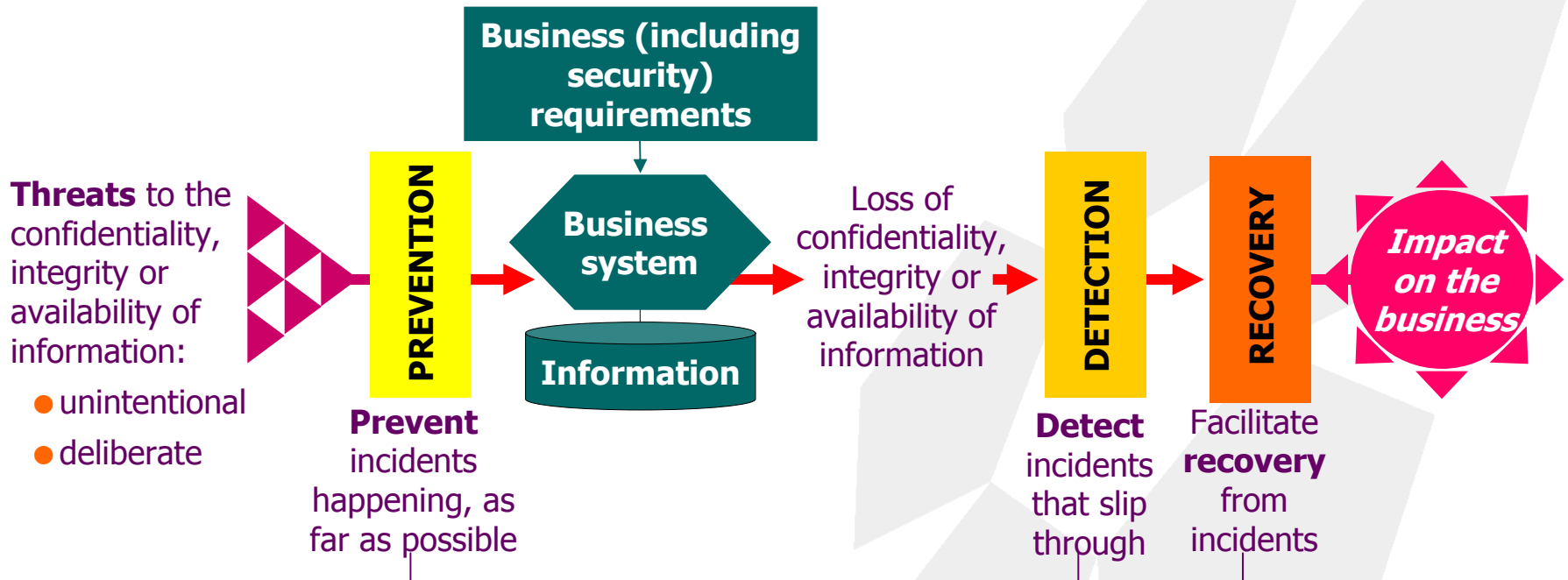
*The **method** of protection depends on the **form** of the information*

# How information risk influences other business risks



*Information is needed to manage each category of risk*

# Getting information risk under control



## Arrangements for protecting information - grouped into 'FIRM control areas'

- Policies and standards
- Ownership
- Organization
- Risk identification
- Awareness
- Service agreements
- User capabilities
- IT capabilities
- System configuration
- Data back-up
- Contingency arrangements
- Physical security
- Access to information
- Change management
- Problem management
- Special controls
- Audit/review
- (Business practices)

## The **FIRM** methodology

---

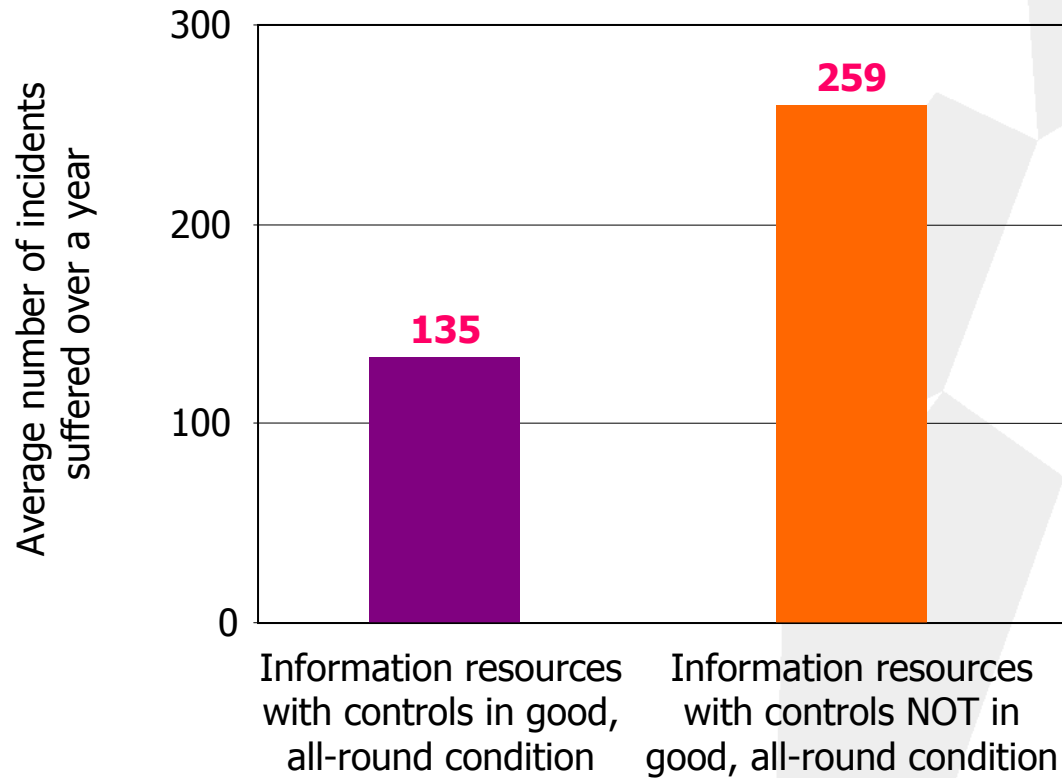
***FIRM** is a fully-developed methodology for managing information risk across an enterprise:*

- a ground-breaking, **quantitative** and **measurement-based** approach
- published by the Information Security Forum - an association of 250+ of the world's leading organisations who come together to fund and take part in a practical research programme in information security
- developed by Citicus's co-founder Marco Kapp on behalf of and in conjunction with the Forum
- supported by statistical analysis into the massive body of statistics collected by the Forum
- has generated exceptional interest among Forum Members
- supports BS7799 and ISO 17799 as well as the Forum's Standard of practice
- key features of **FIRM** are accessible through **Citicus ONE's** well-designed Help sub-system, and training in its implementation is provided by Citicus

Citicus has a exclusive, worldwide right to develop and sell automation which enables organisations to implement the **FIRM** methodology.

## Good controls drive down the **volume** of incidents

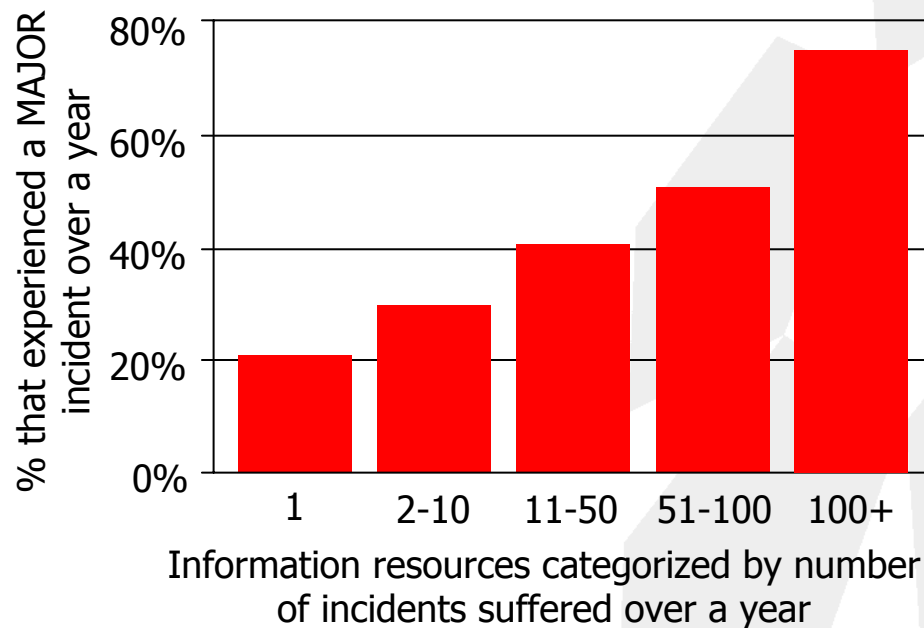
*The average number of incidents suffered a year is halved when controls are in 'good, all-round condition'*



Citicus analysis of some 210,000 incidents affecting 844 information resources covered by the Information Security Forum's 2000-2002 Security Status Survey.

## Why reducing the **volume** of incidents is important

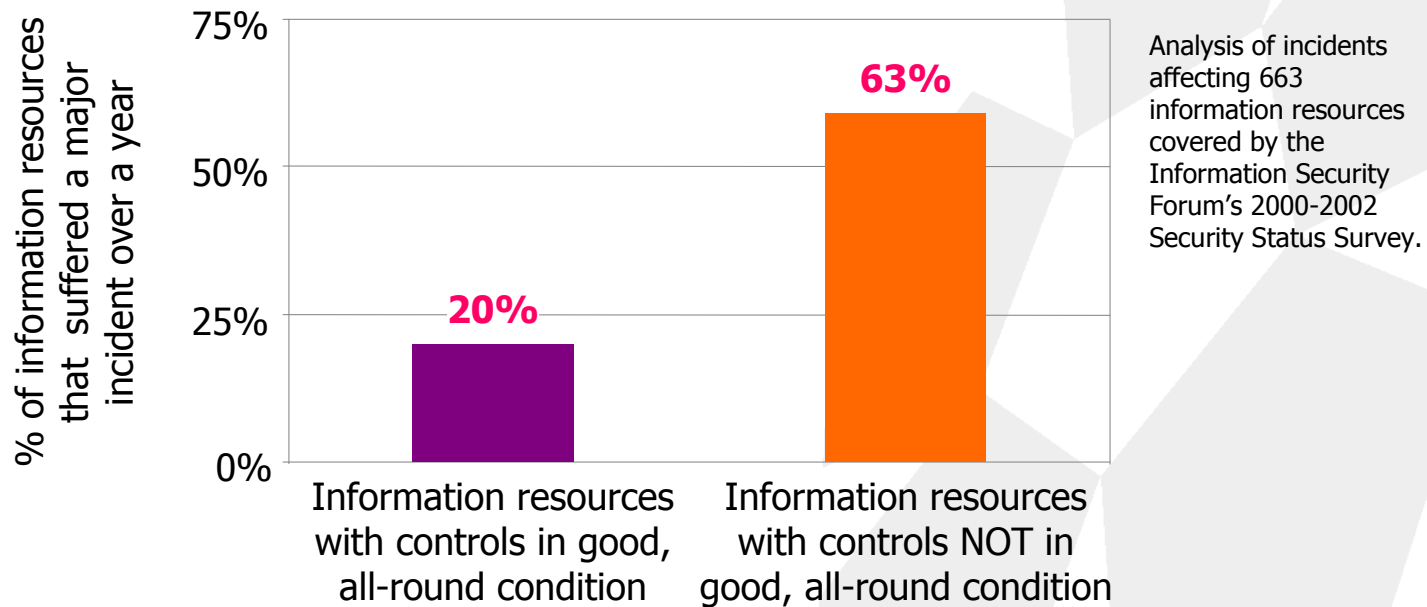
*Eliminating minor incidents is important, since the chance of suffering a MAJOR incident climbs as the number of minor incidents increases*



Citicus analysis of incidents affecting 844 information resources covered by the Information Security Forum's 2000-2002 Security Status Survey.

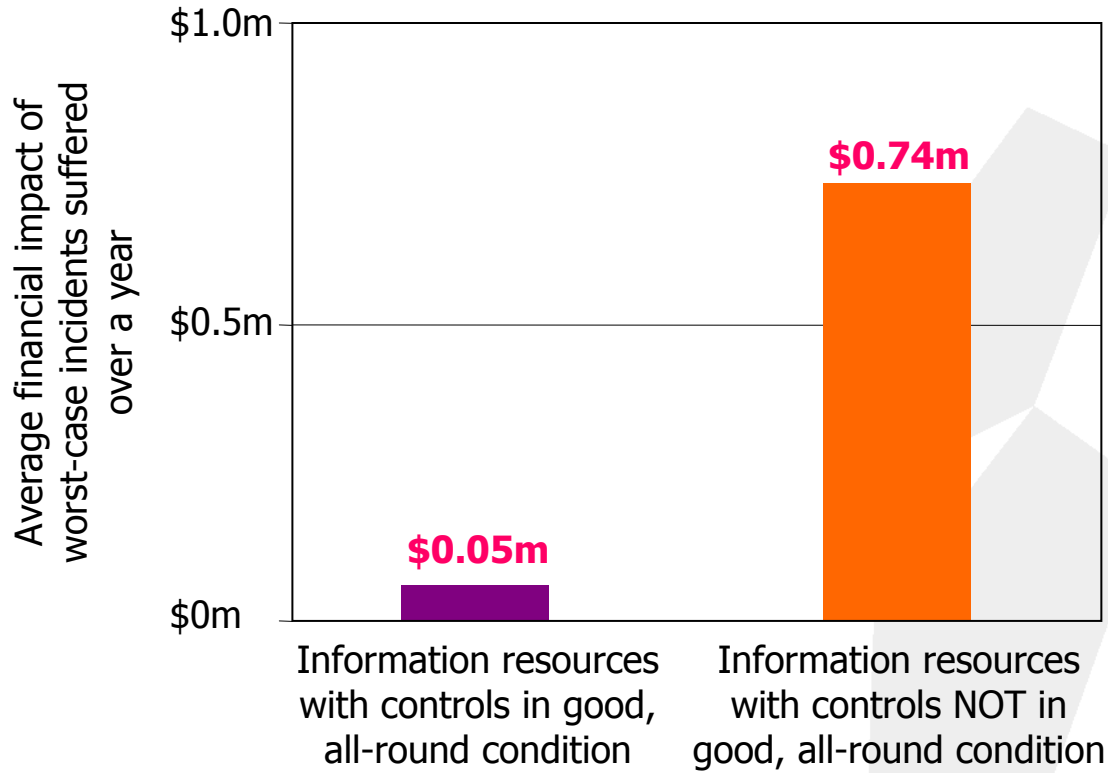
## Good controls slash the odds of suffering **major** incidents

*Controls that are in 'good, all-round condition' reduce the probability of experiencing MAJOR incidents by more than a factor of three*



# Good controls lead to big savings

*Controls that are in 'good, all-round condition' dramatically reduce the **financial impact** of worst-case incidents*



Analysis of 244 worst-case incidents for which financial data was provided covered by the Information Security Forum's 2000-2002 Security Status Survey

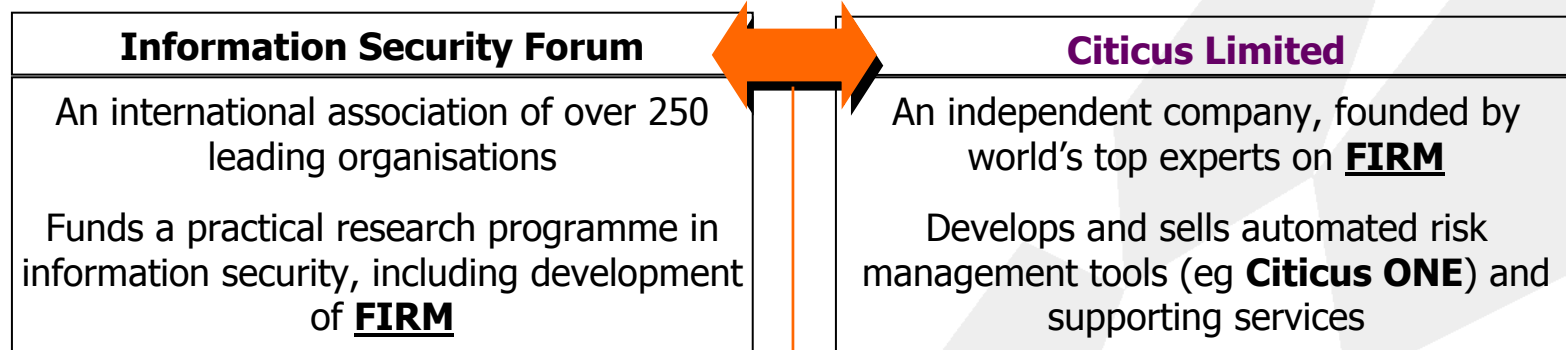
## How we work

**Citicus ONE** was the outcome of CDP1 - our first collaborative development programme. Our launch partners and current customers are leading, global corporations, active in the following fields:

Main activity	Where based
Financial services	USA, UK, Switzerland, South Africa
Electronics	USA, France, Northern Europe
Consumer products	USA, UK, Netherlands
Paper products	Sweden
Energy	UK, Norway
Air transport	UK
IT services	USA, UK, Germany, Switzerland
Pharmaceuticals	Europe
Agro-chemicals	Switzerland
Professional services	UK
Telecommunications	UK
Retail	UK
Publishing	Germany
Government	UK, Ireland, Netherlands



## Our continuing relationship with the Information Security Forum



### Unique, collaborative agreement announced October 2001

ISF owns the published **FIRM** methodology and extension to e-commerce (ie e-risk evaluation tool)

ISF receives a royalty on sales of **Citiculus ONE**

ISF Members can obtain **Citiculus ONE** at a special discount

Citiculus has exclusive, world-wide right to develop and sell **FIRM** automation, including its extension to e-commerce

Citiculus pays a royalty to the ISF on each sale of **Citiculus ONE**

Citiculus offers **Citiculus ONE** to ISF Members at a special discount

Commitment to work together on on-going development of **FIRM** and on supporting activities (eg ISF's **FIRM** training workshops for Members)

# Citicus key personnel

---

Citicus Limited is run by a team with unrivalled experience in measuring and managing information risk:

## **Simon Oxley, Managing Director, Citicus Limited**

- 18 years in the information security field
- Was head of information security at National Power and Reuters
- Member of the ISF's Council, 1992-94
- Led the ISF's work on e-commerce, active content, cryptography, web security and security architecture; contributed to many other ISF projects, including the one that led to **FIRM**



## **Sian Alcock, Director, Citicus Limited**

- Spent 3 years developing and analyzing the results of the world's most comprehensive survey of information security practices
- Oversees our product development, maintenance services and user training



## **Marco Kapp, Director, Citicus Limited**

- 30 years experience of IT including developing and running major systems, and providing advice and assistance to leading IT users, suppliers and public policy-makers
- Spent 10 years as a Director of Coopers & Lybrand's UK consulting practice
- Instrumental in establishing the ISF and directed its first year of operation
- Led or contributed to numerous ISF projects, particularly those involving standards of practice and quantitative risk work
- Chief architect of the ISF's **FIRM** methodology



## For further information

---

*You can contact Citicus Limited as follows:*

### **Direct contact**

Simon Oxley	
Email	<a href="mailto:simon.oxley@citicus.com">simon.oxley@citicus.com</a>
Tel	+44 (0)1729 825 555
Marco Kapp	
Email	<a href="mailto:marco.kapp@citicus.com">marco.kapp@citicus.com</a>
Tel	+44 (0)1306 742 072
Sian Alcock	
Email	<a href="mailto:sian.alcock@citicus.com">sian.alcock@citicus.com</a>
Tel	+44 (0)20 8870 9279.

### **Head office**

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

Email	<a href="mailto:info@citicus.com">info@citicus.com</a>
Web	<a href="http://www.citicus.com">www.citicus.com</a>
Tel	+44 (0)20 7203 8405
Fax	+44 (0)20 7203 8409.

