

Introducing Citicus ONE Release 3.3

Managing information risk ... and beyond

Citicus Limited

www.citicus.com

What our award-winning **Citicus ONE** software can do for you

Citicus ONE Release 3.3 equips you to:



Establish a **highly-efficient, continuous** process for measuring and managing risk and compliance across your organization



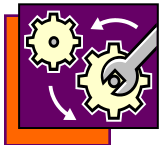
Measure the **criticality** and **risk** of business systems, IT infrastructure, business processes, sites, suppliers and other assets **objectively** and in **business terms**



Measure **compliance with relevant standards of practice** including internal policies, external codes of practice (eg SOGP, ISO2700x, COBIT, PCI, ITIL) and any legislation or regulations that applies (eg privacy regulations, Sarbanes-Oxley, Basel II, health and safety rules)



Assess and record **incidents**, including their business impact and root causes



Record and track **remediation activity**, including oversight of all issues until they are resolved and both the costs and benefits of remedial action

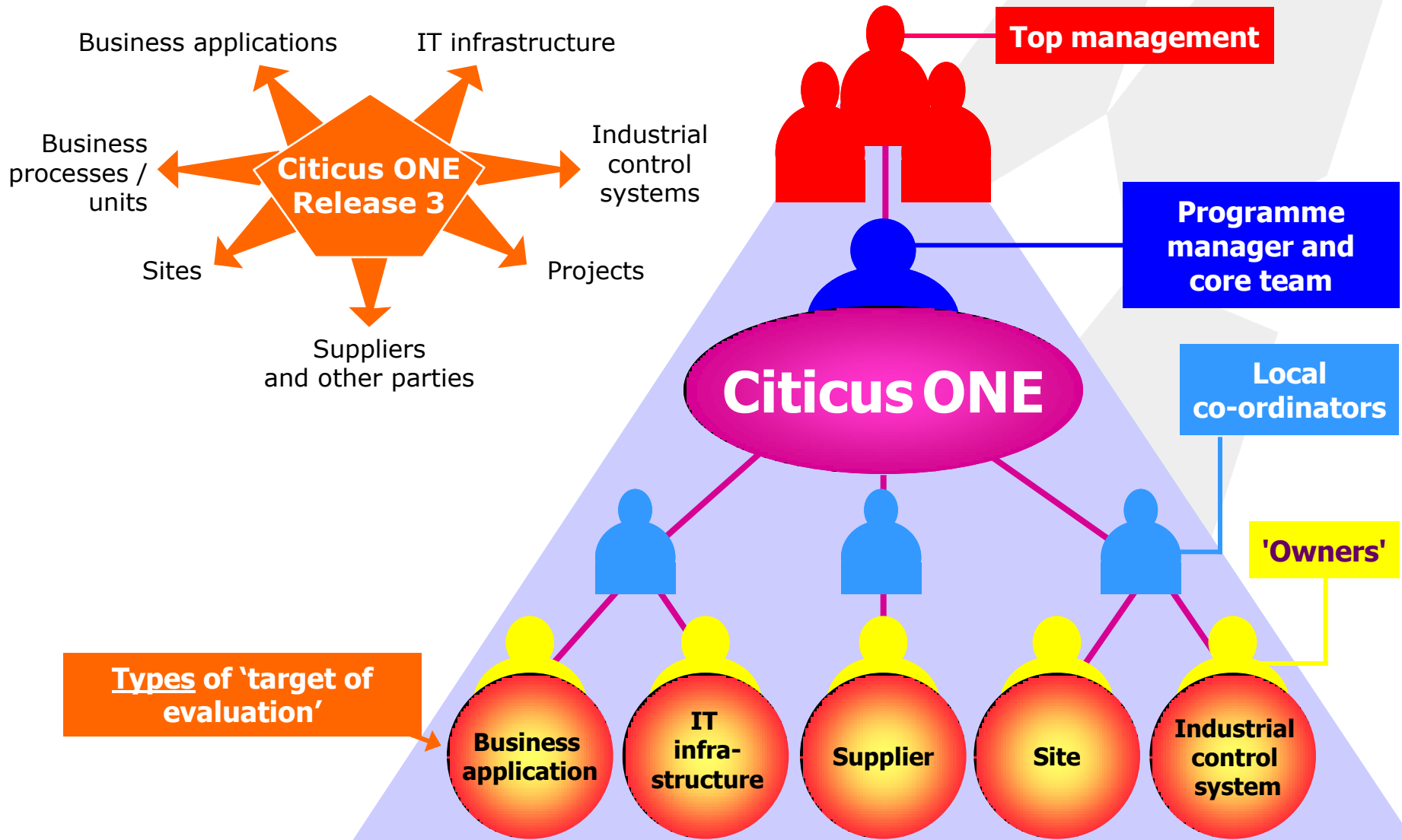


Report to management on risk in succinct, business-oriented terms, with aggregation across different areas of risk



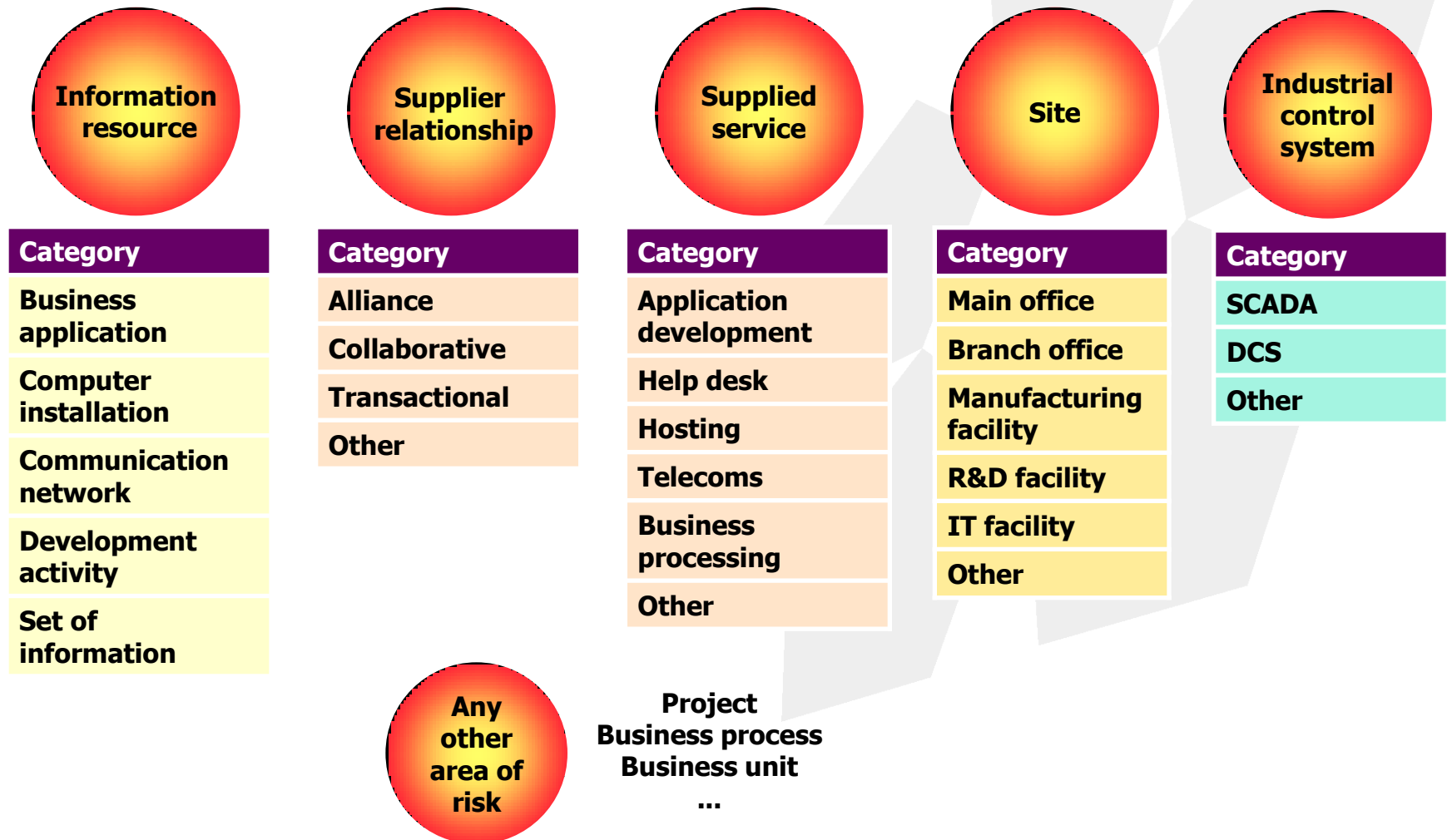
Exchange data with other systems

Determining what you want **Citicus ONE** to evaluate



Types of 'Target of evaluation' supported out-of-the-box

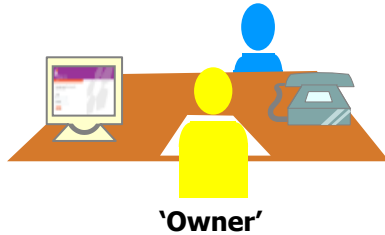
*Several target types are supported 'out of the box'. Additional ones can be set up at any time using **Citicus ONE** and **Citicus Workbench**.*



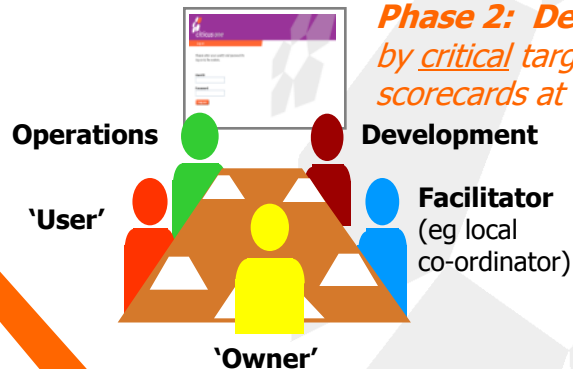
Citicus ONE supports a proportionate risk management process

'Phase 0: Discovery'

Identify and 'unpack' targets of evaluation, and identify their 'owners'



Phase 1: Criticality assessments: Assess each target of evaluation's criticality



Phase 2: Deeper dives: Evaluate risk posed by critical targets of evaluation by completing risk scorecards at 3-hr risk workshops

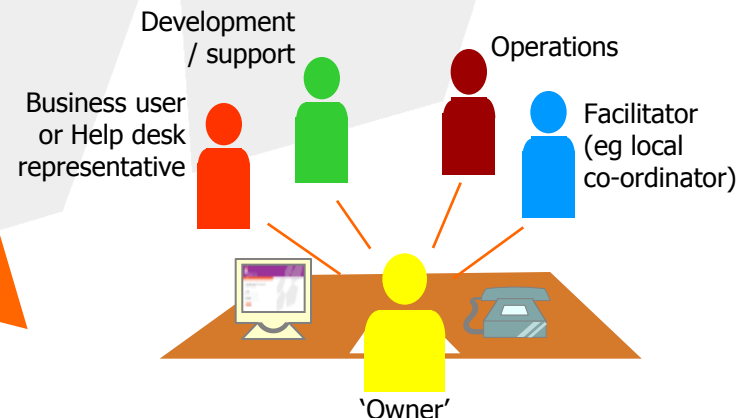
The criticality of hundreds of targets of evaluation can be evaluated in a few weeks – thousands might take 6 months to complete. Once completed, evaluations can be updated in minutes.

You can also use **Citicus MoCA** for iPhone, iPad and iPod touch to complete criticality assessments.



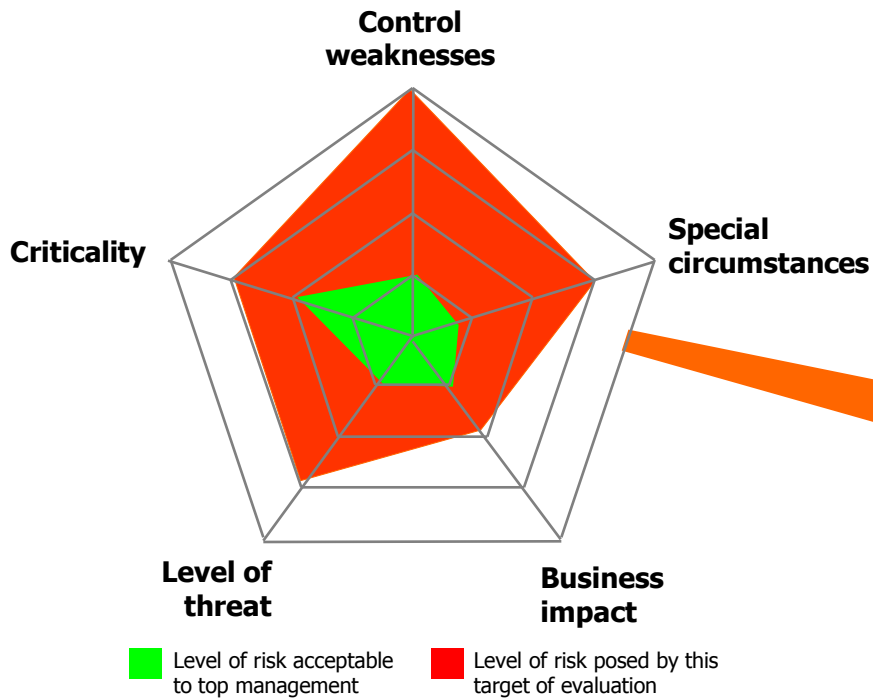
Embed as a continuing process into the business

Phase 3: Update: Owners' / completers update scorecards / remediation plans

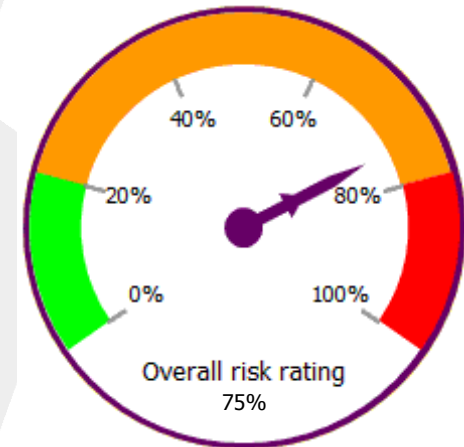


Risk metrics

To get a good handle on risk **Citicus ONE** measures the status of 5 determinants / indicators of risk. These are aggregated into a single risk metric.



Individual risk chart

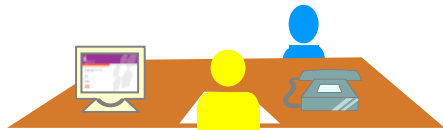


Risk: ■ Low ■ Medium ■ High

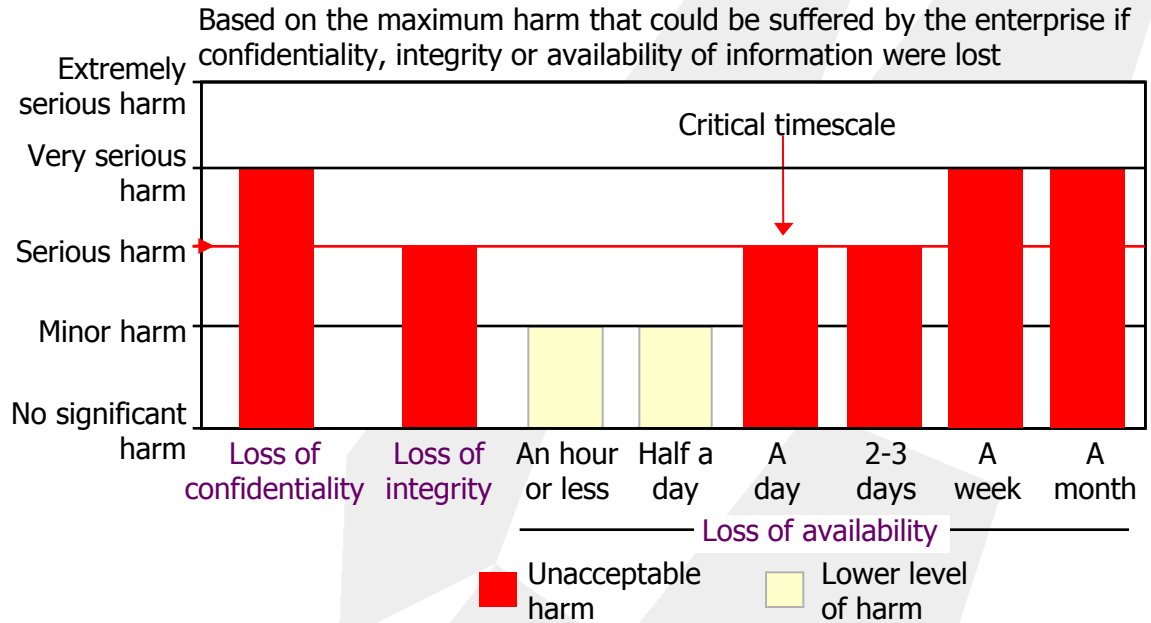
Overall risk rating

Phase 1: Assessing criticality in a business-oriented manner

An 'owner' can complete a criticality assessment on-line in 20 minutes



'Owner' of an information resource



The results of different Criticality assessments can be consolidated into a Criticality league table, providing a risk-oriented inventory of the organization's 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

Assessing impact objectively with a Harm reference table

Excerpt of a sample Harm reference table

NATURE OF HARM	Appropriate measure	LEVEL OF HARM				
		A Extremely serious	B Very serious	C Serious	D Minor	E None
Financial loss (lost revenue, unforeseen costs, penalties, fraud)	Financial impact:	\$10+ million	\$1 - 10 million	\$100 thousand - 1 million	\$10 - 100 thousand	\$0 - 10 thousand
Degraded performance (failure to achieve targets, loss of productivity)	Targets under-achieved by:	10%+	5% to 10%	1% to 5%	Less than 1%	No impact
	Wasted staff-hours:	10,000+ hours	5,000 to 10,000 hours	1,000 to 5,000 hours	100 to 1,000 hours	0 to 100 hours
Damaged reputation (negative publicity, regulatory action, litigation)	Extent of negative publicity	Prolonged widespread negative publicity	Brief widespread negative publicity	Prolonged local negative publicity	Brief local negative publicity	No impact

Minor adaptation required to cover types of harm that matter to a specific organisation

Phase 2: Evaluating risk and compliance, in as much detail as you wish

2-page Risk scorecard



Risk factors can be fully evaluated at 3-hour facilitated risk workshops:

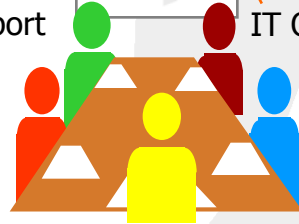
- Criticality
- Status of controls
- Special circumstances
- Experience of incidents
- Business impact of incidents



Supporting harm reference table

Harm reference table	
Low	Medium
High	Critical

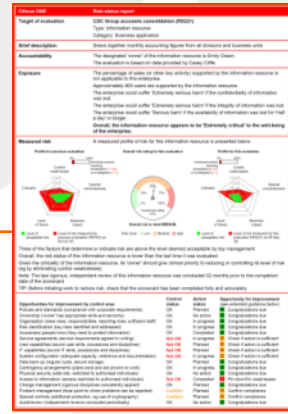
Application support
Business user or Help desk specialist



Business 'owner'

IT Operations

Facilitator (eg local co-ordinator)



Individual risk status report

Supporting standard of practice or compliance checklist

Control area	Awareness
Start description: People know they need to protect information	
Required standard of practice	Current status
05.001 Information security education and training	A A B C D E F
05.002 All employees associated with the information resource and, where relevant, third party users, should receive appropriate training and register updates in organisational policies and procedures.	Q Q Q Q Q Q Q
05.004 Continuity against malicious software	A A B C D E F
05.005 User awareness procedures to protect against malicious software should be implemented.	Q Q Q Q Q Q Q



Compliance status report

Assessing the strength of controls in detail

Control area		Data back-up							
Short description		regular cycle, secure storage							
Required practice		Current status				Recommended test	Source		
D1.10.1	Information back-up								
D1.10.2	Back-up copies of essential business information and software should be taken and tested regularly.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Verify that back-ups are taken and can be reliably restored before unacceptable harm is suffered. Confirm by carrying out a restore operation.	A8.4.1
D1.10.3	Safeguarding of important records								
D1.10.4	Important records relating to an information resource should be protected from loss, destruction and falsification.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Identify such records and their retention periods / media. Verify that they are stored in ways that satisfy statutory / regulatory requirements, and the enterprise's own needs; and permit recovery throughout their required life.	A12.1.2
<i>Items D1.10.5 to D1.10.7 have been suppressed because they do not apply to this target of evaluation.</i>									

The checklist allows a detailed assessment of control status in a way which allows the compliance with key standards to be measured and reported.

Recording additional details while completing a checklist

Control area on scorecard

Data back-up (regular cycle, secure storage)

ISO27001 Standard of practice for this control area

Control area		Data back-up					
Short description		regular cycle, secure storage					
Required practice		Current status		Recommended test		Source	
D1.10.1	Information back-up						
D1.10.2	Back-up copies of essential business information and software should be taken and tested regularly.	1	2	3	4	N	X
		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
D1.10.3	safeguarding of important records						
D1.10.4	Important records relating to an information resource should be protected from loss, destruction and falsification.	1	2	3	4	N	X
		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Items D1.10.5 to D1.10.7 have been suppressed because they do not apply to this target of evaluation.							

Status of this particular statement of required practice (control item D1.10.02)

Checklist item	Current status
D1.10.2 Back-up copies of essential business information and software should be taken and tested regularly.	2 Our arrangements comply with the stated standard
Guidance to evaluators	Source
	A8.4.1
You can supplement your response by entering comments in the box below and / or attaching one or more files.	
Your comments	Attachments
<input type="text"/>	0
Attach ...	
Recommended test	
Verify that back-ups are taken and can be reliably restored before unacceptable harm is suffered. Confirm by carrying out a restore operation.	
If you verified compliance with required practice by testing, please describe your method of testing and its results.	
Test applied	Attachments
<input type="text"/>	0
Attach ...	
If you believe that required practice does <u>not</u> apply to this target of evaluation, please describe your reasoning.	
Reason not applicable	Attachments
<input type="text"/>	0

'Owners' obtain good-looking management information on risk status

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

Page 2 highlights 'dependency risk'

Citicus ONE Risk status report

Target of evaluation
 CDC Global email (R8198)
 Type: Information resource
 Category: Business application

Brief description
 Corporate email system, run by Group Central Services

Accountability
 The designated 'owner' of the information resource is Harry Grey. The evaluation is based on data provided by Eve Everett.

Exposure
 The percentage of sales (or other key activity) supported by the information resource is not applicable to this enterprise.
 Approximately 30,000 users are supported by the information resource.
 The enterprise could suffer 'Very serious harm' if the confidentiality of information was lost.
 The enterprise could suffer 'Minor harm' if the integrity of information was lost.
 The enterprise could suffer 'Serious harm' if the availability of information was lost for 'Less than an hour' or longer.
 Overall, the information resource appears to be 'Extremely critical' to the well-being of the enterprise.

Measured risk
 A measured profile of risk for this information resource is presented below.

Four of the factors that determine or indicate risk are above the level deemed acceptable by top management. Overall, the risk status of this information resource is lower than the last time it was evaluated. Given the criticality of the information resource, its 'owner' should give utmost priority to reducing or controlling its level of risk (eg by eliminating control weaknesses).

Note: It is not known whether a rigorous, independent review of this information resource has ever been conducted.
 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	No action	Congratulations due
Ownership ('owner' has appropriate skills and seniority)	Not OK	No action	Pin down/fix weaknesses
Organisation (clear roles, responsibilities, reporting lines; sufficient staff)	OK	No action	Congratulations due
Risk identification (key risks identified and addressed)	OK	No action	Congratulations due
Awareness (people know they need to protect information)	OK	No action	Congratulations due
Service agreements (service requirements agreed in writing)	Confirms	No action	Confirm compliance
User capabilities (sound user skills, procedures and disciplines)	OK	No action	Congratulations due
IT capabilities (sound IT skills, procedures and disciplines)	OK	No action	Congratulations due
System configuration (adequate capacity, resilience and documentation)	OK	No action	Congratulations due
Data back-up (regular cycle, secure storage)	OK	No action	Congratulations due
Contingency arrangements (plans exist and are proven to work)	OK	No action	Congratulations due
Physical security (safe site, restricted to authorised individuals)	OK	No action	Congratulations due
Access to information (access restricted to authorised individuals)	Not OK	No action	Pin down/fix weaknesses
Change management (rigorous discipline consistently applied)	Not OK	No action	Pin down/fix weaknesses
Problem management (focal point to whom problems can be reported)	Not OK	No action	Pin down/fix weaknesses
Special controls (additional protection, eg use of cryptography)	Not OK	No action	Pin down/fix weaknesses
Audit/review (independent reviews conducted periodically)	Not OK	No action	Pin down/fix weaknesses

Twin risk charts show improvement from one evaluation to the next

Highlights and prioritises opportunities for further action in control areas categorised as **Not OK**

Citicus ONE Risk status report

Understanding your opportunities for improvement

- 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.
- 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.
- 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.
- 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*.

Contribution to risk profile
 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 evaluation period	Equivalent value for risk chart
Criticality	Extremely critical	100%
Control weaknesses	7 control weaknesses apply	41%
Special circumstances	5 special circumstances apply	71%
Level of threat	11-50 incidents a year	50%
Business impact	Minor harm	25%

Dependencies
 The table below lists related targets of evaluation, the nature of the relationship and their risk status as measured on the date last evaluated, sorted by criticality, then by control weaknesses.

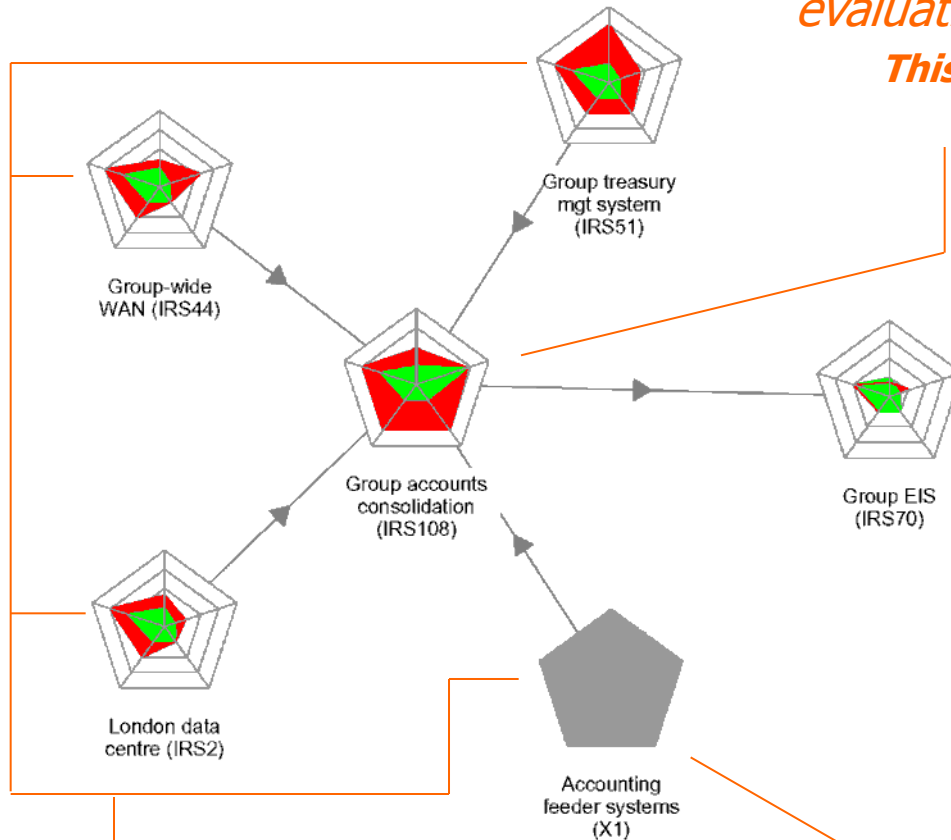
Related target of evaluation	Nature of relationship	Commentary	Risk status on date last evaluated
Name: EMA London data centre Type: Information resource Category: Computer installation 'Owner': Bill O'Connor Purpose of evaluation: For real	EMA London data centre supports CDC Global email	Hosts our email server	 (R8155), evaluated on 09 Oct '05
Name: CDC Group-wide WAN Type: Information resource Category: Communication network 'Owner': Gabriela Fernandez Purpose of evaluation: For real	CDC Group-wide WAN supports CDC Global email	Carries all email traffic	 (R8150), evaluated on 09 Oct '05

Attributes
 The following attributes have been assigned to this information resource

- Application name (harmonized): CDC Global email
- Application name (local): CDC email
- Application type: Package-based: Yes
- Application version: Microsoft Exchange Server 2003 supporting mainly Microsoft Outlook 2002 clients
- Database software (type and version): Legato archival server
- Functional area(s) supported: All
- Geographical scope: Global: Yes
- Handles e-mail: Yes
- Implementation date: Jan 2004
- IT continuity: Covered by HQ BCP
- Maximum allowable data loss: 1 in 10 million e-mails
- Operating system(s) employed: Windows Server 2003
- Planned retirement date: Not yet identified

Dependency risk maps help 'owners' look at risk in context

Citicus ONE allows you to plot **dependency risk maps** for any or all targets of evaluation.



This target of evaluation sits at the centre of an **individual dependency risk map**.

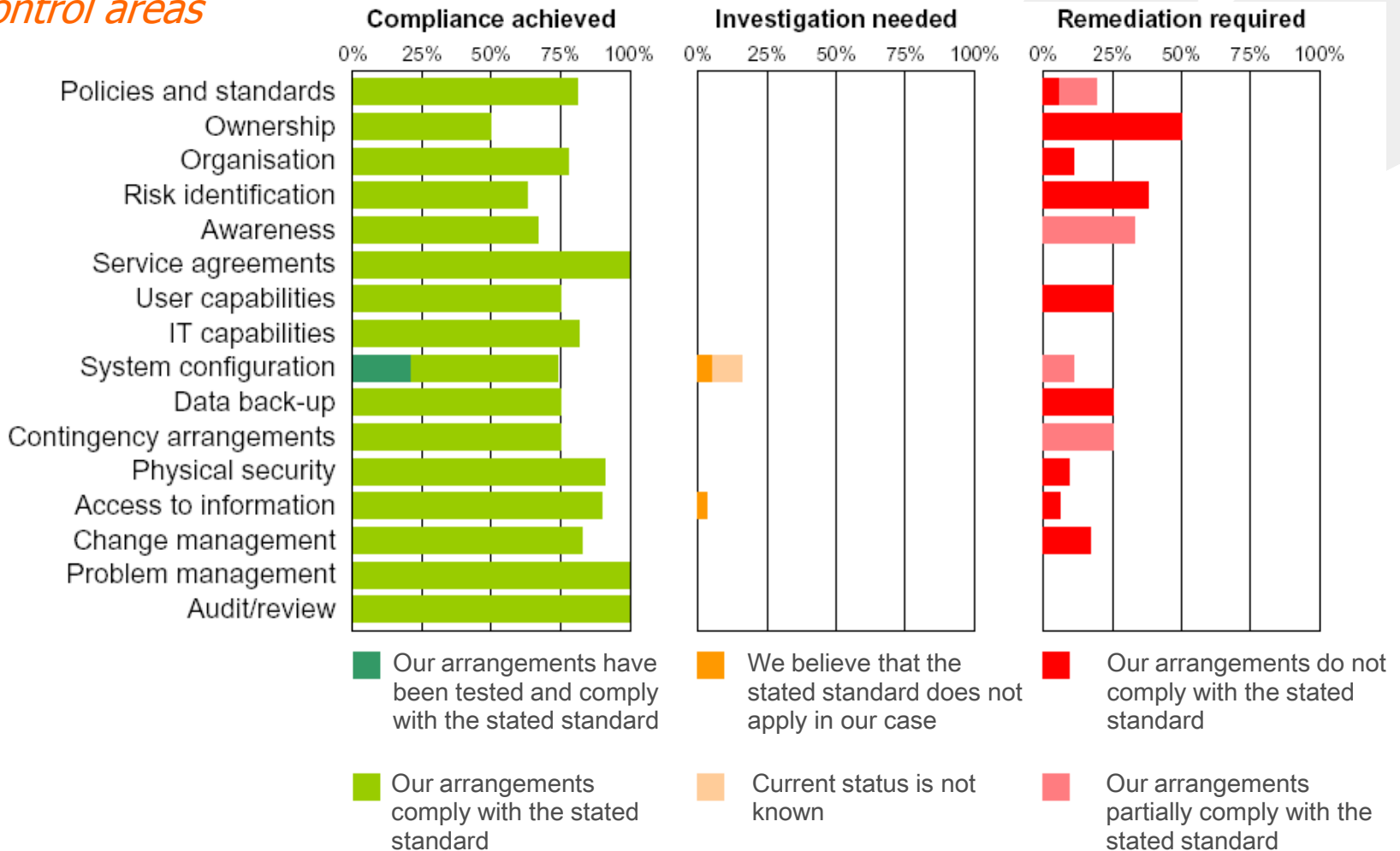
What relies on this one: the risk status of targets of evaluation that rely on this one can be identified by the outward-pointing arrowhead on the connecting line.

What this one relies on: the risk status of supporting targets of evaluation can be identified by the inward-pointing arrowheads on the connecting lines.

Unknown risk: the risk status of this target of evaluation is unknown because no evaluation has been performed.

Compliance status reports provide more detail on controls

Citicus ONE provides an overview of compliance with a customizable set of control areas



Compliance trend reports show reduction in risk over time

Citicus ONE	Compliance trend report										
Target of evaluation	CDC Group accounts consolidation (RS236) Type: Information resource Category: Business application										
Brief description	Draws together monthly accounting figures from all divisions and business units										
Compliance scope shown in this report	This report presents the compliance status of CDC Group accounts consolidation evaluated using the range of controls specified below. Compliance checklist: SA.U.3 CDC general IT standard of practice with recommended tests (ISO27001 and UK data protection controls) Control area: All control areas Control item: All controls										
Compliance status over time	The chart below presents the change in status with time of the range of controls specified above that have been evaluated for CDC Group accounts consolidation. The level of compliance evaluated in the current risk scorecard is shown, along with up to three previous evaluations where available. In this case, two previous evaluations are available. For a more detailed analysis of compliance status at any point in time see the Compliance status report associated with a specific risk scorecard.										
<p style="text-align: center;">Compliance focus: All control areas</p> <p style="text-align: center;">Evaluation history for CDC Group accounts consolidation</p>											
Appendix	<p>The compliance status shown in this report is derived from the responses in completed checklists as shown in the table below.</p> <table border="1"> <thead> <tr> <th>Compliance status</th> <th>Checked response</th> </tr> </thead> <tbody> <tr> <td>Compliance achieved</td> <td>1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard</td> </tr> <tr> <td>Investigation needed</td> <td>N We believe that the stated standard does not apply in our case¹ X Current status is not known</td> </tr> <tr> <td>Remediation required</td> <td>3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard</td> </tr> <tr> <td>Not evaluated / Not applicable</td> <td>Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'</td> </tr> </tbody> </table> <p>¹ Although these controls have been rated as not applicable, they are defined as baseline controls in the checklist. Their status should therefore be verified.</p>	Compliance status	Checked response	Compliance achieved	1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard	Investigation needed	N We believe that the stated standard does not apply in our case ¹ X Current status is not known	Remediation required	3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard	Not evaluated / Not applicable	Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'
Compliance status	Checked response										
Compliance achieved	1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard										
Investigation needed	N We believe that the stated standard does not apply in our case ¹ X Current status is not known										
Remediation required	3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard										
Not evaluated / Not applicable	Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'										
Checklist completed by	Casey Cliffe										
Evaluation date	12 Jun '09										

Individual compliance trend report

Citicus ONE	Consolidated compliance trend report										
Report title	Compliance trend for whole enterprise (HLR.17)										
This report	This report shows the variation over time of the extent of compliance of a selected range of targets of evaluation with a specified control item, control area or compliance checklist.										
Report focus	This report covers targets of evaluation of all types, evaluated using the compliance checklist identified below. Compliance checklist: SA.U.3 CDC general IT standard of practice with recommended tests (ISO27001 and UK data protection controls), including variants Control area: All control areas Control item: All controls Evaluations performed using previous versions of the focus checklist are included in the report but ratings for obsolete controls / control areas will not be featured. See the Featured evaluations report for a list of targets of evaluation that are included.										
Compliance status over time	The chart below presents the status of the range of controls specified above across the 12 targets of evaluation that fall within the scope of the report. For each point in time, the number of targets of evaluation included is presented in brackets.										
<p style="text-align: center;">Compliance focus: All control areas</p> <p style="text-align: center;">Evaluation history</p>											
<p>The compliance status shown in this report is derived from the responses in completed checklists as shown in the table below.</p> <table border="1"> <thead> <tr> <th>Compliance status</th> <th>Checked response</th> </tr> </thead> <tbody> <tr> <td>Compliance achieved</td> <td>1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard</td> </tr> <tr> <td>Investigation needed</td> <td>N We believe that the stated standard does not apply in our case¹ X Current status is not known</td> </tr> <tr> <td>Remediation required</td> <td>3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard</td> </tr> <tr> <td>Not evaluated / Not applicable</td> <td>Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'</td> </tr> </tbody> </table> <p>¹ Although these controls have been rated as not applicable, they are defined as baseline controls in the checklist. Their status should therefore be verified.</p>		Compliance status	Checked response	Compliance achieved	1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard	Investigation needed	N We believe that the stated standard does not apply in our case ¹ X Current status is not known	Remediation required	3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard	Not evaluated / Not applicable	Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'
Compliance status	Checked response										
Compliance achieved	1 Our arrangements have been tested and comply with the stated standard 2 Our arrangements comply with the stated standard										
Investigation needed	N We believe that the stated standard does not apply in our case ¹ X Current status is not known										
Remediation required	3 Our arrangements partially comply with the stated standard - more work is needed 4 Our arrangements do not comply with the stated standard										
Not evaluated / Not applicable	Control areas that have not yet been evaluated or controls that are defined as discretionary and have a response of 'N We believe that the stated standard does not apply in our case'										
Commentary	Good improvement over the last quarter! Let's keep the progress going.										

Consolidated compliance trend report

Drilling down to see the status of an individual risk factor (eg BCP/DR)

Risk factor analysis report

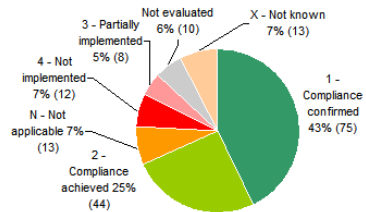
Citicus ONE Risk factor analysis report

Report title XYZ Global Services

This report This report shows the status of an individual control item across the targets of evaluation covered by the scope of this report.

Selected risk factor Type: Control item
Control area: System configuration
Checklist item: 09.004 Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
Controls checklist: ABC checklist of controls based on BS7799 (SA.U.12)

Overview of control status The chart below presents an overview of the status of the selected control item across the 175 targets of evaluation that have been evaluated using the controls checklist identified above. For each status, the percentage (and number) of targets of evaluation with that status is indicated.

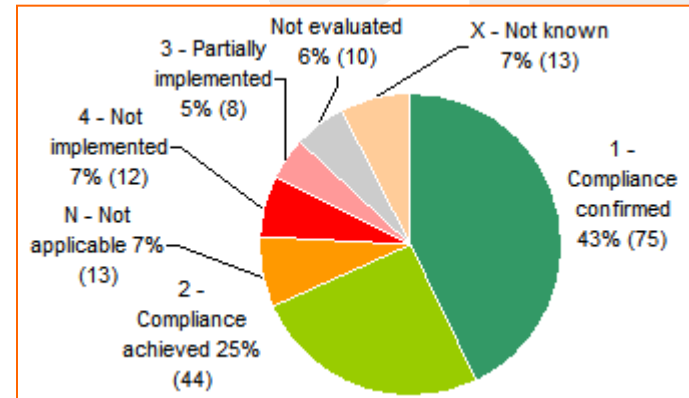


Note: 100% represents the 175 targets of evaluation to which this risk factor applies.

Control status in more detail The table below presents the status of the selected control item in each of the individual targets of evaluation within the scope of the report.

Target of evaluation	Owner	Date last evaluated	Part of enterprise	Status of control item
CDC Global email (RS8)	David Tilbury	10 Jan '08	Shared services	1 - Compliance confirmed
CDC Group accounts consolidated (RS39)	Honor Black	14 Apr '08	Shared services	1 - Compliance confirmed
EMA Dublin call centre (RS34)	Sam Jackson	11 Sep '07	Shared services	1 - Compliance confirmed
EMA E-banking application (RS84)	Richard Cliff	30 Jun '08	Retail banking EMEA	2 - Compliance achieved
CDC Group treasury management (RS77)	Steve Jones	14 Mar '08	Shared services	2 - Compliance achieved
CDC Master contracts register (RS9)	Marianne Johannsen	03 Jan '08	Shared services	3 - Partially implemented
CDC Group payroll (RS66)	Bob Smith	22 Mar '08	Shared services	3 - Partially implemented
EMA COSIMA (RS23)	Daniel van Putten	03 Jan '08	Retail banking EMEA	3 - Partially implemented
NY Customer relationship system (RS44)	Marianne Clifton	03 Jan '08	Shared services	4 - Not implemented
UK data centre (RS17)	Serena McClaren	03 Jan '08	Shared services	N - Not applicable
UK In-store processing (RS13)	Charles Rochelle	03 Jan '08	Shared services	X - Not known
CDC Group-wide WAN (RS4)	Marilyn Roberts	03 Jan '08	Shared services	Not evaluated

The pie chart shows the status of a risk factor across multiple targets and the table shows what is driving each region of the chart



Target of evaluation	'Owner'	Evaluated	Status of control item
CDC Global email (RS8)	David Tilbury	10 Jan '08	1 - Compliance confirmed
CDC Group accounts consolidated (RS39)	Honor Black	14 Apr '08	1 - Compliance confirmed
EMA Dublin call centre (RS34)	Sam Jackson	11 Sep '05	1 - Compliance confirmed
EMA E-banking application (RS84)	Richard Cliff	30 Jun '08	2 - Compliance achieved

Helping all involved manage remediation activity

Results of an evaluation

Citicus ONE

Individual results

CDC Group accounts consolidation (IRS163)#

The individual results for CDC Group accounts consolidation (IRS163)# are presented under the following headings:

	Page
Information risk status report	2
Guidance on driving down risk	5
Actions to drive risk down	8
Information risk scorecard	11
Recorded notes and comments	13

Owner: Emily Green
Scorecard submission date: 27 Feb 2005
Purpose of monitoring: For real

Evaluators have two ways of identifying the remedial actions needed to fix weaknesses identified by evaluations

Route 1

Action plan

Citicus ONE

Action plan

This action plan sets out remedial actions that meet the following criteria, and their current status:

Reference	Applies to	Part of enterprise
CDC Group accounts consolidation (AP)	Information resources	Group Finance

Action item	Remedial action (in concrete actions that will measurably reduce risk)	Projected cost	Projected benefit	Priority	Lead role	Completion dates		Current status
						Target	Actual	
AP 1	Produce 1-help material and topic paper reporting out the roles of a number of financial info in one Top Co.	2 days effort	Foster synergy	High	EA	31 Dec 2002	7 Jun 2003	Completed
AP 2	Email topic paper on roles / responsibilities to contacts in each cop co and ask them to advise if any difficulty in fulfilling role.	5 min work	Help reduce errors	Med	S Richardson	5 Jun 2003	7 Jun 2003	Completed
AP 3	Add Help topic on roles, responsibilities and role available to web based front-end, and enable easy access by a user.	3 days effort	Reduce errors	High	WTI	5 Jun 2003	5 Jun 2003	Completed
AP 4	Package up application and our lead developer to develop clear interfaces and problem handling process, integrated with our maintenance	2 days effort on both sides	Foster resolution of issues	High	Emily Green	1 Dec 2004		In progress
		2 weeks of effort	Remedy key weaknesses	High	WTI	31 Jan 2005		In progress

Route 2

Individual weaknesses can be recorded as issues, each with a unique reference

Citicus ONE

Schedule of issues

This schedule highlights issues requiring remedial action that meet the following criteria, and the status of the associated remedial actions:

Issue reference	Applies to	Part of enterprise	Issued by / period	Additional selection criteria	Date	Prepared by
CDC Group accounts consolidation (SI)	Information resources	Group Finance	Entered to current date	None	8 Oct 2005	Alan Albany

Issue ID	Issue	Priority	Issue status	Remedial action	Projected cost	Projected benefit	Action status	Lead role
SI 2	Special controls (additional protection, eg use of cryptography) cannot be complete in this section.	Low	Open	CDC Group accounts consolidation AP 16 Complete checklist for control areas Special controls and Change Management	2 hours work	Pin down our status	Not yet started	Gwery Cliffe
SI 3	Change management (process description) consistently applied. We should get our technical guys to complete this section.	Med to High	Open	CDC Group accounts consolidation AP 16 Complete checklist for control areas Special controls and Change Management	2 hours work	Pin down our status	Not yet started	Gwery Cliffe
SI 4	Too many people have access through general user IDs / passwords. That is against company policy. It raises the control control access to sensitive financial data properly and users often see more than they should.	Med to High	Open	CDC Group accounts consolidation AP 18 Upgrade access controls to achieve all 8 critical accountability. It requires control cover who can see what and when	1 days effort	Foster synergy, less chance of misuse	Completed	Gwery Cliffe

Issues can be linked to the action item(s) needed to resolve them

Schedule of issues

Linking notes and comments to issues and action items

Recorded comment



*"Back-ups are stored on an open shelf "
(IRS 163.CC.2)*

Issue

Description	SI.1 Back-ups of sensitive data are held insecurely
Priority	Medium
Issue status	Open
Date raised	14th Sep 2010
Origin	IRS 163.CC.2
Related action(s)	AP.1, AP.2

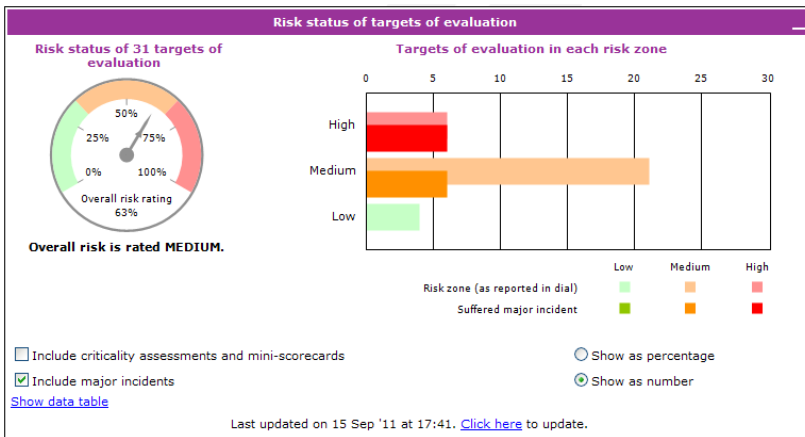
*Recorded notes and comments may be edited to express them as Issues or action items
Issues can be linked to action items and their status updated automatically*

Action items

Description	AP.1 Acquire fire-proof safe for storing back-up media
Cost	\$1000
Benefit	Reduce risk of loss / misuse
Priority	Medium
Lead role	J Smith, IT Procurement
Target completion	Nov 14 th 2010
Actual completion	Oct 8 th 2010
Current status	Completed

Description	AP.2 Transfer back-up media to fire-proof safe
Cost	0.5 man days
Benefit	Reduce risk of loss / misuse
Priority	Medium
Lead role	T Atkins, Ops Supervisor
Target completion	Nov 14 th 2010
Actual completion	
Current status	Not yet started

Consolidated reporting – your personal risk metrics dashboard



Risk management activity

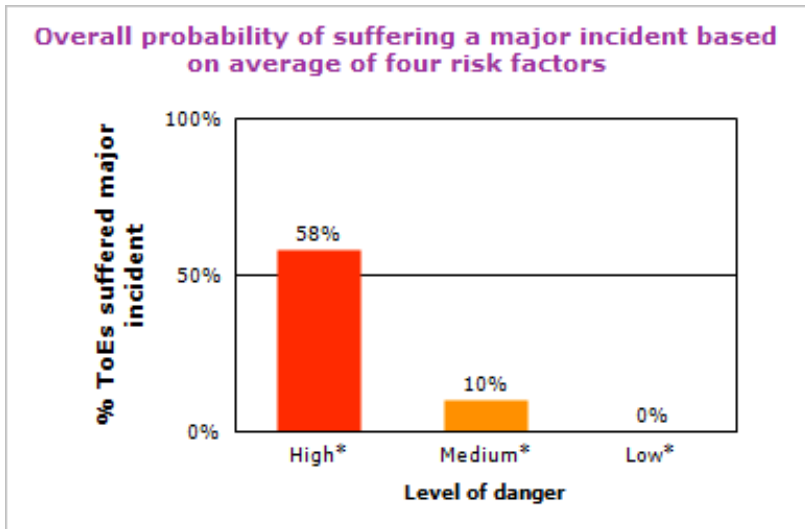
Activity Last month To date

Targets of evaluation defined	3	49
Risk scorecards submitted	8	69
Criticality assessments submitted	2	21
Mini-scorecards submitted	1	1
Evaluations submitted for undefined targets of evaluation	0	1
Evaluations in progress	10	21
Evaluations that are overdue for completion	-	42 (86%)
Incident assessments submitted	1	12
Issues defined	8	44
Issues closed	0	4
Actions defined	7	97
Actions completed	0	23
Actions that are overdue for completion	-	65 (88%)
High-level results defined	1	17
Users defined	2	61
Parts of enterprise defined	0	28

Last updated on 15 Sep '11 at 15:36. [Click here](#) to update.

What is the risk distribution of our assets?

What is the status of my risk management programme?



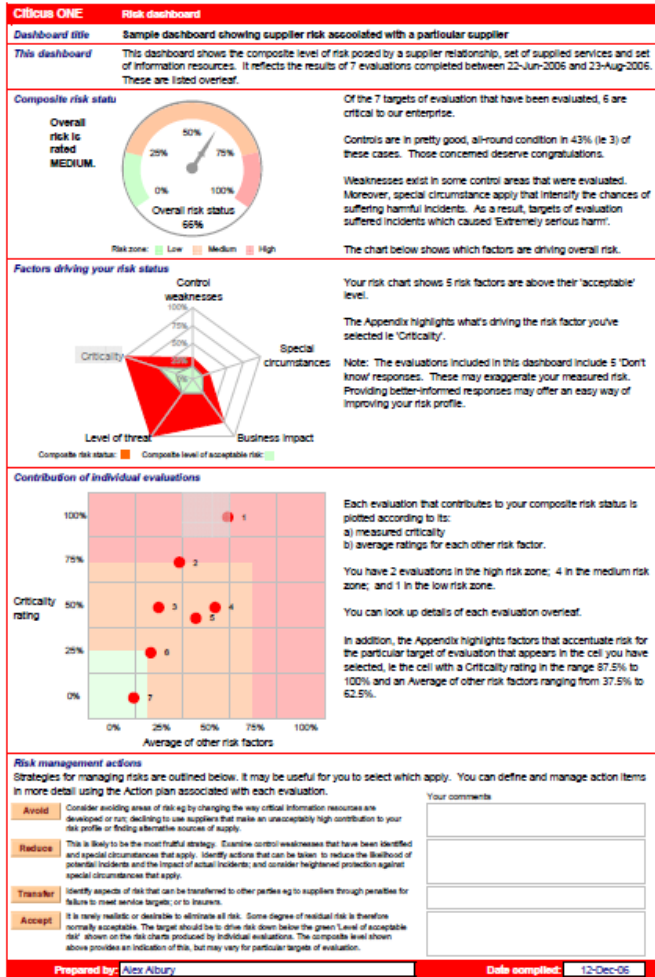
What's the likelihood of these systems suffering major incidents?

System / Assessment	Priority	Compliance	Critical	Overall Condition	Level of Detail	Business Critical
UK Bank system (02101)*	1	100%	100%	97%	100%	97%
ODC Groupwide (02103)*	2	100%	100%	97%	99%	99%
SW Customer data centre (02105)*	2	100%	84%	71%	100%	99%
ODC Security (02107)*	4	100%	72%	100%	99%	99%
ODC Group Treasury management (02102)*	2	100%	71%	42%	99%	99%
UK Boston data centre (02147)*	2	100%	65%	67%	74%	99%
SW Logistics system (02136)*	7	100%	47%	34%	99%	99%
ODC Group asset management (02081)*	2	100%	41%	71%	74%	99%
SW London data centre (02105)*	2	100%	41%	24%	99%	99%
UK Finance processing (02170)*	10	100%	34%	43%	99%	99%
UK Logistics (02175)*	11	100%	34%	34%	99%	99%
ODC Global email (02196)*	12	100%	13%	71%	99%	99%
SW Banking association (02202)*	13	100%	0%	67%	75%	99%
UK Billing system (02200)*	14	75%	71%	67%	75%	99%
Production control system (02171)*	15	75%	45%	67%	99%	99%
ODC Group ES (02148)*	16	75%	34%	34%	99%	99%
ODC Group control (02105)*	17	50%	74%	14%	99%	99%
UK Customer relationship system (02208)*	18	50%	41%	34%	99%	99%
UK Sales information system (02277)*	19	50%	34%	43%	99%	99%
UK Boston Data Order Management (02104)*	20	50%	35%	34%	99%	99%
UK Payroll system (02203)*	21	50%	18%	14%	99%	99%
UK Direct marketing (02242)*	22	50%	24%	43%	99%	99%
ODC Data handling (02204)*	23	50%	17%	6%	99%	99%
UK Fraud recording (02204)*	24	50%	18%	43%	99%	99%
UK Credit scoring (02205)*	25	50%	0%	0%	99%	99%
ODC Member contact register (02201)*	26	50%	0%	14%	31%	99%
Average score		73%	44%	43%	94%	94%
Preparation with 'incidents' for control maintenance						95%
SW Bank UK (02104)*						96%
SW Bank UK (02104)*						96%

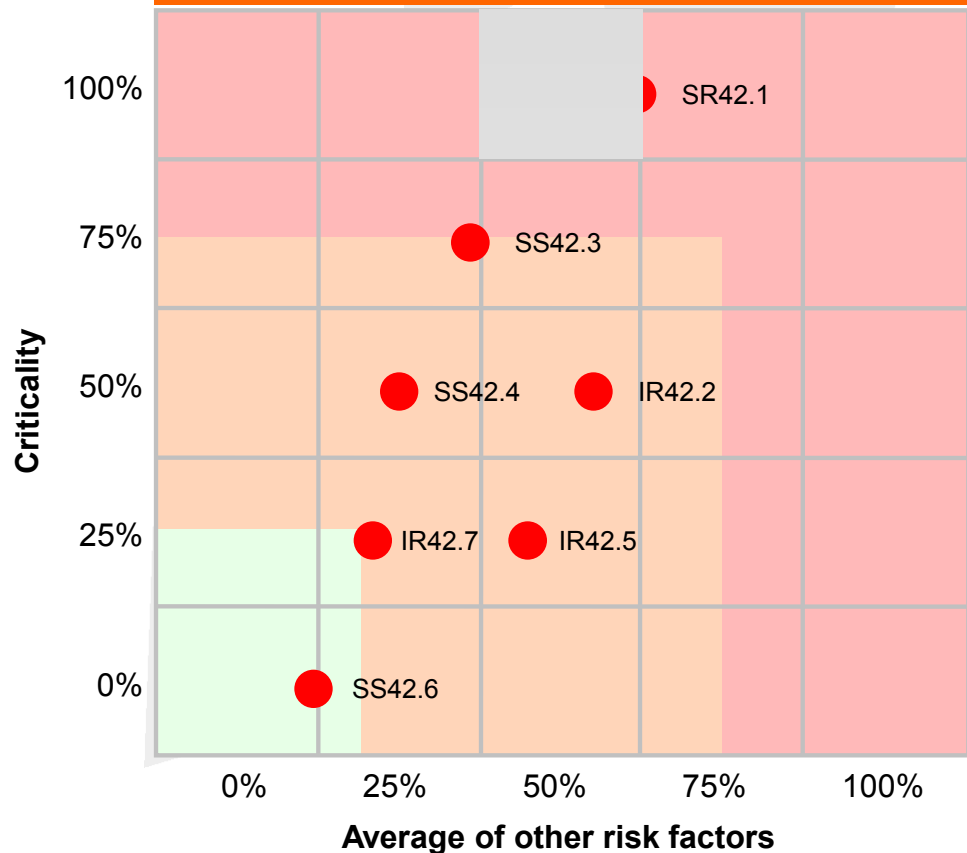
Legend: Low Medium High

Consolidated reporting – key risk drivers

Citicus ONE risk dashboard



The 'clickable' scatter diagram shows the contribution of individual evaluations and enables you to see what's driving risk in particular regions of the chart



Consolidated league tables show where the key risks lie

Citicus ONE ranks targets of evaluation in descending order of risk

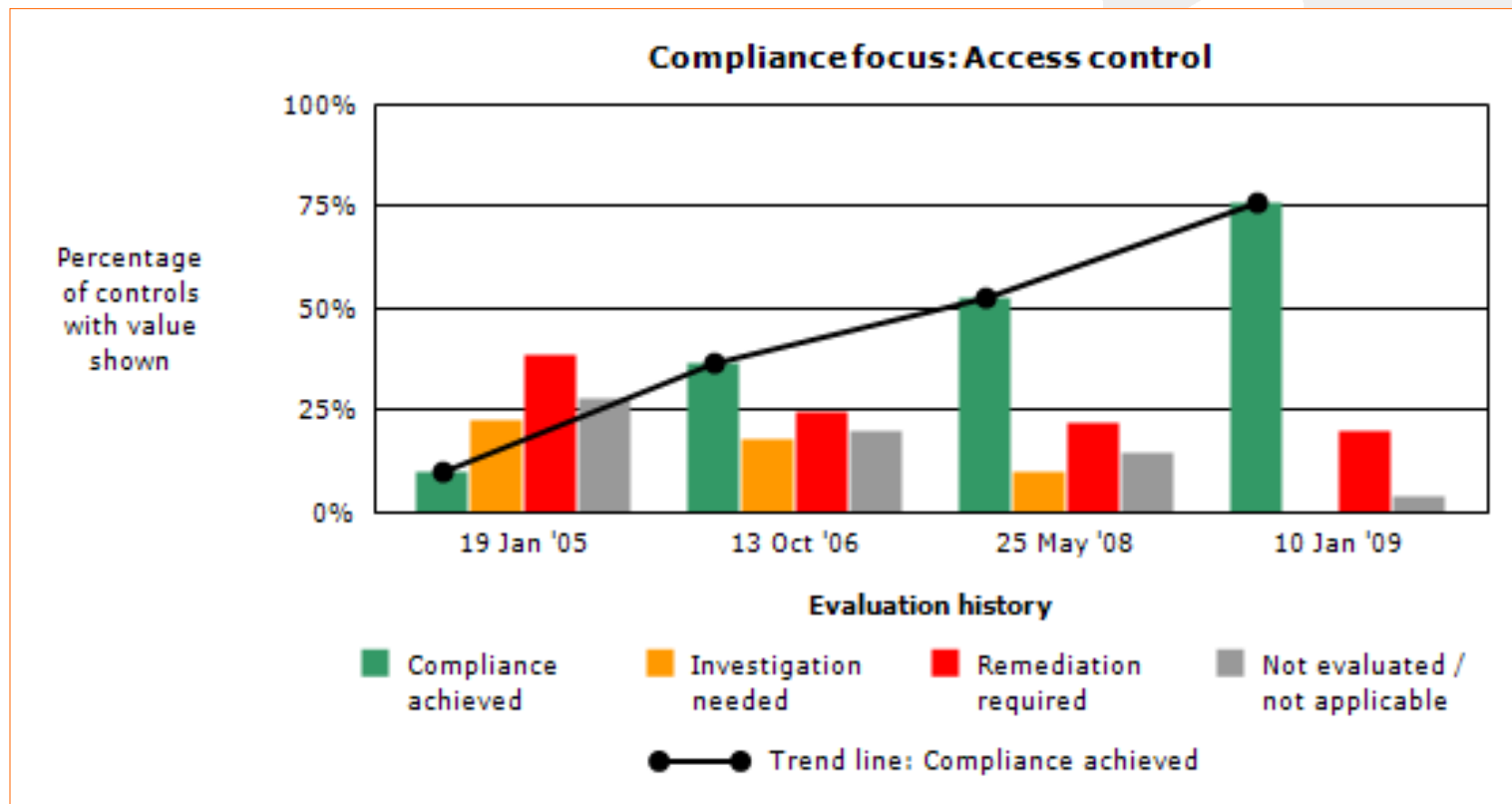
Top 10 entries			Control	Special	Level of	Business	Colour codes indicate the danger posed by each component of risk:
Targets of evaluation	Rank	Criticality	weaknesses	circumstances	threat	impact	
SecurNet (RS151)	1	100%	76%	86%	50%	25%	<div style="border: 1px solid black; background-color: red; color: white; padding: 2px; display: inline-block;">High</div> <div style="border: 1px solid black; background-color: orange; color: black; padding: 2px; display: inline-block;">Med</div> <div style="border: 1px solid black; background-color: green; color: black; padding: 2px; display: inline-block;">Low</div>
Credit card processing (RS156)	2=	75%	100%	57%	100%	50%	
Global email (RS49)	2=	75%	100%	57%	100%	50%	
Boston data center (RS191)	4	75%	100%	29%	100%	75%	
London data centre (RS155)	5	75%	94%	71%	100%	50%	
Global intranet (RS150)	6	75%	94%	86%	75%	50%	
Supplier data (RS124)	7	75%	94%	71%	100%	25%	
HQ LAN (RS67)	8	75%	88%	57%	100%	100%	
Pacific data centre (RS131)	9	75%	88%	71%	75%	25%	
Group EIS (RS148)	10	75%	82%	100%	100%	75%	
Bottom 10 entries							<p><i>You can control colour and sorting</i></p>
Relationship mgt (RS156)	136	25%	6%	43%	50%	25%	
Group payroll (RS167)	137	25%	0%	29%	50%	0%	
ePurchasing site (RS160)	138	25%	0%	0%	50%	25%	
Prices database (RS142)	139	0%	100%	29%	75%	25%	
UK sales information (RS12)	140	0%	82%	43%	100%	25%	
UK standby net (RS136)	141	0%	65%	14%	50%	0%	
Boston Order Proc. (RS190)	142	0%	59%	29%	100%	50%	
European data centre (RS46)	143	0%	47%	57%	50%	0%	
LaForce site LAN (RS101)	144	0%	41%	14%	100%	25%	
Erland site LAN (RS42)	145	0%	24%	14%	100%	25%	

Note: Names have been changed to preserve confidentiality but ratings are genuine

Copyright © Citicus Limited, 2011. All rights reserved.

Compliance trend reports provide a timeline of compliance status

Compliance with a specified standard can be tracked as a trend line. You can plot the overall status of all controls in the employed checklist or focus on an individual control area of interest.



Examples of successful practice

Global branded food manufacturer

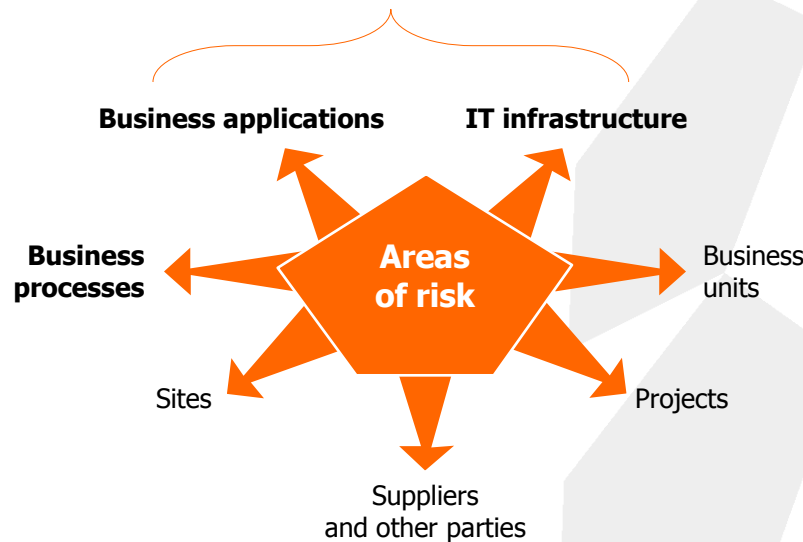
Global program driven by strong, personable programme manager (2 people at centre, 3 in regions) based in Group Compliance & Controls

- ~ 1,200 evaluations since 2005
 - 1,000 criticality assessments
 - 200 'deep dive' risk assessments

IT assessments use **FIRM+ Criticality assessments + Risk scorecards** supported by ISO 27000 **standard of practice**

- 17 control areas
- 150 controls

IT assessments embedded in system development and IT procurement processes



"By implementing a business oriented and systematic risk assessment process, real benefits can be achieved as compliance and security requirements can be quickly satisfied without unnecessary burden, and resources properly allocated throughout the organization"



- Software currently being configured with **checklists** that enable evaluation of:
- Food defence practices
 - Compliance with bribery/child labour laws (for Dow Jones Sustainability index)
 - Suppliers
 - Particular business processes

COLLABORATIVE DEVELOPMENTS

- Supplier risk capability
- Data exchange

Global tobacco company

Global program driven by strong, personable programme manager (2 people at centre) based in IT; 50 trained local co-ordinators)

~ 2,500 evaluations since 2004
Program being extended to cover factory automation

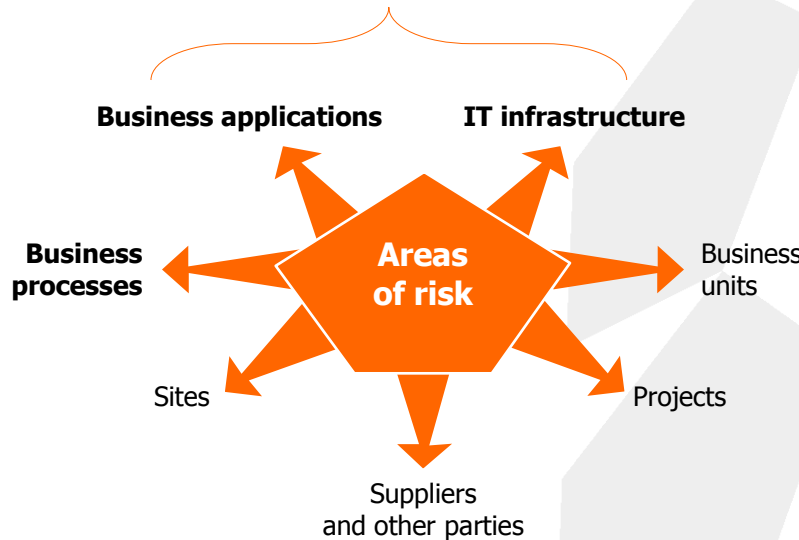
IT assessments initially used **FIRM+ Criticality assessments** + **Scorecards** supported by home-grown **standard of practice**

- 17 control areas
- 100 controls

Standard of practice turned into a '**smart checklist**' in 2009 driven by user-controllable attributes

Citicus ONE employed as 'system of systems'

Characteristics of systems recorded as attributes



"With a portfolio of more than 500 computer systems supporting diverse business functions and application/data owners across the world, ad hoc assessment for policy compliance and IT governance needed to be replaced with systematic and transparent information risk management processes."



COLLABORATIVE DEVELOPMENTS

- Attribute sophistication
- Risk management metrics

Other large-scale **Citicus ONE** implementations

Customer	Completed evaluations	Geographical scope	Bases of evaluation	Program management
Insurance/ financial services	>18,000	70+ countries	Criticality assessments, Scorecards + 2 home-grown checklists (~60 control items)	3 at centre, 1+ local co-ordinator in every business unit
Global brands	2,300	150 countries	Criticality assessments, Scorecard + home-grown 'smart' checklist (~100 control items)	2 at centre, 5 regional co-ordinators, 15-20 local co-ordinators
Insurance/ financial services	1,200	North America	Criticality assessments, Scorecard + ISF SoGP. Harm reference table being used for other areas of risk. Some tweaks needed.	3-4 at centre. No local co-ordinators
Central Government	600	30+ Ministries in major Canadian province	ISF Health check used for Ministry-level evaluations. 'Smart' checklists based on ISF SoGP used for information systems	2-3 at centre, 1-2 local co-ordinators in each Ministry



About Citicus Limited



Who we are

- Citicus Limited was formed in 2000 to provide world-class risk management software products and supporting services
- Wholly-owned by its directors and staff
- Based in UK (London, Cheltenham)
- Exclusive, worldwide right to sell **FIRM** automation – reflecting Citicus directors’:
 - *long-standing involvement with the Information Security Forum (ISF)*
 - *lead role in the development of this groundbreaking risk measurement and management methodology*
- Relations with customers based on a collaborative way of working
- Our relationship with the ISF is continuing (eg access to Survey data, involvement in **FIRM** and IRAM development)

Simon Oxley
Managing director



- Headed information security departments at National Power and Reuters
- Took both companies into ISF and served on ISF Council 1992-94
- Heads Citicus management team and leads our commercial activities
- Oversees our relations with standards-makers (eg ISF, BSI-ISO, ISACA)

Marco Kapp
Director



- Established ISF while a director of C&L's UK consulting practice
- Author of ISF's first standard and numerous reports on risk
- Chief architect of ISF's **FIRM** methodology
- Chief architect of collaborative Supplier Risk Assessment (SRA) project – which culminates on delivery of **Citicus ONE** Release 3

Sian Alcock
Director



- Extensive experience in analysing ISF survey results
- Developed new, quantitative insights into what drives risk up / down
- Lead author of ISF report on The impact of security management
- Oversees design, development and delivery of **Citicus ONE**

Our customers and geographic focus

Citicus ONE is currently helping customers to measure and manage the risk posed by many thousands of systems in over 150 countries

Representative customers

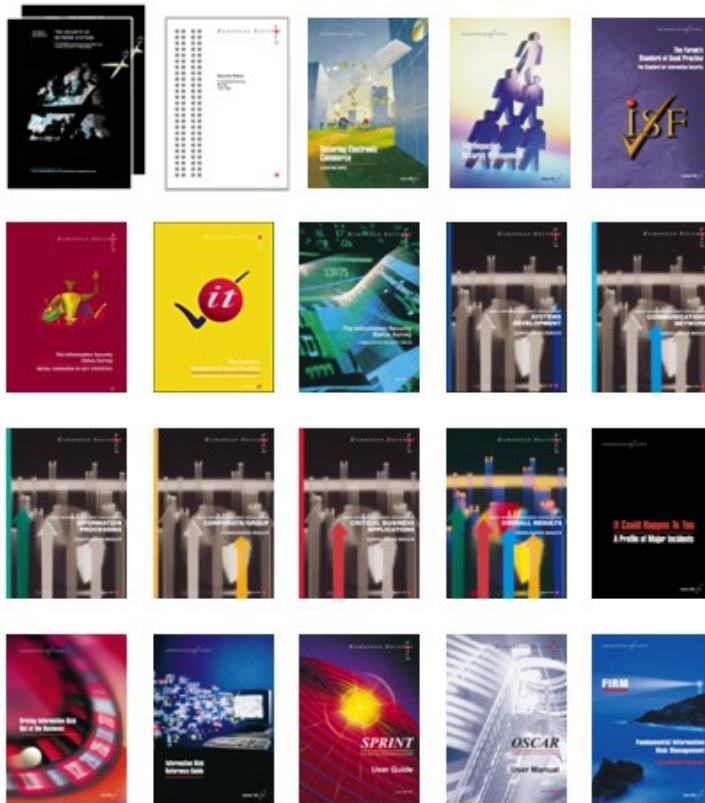


We support deployments all over the world via training and services delivered from the UK. We can orchestrate global support if needed.

Main activity	Where based
Banking	US, Saudi Arabia, UAE
Consumer products	Netherlands, Switzerland, UK, USA
Energy	UK, Germany
Government	Canada, Ireland, UK, Netherlands
Insurance	France, USA
IT and professional services	Germany, Scandinavia, Switzerland, UK, USA
Manufacturing	France, Netherlands, Scandinavia
Telecommunications	Kenya

Citicus ONE is based on solid, *factual* evidence

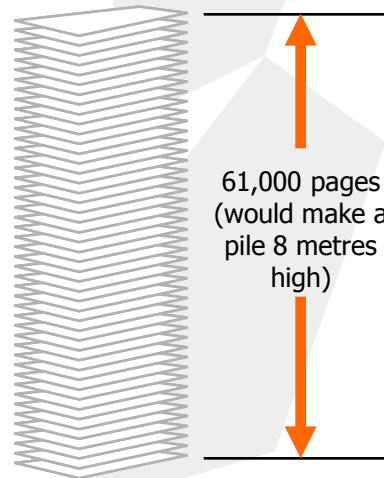
Citicus ONE Release 3 is the end-product of an unrivalled volume of research - conducted by the founders of Citicus Limited for and / or in conjunction with leading organizations around the world. Results of this research over the last 20 years are illustrated below.



Example: The ISF 1998 survey involved over 1,000 people:

- in-depth analysis of 800,000 facts about by 969 surveyed systems, including the controls applied to them, incidents they suffered and other key characteristics
- intensive review by practitioners
- provided major insights into what drives information risk

969 survey questionnaires:



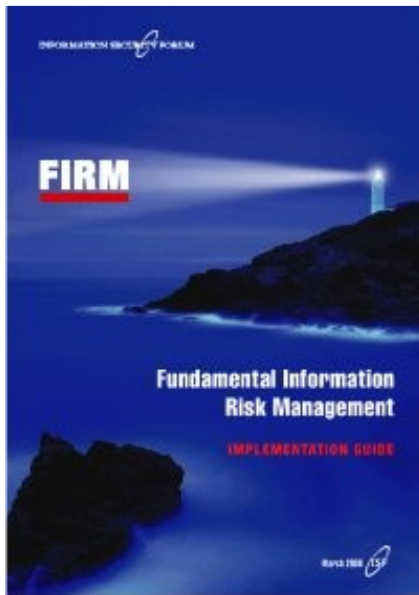
ISF: Information security Forum

*We developed the FIRM risk management methodology for and in conjunction with the Information Security Form (ISF). It reflects all the above research and is automated by our **Citicus ONE** software. Release 3 extends FIRM to cover all areas of operational risk.*

FIRM risk management methodology

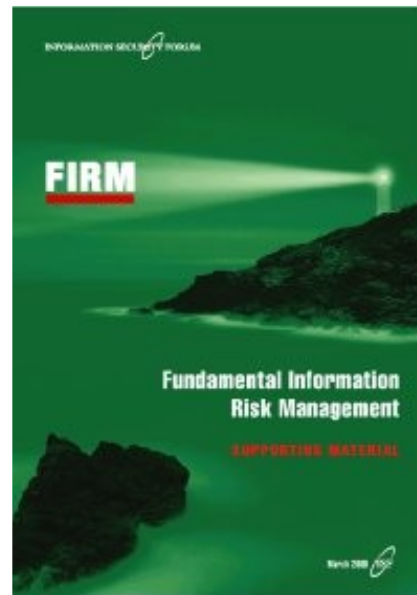
Developed by founders of Citiculus Limited for and in conjunction with the Information Security Forum (ISF) in 2000

FIRM Implementation Guide (2000)



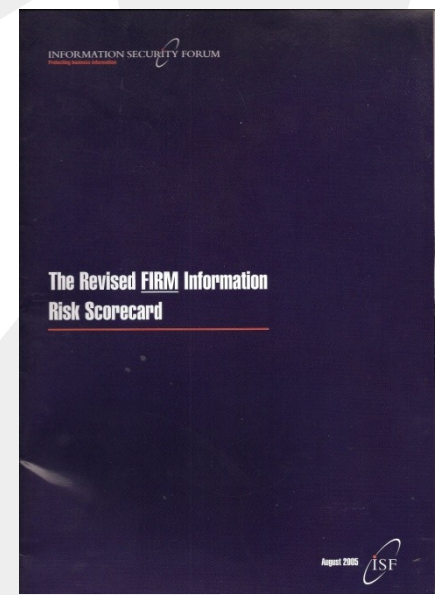
- The problem
- Key challenges
- The methodology
- 6-step implementation process

FIRM Supporting material (2000)



- Terminology, concepts and role definitions
- Operational tools
- Examples of successful practice
- Advice on making selective improvements

Revised FIRM Scorecard (2005)



- Rearranged presentation
- Updated content to align with other ISF tools (eg SoGP, Healthcheck, IRAM)