Sarbanes-Oxley compliance: evaluating application and IT infrastructure controls realistically and efficiently

About this white paper

The U.S. Sarbanes-Oxley Act of 2002 is bringing about far-reaching reform of business practices, and sets challenging new standards for the accuracy, completeness and timeliness of financial reporting.

Business, IT, or security staff concerned about the controls applied to IT-based information systems need to understand what the Act calls for. Conversely, teams engaged in achieving compliance with the Act need to understand the latest research about the controls applied to IT-based financial systems.

This paper is aimed at both groups. It explains the Act in broad terms, highlights the danger of unrealistic evaluations, and shows how the measurement and management processes built into **Citicus ONE** can be used to evaluate the completeness and effectiveness of controls applied to financial systems realistically and efficiently, so as to provide real business benefits.

Benefits of Sarbanes-Oxley compliance

The purpose of the Act is to protect the interests of investors and to serve the wider public interest, by:

- outlawing practices that have proven damaging (eg over-close relationships between auditors and management)
- requiring companies to comply with onerous new standards of practice for financial reporting
- intensifying penalties for misleading investors (eg fines of up to $5 million or 20 years in jail for issuing financial reports that do not meet Sarbanes-Oxley requirements).

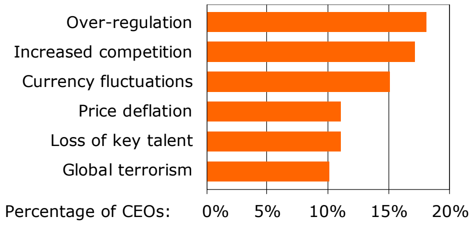
For senior executives, therefore, the benefits of compliance are personal and very direct.

Costs of Sarbanes-Oxley compliance

Analysts have estimated the 2004 cost of compliance as $3-8 million for a Fortune 500 company; $5.5 billion for U.S. listed companies in total. Most of this will come off companies' bottom lines.

Thus, it is not without cause that CEOs around the world now see 'over-regulation' as a major threat to their businesses, as shown below.

What CEOs currently see as the biggest threats to their businesses



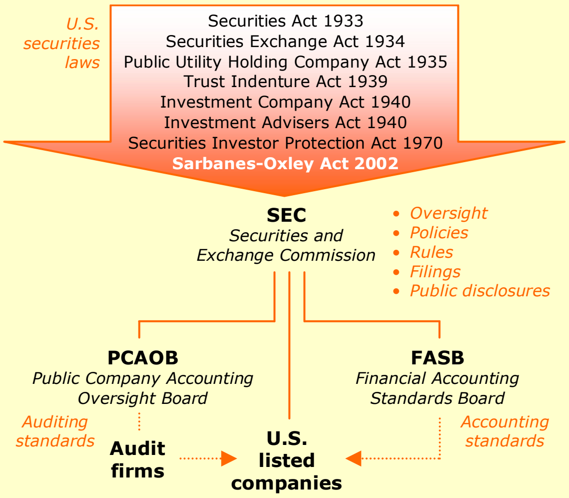
Source: PriceWaterhouseCoopers survey of 1,394 CEOs (Q4-2003).

Broad thrust of the Sarbanes-Oxley Act

The Act that U.S. Senator Paul Sarbanes and Congressman Michael Oxley co-sponsored became law in 2002, following the Enron disaster. Its aims were to restore confidence in 'corporate America' and to protect investors by changing the way business is run and how results are reported by companies listed on the major U.S. stock exchanges. To these ends, it:

- established a new body to oversee audit firms (PCAOB)
- strictly limits what accounting firms can do for their audit clients
- empowered the SEC to oversee the accounting standards-setting process via the FASB
- requires U.S. listed companies to establish powerful, independent audit committees
- requires CEOs and CFOs personally to certify their financial reports and the effectiveness of internal controls over financial reporting
- requires strict segregation of securities analysts from investment banking activity
- raised penalties for violations of securities laws and SEC rules, and introduced new ones
- initiated studies heralding further changes in future (eg shape of the accounting industry).

The new landscape for corporate governance in America created by Sarbanes-Oxley is shown below.


U.S. securities laws
Securities Act 1933
Securities Exchange Act 1934
Public Utility Holding Company Act 1935
Trust Indenture Act 1939
Investment Company Act 1940
Investment Advisers Act 1940
Securities Investor Protection Act 1970
Sarbanes-Oxley Act 2002
SEC
Securities and Exchange Commission
• Oversight
• Policies
• Rules
• Filings
• Public disclosures
PCAOB
Public Company Accounting Oversight Board
FASB
Financial Accounting Standards Board
Auditing standards
Accounting standards
Audit firms
U.S. listed companies

The Act applies to subsidiaries of U.S. corporations based all over the world; and to non-U.S. companies that are listed on major U.S. stock exchanges. It is also influencing developments in other jurisdictions.

Thus, directly or indirectly, Sarbanes-Oxley affects or will affect corporate governance practices worldwide.

Financial reporting requirements

Sarbanes-Oxley requires CEOs and CFOs[1] to certify the accuracy and completeness of the information they publicly disclose via the U.S. Securities and Exchange Commission (SEC). This includes quarterly, half-yearly and annual reports on their enterprise's financial condition, cash flows and activities.

Its aim is to make top executives personally responsible for the information they provide to actual and potential investors, banks, customers, suppliers and other interested parties. Certification requirements are onerous, as can be seen from the outline below.

What CEOs / CFO's must do

1. Review the information provided in each filed report.
2. Confirm that the information in the report:
   a) is accurate and complete (ie it contains no material untruths or omissions)
   b) fairly represents the enterprise's financial condition, cash flows and activities.
3. Confirm that they are personally responsible for establishing and maintaining adequate controls over financial reporting and that they have ensured that:
   a) controls are designed to provide reasonable assurance about the accuracy and completeness of the information provided, and its compliance with generally-accepted accounting principles
   b) the effectiveness of disclosure controls in force at the end of the reporting period is evaluated, based on a recognized control framework[2]
   c) any material changes to internal controls over financial reporting that occurred in the last quarter are disclosed in the report
   d) their audit committee and auditors are advised of:
      i) significant or material control weaknesses likely to affect the recording, processing, summarizing or reporting of financial information
      ii) cases of fraud involving employees concerned with controls applied to financial reporting.

[1] *Certification is required by 'principal executive officers' and 'principal financial officers' of listed companies. Some companies have slightly different requirements.*

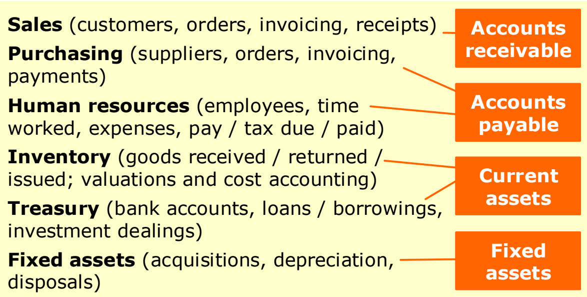
[2] *The Committee of Sponsoring Organizations (COSO) of the Treadway Commission's Internal Control -- Integrated Framework, 1992, or equivalent.*

For major U.S. companies, these requirements apply in full to annual reports due from mid-June 2004 onwards and to other filings thereafter.

Is a clean bill of health realistic?

Certifying the adequacy of controls over filings requires detailed evaluation of the controls applied to business processes that support financial reporting, such as those below.

Business processes that support financial reports



Sales (customers, orders, invoicing, receipts)

Purchasing (suppliers, orders, invoicing, payments)

Human resources (employees, time worked, expenses, pay / tax due / paid)

Inventory (goods received / returned / issued; valuations and cost accounting)

Treasury (bank accounts, loans / borrowings, investment dealings)

Fixed assets (acquisitions, depreciation, disposals)

Such processes are generally carried out using IT-based **business application systems,** supported by **IT infrastructure** such as data centres and networks at corporate, regional, national or local level.

A solid, up-to-date understanding of what makes the controls applied to both **application systems** and **IT infrastructure** effective is therefore essential.

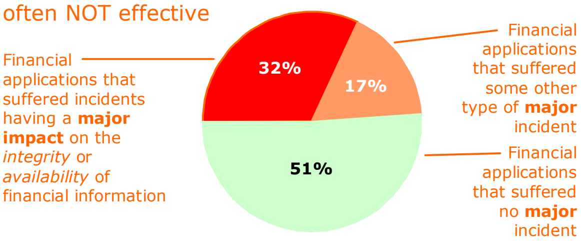
Put bluntly, without such an understanding, any evaluation of the adequacy of the controls applied to financial reporting is likely to be incomplete and may well be grossly misleading.

This is because recent, independent research[3] shows that even in leading companies:

- when it comes to business-critical applications and IT infrastructure, **control deficiencies are the norm not the exception** (on average, the controls applied to business-critical financial systems are only fractionally better than those applied to other applications)
- as a result, on average there is a **49% chance in any one year of a financial application suffering a major information incident** ie one that compromises the integrity, availability or confidentiality of the information that it handles.

In fact it is the **integrity** and **availability** of information that such incidents typically compromise, as can be seen in the chart below.

Controls applied to financial application systems are often NOT effective



Source: Citicus analysis of data about major incidents affecting 179 critical business applications that support financial reporting, over the course of a year. [3]Base data is from the Information Security Forum's 2000-02 information security status survey.

These findings stem from the world's most advanced survey of the controls applied to business-critical systems. Few control evaluators have an in-depth understanding of these statistics or their implications.

Without this know-how, there is a real danger of their under-estimating or exaggerating the significance of control weaknesses and of issuing evaluation reports that are superficial and not in tune with reality. This may lead to CEOs and CFOs issuing misleading Sarbanes-Oxley certifications – with all that implies.

Evaluating IT-related controls realistically

Citicus ONE is an award-winning evaluation tool that encapsulates years of research into what makes IT-related controls effective. Evaluators can use it to evaluate the controls applied to IT-based application systems and infrastructure **reliably** and **efficiently**.

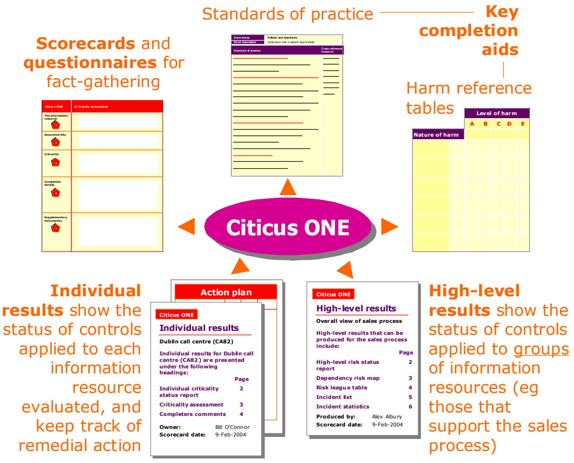
Its capabilities are summarized on the following pages, along with an explanation of how it supports compliance activity.

What is Citicus ONE?

Citicus ONE is a proven, web-based system for managing 'information risk' across an enterprise (ie the chance or probability of the enterprise suffering harm as a result of a loss of the integrity, availability or confidentiality of information). It is designed to:

- equip evaluators to measure reliably the completeness and effectiveness of the controls applied to IT applications and infrastructure, and the level of risk these pose to the business
- encourage and assist system 'owners' to drive risk down to an acceptable level.

As illustrated below, it does so by presenting polished scorecards, questionnaires, and completion aids; and producing succinct, business-oriented results that can be readily understood by those involved in bringing controls up to the required standard.


Standards of practice
Key completion aids
Scorecards and questionnaires for fact-gathering
Harm reference tables
Level of harm
A B C D E
Nature of harm
Citicus ONE
Individual results show the status of controls applied to each information resource evaluated, and keep track of remedial action
Action plan
Citicus ONE
Individual results
Dublin call centre (CA82)
Individual results for Dublin call centre (CA82) are presented under the following headings:
Page
Individual criticality status report 2
Criticality assessment 3
Completers comments 4
Owner: Bill O'Connor
Scorecard date: 9-Feb-2004
Citicus ONE
High-level results
Overall view of sales process
High-level results that can be produced for the sales process include:
Page
High-level risk status report 2
Dependency risk map 3
Risk league table 4
Incident list 5
Incident statistics 6
Produced by: Alex Albury
Scorecard date: 9-Feb-2004
High-level results show the status of controls applied to groups of information resources (eg those that support the sales process)

Citicus ONE's scorecards, questionnaires, and completion aids enable evaluations to be carried out efficiently and to collect information reliably. Their form and content reflect:

- solid statistical insights into what makes the *controls* applied to critical systems effective
- detailed study of what makes *risk assessment and management processes* effective.

Its unique research base shows up in the graphical risk charts, risk maps, league tables and risk management reports produced by **Citicus ONE**. These provide evaluators, owners and other decision-makers with clear, concise facts about:

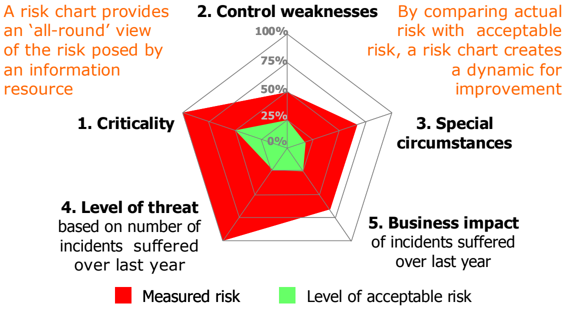
- the extent of control weaknesses and their significance (ie how much harm *could be* caused as a result of the weaknesses found)
- the likelihood of incidents occurring that compromise the integrity, availability or confidentiality of business-critical information
- progress with remedying control weaknesses.

To aid evaluators, **Citicus ONE** records key points that emerge from discussion or testing; gives practical advice on how to reduce risk; and keeps track of action items. It is this combination of features that makes **Citicus ONE** the world's best, fully-fledged information risk management system.

Samples of individual results

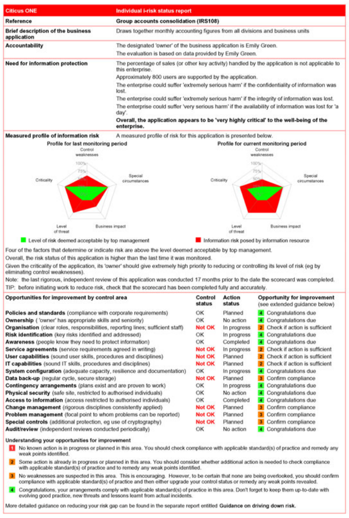
Citicus™ ONE evaluates risk by measuring the five factors that together determine or indicate the chance of the enterprise suffering harm due to a loss of the integrity, availability or confidentiality of information.

It presents the status of these five factors in the form of an easily-understood risk chart (as shown below).



Risk charts are combined with other details to provide each owner with an individualized management report that highlights the status of controls (current versus previous period) and of improvement activity.

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



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.

Profile for last monitoring period
Profile for current monitoring period
Control weaknesses
Special circumstances
Business impact
Level of threat
Criticality
100%
75%
50%
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.

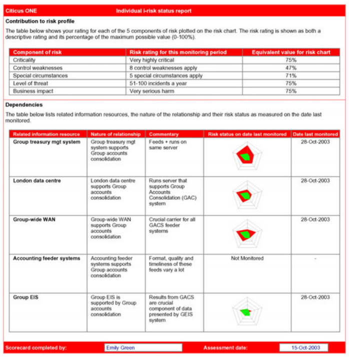
4 Congratulations, your arrangements comply with applicable standard(s) of practice in this area. Don't forget to keep them up-to-date with evolving good practice, new threats and lessons learnt from actual incidents.

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

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

Recognizing that systems rarely stand alone, the status of controls applied to supporting and supported systems is also reported to each owner, thereby helping them understand their 'dependency risk'.

Explains the numeric ratings that drive the red area of the current risk chart, in plain language.



Citicus ONE — Individual i-risk status report

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 monitoring period	Equivalent value for risk chart
Criticality	Very highly critical	75%
Control weaknesses	8 control weaknesses apply	47%
Special circumstances	5 special circumstances apply	71%
Level of threat	51-100 incidents a year	75%
Business impact	Very serious harm	75%

Dependencies

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 on date last monitored	Date last monitored
Group treasury mgt system	Group treasury mgt system supports Group accounts consolidation	Feeds + runs on same server		28-Oct-2003
London data centre	London data centre supports Group accounts consolidation	Runs server that supports Group Accounts Consolidation (GAC) system		28-Oct-2003
Group-wide WAN	Group-wide WAN supports Group accounts consolidation	Crucial carrier for all GACS feeder systems		28-Oct-2003
Accounting feeder systems	Accounting feeder systems supports Group accounts consolidation	Format, quality and timeliness of these feeds vary a lot	Not Monitored	-
Group EIS	Group EIS is supported by Group accounts consolidation	Results from GACS are crucial component of data presented by GEIS system		28-Oct-2003

Scorecard completed by: Emily Green — Assessment date: 15-Oct-2003

Shows the risk status of any systems that support or are supported by this one.

Together, these individual reports encourage owners to take a personal interest in driving risk down, keep track of their progress in doing so, and press for improvement up and down the line. This helps maintain the dynamic for improvement.

Sample high-level results

Citicus ONE enables evaluators to produce insightful high-level results by aggregating data from individual results, eg all corporate systems or all systems that support the sales process. Two types of high-level result are illustrated below.

Information risk league tables can be used to identify which business applications or components of your IT infrastructure have the most control weaknesses or pose the greatest risk to an enterprise.

Top 10 information resources in information risk league table

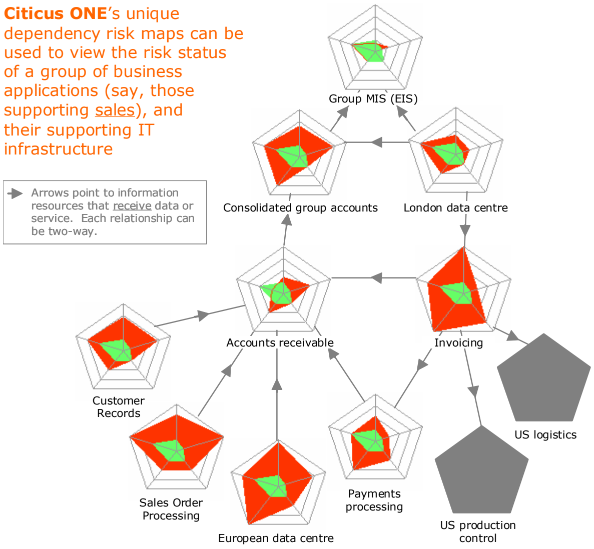
Information resource	Risk ranking	Criticality	Control weaknesses	Special circumstances	Level of threat	Business impact
SecurNet (IRS10)	1	100%	82%	86%	100%	100%
New York data centre (IRS89)	2	100%	76%	100%	50%	25%
European data centre (IRS100)	3	75%	100%	57%	100%	50%
Group treasury mgt (IRS102)	4	75%	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%

Comparisons with other companies can be made by including benchmark data provided by Citicus Limited.

Dependency risk maps™ look at risk in a different way. They show the relationships between groups of related applications (eg all those supporting the sales process), and the IT infrastructure that supports them, and highlight their risk status.



Citicus ONE's unique dependency risk maps can be used to view the risk status of a group of business applications (say, those supporting sales), and their supporting IT infrastructure

Arrows point to information resources that receive data or service. Each relationship can be two-way.

Evaluators can use such risk maps to set priorities for further evaluations and improvement, and to identify risk 'pinch points'.

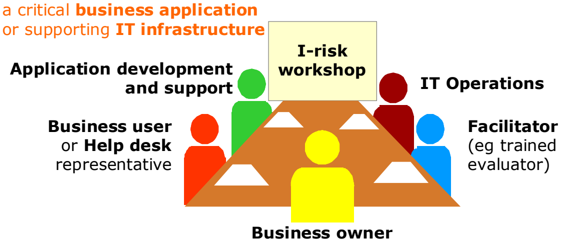
Along with the other high-level results produced by **Citicus ONE** (high-level risk status reports, criticality league tables, incident lists and statistics), these graphical outputs can be used to communicate the risk status of your organisation's financial reporting systems to internal decision-makers, Audit Committees and auditors, as required by Sarbanes-Oxley regulations.

Two-phase evaluation cycle

Unrealistic or inefficient evaluation processes quickly fall into disrepute. What's needed is a way of evaluating controls that treads lightly on an organization, produces reliable information and confers real business benefits.

The evaluation process supported by **Citicus ONE** is designed to achieve these objectives. It combines self-assessments with facilitated evaluations led by trained staff.

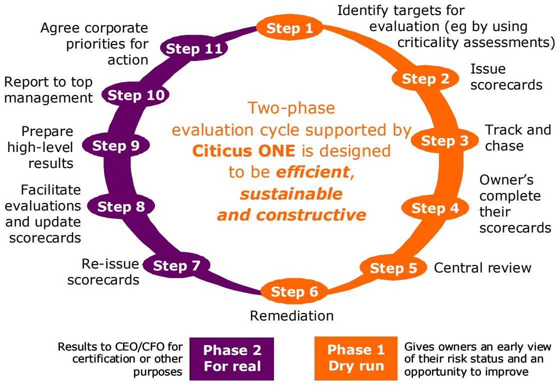
A facilitated evaluation brings business and IT people together to assess the completeness and effectiveness of controls applied to a critical **business application** or supporting **IT infrastructure**



I-risk workshop
Application development and support
IT Operations
Business user or Help desk representative
Facilitator (eg trained evaluator)
Business owner

Both types of evaluation are orchestrated in a two-phase cycle that is designed to encourage and assist owners of individual business applications or supporting IT infrastructure to:

- reduce the number of information incidents they have to contend with (by identifying and remedying their root causes)
- bring controls up to scratch.



Step 1
Identify targets for evaluation (eg by using criticality assessments)
Step 2
Issue scorecards
Step 3
Track and chase
Step 4
Owner's complete their scorecards
Step 5
Central review
Step 6
Remediation
Step 7
Re-issue scorecards
Step 8
Facilitate evaluations and update scorecards
Step 9
Prepare high-level results
Step 10
Report to top management
Step 11
Agree corporate priorities for action
Two-phase evaluation cycle supported by Citicus ONE is designed to be efficient, sustainable and constructive
Results to CEO/CFO for certification or other purposes
Phase 2 For real
Phase 1 Dry run
Gives owners an early view of their risk status and an opportunity to improve

Involving business and IT people in the process encourages people 'on the ground' to focus on what matters and to get things done.

The two-phase approach - combining self-assessment with facilitated evaluations - also enables evaluators to deploy their efforts efficiently, as illustrated by the sample evaluation plan below.

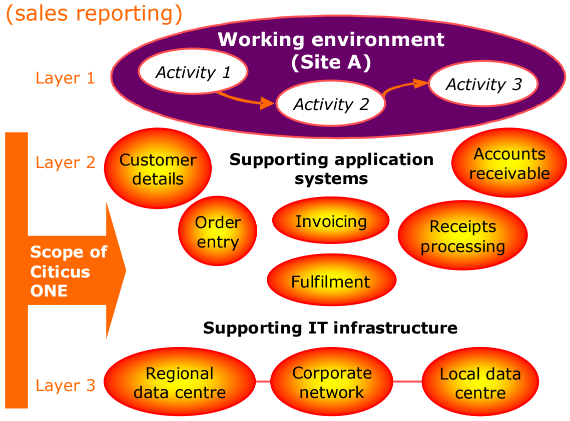
Evaluation plan for:	**Year 1**				**Year 2**			
Sales process	**Q1**	**Q2**	**Q3**	**Q4**	**Q1**	**Q2**	**Q3**	**Q4**
Accounts receivable	🟧	🟪	🟧	🟧	🟪	🟧	🟧	🟪
Payments processing	🟧	🟧	🟪	🟧	🟧	🟪	🟧	🟧
Sales order processing		🟧	🟧	🟪	🟧	🟧	🟧	🟪
Invoicing		🟪	🟧	🟪	🟧	🟪	🟧	🟪
Customer records			🟪	🟧	🟧	🟧	🟪	🟧
US logistics		🟧	🟧	🟧	🟧	🟧	🟪	🟧
US production control				🟧	🟧	🟧	🟧	🟪
European data centre	🟧		🟧		🟪		🟧	
London data centre		🟧		🟧		🟪		🟧

🟧 Self-assessment 🟪 Facilitated evaluation + testing

Citicus ONE's fit with compliance activity

Sarbanes-Oxley requires evaluation of all the controls applied to financial reporting processes. The make-up of a typical process is shown below. It is the bottom two layers of the process that are best evaluated using **Citicus ONE**, as the tool is optimised for this purpose.

Make-up of a typical financial reporting process (sales reporting)



Within each layer, **Citicus ONE** can cover two types of control, ie:

- **generally-applicable controls** ie that apply to all business-critical information systems
- **additional, process-specific controls** that cover threats to particular classes of system (eg those supporting the sales process).

Examples of each type of control are shown below.

Breakdown of controls applied to a typical financial reporting process (sales reporting)

	Control environment	
Nature of controls	**Working environment (sites and activities)**	**Supporting applications and IT infrastructure**
Generally-applicable controls	Accounting policies Personnel policies Problem / incident management procedures Workplace security measures	Controls as set out in your corporate standard of practice for IT or some other recognised standard of practice (eg the ISF Standard, ISO 17799, COBIT)
Additional, process-specific controls	Control objectives for this process Arrangements made for handling: • orders obtained via fax / mail. • payments made by cash, cheques etc Supervision of discounts, refunds, adjustments and other special procedures Staff training Cover for key positions	Functionality to ensure eg: • orders are within credit limits • special terms are properly approved • credit notes correspond to invoice • invoices are recorded in their proper period • cash receipts are accurately recorded • customer details are accurately recorded • Notification of shipments / fulfilments

Citicus ONE can be used to evaluate the two classes of control in this column

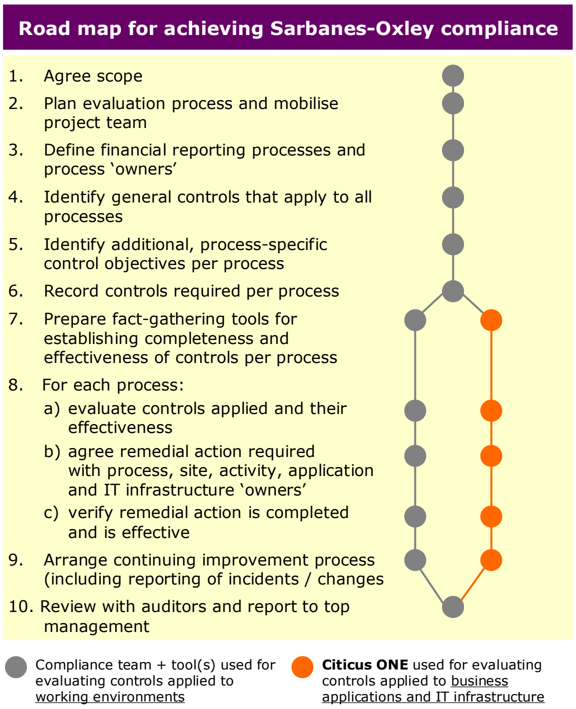
To save work, **Citicus ONE** comes pre-loaded with a number of widely-recognised standards of practice.

These can be easily customised to suit your organisation's particular needs and variants can be prepared incorporating the additional, process-specific controls, in line with your control objectives.

Achieving integration

Individual companies have different views of how to achieve compliance with Sarbanes-Oxley. However, the following generic road map helps show, in broad terms, where **Citicus ONE** fits into the picture.

Road map for achieving Sarbanes-Oxley compliance



1. Agree scope
2. Plan evaluation process and mobilise project team
3. Define financial reporting processes and process 'owners'
4. Identify general controls that apply to all processes
5. Identify additional, process-specific control objectives per process
6. Record controls required per process
7. Prepare fact-gathering tools for establishing completeness and effectiveness of controls per process
8. For each process:
   a) evaluate controls applied and their effectiveness
   b) agree remedial action required with process, site, activity, application and IT infrastructure 'owners'
   c) verify remedial action is completed and is effective
9. Arrange continuing improvement process (including reporting of incidents / changes
10. Review with auditors and report to top management

● Compliance team + tool(s) used for evaluating controls applied to working environments

● **Citicus ONE** used for evaluating controls applied to business applications and IT infrastructure

The road map assumes that a multi-disciplinary compliance team is set up to drive compliance activity.

The team identifies key financial reporting processes and control objectives / requirements. Those applying to working environments are separated from those that apply to business applications and IT infrastructure and each class of control is then set up in the appropriate evaluation tool.

The two types of evaluation then proceed in parallel and the results are brought together in Step 10.

Such a harmonised approach can:

- improve the **efficiency** and **value** of the evaluation process
- improve the **accuracy** and **realism** of evaluations
- cut the **cost of compliance**.

Further information

Expert advice on evaluating controls and training in the use of **Citicus ONE** is available from Citicus Limited.

For further information on how we can help you obtain a clean bill of health for your financial reporting systems, contact:

Citicus Limited	Tel:	+44 (0)20 7203 8405
Holborn Gate	Fax:	+44 (0)20 7203 8409
330 High Holborn	E-mail:	info@citicus.com
London WC1V 7QT	Web:	www.citicus.com
England		