Citicus ONE
Help material

Glossary of risk terms

About this material

This glossary explains terms employed on the browser pages or **Help** system presented by **Citicus ONE** Release 4.1 that have a special meaning in relation to risk. Explanations are included for a few other terms that you may come across in the risk arena.

The main purpose of the glossary is definitional. However, in a few cases entries provide guidance which relates to use of **Citicus ONE**.

Some explanations refer to subsidiary terms which are underlined. Clicking one will take you to its definition.

If using **Citicus ONE**, after viewing it you can use your browser's **Back** button to return to the term you were originally viewing or simply click **Close Help window** in the glossary's navigation bar.

Citicus Limited

May 2014
www.citicus.com

Contents

Acceptable risk

Back to index

The level of risk that is acceptable to the top management of the enterprise or part of the enterprise, expressed in the form of a determination of acceptable risk.

Top management should determine what level is acceptable since they are ultimately responsible for managing risk. The level may vary in different situations (eg the level may be lower for safety-critical or financial systems than for other systems). Thus, multiple determinations may be required.

Responsibility for agreeing determinations of acceptable risk lies with custodians of the system at enterprise level, and local co-ordinators within individual parts of the enterprise. and. Once agreed they can be incorporated in a basis of evaluation (custodians and local co-ordinators can see custodian **Help** topic C**ustomising the system** | **Bases of Evaluation** and **Customising the system** | **Components** | **Component 9 Determinations of acceptable risk** for further details).

Note: **Citicus ONE** uses the same terms for expressing acceptable risk and actual risk. This enables the risk posed by a target of evaluation to be compared with the acceptable level. It also enables decision-makers to focus attention on targets of evaluation that exceed that level ie those posing an unacceptable risk to the enterprise.

Acceptable value

Back to index

An expression in plain language (eg 'Highly critical') that is used in:

- identifying the level of risk that is acceptable to top management, and
- communicating this to those involved in managing risk, in the form of a determination of acceptable risk.

An acceptable value can be selected for each component of risk. A set of such values constitutes a determination of acceptable risk. Once created by a custodian or local co-ordinators a determination can be applied to particular targets of evaluation.

The determination that applies to your target of evaluation controls the green area of the risk chart(s) shown on your Individual risk status report. The full determination can be found at the end of your Guidance on driving down risk.

Action item

Back to index

A description of a particular task or activity recorded in an action plan maintained by **Citicus ONE**, that needs to be - or has already been - completed to fix a problem or concern highlighted by an evaluation (eg a control weakness or other vulnerability), along with its:

- action ID (eg AI.2)
- applies to ie the part of enterprise or target of evaluation, it applies to or the identity of who recorded it in the system eg ‘Entered by Alex Albury (alburya)’
- date raised (eg 12 Mar 2012)
- priority (ie the relative importance of this task / activity)
- lead role ie who is responsible for carrying out the task
- current status (ie ‘Not yet started’, ‘In progress’, ‘Completed’ or ‘Abandoned’)
- completion dates (target and actual)
- cost (eg ‘No expenditure needed’)

- linked control improvements - ie links to related controls -these can be established for information only or set so that the system updates the status of each related control (either entirely automatically or subject to a user's review and approval) when linked issues / actions are closed or completed
- Other benefit (eg ‘Improved service, fewer support calls’)
- assignable attributes - values of any that have been set up in the system to characterize action items or provide additional information about them. Attributes employed for this purpose need to be defined and published for use with actions, by a custodian or local co-ordinator of the system. Guidance is available to them under **Customizing the system | Attributes** in the custodian's **Help index**

You can view the action plans you are entitled to see by clicking **Issues / Actions** on the system's Menu bar, then clicking the name of the particular action plan you are interested in. Instructions on how to add or modify action items are provided on its page of the system.

Action plan

Back to index

A document recording tasks and activities, priorities, responsibility for carrying them out and projected / actual completion dates. In managing risk, the tasks and activities normally involve:

- planning, organizing, conducting and writing-up risk evaluations
- remediation (ie tasks and activities concerned with correcting control weaknesses or other ways of driving down risk).

Citicus ONE maintains such action plans at enterprise, part of enterprise, and target of evaluation level. It also automatically maintains a digest called ‘My action plan’ for each user of the system, which draws together all actions for which that user has responsibility.

See the Action plan entry in **Citicus ONE**'s Glossary of system terms for further information (including how action items can be generated automatically and / or linked to control improvements and to evaluation issues.

Actual risk

Back to index

The level of risk posed by an individual target of evaluation. This is measured using a scorecard and displayed:

- dynamically on-screen as you complete your scorecard
- on the individual risk status report that is generated when you submit your completed scorecard.

Note: **Citicus ONE** uses the same terms for expressing actual and acceptable risk. This enables the risk posed by a target of evaluation to be compared to a level regarded as acceptable. In turn, this enables decision-makers to focus attention on targets of evaluation that exceed that level ie those posing an unacceptable risk to the enterprise.

Algorithm

Back to index

A set of rules and / or process for calculation using a computer. In **Citicus ONE** the term is used in relation to the rules and process employed in calculating criticality. The exact rules are proprietary.

Arrangement

Back to index

When considering risk, the word 'arrangement' is synonymous with control ie it means a policy, method, procedure, device or programmed mechanism which is designed to reduce the likelihood or business impact of incidents that could affect a target of evaluation.

Assessment

Back to index

A form presented by the system for fact-gathering purposes. Three types of assessment can be presented:

- Criticality assessment: a 1-page form that establishes accountability for a target of evaluation and measures its criticality
- Incident assessment (v1.0): the original version of a 2-page form that collects details of an information incident
- Incident assessment (v2.0): Based on the original version, this later version also probes the amount and cost of staff time lost due to an incident. This version is recommended.

A sample of each assessment can be found under **Other aids** on the **Help** index.

Attribute

Back to index

A characteristic of a target of evaluation (eg ‘Processes personal data’), , issue or action item identified as important by a custodian or local co-ordinator of the risk management process supported by the system.

Attributes can be set up by a custodian or local co-ordinator of the system. Once set up, they may be assigned to targets of evaluation, issues or action items by custodians or local co-ordinators or by individuals completing risk evaluations. Attributes so assigned are recorded in the results of evaluations.

Note: If editing by owners/completers is disallowed, attributes will be 'greyed out' (ie presented in grey type) when presented on the **Assign attributes** page of the system. There are two conditions when such editing may be disallowed:

- the system automatically disallows owners and completers from setting or varying any attribute that is employed as a common key in a data exchange (this is to maintain strict control over who can see information held in the external system)
- the custodian or local co-ordinator who sets up an attribute in the system can also choose to disallow owners and completers from setting or varying an attribute's values.

Auditors

Back to index

Individuals authorized and equipped to carry out rigorous, independent reviews of the quality of arrangements made to control risk in particular areas of the enterprise, including the controls applied to targets of evaluation.

Auto-select

Back to index

A category of checklist item that appears in a standard of practice, controls checklist, special circumstances list / checklist or threat list / checklist. Such items are distinguished by the fact that their applicability depends on the criticality of a target of evaluation or attributes it may have which are assigned by its owner, a custodian of the system or local co-ordinator.

Standards of practice, lists and checklists used for evaluation purposes often contain such requirements and **Citicus ONE** enables originators to categorize them as such. When **Citicus ONE** presents a standard of practice, list or checklist for completion, such items are presented only if they apply. Otherwise, they are suppressed and a note is inserted stating that this has been done.

Availability

Back to index

The property of a target of evaluation being accessible and useable when required by business users. Availability can have two aspects:

- **response time**: the length of time taken to respond to business users' requests for service (eg for information if the target of evaluation is an information resource)
- **up time**: the dates and times during which the target of evaluation is available to business users.

In both cases, measurements should be made from the users' perspective. This may well vary from that measured by technical staff responsible for managing the target of evaluation.

Availability rating

Back to index

A rating - and associated value - that indicates the level of harm that could be suffered by the enterprise as a result of a loss of availability of a target of evaluation.

For targets of evaluation that have been assessed with the CIA or QCD methods of measuring criticality, the availability rating is reported in their criticality status report and as one of the columns in the criticality league table.

The availability rating - and associated value - is expressed on the following five-point scale:

Availability rating	Value for charts and league tables
A Extremely serious harm	100%
B Very serious harm	75%
C Serious harm	50%
D Minor harm	25%
E No significant harm	0%

Note: The descriptions of the availability ratings shown above (eg 'Extremely serious harm') are the default descriptions but they can be customized. They are defined in the applicable harm reference table.

The calculation of the availability rating depends on which criticality algorithm is used, as shown below:

Criticality algorithm	Method of calculating availability rating
FIRM algorithm	The availability rating is the same as the critical availability rating.
FIRM+ algorithm	The availability rating is the same as the maximum availability rating.

Baseline

Back to index

A category of checklist items that appear in a standard of practice, controls checklist special circumstances list / checklist or threat list / checklist which always apply (eg *'data should be* *backed up periodically'*). Such items are distinguished by the fact that they are always presented and should be complied unless there are exceptional reasons for not doing so.

Standards of practice, lists and checklists used for evaluation purposes are generally made up largely of such requirements and **Citicus ONE** enables originators to categorize them as such.

They are always included when **Citicus ONE** presents a standard of practice, special circumstances list or threat list for review or checklist for completion.

Basis of evaluation

Back to index

A term employed by **Citicus ONE** to describe a detailed specification of the issues to be probed when evaluating the risk status of a particular type of target of evaluation (eg a business system, a supplier), abbreviated BoE. A BoE defines the questions that probe::

- the criticality of a target of evaluation
- the status of its controls ie the arrangements made to protect the target of evaluation
- special circumstances that heighten its need for protection
- level of threat as determined by the number of incidents suffered over the last year
- the business impact of those incidents.

A basis of evaluation also specifies:

- a harm reference table, which enables questions about criticality and business impact to be answered consistently and objectively
- one or more determinations of acceptable risk, which can be applied to targets of evaluation according to their criticality or other features
- the identity of attributes set up in the system which are to be incorporated in scorecards or assessments as additional questions.

Different bases of evaluation can be set up for evaluating different types of target of evaluation.

BS7799

Back to index

Short for British Standard BS7799. Claimed to be the 'world's most widely recognized information security standard', BS7799 aims to provide comprehensive guidance on the measures needed to protect the confidentiality, integrity and availability of information handled via IT.

Stemming from a 1990's initiative by the UK Department of Trade and Industry, BS7799 was developed in consultation with leading companies and nowadays takes the form of guidance notes and recommendations, published in two parts:

- Part 1, known as the 'code of practice', discusses control requirements at some length.
- Part 2 condenses this and introduces the concept of an 'information security management system' (ISMS).

In 2000, Part 1 was adopted as an international standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), who publish it as ISO/IEC 17799:2000 Information technology — Code of practice for information security management.

Part 2 originally published as BS7799-2:2002 - Specification for information security management systems later became ISO/IEC 27001. **Citicus ONE** incorporates the 2005 and 2013 editions of this widely used standard. Thus, compliance with these works can be established 'out of the box' using **Citicus ONE**.

Business application

Back to index

One of the five categories of information resource that **Citicus ONE** is set up to evaluate ‘out of the box’.

A business application comprises software plus associated data, business users, IT staff, documentation, equipment, services and facilities employed in carrying out a particular business process or set of processes.

Examples of typical business applications

As shown below, an application may be narrow in scope (eg ‘Fault recording’) or very wide (eg ‘CDC financials’).

Sample applications
Billing system
Cashier support system
CDC financials
Contracts register
Fault recording
Global email
Goods inward system
Group accounts consolidation system
Group executive information system (EIS)
Group treasury management system
Payroll system
Performance recording system
PoS cash register system
Production control system
Sales information system
Logistics system

Evaluating the information risk posed by a business application

The information risk posed by a business application is best evaluated by considering:

- its business purpose and use
- the arrangements made to preserve the confidentiality, integrity and availability of business information it handles during development and once in operational use
- experience of information incidents over the recent past.

Such evaluations should be conducted on behalf of the business owner of the application and involve both business and IT personnel.

Business applications that support many business processes

Business applications that support many different business purposes (such as those implemented using Oracle Financials or SAP ERP) can be difficult to evaluate because of their varied use.

The difficulty can be overcome by dividing such business applications into a set of sub-applications, each with a defined business owner, supported by the application software as a whole managed by a defined IT infrastructure owner, responsible for its technical development / operation.

Using **Citicus ONE**, each area of responsibility can be evaluated with a separate scorecard. Results can then be aggregated using a Dependency risk map and Consolidated risk status report compiled in order to assess the risk posed by the application as a whole.

Business impact

Back to index

The business impact of incidents is an important indicator of risk, since it enables risk to be discussed in business terms. It is evaluated based on the level of harm caused to the business by incidents ie events resulting in an actual loss of the critical aspects of the target of evaluation. These aspects depend on the type of target of evaluation, eg for an information resource they are the confidentiality, integrity or availability of the information associated with it, and for a supplier or supplied service they are the quality, cost and delivery of the associated service.

Citicus ONE evaluates the business impact by considering both the level of harm and the nature of harm caused by incidents.

In the case of an incident assessment, the nature and level of harm are determined in reference to an individual incident. In the case of a criticality assessment or scorecard, the nature and level of harm refer to the composite impact of incidents experienced over a time period.

To help you with your evaluation, when you complete a scorecard or assessment, you can view or print off a Harm reference table, which defines the nature and level of harm in terms that are meaningful within your enterprise.

Business impact rating

Back to index

A rating - and associated value - that indicates the maximum level of harm suffered by the enterprise, as a result of an incident affecting a particular target of evaluation.

The rating - and associated value - are expressed on the following five-point scale.

Business impact rating	Value for charts and league tables
A Extremely serious harm	100%
B Very serious harm	75%
C Serious harm	50%
D Minor harm	25%
E No significant harm	0%

Business owner

Back to index

The person or persons responsible for the use of a target of evaluation (eg a business application, a facility or a supplied service), for safeguarding it, and for ensuring that it poses an acceptable level of risk to the enterprise. The term is apostrophized to distinguish this management role from the concept of legal ownership and possession.

The role should be filled by an individual (not a group of individuals), who should:

- be responsible for the business processes most dependent on the target of evaluation
- be of appropriate seniority (ie neither too senior nor too junior)
- have the skills (knowledge of the business process, managerial) plus the time and inclination to fulfil his or her ownership role.

While individual accountability is the ideal; **Citicus ONE** enables you to identify multiple owners of a target of evaluation if you wish.

For further details, see owner and IT infrastructure owner.

Business user

Back to index

A person authorized to access some or all of the information handled by an information resource, who enters or obtains it either **directly**, using the capabilities of the information resource, or **indirectly** via one linked to it in some way.

Types of user to consider are illustrated in the table below.

Categories of user	Types of user to consider
Internal business users	Employees of your organization (eg management, professional, technical, administrative, sales or production workers) Contract staff
External business users	Employees of corporate: • customers • agents or other market intermediaries • suppliers of products or services • competitors Employees of government departments or other public bodies Individuals: • personal customers • private citizens

Checklist

Back to index

A list presented by **Citicus ONE** that you can use to record the status of a particular risk factor in detail. Each is divided into areas that correspond to the bullet points shown on its parent scorecard. If you complete an area of a checklist, your responses are used to answer the corresponding part of the scorecard automatically.

Completion may be made optional or mandatory. If mandatory, each area of the checklist must be completed before the parent scorecard can be successfully submitted; if optional, each area may either be left blank or fully completed for submission to succeed.

For further information see:

- Controls checklist (also known as a Compliance checklist)
- Special circumstances checklist
- Threat checklist.

CIA

Back to index

Abbreviation for the confidentiality, integrity and availability of information.

Citicus ONE

Back to index

A web-based system for measuring and managing information risk, supplier risk and other areas of operational risk objectively, efficiently and in business terms.

COBIT

Back to index

A widely-used standard of practice for IT published by the IT Governance Institute – a body formed under the auspices of the US Information Systems Audit and Control Association (ISACA) - which provides a reference framework for management, users, and internal audit, control and security practitioners. Citicus Limited contributed to the development of its fourth edition.

Comfort zone

Back to index

A short-hand term for the green area of a risk chart produced by **Citicus ONE**. The green area depicts the level of risk that is acceptable to top management of your enterprise. The level embraces five key determinants or indicators of risk.

Each of these is controllable in different ways, although in the case of two of them (namely criticality and special circumstances), the degree of control is limited.

For these two cases you can, first, check that the responses you have given to the questions that affect these components of risk are realistic. If your measured risk still exceeds the comfort zone, you may apply for a special determination of acceptable risk.

Your local co-ordinator or a custodian or of the system will be pleased to issue one with the green area set to the same as your measured risk. In return, he or she may make the determination of acceptable control weaknesses more restrictive.

Completer

Back to index

.A role assigned to a user of **Citicus ONE**, that enables him or her to complete the fact-gathering forms involved in a particular evaluation on behalf of the designated owner of the subject of the evaluation (ie a target of evaluation).

Compliance

Back to index

The act or manner of fulfilling a requirement set by others (eg by external regulators or management).

Compliance results

Back to index

Four types of result are compiled by **Citicus ONE** when a controls checklist is completed, namely:

- Compliance status report (full or selective)
- Schedule of controls (full or selective)
- Controls checklist
- Compliance league table (full or selective).

Selective results report the status of control items within a standard of practice that have been designated as relevant to a particular selective compliance reporting requirement (eg Sarbanes-Oxley).

An example of each result is available in the **Citicus ONE Help** system under Other aids.

Compliance checklist

Back to index

A method of establishing compliance with a standard of required practice. The controls checklists provided by **Citicus ONE** have the same purpose and the two terms are synonymous.

A sample controls / compliance checklist is available in the **Citicus ONE Help** system in the Sample results under Other aids.

Compliance gauge

Back to index

A graphical indicator of the proportion of the control items in a checklist which require remediation or further investigation. The compliance gauge is shown in conjunction with the risk chart on individual risk status reports to give a more detailed view of the status of controls. The compliance gauge can only be displayed if a status of arrangements checklist has been completed.

Component of risk

Back to index

A factor that determines or indicates risk, also referred to as a risk factor. In fact, these terms may be used interchangeably.

Citicus ONE incorporates a well-defined, business-oriented model of risk which incorporates five distinct components of risk. To provide an all-round picture of risk, each component is measured and the results brought together for presentation to decision-makers.

The five components of risk are:

- **criticality**: this is one of the two major determinants of risk. It is evaluated based on the business impact of a worst-case possible incident that could compromise one or more key aspects of a target of evaluation (eg the confidentiality, integrity or availability of information associated with an information resource or the quality, cost or delivery of a supplied service).
- **control weaknesses**: this is the other major determinant of risk - and the one most easily controlled. It is evaluated by assessing the status of arrangements made to protect the target of evaluation in defined control areas.
- **special circumstances**: these are circumstances other than control weaknesses - such as complexity - that increase the chance of major incidents occurring. The more that apply, the greater the risk. Statistically, special circumstances have a lower impact on risk than control weaknesses.
- **level of threat**: this is an important indicator of risk. It is measured based on the number of incidents experienced over a period. This recognizes that targets of evaluation which suffer incidents in one period are likely to suffer a similar number in future unless remedial action is taken. Statistical analysis confirms that the greater the number of incidents experienced over a time period, the greater the likelihood of major incidents occurring in future.
- **business impact**: the level of harm caused by actual incidents is another important indicator of risk, since it enables risk to be discussed in business terms. It is evaluated based on the maximum harm caused to the business by actual incidents over a time

period. This is similar to the way criticality is evaluated. However, in this case the evaluation reflects the business impact of actual incidents, rather than of a possible worst-case incident.

Note: these components have been identified through extensive analysis of a mass of statistics about business-critical targets of evaluation. **Citicus ONE** measures each one in order to provide an all-round view of risk.

Confidentiality

Back to index

The property of information being secret or private within a predetermined group.

Confidentiality rating

Back to index

A rating - and associated value - that indicates the maximum level of harm that could be suffered by the enterprise as a result of a loss of confidentiality of information.

The rating - and associated value - are expressed on the following five-point scale.

Confidentiality rating	Value for charts and league tables
A Extremely serious harm	100%
B Very serious harm	75%
C Serious harm	50%
D Minor harm	25%
E No significant harm	0%

Consolidated risk status report

Back to index

A type of result compiled by **Citicus ONE** that shows the risk status of a group of targets of evaluation in the form of a succinct report for decision-makers. An example is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Continuity

Back to index

The property of a target of evaluation being available to perform its designated function without interruption.

Continuity rating

Back to index

A rating - and associated value - that indicates the level of harm that could be suffered by the enterprise as a result of a loss of continuity of a target of evaluation.

For targets of evaluation that have been assessed with the VPC method of measuring criticality, the continuity rating is reported in their criticality status report and as one of the columns in the criticality league table.

The continuity rating - and associated value - is expressed on the following five-point scale:

Continuity rating	Value for charts and league tables
A Extremely serious harm	100%
B Very serious harm	75%
C Serious harm	50%
D Minor harm	25%
E No significant harm	0%

Note: The descriptions of the continuity ratings shown above (eg 'Extremely serious harm') are the default descriptions but they can be customized. They are defined in the applicable harm reference table.

Its calculation depends on which criticality algorithm is used, as shown below:

Criticality algorithm	Method of calculating continuity rating
FIRM algorithm	The continuity rating is the same as the critical continuity rating.
FIRM+ algorithm	The continuity rating is the same as the maximum continuity rating.

Control

Back to index

A policy, method, procedure, device or programmed mechanism which is either designed to protect a target of evaluation (eg data back-up), or that otherwise influences the level of protection provided (eg operator training and supervision).

Individual controls may:

- **prevent** incidents occurring (eg no combustible material in machine rooms)
- **detect** incidents that do, nevertheless, occur (eg fire detector)
- help an enterprise **recover** from incidents without unacceptable harm being suffered (eg fire alarms, sprinklers, contingency plan, back-up machine room).

Extensive statistical analysis indicates that, to keep risk at an acceptable level, controls need to be in good all-round condition.

Control area

Back to index

(1) A set of related arrangements or controls designed to protect a target of evaluation (eg data back-up), or that otherwise influence the level of protection provided (eg service agreements).

(2) Part of a standard of practice set up in **Citicus ONE** that covers a set of related arrangements or controls required to protect a target of evaluation. When used in this

context, the control areas in a standard are its top level of structure. They are listed in the Controls sections of risk scorecards and mini-scorecards. Their content may be defined by subordinate control items, which appear in the standard of practice or controls checklist (otherwise known as a compliance checklist) that 'sits underneath' the scorecard.

The scope of your control areas is important since extensive statistical research has demonstrated that the level of risk is largely determined by avoidable control weaknesses; and that the most productive way of reducing risk is to have controls in 'good all-round condition'.

In other words, controls must cover the full spectrum of threats that can and do compromise the key properties of a target of evaluation (eg confidentiality, integrity and availability for an information resource).

The FIRM methodology on which **Citicus ONE** is based, structures controls for information resources under 17 control areas. Their identification reflects in-depth statistical analysis of control strengths/weaknesses affecting thousands of business-critical systems. Thus, if you depart from these you should check that your control areas at least cover the same ground.

These control areas are listed under FIRM control areas. A similarly broad spectrum of control areas has been devised for the other types of target of evaluation that may be assessed using **Citicus ONE**'s in-built capabilities.

Control item

Back to index

A control objective, statement of required practice, note, heading or explanatory phrase forming part of a control area within a standard of practice or compliance checklist maintained using **Citicus ONE**.

Controls checklist

Back to index

The **controls checklist** presented by **Citicus ONE** forms part of a fully integrated, multi-level approach to managing risk which combines high-level evaluation using a succinct scorecard which probes the status of control areas (eg data back-up) with more-detailed evaluation using a checklist, which probes the status of controls (eg whether back-ups are encrypted) within each area. Such checklists are often referred to as compliance checklists and in this context the two terms are synonymous. Brief details follow.

Measuring compliance with your corporate standard of practice

A custodian or local co-ordinator of the risk management process supported by **Citicus ONE** can:

- convert any standard of practice maintained by the system into a controls checklist, automatically and at varying levels of detail
- arrange for the checklist to be presented for completion by owners of targets of evaluation or people acting on their behalf, by issuing scorecards which have a subordinate checklist
- choose whether completion of the checklist is mandatory or optional. If mandatory, it must be completed in full each time a scorecard is issued that it applies to. Otherwise, it can be completed in whole, in part or not at all at the owner's discretion.

What's in it for owners?

By completing a **Citicus ONE** controls checklist, an owner of a target of evaluation can, with modest effort:

- establish the adequacy and completeness of its controls ie the arrangements made to protect his or her target of evaluation

- establish the degree to which his or her controls comply with required practice
- obtain a succinct compliance status report supported by detailed schedules spelling out control strengths / weaknesses
- track improvement over time (since **Citicus ONE** automatically compares the results of successive evaluations).

Presentation of a controls checklist for completion

When a scorecard is issued for a target of evaluation to which a checklist has been prepared, evaluators can gain access to the checklist a control area at a time. In effect, the checklist sits 'underneath' the control areas on the scorecard.

The owner of the target of evaluation can see whether such a checklist is available, and if so whether its completion is optional or mandatory.

Checklist / scorecard integration

Responses entered into a compliance checklist are automatically 'rolled up' by the system, ie it uses them to answer the corresponding part of the associated scorecard automatically.

A full set of results is then generated from the checklist, which complements those that an owner obtains from completion of his or her scorecard.

A sample checklist is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Control self-assessment

Back to index

An assessment or examination of controls (ie the arrangements made to protect the enterprise from harm), carried out by people involved in the activity to which the controls apply (eg a project leader, member of a project team, Help desk staff, business user or supervisor) with or without the aid of a facilitator (eg a local co-ordinator).

Control weakness

Back to index

A control weakness arises when a required control is not implemented, is implemented incorrectly or is implemented but not fully or properly applied.

A **Citicus ONE** scorecard does not directly measure whether individual controls are implemented or applied. Instead, it probes whether the adequacy of controls in particular control areas has been established by recent, rigorous review. If so, a control area is rated as strong. Otherwise it is rated as weak, whether or not weaknesses are known or suspected.

This reflects detailed analysis of thousands of controls applied to hundreds of business-critical targets of evaluation. The analysis indicates that extensive weaknesses are the norm, not the exception. Thus, weaknesses are assumed unless there is firm evidence to the contrary.

A controls checklist (otherwise known as a compliance checklist) can an be presented 'underneath' the scorecard to establish whether individual controls are implemented or applied. When such a checklist is completed, responses on the checklist are used to fill in the equivalent part of the scorecard automatically.

Control weaknesses rating

Back to index

A value in the range 0% to 100% that indicates what proportion of the control areas featured on the risk scorecard are rated as weak. The value appears in risk charts, risk league tables and other results.

COSO

Back to index

Short for The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a US voluntary organization set up in 1985 to sponsor the US National Commission on Fraudulent Financial Reporting (often known as the Treadway Commission after its first chairman). In 1992, COSO published a major treatise on internal controls (Internal control – Integrated Framework) and in September 2004 issued a wider work called Enterprise Risk Management — Integrated Framework.

Cost

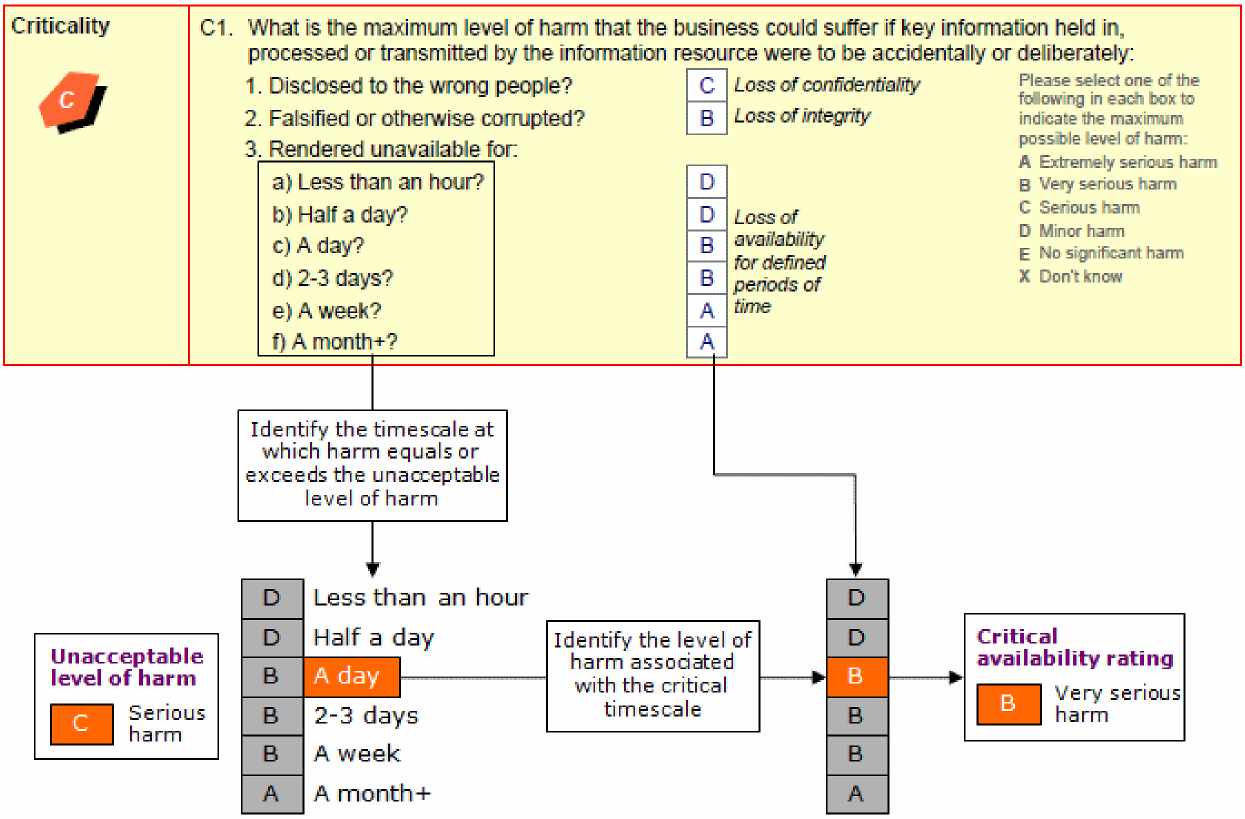
Back to index

An aspect of a supplier relationship, supplier or supplied service that needs to be protected, identifying what the enterprise has agreed to pay for products/services provided.

Critical availability rating

Back to index

The level of harm associated with the critical timescale of the target of evaluation, ie the period of unavailability at which harm equals or exceeds the level of harm that top management deem to be unacceptable (see level of unacceptable harm).



Criticality

C1. What is the maximum level of harm that the business could suffer if key information held in, processed or transmitted by the information resource were to be accidentally or deliberately:

1. Disclosed to the wrong people? C *Loss of confidentiality*
2. Falsified or otherwise corrupted? B *Loss of integrity*
3. Rendered unavailable for:

a) Less than an hour?	D	*Loss of availability for defined periods of time*
b) Half a day?	D	
c) A day?	B	
d) 2-3 days?	B	
e) A week?	A	
f) A month+?	A	

Please select one of the following in each box to indicate the maximum possible level of harm:

A Extremely serious harm
B Very serious harm
C Serious harm
D Minor harm
E No significant harm
X Don't know

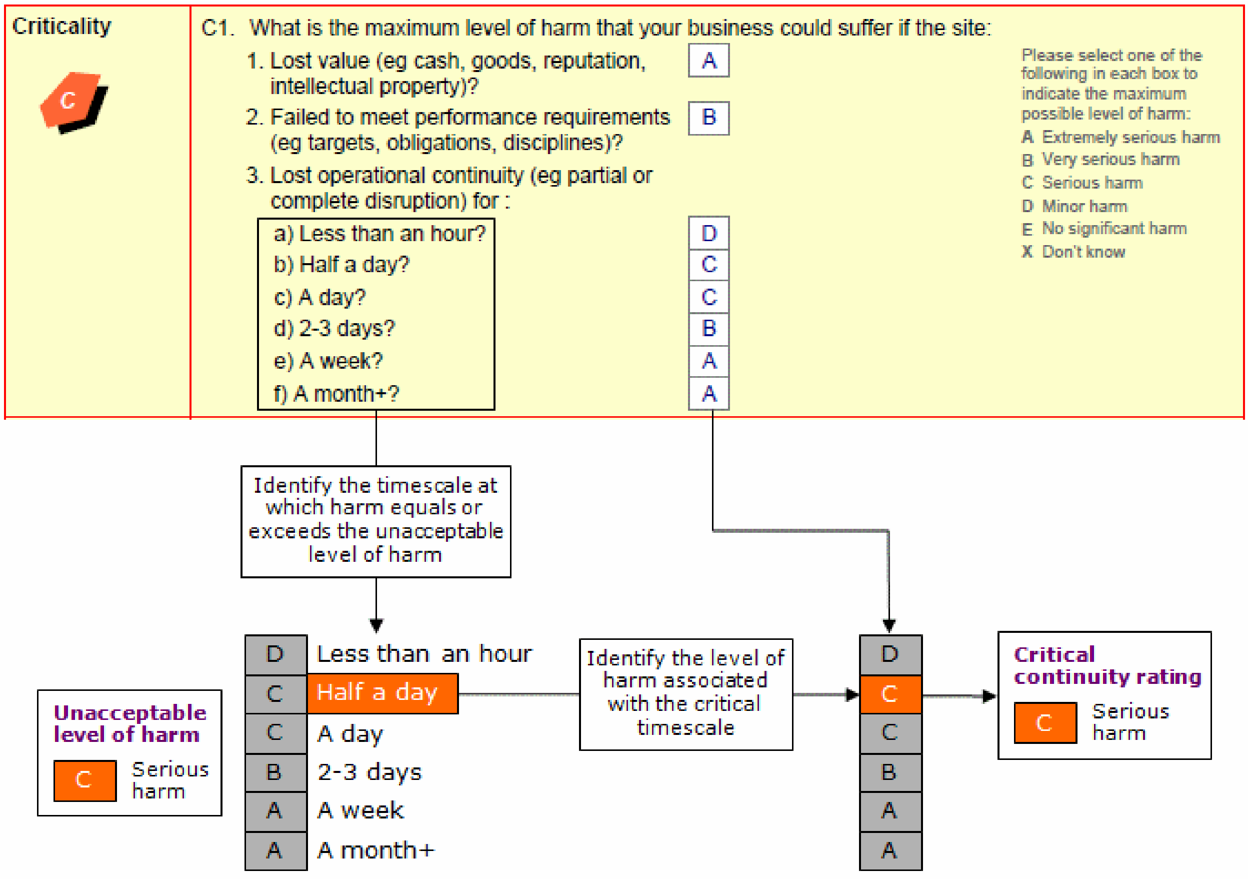
C
Identify the timescale at which harm equals or exceeds the unacceptable level of harm
D Less than an hour
D Half a day
B A day
B 2-3 days
B A week
A A month+
Unacceptable level of harm
C Serious harm
Identify the level of harm associated with the critical timescale
D
D
B
B
B
A
Critical availability rating
B Very serious harm

The critical availability rating is used to define the availability rating when the FIRM algorithm is employed for assessing criticality using the CIA or QCD methods.

Critical continuity rating

Back to index

The level of harm associated with the critical timescale of the target of evaluation, ie the period of lost operational continuity at which harm equals or exceeds the level of harm that top management deem to be unacceptable (see level of unacceptable harm).



Criticality

C1. What is the maximum level of harm that your business could suffer if the site:

1. Lost value (eg cash, goods, reputation, intellectual property)? A
2. Failed to meet performance requirements (eg targets, obligations, disciplines)? B
3. Lost operational continuity (eg partial or complete disruption) for :

a) Less than an hour?	D
b) Half a day?	C
c) A day?	C
d) 2-3 days?	B
e) A week?	A
f) A month+?	A

Please select one of the following in each box to indicate the maximum possible level of harm:

A	Extremely serious harm
B	Very serious harm
C	Serious harm
D	Minor harm
E	No significant harm
X	Don't know

C
Identify the timescale at which harm equals or exceeds the unacceptable level of harm
Unacceptable level of harm
C Serious harm
D Less than an hour
C Half a day
C A day
B 2-3 days
A A week
A A month+
Identify the level of harm associated with the critical timescale
D
C
C
B
A
A
Critical continuity rating
C Serious harm

The critical continuity rating is used to define the continuity rating when the FIRM algorithm is employed for assessing criticality using the VPC method.

Critical timescale

Back to index

The shortest timescale at which a loss of a target of evaluation's availability or continuity, or a delay in delivery, could cause unacceptable harm (eg 'a week'). By default the timescale is expressed on the following six-point scale:

- Less than an hour
- Half a day
- A day
- 2-3 days
- A week
- A month+.

These timescales provide a natural ladder of timescales that people can relate to. The words have their normal everyday meaning. So a day means a calendar unit lasting 24 hours. In an office environment that is normally around 8 hours of activity. In a plant, it's often 3 x 8hr shifts.

Note: In order to facilitate comparison between targets of evaluation with different availability ratings, the critical timescale is taken to be the longest of the measured time periods (eg 'a month+') if the unacceptable harm is not reached. This enables priority to be given to targets of evaluation that could cause unacceptable harm if availability were lost for shorter time periods.

The recovery controls applied to a target of evaluation (eg use of a stand-by processing facility, use of alternative telecommunications links or suppliers, fall-back to an earlier version) should permit it to resume functioning within the critical timescale. These controls should be tested under realistic conditions to check that they can indeed achieve recovery within the critical timescale of the target of evaluation concerned.

Criticality

Back to index

Criticality is one of the main determinants of risk. Using **Citicus ONE**, it is evaluated by considering the maximum level of harm that could arise if key properties or aspects of a target of evaluation were compromised.

These key properties/aspects depend on a target of evaluation's type as follows:

Target type	Key properties / aspects used to assess criticality
Information resources	Confidentiality, integrity and availability (CIA)
Suppliers, supplier relationships and supplied services	Quality, cost and delivery (QCD)
Other target types	Value, performance and continuity (VPC)

When assessing criticality, the following factors are taken into account:

- the maximum levels of harm that could be caused as a result of key properties / aspects of a target of evaluation being compromised should the worst credible loss event happen
- the effect of losing its availability / continuity – or suffering delayed delivery - for particular time periods
- the level of harm regarded as unacceptable by top management
- the critical timescale of your target of evaluation (ie the timescale at which unacceptable harm is suffered if availability or continuity is lost or delivery delayed)
- weightings that are designed to highlight targets of evaluation susceptible to the more severe levels of harm and those where severe harm can be caused by brief losses of availability.

The process considers the business impact of the **worst-case** incident that could be suffered by a target of evaluation irrespective of its cause. This is form of scenario-based, business impact analysis is easy to perform and encourages a business-oriented approach to risk. To encourage realism, objectivity and consistency, the business impact is determined by, or in conjunction with, the business owner(s) of the target of evaluation by reference to a harm reference table that applies enterprise-wide or at least across the part of the enterprise concerned.

The result is a criticality rating expressed on the following six-point scale.

Criticality rating	Value for charts and league tables
A. Extremely critical	100%
B. Very highly critical	75%
C. Highly critical	50%
D. Critical	25%
E. Important but not critical	0%
F. Regular	0%

This can then be compared with that of other targets of evaluation in order to identify their relative importance to the enterprise.

This systematized approach overcomes a problem that arises when owners assess criticality unaided. Left to themselves, almost all rate their targets of evaluation the same way (ie as extremely critical). Whilst understandable, this obscures those that pose the greatest risk.

Note: The criticality of IT infrastructure can be assessed the same way. However, where used to support multiple business applications, infrastructure criticality is best identified by inspecting the criticality ratings of the business applications concerned. These can be looked at in aggregate using a Dependency risk map or Criticality league table compiled by **Citicus ONE**.

Note: The information gathered when assessing criticality using **Citicus ONE** is valuable in developing business continuity, disaster recovery or IT contingency plans. The criticality rating for individual targets of evaluation can also be used to check that such plans enable recovery within critical timescales.

Note: The calculation of criticality is influenced by parameters that can be controlled by the custodian of the risk management process supported by **Citicus ONE**. Guidance on these is provided in the custodian's **Help** topic entitled **Criticality settings**. Custodians and local co-ordinators can find this under **Customizing the system** | **Scoring options** in their custodian's **Help index**.

Criticality assessment

Back to index

A form used by **Citicus ONE** to measure the criticality of an target of evaluation and to establish or confirm who is responsible for it (ie who is its owner).

It is designed so that an owner can complete one in minutes, without any training.

A guide entitled **How to complete a Criticality assessment** is available via **Citicus ONE**'s **Help** facility (see under **Other aids**).

Criticality rating

Back to index

A rating - and associated value - that indicates the relative importance of a target of evaluation to your organization, based on the maximum level of harm that could arise if key properties of the target of evaluation were compromised (eg confidentiality, integrity or availability for an information resource or quality, cost or delivery for a supplied service), taking into account:

- the natures and levels of harm that could be caused as a result of their being compromised
- the effect of losing availability or continuity or suffering delayed delivery for particular time periods
- the level of harm regarded as unacceptable by top management
- the critical timescale of your target of evaluation (ie the timescale at which unacceptable harm is suffered if availability or continuity is lost or delivery delayed)
- weightings that are designed to highlight targets of evaluation susceptible to the more severe levels of harm and those where severe harm can be caused by brief losses of availability.

The rating is expressed on the following six-point scale.

Criticality rating	Value for charts and league tables
A. Extremely critical	100%
B. Very highly critical	75%
C. Highly critical	50%
D. Critical	25%
E. Important but not critical	0%
F. Regular	0%

Custodian

Back to index

A person responsible for the overall use of **Citicus ONE** across an enterprise (eg the head of risk or equivalent at corporate level; someone in the corporate information security department or equivalent, acting as a risk-reduction programme manager).

Additional custodians may be appointed (eg to share the workload, or to provide cover in case of absence). In this case, one must be designated as the primary custodian.

Ideally, he or she will be the person who manages the risk reduction programme day-to-day. This individual should, either directly or via local co-ordinators in different parts of the enterprise:

- encourage and assist 'owners' of targets of evaluation to complete assessments, scorecards and compliance checklists
- help owners to understand their individual results, and to develop action plans for driving down risk
- develop action plans at corporate level, designed to help owners drive down risk enterprise-wide
- provide a high-level assessment of risk to key decision-makers within the enterprise.

What's in it for a custodian? A custodian will visibly contribute to the sound governance of the enterprise, and foster its operational success by helping owners to reduce the:

- disruptive effects of information incidents
- chances of major incidents occurring.

Decision-makers

Back to index

An individual expected to make informed decisions about risk, and how to control it. **Citicus ONE** reinforces a well-defined model of good practice in managing risk.

The model recognizes six key groups of decision-makers:

- top management: who are ultimately responsible for evaluating the risks faced by their enterprise, keeping them under control and communicating key risks to stakeholders
- high-level steering group: this provides a multidisciplinary forum for highlighting key risks and agreeing priorities for action at enterprise-level to drive risk down
- owners: responsibility for keeping the risk posed by an target of evaluation within acceptable limits is best delegated to a designated individual of appropriate seniority (not too high, not too low), equipped to manage the target of evaluation properly
- custodian: responsibility for measuring and managing risk down is best assigned to an individual (eg a corporate risk or security manager) equipped with the seniority, know-how, tools, time and resources needed to identify key areas of risk and help owners drive risk down (where more than one custodian is appointed, one should be designated as the primary custodian)
- local co-ordinators: in a large enterprise custodians should be supported by a network of local co-ordinators, who each fulfil a similar role but within a particular part of the enterprise
- auditors: internal or external auditors can both contribute to the **Citicus ONE** monitoring processes (eg by checking the accuracy of completed scorecards when conducting reviews). They can also benefit from the system (eg using **Citicus ONE**'s risk league tables to prioritize areas of work in their risk-based audit plans).

Delivery

Back to index

An aspect of a supplier relationship, supplier or supplied service identifying the agreed timescales within which products/services are to be provided.

Dependency risk map

Back to index

A type of result compiled by **Citicus ONE** that shows the risk status of a group of targets of evaluation in the form of a diagram. See the Glossary of system terms for further information.

Determination of acceptable risk

Back to index

A set of acceptable values - one for each component of risk - that defines the maximum level of risk that top management regard as acceptable, together with a risk chart that depicts those values on a common scale.

Citicus ONE enables custodians of the system and local co-ordinators to specify acceptable values in plain language. Each value has a corresponding percentage which determines the magnitude of risk on a risk chart.

The result is a determination of acceptable risk that can be easily communicated to decision-makers, since it includes both plain language and graphical elements.

The determination that applies to your target of evaluation can be seen in two places. Firstly, it shows up as the green area of the risk chart featured on your Individual risk status report.

In addition, the full determination is presented at the end of your Guidance on driving down risk, which forms part of your individual results.

If you feel the determination that applies to your target of evaluation is too stringent, or not stringent enough, you can ask your local co-ordinator or a custodian of the system to vary the determination. His or her contact details can be found at the foot of your **User details** page of the system. You can get to this by clicking **User details** in the system's menu bar then selecting **My details.**

Discretionary

Back to index

A category of control item that appears in a standard of practice or compliance checklist, distinguished by the fact that owners of individual targets of evaluation can decide for themselves whether they wish to implement it. Standards of practice often make items discretionary by including wording such as '…should be considered…'.

In general, such formulations are best avoided. However, **Citicus ONE** enables originators of standards to employ them and to categorize control items as such for scoring purposes.

Specifically, when **Citicus ONE** is reviewing responses to a compliance checklist in order to fill in the corresponding part of the associated scorecard automatically, responses of 'not applicable' are not treated as weaknesses if they apply to control items categorized as **discretionary** in the associated checklist. Otherwise, they are.

DoAR

Back to index

Short for determination of acceptable risk.

Enterprise

Back to index

A private- or public-sector organization - or part of one that can be considered as an organization in its own right for monitoring purposes.

Citicus ONE is designed to measure and manage down risk across an **enterprise** as defined above. For the purposes of managing risk, the enterprise may be divided into subordinate parts (eg departments, business areas, subsidiaries, regional offices). Indeed in a large enterprise, or one made up of units with different cultures, this is strongly recommended.

The division into parts is controlled at the top level by one or more custodians of the system, who will normally identify local co-ordinators to manage the monitoring process within its subordinate parts.

Local co-ordinators can sub-divide their parts into subordinate parts and so on, without restriction.

To maintain a coherent structure of control, the local co-ordinators of a part of the enterprise automatically gain the same role in its subordinate parts.

Evaluation

Back to index

An action-oriented management process that involves:

- measuring risk
- presenting measurements to decision-makers
- initiating remedial action to reduce risk to an acceptable level
- re-measurement to determine the effectiveness of remedial action (ie the extent to which such action fulfils its purpose).

Evaluation cycle

Back to index

The length of time between a target of evaluation being monitored 'for real' (ie with results included in league tables and analyses provided to top-level decision makers).

Note: **Citicus ONE** supports a constructive, two-phase evaluation cycle wherein a scorecard is completed at two points in the cycle. The first - called the 'dry run' - is designed to give owners an early impression of their risk status and time to do something about it. The second - called 'for real' - is designed to provide results that go up to top-level decision-makers.

Facilitated risk workshop

Back to index

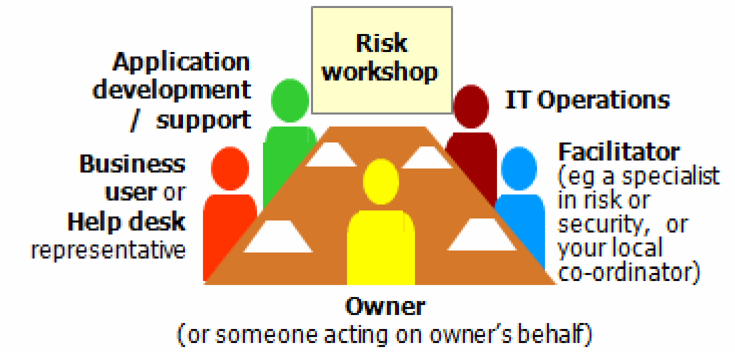
The optimum method of assessing the risk posed by a target of evaluation to the enterprise which involves employees responsible for its development, operation, maintenance and / or use combining their views through structured and facilitated discussion.

The method:

- brings together the range of individuals needed to assess risk from different perspectives (eg business, technical, day-to-day operation / use)
- orchestrates discussion through a structured process, led by a facilitator
- records the results of the discussion in an objective, business-oriented manner that stands up to inspection by reviewers and decision-makers, and that can be compared to and consolidated with the results of similar reviews of other targets of evaluation
- highlights where action is needed to keep risk within a level acceptable to management of the enterprise and its stakeholders.
- identifies the specific actions needed, and responsibilities for carrying them out.

A facilitated workshop of this type (in this case evaluating the risk posed by a business system) is illustrated below.

Completing a scorecard in workshop mode


Risk workshop
Application development / support
IT Operations
Business user or Help desk representative
Facilitator (eg a specialist in risk or security, or your local co-ordinator)
Owner (or someone acting on owner's behalf)

Risk scorecards presented by **Citicus ONE** are specially-designed to structure and record the results of such workshops.

Guidance on facilitating them can be downloaded from the system by clicking Facilitating a risk workshop (PDF 1.4 MB). Material you can send to attendees in advance can also be downloaded by clicking Preparing for a risk workshop (PDF 190 KB).

Using this method- supported by the functionality and guides provided by **Citicus ONE** - a risk workshop can be completed in three hours. People generally enjoy the process and find it stimulating.

Because the process is systematized and results are stored within the system, they can be distributed to decision-makers as attractive PDFs, consolidated with others carried out within your organization and updated any time with minimal effort

Facilitator

Back to index

In the context of managing risk using **Citicus ONE**, a person responsible for orchestrating discussion at a facilitated risk workshop. He or she contributes by:

- taking participants through the agenda
- keeping the workshop to time
- stimulating and guiding the discussion
- recording responses and comments into **Citicus ONE**
- using **Citicus ONE** to produce results
- after the meeting, drafting a Schedule of issues and / or Action plan to keep risk within an acceptable level.

He or she needs the ability to keep the discussion up-beat and focussed, and to contribute insights about expected standards of practice, the implications of incidents and the status of controls.

A facilitator should know how to use **Citicus ONE** or be supported by a colleague who does.

Guidance on facilitating such a workshop can be downloaded by clicking Facilitating a risk workshop (PDF 1.4 MB) and material you can send to attendees in advance can be downloaded by clicking Preparing for a risk workshop (PDF 190 KB).

Financial impact of incidents

Back to index

The **Citicus ONE** incident assessment collects information about the business impact of incidents. This is used to identify the financial impact of individual incidents reported on an ***Incident list*** – a type of high-level result produced by the system.

The financial impact of incidents is expressed as the reduction in value of the business given by the formula:

Reduction in the value of the business = Loss of income x 10% (a nominal profit margin) + Unforeseen costs + Loss of tangible assets.

The values for **Loss of income**, **Unforeseen costs** and **Loss of tangible assets** are the mid-points of the range ticked on the incident assessment.

The calculation as a whole is performed only if a range is ticked in response to each of the three financial impact questions. If a response of Don't know is ticked to one or more of the questions, the **Reduction in the value of the business** is reported as 'Unknown'.

This process yields a estimate of the total financial impact of an incident which is good enough for risk management purposes.

FIRM

Back to index

A methodology for managing information risk developed by the founders of Citicus Limited for and in conjunction with the Information Security Forum (ISF). The name is an acronym for Fundamental Information Risk Management.

First published by the ISF in March 2000, the methodology has been enthusiastically received by ISF Members and has been used to do well over 25,000 evaluations in 150+ countries.

By agreement with the ISF, **Citicus ONE** implements core components of **FIRM**, along with Citicus-designed refinements that improve its immediacy, scope and value. These help users not just to **evaluate** risk but to **drive risk down to acceptable levels**. The enhancements include:

- production of Individual risk status reports as soon as scorecards are submitted
- production of Guidance on driving risk down
- automatic conversion of standards of practice into controls checklists which probe status of controls at any level of detail
- production of dependency risk maps
- improvements to the criticality algorithm, the harm reference table and incident assessment
- maintenance of action plans and issue schedules at target of evaluation, part of enterprise and enterprise levels
- arrangements for **tracking progress** over time
- extension of the approach to other areas of operational risk.

Note: The approach to measuring risk that features in **Citicus ONE** and the FIRM methodology is exceptionally rigorous. It reflects in-depth analysis of a mass of data about 969 business-critical targets of evaluation, supported by case studies and work group discussion. For copies of the published FIRM methodology, contact the Information Security Forum directly.

FIRM control areas

Back to index

The FIRM methodology supported by **Citicus ONE** is designed to help you drive information risk down by remedying weaknesses in 17 control areas. These are known as **FIRM control areas**.

They reflect extensive statistical research into what factors are key in driving information risk down. Their status is probed by the pre-set scorecards delivered by **Citicus ONE**, and most Citicus-supplied standards of practice for use in information risk evaluations are structured the same way.

These control areas are listed below for your convenience. They are not sacrosanct – you can structure your standards of practice under other headings and have more or fewer of them if you wish. **Citicus ONE** will automatically tailor your scorecard to suit.

However, in considering how to structure your own standards of practice / controls checklists, thus which areas to probe on your scorecards, you should aim to cover at least the same ground, as completeness of controls is imperative if you wish to drive information risk down.

FIRM Control area		Its main focus and scope
1	Policies and standards	Compliance with corporate requirements
2	Ownership	Owner has appropriate skills and seniority
3	Organization	Clear reporting lines, sufficient staff, sound skills
4	Risk identification	Key risks identified and addressed
5	Awareness	People know they need to protect information
6	Service agreements	Service requirements agreed in writing
7	User capabilities	Sound business skills, procedures and supervision

8	IT capabilities	Sound it skills, disciplines and supervision
9	System configuration	Adequate capacity, resilience and documentation
10	Data back-up	Regular cycle, secure storage
11	Contingency arrangements	Plans exist and are proven to work
12	Physical security	Safe site, restricted to authorized individuals
13	Access to information	Access restricted to authorized individuals
14	Change management	Rigorous disciplines consistently applied
15	Problem management	Focal point to whom problems can be reported
16	Special controls	Additional protection, eg anti-virus measures
17	Audit/review	Independent reviews conducted periodically

GLBA

Back to index

Short for the US Gramm-Leach-Bliley Act of Congress, also known as the Financial Services Modernization Act of 1999. This Act was introduced to enhance competition in the financial services industry.

Amongst other things, it limits the ability of financial institutions operating in the US to collect and disclose consumers' personal financial information and requires such institutions to:

- safeguard consumers' personal financial information
- advise consumers about the policies and practices they apply to the disclosure of such information to third parties.

These 'privacy' provisions extend to companies who receive such information, whether or not they are financial institutions. They can be easily entered as rules into **Citicus ONE** and presented to owners of applicable systems as checklists.

Good, all-round condition

Back to index

Arrangements are in this condition when no significant weaknesses exist in any of the control areas probed by your scorecard. To establish this, you need to initiate a rigorous review (ie one using comprehensive checklists to establish compliance with a recognised standard of practice). This can be performed by your own staff, internal audit, consultants or some other party.

Citicus ONE can present controls checklists (otherwise known as compliance checklists) to help you do so.

Such a review will normally classify weaknesses according to whether they are significant or minor. Significant weaknesses, clearly, need to be rectified promptly. You can keep track of progress in remedying them using **Citicus ONE**'s schedule of issues and / or action plan.

Governance

Back to index

The way in which a country, business or other organization is controlled and run. This term has come to the fore as a result of pressure from governments and others seeking to protect the interests of shareholders and other stake-holders in an enterprise.

Much of the discussion centres on the management of risk. It is now largely common ground that management have a duty to identify, disclose and manage key areas of risk properly, on behalf of stakeholders.

The risk management process supported by **Citicus ONE** can contribute to this by subjecting information risk – one of the largest and fastest growing areas of risk facing leading organizations today – supplier risk and other areas of operational risk to systematic measurement, reporting and control.

Guidance on driving risk down

Back to index

A type of result compiled by **Citicus ONE** that provides custom guidance to the owner of an target of evaluation on how to drive risk down. An example is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Harm reference table

Back to index

A compact form designed to help you and your co-workers to select levels of harm in a consistent manner (ie all sharing the same definitions). The form identifies different **natures of harm** (eg Financial loss), and for each one defines five **levels of harm**.

A sample form is available via **Citicus ONE**'s **Help** facility (see under **Other aids**). Your custodian or local co-ordinator may customize this to suit your enterprise.

You can access the harm reference table that applies to you whenever you are completing or reviewing sections of a scorecard or assessment that probe levels of harm.

The harm reference table can be used as an interactive, clickable version accessed by clicking on the text of a question in the 'criticality' section of a criticality assessment or risk scorecard, the 'business impact' section of a risk scorecard or the 'impact on the business' section of an incident assessment.

Alternatively, you can access a read-only version suitable for printing by, clicking where indicated at the head of your **Enter responses** page. You can also gain access to the read-only version, when completing a scorecard or criticality assessment, by clicking **What level of harm should I select?** which appears underlined in blue at the foot of your **Enter responses page**. Your harm reference table will then be presented in a separate window.

High-level risk status report

Back to index

See consolidated risk status report.

High-level steering group

Back to index

A multidisciplinary forum capable of highlighting key risks and agreeing priorities for action at enterprise-level to drive risk down.

The group should be chaired by someone who is or reports to top management and comprise owners of business-critical targets of evaluation, IT managers, and specialists representing risk management, internal audit and security professionals. A custodian of the **Citicus ONE** system should be represented and play a leading role in its deliberations.

Ideally, the forum should meet three or four times a year to:

- receive a report on the risk status of the enterprise, highlighting key risks and recommended priorities for action
- review the report
- agree priorities for action
- issue a digest of the risk status of the enterprise to top management.

Why should a high-level steering group adopt this role? A high-level steering group that brings together a cross-section of decision-makers and meets three or four times a year is the ideal forum for highlighting key risks and agreeing priorities for action. Monitoring risk should be a natural aspect of its activity.

HIPAA

Back to index

Short for US Health Insurance Portability and Accountability Act of Congress. Enacted in 1996, this legislation required the US government to set standards for the electronic exchange, privacy and security of health information. A resultant ‘privacy rule’ was published in August 2002 and a ‘security rule’ in February 2003. These rules apply to health plans, healthcare clearinghouses, and certain health care providers. They can be easily entered into **Citicus ONE** and presented as checklists.

HRT

Back to index

Short for harm reference table, a concept developed by Citicus Limited that features strongly in the risk management process enabled by **Citicus ONE**.

Human error

Back to index

A type of event that afflicts IT-based information systems that may, and often will, compromise the confidentiality, integrity or availability of information handled by one or more systems.

Note: Human errors become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table illustrates the types of human error that need to be considered.

Types of human error to consider
User errors (eg mistakes in inputting data)
Errors by staff who run computers
Errors by staff who run networks
Other forms of error

Please note:

- the types of human error presented in the table above are ranked in order of likelihood (the most likely appearing first)
- the ordering reflecting the results of the Information Security Forum’s Information Security Status Survey, 2000
- the breakdown above is for consideration when completing a risk scorecard.

Incident

Back to index

An event, or chain of events, that results in an adverse business impact on the enterprise.

Research shows that the number of minor incidents suffered over a period is a very good predictor of the likelihood of suffering a major incident in future.

This is why **Citicus ONE** probes the number that have occurred and encourages action that minimizes the chances of their recurrence.

Note: incidents are events or chains of event that *have* happened , whereas threats are ones that *might* happen. Thus threats and incidents are different sides of the same coin

Typical incident categories for the different types of target of evaluation set up in the system are illustrated in the table below. A custodian or local co-ordinator of the system can customize these by varying the bases of evaluation used to configure the scorecards and assessments presented by **Citicus ONE.**

The number of incidents experienced in the categories you choose can then be recorded using a **Citicus ONE** risk scorecard; and **Citicus ONE's** incident assessment form can be completed to record details of particularly damaging incidents.

Type of target of evaluation	Typical incident categories
Information resource	• Malfunctions of software or hardware • Loss of services, equipment or facilities • Overloads • Human error • Unforeseen effects of change • Other undesirable acts (eg access violations, virus attacks).
Privacy	• Information leakage • Loss or theft of unencrypted personal data • Unintentional distribution of personal data • Misuse of personal data • Improper processes • Improper handling
Industrial control system	• Malfunction of hardware • Malfunction of software • Loss of essential services • Damage/disruption through environmental events • Overloads • Human error • Unforeseen effects of change • Unauthorised malicious action

Type of target of evaluation	Typical incident categories
Supplier relationship, **Supplier,** **Supplied service**	• Commitments not met • Lack of professionalism • Significant disputes • Uncompetitive performance • Gross misconduct • Business interrupted
Site	• Malfunction of plant / machinery • Loss of external services • Loss of access to site • Natural disaster • Staff shortage / dispute • Work-related illness, injury or death • Anti-social or criminal activity

Subordinate threats may be defined at lower level. For example, in the incident assessment for industrial control systems provided by **Citicus ONE** 'out of the box', the 'Unauthorised malicious action' category covers the following subordinate /types of incident/threat:

- Inappropriate control (eg improper use)
- Theft of equipment
- Industrial espionage/theft of information
- Introduction of malware (eg worms, trojans, computer viruses)
- Denial of service attacks
- Terrorism/sabotage/vandalism
- External system penetration
- Unauthorised access by insiders
- Fraud
- Other unauthorised malicious action.

Incident assessment

Back to index

A 2-page form used by **Citicus ONE** to capture details of an individual incident. The form is suitable for collecting details of an incident serious enough to warrant individual attention.

Two versions of the form are available: v1.0 and v2.0. The more-recent one – v2.0 - is identical to the original except that it probes staff time lost through an incident. This version is applied by default.

Incident list

Back to index

A type of result compiled by **Citicus ONE** that lists individually-significant incidents recorded over a period, ranked according to the harm they caused to the enterprise. An example is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Incident statistics

Back to index

A type of result compiled by **Citicus ONE** that provides a breakdown of individually-significant incidents recorded over a period. An example is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Independent party

Back to index

A person or persons not involved in the activity being assessed (eg an internal facilitator, external consultant, internal or external auditor).

Independent review

Back to index

A detailed assessment or examination carried out by people who are not involved in the activity being assessed (eg internal facilitators, external consultants, internal or external auditors).

Independent reviewers may wish to employ their own checklists. However, ideally they should be probing compliance with an explicit standard of practice set by management. Using **Citicus ONE** this can be achieved as any such standard, if entered into the system, can be easily converted into a controls checklist (otherwise known as a compliance checklist) for presentation by the system.

Individual results

Back to index

A set of results compiled by **Citicus ONE** when you complete a criticality assessment, risk scorecard or incident assessment. For details see **Help** topic **Gaining access to your individual results** in the **Owner's Help index**.

Individual risk status report

Back to index

A type of result compiled by **Citicus ONE** that shows the risk status of single target of evaluation in the form of a succinct 2-page report for decision-makers. An example is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Information asset

Back to index

A collective term covering information and the facilities used to capture, record, transmit, process and display it. In **Citicus ONE**, the term information resource has precisely the same meaning and is preferred. However, you can safely substitute **information asset** for information resource without change of meaning.

Information incident

Back to index

An event, or chain of events, that compromises the confidentiality, integrity or availability of information.

Categories of information incidents that influence information risk include:

- malfunctions of software or hardware
- loss of services, equipment or facilities
- overloads
- human error
- unforeseen effects of change
- other undesirable acts (eg access violations, virus attacks).

Information protection

Back to index

A field of endeavour concerned with protecting the confidentiality, integrity and availability of information.

Information resource

Back to index

A target of evaluation type covering information and the facilities used to capture, record, transmit, process and display it.

Information resources can be subdivided into categories of **data sets**, **business applications**, **computer installations**, **communications networks** and **system development** activities.

Examples of typical information resources

Example name	Category of information resource
Billing system	Business application
Cashier support system	Business application
CDC financials	Business application
Contracts register	Business application
Customer relationship system	Business application
Dublin call centre	Computer installation
European data centre	Computer installation
Fault recording system	Business application
Global email	Business application
Group accounts consolidation system	Business application
Group executive information system (EIS)	Business application
Group treasury management system	Business application
Group-wide WAN	Communications network
Logistics system	Business application
London data centre	Computer installation
New York data centre	Computer installation
Payroll system	Business application
Performance recording system	Business application
SecurNet	Communications network
Supplier database	Data set
UK data centre	Computer installation
Vehicle management (new system)	Systems development activity

Information risk

Back to index

The chance or possibility of harm being caused to an enterprise as a result of a loss of the confidentiality, integrity or availability of information.

Citicus ONE evaluates the level of risk associated with an information resource by measuring five determinants or indicators of information risk, namely:

- the criticality of the information resource to the enterprise
- control weaknesses that affect the likelihood of the information resource preserving the confidentiality, integrity or availability of information
- special circumstances that heighten the probability of the information resource being disrupted by incidents
- the level of threat to the information resource, measured by the number of incidents suffered over the last 12 months
- the business impact of incidents that compromised the confidentiality, integrity or availability of information over a period.

The methods employed in measuring each factor are based on rigorous analysis of large bodies of data about hundreds of business-critical targets of evaluation. They therefore provide a meaningful picture of risk.

See also risk, supplier risk and operational risk.

Information security

Back to index

A field of endeavour concerned with the protection of the confidentiality, integrity and availability of information.

Information Security Forum

The Information Security Forum (ISF) is an international association of leading organizations which funds and co-operates in the development of a practical research programme in information security.

For further information, contact the ISF directly via e-mail: info@securityforum.org or view the ISF web site at www.securityforum.org.

Integrity

Back to index

The property of information being a correct and sound representation of an authorized business process. Integrity has three aspects:

- **completeness**: the property of information being present in its entirety
- **accuracy**: the property that information is exactly as intended
- **validity**: the property that information reflects authorized business processes.

Integrity rating

Back to index

A rating - and associated value - that indicates the maximum level of harm that could be suffered by the enterprise as a result of a loss of integrity of information.

The rating - and associated value - are expressed on the following five-point scale.

Integrity rating	Value for charts and league tables
A Extremely serious harm	100%
B Very serious harm	75%
C Serious harm	50%
D Minor harm	25%
E No significant harm	0%

Internal control

Back to index

In day to day usage, internal control is just another way of describing a system of controls. In the context of risk that means the ‘policies, methods, procedures, devices or programmed mechanisms designed to protect the key properties (eg CIA or QCD) of a target of evaluation (eg locks, access controls, segregation of duties), or that otherwise influences the level of protection provided (eg awareness, training).’

In other contexts, the term has different meanings, some rather tortuous and subject to debate by lawyers, accounting bodies, regulators and advocates of particular approaches.

In particular, the term ‘internal control’ has a more or less prescribed meaning when it comes to Sarbanes Oxley legislation. The discussion is published on the website of the US Securities and Exchange Commission (SEC).

ISF Standard of practice

Back to index

Short for the **Standard of good practice for information security (SOGP)** published by the Information Security Forum (ISF). The standard aims to provide a challenging but achievable target against which organizations of all sizes can measure their performance in managing information security. The standard provides comprehensive guidance on the measures needed to protect the confidentiality, integrity and availability of information handled via IT.

The ISF standard of practice stands out against other works in that it is:

- **kept up-to-date**: since first published in 1996, the ISF standard has been updated every two years to take account of developments in the use of IT by leading organizations
- **research-based**: the standard takes account of the results of ISF research projects, including its regular survey of the controls applied to mission-critical systems by leading organizations.

Citicus ONE can evaluate compliance with this standard of practice 'out of the box'.

ISO17799

Back to index

Short for ISO/IEC 17799:2000 Information technology — Code of practice for information security management. This is an international standard published by the International

Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is based on and is equivalent to Part 1 of British Standard BS7799 – which is claimed to be the 'world's most widely recognized information security standard'.

Citicus ONE can evaluate compliance with this standard of practice 'out of the box'.

ISO27001

Back to index

Short for ISO/IEC 27001:2005 Information technology - Security techniques – Information security management systems – Requirements. This is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is based on Part 2 of British Standard BS7799 – which specifies the requirements for an information security management system and summarizes the controls described in ISO17799.

Citicus ONE can evaluate compliance with this standard of practice 'out of the box'.

Issue

Back to index

A problem or concern identified by one or more evaluations carried out using **Citicus ONE** that is recorded in a schedule of issues maintained by system, along with its:

- issue ID (eg I.2)
- applies to (ie the part of the enterprise or target of evaluation it applies to or the identity of who recorded it in the system eg 'Entered by Alex Albury (alburya)')
- priority (eg 'High', 'Medium', 'Low')
- issue owner (ie who responsible for the issue and its resolution)
- current status (ie 'Open', 'Closed' or 'Abandoned')
- date raised (eg 12 November 2013)
- target / actual resolution dates
- links to related action items ones that will resolve the issue when completed
- links to related controls (ie linked control improvements), these can be for information only or can be set so that the system updates the status of each related control (either entirely automatically or subject to a user's review and approval) when all issues / actions linked to it are closed or completed
- values of any attributes that have been set up in the system to characterize issues or provide additional information about them. Attributes employed for this purpose need to be defined and published for use with issues by a custodian or local co-ordinator of the system. Guidance is available to them under **Customizing the system | Attributes** in the custodian's **Help index**.

You can enter issues into a **Schedule of issues** you have access to either by hand by clicking **Add new** at the foot of the **Schedule of issues** page of the system, or by clicking **Populate with notes and comments** at the foot of the page. The latter will create individual issues automatically from ratings and comments entered in your most recent evaluation. You can edit these to express them in your own terms.

To use these facilities, click **Issues / Actions** in the system's Menu bar, then select a **Schedule of issues** and follow the on-screen instructions.

Issue schedule

Back to index

See schedule of issues.

IT

Back to index

Short for information technology, the term encompasses the full range of computer and telecommunications equipment and software employed in processing or otherwise handling information including 'phones, fax machines, mobile devices, desktop devices and departmental / enterprise-scale servers.

IT infrastructure

Back to index

IT-based facilities that support or protect business applications, including computer installations, data centres, network operations centres, departmental / enterprise-scale servers, wide or local area networks, firewalls and gateways.

Examples of IT infrastructure

As shown below, IT infrastructure may be very wide in scope (eg 'Group-wide WAN') or very narrow (eg 'Router AB/456-11224').

Example name	Type of target of evaluation
Group-wide WAN	Communications network
Router AB/456-11224	Communications network
SecurNet	Communications network
Dublin call centre	Computer installation
European data centre	Computer installation
London data centre	Computer installation
New York data centre	Computer installation
UK data centre	Computer installation

Why evaluating IT infrastructure is important

Such facilities typically support more than one business application, often many. Thus weaknesses in their control arrangements can heighten information risk for everyone reliant on the infrastructure. Remedying such weaknesses therefore typically offers major benefits.

Evaluating the criticality of particular items of IT infrastructure

The criticality of IT-based facilities may be identified in business terms by examining the criticality ratings of the business applications they support, and their specific needs for protection. These data can be easily obtained from the Dependency risk maps and Criticality league tables produced by **Citicus ONE**.

IT infrastructure owner

Back to index

The person or persons responsible for a computer installation, communications network or systems development activity that supports one or more business applications, for safeguarding it, and for ensuring that it poses an acceptable level of risk to the enterprise. The term is always used in **Citicus ONE** to signify stewardship and accountability not legal ownership or possession.

Ideally, the role should be filled by an individual (not a group of individuals), who should:

- be of appropriate seniority (ie neither too senior nor too junior)

- have the IT and managerial skills plus the time and inclination to fulfil his or her ownership role.

For further details, see owner or business owner.

ITIL

Back to index

Short for IT Infrastructure Library - an internationally accepted and respected approach to IT Service Management promoted by the UK Office of Government Commerce (UK OGC) - an independent part of the UK Treasury with its own Chief Executive.

ITIL incorporates best practice drawn from the public and private sectors internationally. It is supported by a qualifications scheme, accredited training, and tools. The approach supports and is supported by the British Standards Institution's Standard for IT Service Management (BS15000).

Key risk driver

Back to index

A factor that contributes to measured risk being above the acceptable level (eg a control weakness, special circumstance that applies or incident suffered). Such factors can be identified using the ***Risk heat maps*** and ***Risk dashboards*** produced by **Citicus ONE**.

League table

Back to index

A list ranked in order according to one or more values (eg a list of football teams ranked according to the games they have won, drawn or lost in competition with other teams in the list).

Citicus ONE applies this notion when it compiles a type of result which ranks targets of evaluation according to their criticality, risk or level of compliance with a standard of practice. An example of each is available in the **Citicus ONE Help** system under Other aids. See the Glossary of system terms for further information.

Level of harm

Back to index

The **magnitude** of the business impact caused by an actual or possible incident.

Citicus ONE uses the following five-point scale to evaluate the level of harm.

Level of harm
A - Extremely serious harm
B - Very serious harm
C - Serious harm
D - Minor harm
E - No significant harm

Each point on the scale is defined in a Harm reference table, in terms that are meaningful within your enterprise.

Level of threat

Back to index

Level of threat is an important indicator of risk. It can be evaluated based on the number of incidents experienced over a period. This recognizes that targets of evaluation which suffer incidents in one period are likely to suffer a similar number in future unless remedial action is taken. The greater the number of incidents, the greater the likelihood of **major** incidents occurring.

Level of threat rating

Back to index

A rating - and associated value - that indicates the likelihood of threats materializing: the higher the rating, the greater the level of threat.

Citicus ONE evaluates the level of threat to a target of evaluation based on **historical incident data** - more specifically, on the number of incidents suffered by the target of evaluation over a 12 month period.

A scorecard probes how many incidents of various types have been suffered over the year preceding its completion. These responses are added together; the total is expressed as a range; and the range is then used to look-up the corresponding rating as follows:

Level of threat rating	Value for charts and league tables
101+ incidents a year	100%
51-100 incidents a year	75%
11-50 incidents a year	50%
1-10 incidents a year	25%
No incidents a year	0%

This approach is borne out by statistical analysis of many thousand of incidents affecting many hundreds of business-critical targets of evaluation. The analysis shows a strong correlation between the number of incidents experienced in a time period and the chances of suffering a major one.

The method of calculation in more detail: to calculate the total number of incidents, **Citicus ONE** adds together the number of incidents experienced for each type of incident shown on the scorecard. Where the actual number of incidents experienced is entered, this is added to the total. Alternatively, where a radio-button is ticked, the system adds a number which reflects the heading above the ticked radio-button, as follows:

Heading above radio-button	Number of incidents added to total
None	0
1-10	5.5 (ie mid-point of range)
11-50	30.5 (ie mid-point of range)
51-100	75.5 (ie mid-point of range)
101+	101 (ie minimum possible number)

Level of unacceptable harm

Back to index

The **magnitude** of the business impact caused by an actual or possible incident that is unacceptable to top management. In the context of the risk management process supported by **Citicus ONE** this is expressed as a point on the five-point scale **Citicus ONE** employs to express levels of harm. The scale ranges from 'A. Extremely serious harm' to 'E. No significant harm'.

Each point on the scale is defined in a Harm reference table, in terms that are meaningful within your enterprise.

Local co-ordinator

Back to index

A person who manages the **Citicus ONE** risk management process day-to-day within a particular part of the enterprise. There may be different local co-ordinators for different target types, for example for information resources this will normally be the person responsible for promoting good practice in relation to the development, operation and use of information systems within that part of the enterprise.

The part of the enterprise may be a department, business area, subsidiary, regional office or other component of the enterprise.

More than one local co-ordinator may be appointed in each part of the enterprise (eg to cover different areas of risk, to share the workload, or to provide cover in case of absence).

In this case, one must be the **primary local co-ordinato**r. Ideally, he or she should be the person who manages the **Citicus ONE** monitoring process day-to-day in the part of the enterprise concerned. He or she should:

- co-operate with custodians of the system to implement the system in such a way as to respect the local culture
- encourage and assist 'owners' of targets of evaluation to complete scorecards and assessments
- help owners to understand their individual results, and to develop action plans for driving down risk
- develop action plans designed to help owners drive down risk within their part of the enterprise, and contribute to the development of action plans at corporate level
- provide a high-level assessment of risk to key decision-makers within their part of the enterprise.

What's in it for local co-ordinators? A local co-ordinator will visibly contribute to the sound governance of the enterprise, and foster its operational success by helping owners to reduce the:

- disruptive effects of incidents
- chances of major incidents occurring.

Loss of services, equipment or facilities

Back to index

A type of event that afflicts IT-based information systems that may compromise the confidentiality, integrity or availability of information handled by one or more systems.

Such events become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table illustrates the types of loss that need to be considered.

Types of loss of services, equipment or facilities to consider
Loss of external communications links / services
Damage to in-house communications links
Loss of power
Malfunction of ancillary equipment (eg air conditioning, heating / cooling plant)
Theft of equipment
Damage to equipment or equipment rooms
Acts of God (earthquake, fire, extreme weather)
Other losses of services, equipment or facilities

Please note:

- the types of loss of services, equipment or facilities presented in the table above are ranked in order of likelihood (the most likely appearing first)
- the ordering reflecting the results of the Information Security Forum's Information Security Status Survey, 2000.

Major incident

Back to index

An incident (or similar event) that causes an exceptionally high level of harm to an organization. In the context of managing risk, the subjective element of this definition can be avoided by defining incidents as 'major' when they cause a level of harm at or above one of the levels defined by a particular Harm reference table presented by **Citicus ONE**.

A custodian of the system can select one of these as constituting an unacceptable level of harm to your enterprise. It makes good sense to regard this as the cut-off for defining 'major' (ie an incident becomes 'major' if it causes an unacceptable level of harm to your enterprise).

As part of its proportionate incident reporting process, **Citicus ONE** automatically issues an Incident assessment for completion when such an incident is recorded as having happened when completing the **Business impact** section of a scorecard.

Malfunctions of software or hardware

Back to index

A type of event that afflicts IT-based information systems that may compromise the confidentiality, integrity or availability of information handled by one or more systems.

Such events become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table indicates the range of malfunctions that need to be considered.

Help topics | Other aids | Glossary of risk terms

Types of malfunction to consider
Malfunction of business applications based on desk-top software products
Malfunction of software developed in-house
Transmission errors
Malfunction of PC-based file / database servers
Malfunction of computers / communications controllers (excluding PC-based)
Malfunction of system software / communications software (excluding PC-based)
Malfunction of PC-based communications controllers
Malfunction of business applications based on other software products
Other forms of malfunction

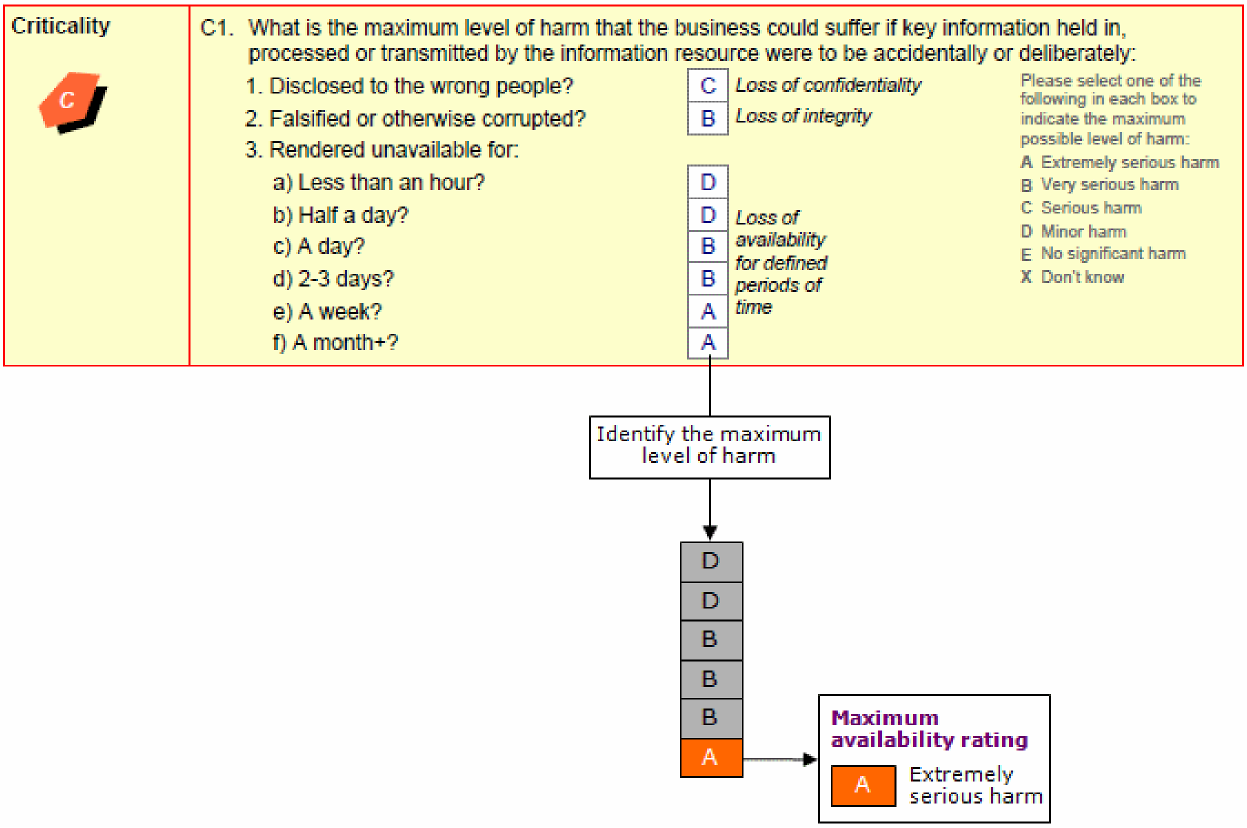
Please note:

- the types of malfunction presented in the table above are ranked in order of likelihood (the most likely appearing first)
- the ordering reflecting the results of the Information Security Forum's Information Security Status Survey, 2000.

Maximum availability rating

Back to index

The maximum level of harm that could be achieved through prolonged unavailability of the target of evaluation.



Criticality

C1. What is the maximum level of harm that the business could suffer if key information held in, processed or transmitted by the information resource were to be accidentally or deliberately:

1. Disclosed to the wrong people?	C	*Loss of confidentiality*
2. Falsified or otherwise corrupted?	B	*Loss of integrity*
3. Rendered unavailable for:		
a) Less than an hour?	D	*Loss of availability for defined periods of time*
b) Half a day?	D	
c) A day?	B	
d) 2-3 days?	B	
e) A week?	A	
f) A month+?	A	

Please select one of the following in each box to indicate the maximum possible level of harm:

A Extremely serious harm
B Very serious harm
C Serious harm
D Minor harm
E No significant harm
X Don't know

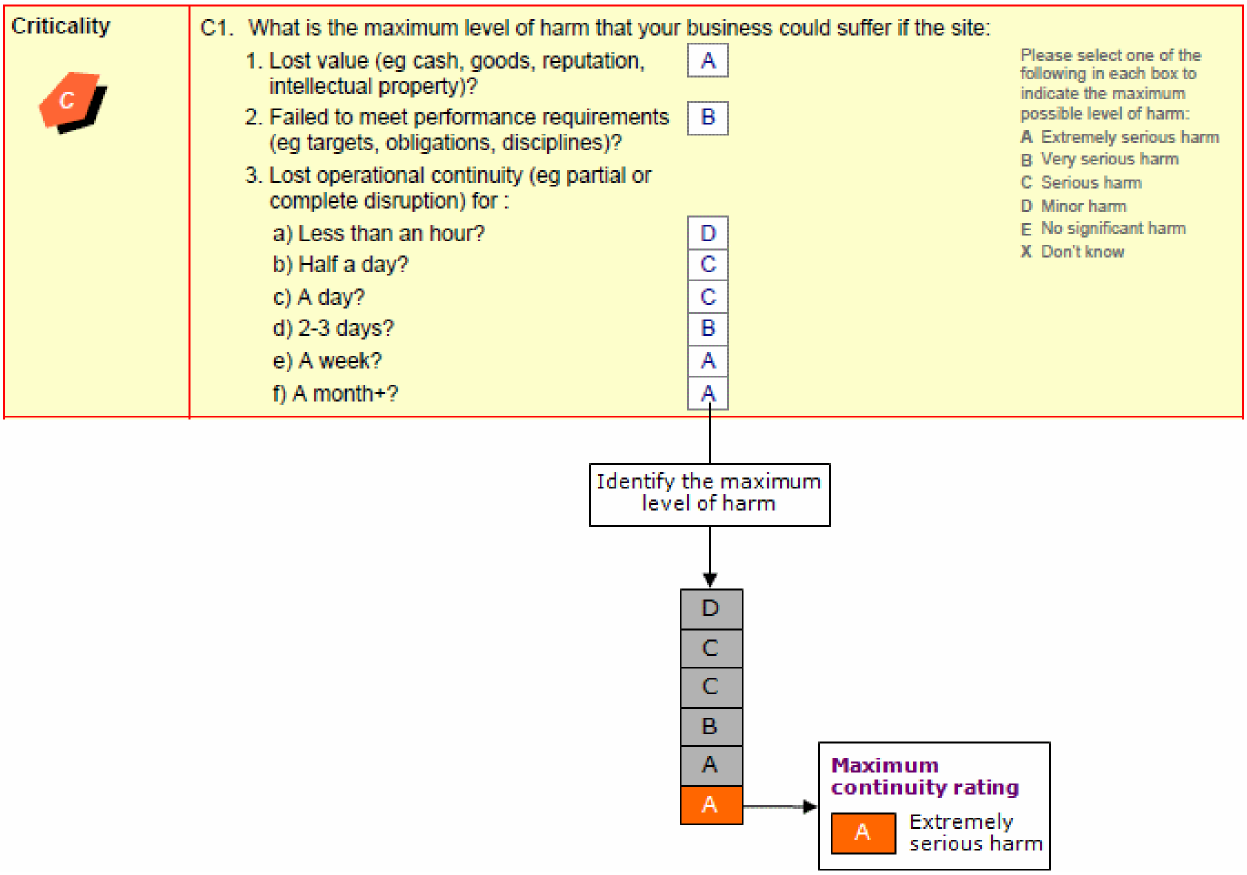
C
Identify the maximum level of harm
D
D
B
B
B
A
Maximum availability rating
A
Extremely serious harm

The maximum availability rating is used to define the availability rating when the FIRM+ algorithm is employed for assessing criticality using the CIA or QCD methods.

Maximum continuity rating

Back to index

The maximum level of harm that could be achieved through prolonged loss of operational continuity of the target of evaluation.



Criticality

C1. What is the maximum level of harm that your business could suffer if the site:

1. Lost value (eg cash, goods, reputation, intellectual property)? A
2. Failed to meet performance requirements (eg targets, obligations, disciplines)? B
3. Lost operational continuity (eg partial or complete disruption) for :
   - a) Less than an hour? D
   - b) Half a day? C
   - c) A day? C
   - d) 2-3 days? B
   - e) A week? A
   - f) A month+? A

Please select one of the following in each box to indicate the maximum possible level of harm:
A Extremely serious harm
B Very serious harm
C Serious harm
D Minor harm
E No significant harm
X Don't know

The maximum continuity rating is used to define the continuity rating when the FIRM+ algorithm is employed for assessing criticality using the VPC method.

Nature of harm

Back to index

The type of harm caused by an incident (or series of incidents). On a scorecard or assessment, each category is described in two parts, namely:

- a fixed **heading**, eg Financial loss,
- **cited examples**, presented, in parenthesis, immediately after the fixed heading, eg (loss of sales, unforeseen costs, legal liabilities, fraud).

The **fixed headings** are designed to probe the full spectrum of harm that your enterprise can suffer eg:

- financial loss
- degraded performance
- loss of management control
- damaged reputation

- impaired growth
- any other way.

The **cited examples** are designed to clarify - very succinctly - what each heading means.

In **Citicus ONE** the **headings** and the **cited examples** can be fully customized to cover the types of harm particularly relevant to your enterprise.

The nature of harm is presented along with a quantified level of harm in the Harm reference table associated with your scorecard or assessment.

You can use this to resolve any uncertainty you may have as to the nature of harm caused by the actual or potential incident (or series of incidents).

OECD

Back to index

The Organization for Economic Co-operation and Development was founded in 1960 to further the social and economic interests of world's most powerful nations, including France, Germany, Italy, Spain, UK, USA and Japan. It now has 30 members.

Best known for its economic statistics and forecasts, the OECD has influenced the development of IT-related legislation in many countries (notably in the data protection arena) and fosters good governance in the public service and in corporate activity. It published Principles of Corporate Governance in 1999; and in 2002 published Guidelines for the security of information systems and networks.

Other areas of operational risk

Back to index

The chance or possibility of harm being caused to an enterprise as a result of a target of evaluation's value, performance or continuity being compromised. VPC is a shorthand for these three aspects, which need to be protected.

This definition covers the full spectrum of harm that an organization can suffer when an asset, entity, activity, process or relationship is compromised by whatever cause.

It can be applied to any area of operational risk evaluated using **Citicus ONE**(eg to sites, business processes and so on) and results aggregated with evaluations of information resources, supplier relationships and supplied services, since these are defined and evaluated consistently, by measuring five determinants or indicators of risk, namely:

- the criticality of the target of evaluation to the enterprise
- control weaknesses that affect the likelihood oft he target of evaluation's value, performance or continuity being compromised
- special circumstances that heighten the probability of the target of evaluation suffering incidents
- the level of threat faced by the target of evaluation, measured by the number of incidents suffered over the last 12 months
- the business impact of incidents that compromised the target of evaluation's value, performance or continuity over a period.

Note: This definition is consistent with one put forward by the Bank For International Settlements (BIS) which defines*operational risk as '*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*'. This excludes reputational risk, which many organizations rate as a major issue, and includes certain loss events within the definition which are backed up by a more detailed schedule.

*Source: International Convergence of Capital Measurement and Capital Standards A Revised Framework Comprehensive Version June 2006.

See also risk, information risk and supplier risk.

Other undesirable acts

Back to index

A type of event that afflicts IT-based information systems that may compromise the confidentiality, integrity or availability of information handled by one or more systems.

Such events become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table illustrates the range of undesirable acts that need to be considered.

Types of undesirable act to consider
Introduction of computer viruses
Misuse of in-house telephones by employees to avoid paying for personal calls
Misuse of external services (eg the Internet) by employees
Disclosure of passwords to unauthorized personnel
Introduction of other forms of unauthorized 'executables'
Unauthorized access to the enterprise's targets of evaluation by employees
Unauthorized modification of files / databases
Theft of software
Misoperation or misuse of systems by employees intent on fraud
Improper operation or misuse of systems by employees intent on disruption
Eavesdropping
Theft of information
Unauthorized access via dial-up
Falsification of source / destination of transmitted data
Denial of service attacks
Unauthorized modification of data during transmission
Unauthorized modification of software (eg for gain)
Unauthorized access to the enterprise's targets of evaluation by external hackers
Other undesirable acts

Please note:

- the types of undesirable act presented in the table above are ranked in order of likelihood (the most likely appearing first)

- the ordering reflecting the results of the Information Security Forum's Information Security Status Survey, 2000.

owner

Back to index

The individual responsible the use of a target of evaluation, for safeguarding it and for ensuring that it poses an acceptable level of risk to the enterprise. The term is always used in **Citicus ONE** to signify stewardship and accountability not legal ownership or possession.

In the case of targets of evaluation such as business applications, supplier relationships and supplied services, the owner should be a business owner.

In the case of infrastructure targets of evaluation such as computer installations, communications network, sites and other facilities, the owner should have sufficient expertise to manage the target of evaluation properly.

In both cases, the owner should:

- complete criticality assessments, scorecards, incident assessments and checklists for his or her target(s) of evaluation, as part of the risk management process supported by **Citicus ONE**
- understand their individual results, and develop action plans for driving down risk.

These duties can be carried out by an owner directly. Alternatively, the owner may delegate them to someone acting on his or her behalf.

What's in it for owners? The individual results produced by **Citicus ONE** provide early warning of potential problems. Acting on them will help the owner to reduce the:

- number of times the target of evaluation is disrupted by incidents
- chances of major incidents occurring.

The results will also enable owners to demonstrate their success in driving risk down to an acceptable level.

Overloads

Back to index

A type of event that afflicts IT-based information systems that may compromise the confidentiality, integrity or availability of information handled by one or more systems.

Such events become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table illustrates the types of overload that need to be considered.

Types of overload to consider
Inadequate response times to users who have successfully signed
Unacceptable delays to users attempting to sign
Inability to sign
Other forms of overload

Please note:

- the types of overload presented in the table above are ranked in order of likelihood (the most likely appearing first)
- the ordering reflecting the results of the Information Security Forum's Information Security Status Survey, 2000.

Part of the enterprise

Back to index

Citicus ONE is designed to measure and manage down risk across an enterprise which may be divided into subordinate **parts** (eg individual departments, business areas, subsidiaries, regional offices) for risk management purposes. Indeed in a large enterprise, or one made up of units with different cultures, this is strongly recommended.

The division into parts for risk management purposes is controlled at the top level by one or more custodians of the system, who will normally identify local co-ordinators to manage the monitoring process within subordinate parts.

Local co-ordinators can sub-divide their parts into subordinate parts and so on down, without restriction.

To maintain a coherent structure of control, the local co-ordinators of a part of the enterprise automatically gain the same role in its subordinate parts.

Performance

Back to index

An aspect of a target of evaluation identifying its ability to meet operational objectives, for example as specified in service level targets or agreements.

QCD

Back to index

Abbreviation for quality, cost and delivery, normally employed in relation to a supplier.

Quality

Back to index

An aspect of a supplier relationship, supplier or supplied service identifying the fitness for purpose of the products/services provided.

Recent

Back to index

A term that appears on the risk scorecard in the context of carrying out a review or examination of the controls applied to a target of evaluation.

Where the criticality of a target of evaluation is not known with any accuracy (ie where it has not yet been measured using **Citicus ONE**), interpret it to mean **within the last year**.

Alternatively, where the criticality of the target of evaluation is known, interpret it as follows:

Criticality	Criticality rating	What 'recent' means
Extremely critical	100%	Within the last 2 months
Very highly critical	75%	Within the last 3 months
Highly critical	50%	Within the last 6 months
Critical	25%	Within the last 12 months
Important but not critical	0%	Within the last 24 months
Of regular importance	0%	At owner's discretion

Note: You can see the **criticality rating** of your target of evaluation in the risk charts shown on the **Enter responses** page for the **Criticality** section of your scorecard. You can get to this page by clicking **Evaluations > Evaluations in progress** or Reporting > Results of individual evaluations on the system's Menu bar, clicking the hyperlinked ID of your criticality assessment then viewing your criticality assessment..

Note: You may wish evaluate your target of evaluation more frequently if it is subject to a high-degree of change.

Recorded notes and comments

Back to index

One of the individual results produced by **Citicus ONE** when a criticality assessment or risk scorecard is submitted. An example is available in the **Citicus ONE Help** system under **Other aids**.

The result contains two classes of entry:

- **notes** automatically generated by the system to highlight issues requiring remediation or follow-on action (eg "*Note: Identify and remedy the root cause(s) of the 1-10 malfunctions of software or hardware that has been suffered over the last 12 months.*")
- **comments** recorded by the evaluator whilst answering the questions on the assessment or scorecard. Such comments are often highly revealing. They may explain responses; identify praiseworthy accomplishments; highlight control weaknesses (eg "*back-ups taken but left on open shelf*"); or make clear that arrangements need to be strengthened ("*numerous input errors as staff often mis-hear what people are saying at the other end of the line*").

Such notes and comments are drawn together to help evaluators and reviewers keep track of key points are ensure none are overlooked. To help evaluators further, the notes and comments that are recorded may, if desired, be loaded into the schedule of issues and / or action plan associated with the evaluated target of evaluation. For guidance on this process, see Populate with notes and comments in the **Glossary of system terms**.

Remedial activity

Back to index

Action taken or required to correct control weaknesses.

Remediation

Back to index

A term often used by specialists in audit, control and risk management. It denotes the changes necessary to correct one or more control weaknesses.

Rigorous

Back to index

A term that appears on the risk scorecard in the context of carrying out independent reviews or self-assessments.

In this context, the term is used to mean a **thorough** examination using a **comprehensive checklist** that establishes whether an **explicit standard of practice** is **achieved or not** in defined control areas.

Citicus ONE can automatically present the standard of practice employed by your organization as a controls checklist (otherwise known as a compliance checklist) and integrate it with your scorecard. See your local co-ordinator or a custodian of the system for details.

Note: Checklists employed by your internal or external auditors and other bodies may fulfil the above criteria. However, to do so, they must probe compliance with an explicit standard of practice, thoroughly.

Risk

Back to index

The chance or possibility of harm being caused to an enterprise or individual. For risk to be to be evaluated in meaningful terms, the **probability** needs to be quantified along with both the **nature** and **level of harm** that could ensue if the worst happened.

Citicus ONE evaluates the level of risk posed to an enterprise by individual targets of evaluation. The risk each poses is quantified by measuring five key determinants or indicators of risk, namely:

- the criticality of the target of evaluation to the enterprise, this is assessed in business terms
- control weaknesses that affect the likelihood of the target of evaluation suffering incidents that compromise one or more of its aspects that need to be protected
- special circumstances (eg scale, complexity, geographical distribution) that heighten the probability of the target of evaluation suffering incidents
- the level of threat to the target of evaluation, measured by the number of incidents suffered over the last 12 months
- the business impact of incidents suffered over a period.

The aspects that need to be protected depend on the area of risk as follows:

Area of risk	Aspects to be protected
Information risk	The confidentiality, integrity or availability of information, taking into account the critical timescale of availability.
Supplier risk	The quality, cost and delivery of goods or services supplied, taking into account the critical timescale of delivery.
Other areas of operational risk	The value, performance or continuity of the target of evaluation, taking into account the critical timescale of any loss of continuity.

Once evaluated the risk posed by individual targets of evaluation is aggregated to provide an overall picture of risk posed to the enterprise.

This method of evaluation employed reflects years of in-depth, quantitative research into incidents affecting many thousands of mission-critical targets of evaluation. This yielded the definition of information risk employed by **Citicus ONE** – which has been widely adopted around the world. Equivalent definitions of supplier risk and other areas of operational risk that are also supported, which enables the entire spectrum of operational risk be measured and managed in a consistent, scalable and business-oriented manner.

Risk factor

Back to index

A factor that determines or indicates risk, also referred to as a component of risk. These terms may be used interchangeably.

Citicus ONE incorporates a well-defined, business-oriented model of risk which incorporates five distinct risk factors. To provide an all-round picture of risk, each factor is measured and the results brought together for presentation to decision-makers.

The five factors are:

- **criticality**: this is one of the two major determinants of risk. It is evaluated based on the maximum harm that could arise if one or more of a target of evaluation's key aspects were compromised. These aspects depend on your target of evaluation's type as follows:

Target type	Key aspect
Information resource	The confidentiality, integrity or availability of information, taking into account the timescale of any loss of availability.
Supplier relationship or supplied service	The quality, cost and delivery of the goods or services supplied, taking into account the timescale of delay in delivery.
Site plus all other cases	The value, performance or continuity of the target of evaluation, taking into account the timescale of any loss of continuity.

- **control weaknesses**: this is the other major determinant of risk - and the one most easily controlled. It is evaluated by assessing the status of arrangements made to protect the aspects identified above within particular control areas. In the case of a scorecard covering the 17 FIRM control areas, each of which has been proven to be significant by statistical means.
- **special circumstances**: these are circumstances other than control weaknesses - such as complexity - that increase the chance of major incidents occurring. The more that apply, the greater the likelihood of incidents being suffered, hence the greater the risk.
- **level of threat**: this is an important indicator of risk. It is measured based on the number of incidents experienced over a period. This recognizes that targets of evaluation which suffer incidents in one period are likely to suffer a similar number in future unless remedial action is taken. Statistical analysis confirms that the greater the number of incidents experienced over a time period, the greater the likelihood of major incidents occurring in future.
- **business impact**: the level of harm caused by actual incidents is another important indicator of risk, since it enables risk to be discussed in business terms. It is evaluated based on the maximum harm caused to the business by actual incidents over a time period. This is similar to the way criticality is evaluated. However, in this case the evaluation reflects the business impact of actual incidents, rather than of a possible worst-case incident.

Note: these factors have been identified through extensive analysis of a mass of statistics about business-critical targets of evaluation. **Citicus ONE** measures each one in order to provide an all-round view of risk.

Risk scorecard

Back to index

A 2-page form used to:

- measure the level of risk posed by a target of evaluation
- identify any action being taken to strengthen controls
- construct a brief profile of the target of evaluation (eg its identity, nature, no. of users).

The form employed in **Citicus ONE** has been purposefully designed to:

- be easy to fill-in
- measure each component of risk
- collect data that is accurate enough for decision-making purposes.

Features of the form can be customized (by a custodian of **Citicus ONE** or your local co-ordinator); however, the core elements of the form are fixed in order to:

- maintain rigour and completeness
- facilitate comparison (eg production of risk 'league tables').

Risk workshop

Back to index

A method of assessing the risk posed by a target of evaluation to the enterprise which involves employees responsible for its development, operation, maintenance and / or use combining their views through structured discussion.

The method:

- brings together the range of individuals needed to assess risk from different perspectives (eg business, technical, day-to-day operation / use)
- orchestrates discussion through a structured process
- records the results of the discussion in an objective, business-oriented manner that stands up to inspection by reviewers and decision-makers, and that can be compared to and consolidated with the results of similar reviews of other targets of evaluation
- highlights where action is needed to keep risk within a level acceptable to management of the enterprise and its stakeholders.
- identifies the specific actions needed, and responsibilities for carrying them out.

Risk scorecards presented by **Citicus ONE** are specially-designed to structure and record the results of such workshops.

Guidance on facilitating them can be downloaded from the system by clicking Facilitating a risk workshop (PDF 1.4 MB). Material you can send to attendees in advance can also be downloaded by clicking Preparing for a risk workshop (PDF 190 KB).

Using this method- supported by the functionality and guides provided by **Citicus ONE** - a risk workshop can be completed in three hours. People generally enjoy the process and find it stimulating.

Because the process is systematized and results are stored within the system, they can be distributed to decision-makers as attractive PDFs, consolidated with others carried out within your organization and updated any time with minimal effort

See also Facilitated risk workshop and Facilitator.

Sarbanes-Oxley

Back to index

Short for the US Sarbanes-Oxley Act of 2002. This US legislation was co-sponsored by Senator Paul Sarbanes and Congressman Michael Oxley, following the Enron disaster. Its aim is 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.

Among other changes, it strictly limits what accounting firms can do for their audit clients, requires US listed companies to establish independent audit committees and requires CEOs and CFOs to certify the effectiveness of their controls over financial reporting.

The Act gives the US Securities and Exchange Commission far-reaching powers to define the precise obligations of management and advisors, and to enforce them. It is causing companies to take a fresh look at their internal controls, including those applied to business application systems and associated IT infrastructure. Since it applies to subsidiaries of US listed companies and to companies based overseas whose shares are traded on US exchanges, this legislation affects corporate governance practices worldwide.

Note: **Citicus ONE** enables custodians and local co-ordinators to identify which targets of evaluation are financial systems, which support financial systems and all related IT infrastructure. They can also highlight parts of their standard(s) of practice that apply to such systems and generate compliance results that highlight the status of their controls.

Schedule of issues

Back to index

A document recording information about problems and concerns (ie issues) raised by business managers, asset owners, risk evaluators or other stakeholders.

In managing risk, the tasks and activities normally involve:

- planning, organizing, conducting and writing-up risk evaluations
- remediation (ie tasks and activities concerned with correcting control weaknesses or other vulnerabilities).

Citicus ONE maintains schedules of issues at enterprise, part of enterprise, and target of evaluation level.

See the Schedule of issues entry in **Citicus ONE**'s Glossary of system terms for further information about managing problems and concerns (including how issues can be recorded automatically and / or linked to control improvements and to remedial action.

Scorecard

Back to index

A form used to evaluate performance.

The 2-page **risk scorecard** provided by **Citicus ONE** is designed to capture the information needed to measure the level of risk posed by an individual target of evaluation, which may be an information resource, supplier relationship, supplied service, site or other entity within the enterprise. It is designed to be completed by the owner of a target of evaluation who may wish to delegate the task to a completer.

The form is designed to be easy to complete, and can be tailored to suit the needs of your enterprise.

Self-assessment

Back to index

An assessment or examination carried out by people involved in the activity being assessed (eg a project leader, member of a project team, Help desk staff, business user or supervisor) with or without the aid of a facilitator (eg a local co-ordinator).

SEC

Back to index

Short for the US Securities and Exchange Commission, the regulatory agency set up following the 1920's stock market crash to protect the interests of investors and maintain the integrity of the securities markets. Its driving concept is that investors large and small should have access to basic facts about an investment so that they can make informed buying / selling decisions.

In the US it is responsible for ensuring compliance with certain 'securities laws'. The latest of these is the US Sarbanes-Oxley Act of 2002.

These laws apply to all entities which have shares listed on US stock exchanges. Thus its reach extends well beyond the confines of the US.

SoP

Back to index

Short for standard of practice.

SOX

Back to index

Short for the US Sarbanes-Oxley Act of 2002.

Special circumstance

Back to index

A circumstance other than a control weakness that influences the likelihood of threats materializing (eg a high degree of change, complexity, accessibility by external parties).

Citicus ONE measures the proportion of a defined set of special circumstances that apply. Risk rises, the more that apply.

The special circumstances that feature on the risk scorecard can be customized as a part of the basis of evaluation for a particular target type. The ones that appear in the Citicus-supplied bases of evaluation for information risk have been statistically identified as important, based on analysis of thousands of factors that applied to hundreds of business-critical targets of evaluation.

Special circumstance area

Back to index

A special circumstance or set of related special circumstances (eg 'Complexity') listed as a bullet point on a risk scorecard presented by **Citicus ONE**.

Special circumstance rating

Back to index

A value in the range 0% to 100% that indicates what proportion of the special circumstances featured on the risk scorecard apply. The value appears in risk charts and risk league tables.

Special circumstances checklist

Back to index

A checklist defined by a basis of evaluation, to help evaluators complete the special circumstances section of their scorecard. The checklists is displayed when the evaluator click a special circumstance on the scorecard. It enables the evaluator to record which subordinate special circumstances apply, at a lower level of detail than shown the scorecard.

Responses are 'rolled-up' to complete the corresponding question on the scorecard automatically.

Special circumstances list

Back to index

A completion aid defined by a basis of evaluation, to help evaluators complete the special circumstances section of their scorecard. This aid is displayed when the evaluator click a special circumstance shown on the scorecard and presents subordinate special circumstances, at a lower level of detail.

Standard of practice

Back to index

A statement or succinct interpretation of a statement that describes the practices people are required to follow when developing, running or using an target of evaluation.

You can view the statement or interpretation that applies to your target of evaluation by clicking **Standard of practice** in the **Supplementary information** portion of the **Enter responses** page that you use to complete your scorecard or assessment.

You can get to this page by clicking **Evaluations** on the system's Menu bar, clicking **Evaluations in progress** then selecting your target of evaluation's latest scorecard/assessment.

Note: the statement or interpretation may have been prepared by your local co-ordinator, a custodian of the system or by Citicus Limited. It may be or be based on a standard published by your own organization or an external body.

Note: Normally an interpretation will not be the standard itself - which will exist outside the **Citicus ONE** system. It will be provided to help you efficiently determine the status of your arrangements within the control areas featured on your scorecard.

Status of arrangements

Back to index

The adequacy or otherwise of the policies, methods, procedures, devices or programmed mechanisms that have been implemented and applied to reduce the likelihood or business impact of incidents that could affect a target of evaluation. The term 'controls' is often used for such arrangements.

Their status can be established using a **Citicus ONE** risk scorecard or a mini-scorecard of type RSa, RSb or RSd with or without a subordinate controls checklist.

Supplier risk

Back to index

The chance or possibility of harm being caused to an enterprise as a result of a supplier of products or services failing to meet the enterprise’s quality, cost or delivery goals.

Citicus ONE evaluates the level of risk associated with a supplier or supplied service by measuring five determinants or indicators of risk, namely:

- the criticality of the supplier or supplied service to the enterprise
- control weaknesses that affect the likelihood of the supplier or supplied service providing services that meet agreed quality, cost and delivery goals
- special circumstances that heighten the probability of incidents disrupting the supplier or supplied service
- the level of threat to the target of evaluation, measured by the number of incidents suffered over the last 12 months

- the business impact of incidents that compromised quality, cost or delivery over a period.

The methods employed in measuring each factor are based on rigorous analysis of large bodies of data about hundreds of business-critical targets of evaluation. They therefore provide a meaningful picture of risk.

See also risk, information risk and other areas of operational risk.

Target of evaluation

Back to index

An asset, entity, activity, process or relationship that poses a risk to the enterprise, which needs to be evaluated.

Citicus ONE can be used to evaluate targets of evaluations of different types, including:

- information resources*
- suppliers*
- supplier relationships*
- supplied services*
- sites*
- business process
- business units
- privacy-related projects*
- projects.

* These target types are set up in **Citicus ONE** prior to delivery and **Citicus ONE** can be used to evaluate them ’out of the box’.

Target type

Back to index

Short for type of target of evaluation.

Threat

Back to index

A threat is a way in which the key properties of a target of evaluation **could be** compromised. The key properties depend on the target type, eg they are confidentiality, integrity and availability for information resources or quality, cost and delivery for suppliers and supplied services

The threat contrasts with a level of threat, which measures the likelihood of a threat materializing, based on historical incident data.

The categories of threat that should be considered depend of the type of target of evaluation. For example, for information resources, suppliers and supplied services typical threat categories are shown in the table below:

Target of evaluation type	Typical threat categories
Information resource	• Malfunctions of software or hardware • Loss of services, equipment or facilities • Overloads • Human error • Unforeseen effects of change

	• Other undesirable acts (eg access violations, virus attacks).
Supplier relationship, **Supplier,** **Supplied service**	• Commitments not met • Lack of professionalism • Significant disputes • Uncompetitive performance • Gross misconduct • Business interrupted

The threat categories for different target types can be fully customized in **Citicus ONE** and can be supported by underlying checklists of threat sub-categories.

See also Level of threat.

Threat area

Back to index

A threat or set of related threats (eg 'Overloads') listed as a bullet point on a risk scorecard presented by **Citicus ONE**.

Threat checklist

Back to index

A checklist defined by a basis of evaluation, to help evaluators complete the level of threat section of their scorecard. The checklists is displayed when the evaluator click a threat on the scorecard. It enables the evaluator to record which subordinate threats apply, at a lower level of detail than shown the scorecard.

Responses are 'rolled-up' to complete the corresponding question on the scorecard automatically.

Threat list

Back to index

A completion aid defined by a basis of evaluation, to help evaluators complete the level of threat section of their scorecard. This aid is displayed when the evaluator click a threat shown on the scorecard and presents subordinate threats, at a lower level of detail.

Threat rating

Back to index

See Level of threat rating.

Top management

Back to index

The board of directors of a company, its chief executive officer or someone who reports directly to him or her.

He, she or they should:

- insist on being kept informed about risk across the enterprise
- provide a mandate (and resources) for the risk management process
- periodically review a high-level report on the status of risk across the enterprise - which should highlight key areas of risk, improvements since the last period and priorities for action.

Why should top management adopt this role? Top management need to satisfy themselves that risk is being kept at an acceptable level as part of their commitment to good governance.

By reviewing the risk status of the enterprise – and being seen to do so – top management can exert pressure on people to get things right 'on the ground', thereby by reducing the:

- expense of avoidable incidents
- chances of **major** incidents occurring.

Triage

Back to index

A term based on the French word 'trier' – which means 'to sort out'. It was adopted by the allies in WWI – when there was considerable co-operation between French, British, US and other forces – to classify battlefield casualties for treatment. For example, wounded personnel might be classified as:

1. **Lightly wounded**, hence patched up and sent back into action
2. **Seriously wounded with a prospect of recovery**, where they would be hospitalized
3. **Seriously wounded with no prospect of recovery**, where they might be comforted and given pain relief but not hospitalized if there was a shortage of beds, transport or medical staff / facilities.

Nowadays, the term is still widely used within military and medical institutions and can be applied more widely to describe any method of sorting assets into risk-related classes which determine the treatment they will receive. In **Citicus ONE**, this term is used to describe the system's method of categorising targets of evaluation into classes which determine how the risk they pose should be treated.

Further details can be found in **Citicus ONE**'s **Glossary of system terms** under:

- Triage scheme
- Triage level
- Triage criteria
- Triage action
- Triage discipline
- Triage attribute.

Type of target of evaluation

Back to index

A class of asset, entity, activity, process or relationship that poses a risk to the enterprise which needs to be evaluated. A class might include:

- information resources*
- suppliers*
- supplier relationships*
- supplied services*
- sites*
- business processes
- business units
- privacy-related projects*
- projects.

These and similar classes can be set up in **Citicus ONE** and a basis of evaluation assigned to each one that specifies the precise issues to be probed when assessing risk.

* These classes are set up in **Citicus ONE** prior to delivery and can be evaluated 'out of the box'.

UK DPA

Back to index

Short for the UK Data Protection Act 1998. Subject to certain exemptions, this legislation imposes obligations on any private or public-sector organization that processes information which relates to a living individual who can be identified from that information either by itself or in conjunction with other information which is in the organization's possession.

In essence, the Act applies to organizations that process personal data in the UK. Compliance with the act is overseen by the UK Information Commissioner.

Unacceptable harm

Back to index

See level of unacceptable harm.

Unforeseen effects of change

Back to index

A type of event that afflicts IT-based information systems that may compromise the confidentiality, integrity or availability of information handled by one or more systems.

Such events become information incidents if they compromise the confidentiality, integrity or availability of information *in practice* ie if they lead to information being:

- disclosed to the wrong people
- falsified or otherwise corrupted
- rendered unavailable when needed to fulfil a business purpose.

Otherwise they represent a type of threat that needs to be considered when devising arrangements to protect the confidentiality, integrity or availability of information or evaluating risk.

The following table illustrates the types of change event that need to be considered.

Types of change event to consider
Unforeseen effects of introducing new / upgraded business applications
Unforeseen effect of changes to computer / communications equipment
Unforeseen effects of changes to user procedures
Unforeseen effects of changes to operating procedures
Unforeseen effects of organizational changes
Other changes having unforeseen effects

Please note:

- the types of change event presented in the table are ranked in order of likelihood (the most likely appearing first)
- the ordering reflecting the results of the Information Security Forum's Information Security Status Survey, 2000.

User

Back to index

A person authorized to access some or all of the information handled by an information resource. Types of user to consider are illustrated in the table below.

Categories of user	Types of user to consider
Internal business users	Employees of your organization (eg management, professional, technical, administrative, sales or production workers) Contract staff
External business users	Employees of corporate: • customers • agents or other market intermediaries • suppliers of products or services • competitors Employees of government departments or other public bodies Individuals: • personal customers • private citizens
IT staff	IT people who have access to information for: • day-to-day operations • maintenance • administration • development • change management • problem handling • back-up • recovery • other purposes
Reviewers	Specialists involved in conducting compliance, security or other reviews eg: • internal auditors • external auditors • information security practitioners • technical specialists • other reviewers.

Value

Back to index

An aspect of a target of evaluation identifying its tangible and intangible worth to the business, for example in terms of cash, goods, reputation, good will, brand loyalty or intellectual property.

VPC

Back to index

An abbreviation for value, performance and continuity – these aspects are used in assessing the criticality of targets of evaluation that pose a risk to the business which needs to be evaluated, other than information resource or suppliers (which can be evaluated in a compatible but more specific manner.

Vulnerability

Back to index

Vulnerabilities are circumstances (ie control weaknesses and other, special circumstances) that increase the likelihood of threats materializing (ie in the form of actual incidents).

Weighting

Back to index

A numerical method of emphasising the importance of some aspect of a phenomenon or set of data. This echoes the practice of adding extra weight to one side of a pair of scales to favour a buyer or seller, and needs to be used with caution.

By default, **Citicus ONE** applies weightings only when calculating criticality. The system of weightings is designed to segregate targets of evaluation into different bands so that heightened attention can be given to the ones that would cause:

- most damage to your business if a worst-case incident occurs
- unacceptable harm if availability or continuity is lost – or supplies delayed – for very short time periods.

To enable these factors to be combined into a single measure of criticality, the system weights criticality responses and timescales. These weightings were determined based on extensive analysis of data about the criticality of thousands of targets of evaluation ie they have a solid factual justification. They are as follows.

Criticality responses		Timescales	
Level of harm	Weighting	Timescale	Weighting
A - Extremely serious harm	60	Less than an hour	22
B - Very serious harm	30	About half a day	20
C - Serious harm	5	A day	18
D - Minor harm	1	2-3 days	7
E - No significant harm	0	A week	2.4
		A month+	1

Two additional weighting schemes are scheduled for delivery in a forthcoming release (structural weightings, specifiable weightings). Custodians and local co-ordinators can find details of these in the custodian **Help** topic entitled **Customizing the system | Scoring options**.

ENDS

Appendix Cross-references and terms of use

The entries in this glossary are presented on-line by **Citicus ONE**'s **Help** system. To aid comprehension, they are extensively cross-referenced.

Internal hyperlinks (ie those that point to other entries in this Glossary) are all active. Those referring to parts of the following components of **Citicus ONE**'s **Help** system have been re-routed to this Appendix so that this document can stand by itself.

Citicus ONE Help topics

Citicus ONE Glossary of system terms

Terms of use of this material

1. This agreement licenses you to use a document, presentation, spreadsheet or other material belonging to Citicus Limited ("the Material") that:

   a) Citicus provides "as is", by request, in order to help you deploy **Citicus ONE** successfully within your Organization

   b) does not form part of the **Citicus ONE** software or documentation.

2. Unless otherwise agreed, "your Organization" refers to the legal entity defined by your **Citicus ONE** Software Licence, Hosted Service Agreement or equivalent **Citicus ONE** access agreement.

3. **By using or copying the Material, you agree to be bound by the terms of this agreement. If you do not, advise Citicus immediately and do not use, copy or distribute the Material.**

4. Citicus owns title, copyright, and other intellectual property rights in the Material and reserves all rights not expressly granted to you in this agreement.

5. Provided you agree to be bound by and comply with the terms of this agreement, you may, for the purpose of deploying **Citicus ONE** in your Organization:

   a) hold, copy and distribute the Material within your Organization

   b) modify the Material or particular components of it

   c) incorporate the Material in its original or modified form in your own works and distribute them within your Organization.

6. You agree:

   a) that Citicus provides no warranty as to its fitness for purpose or merchantability; shall not be liable for direct, consequential or any other damages arising from its use; does not undertake to diagnose or remedy faults; and does not undertake to maintain the currency of the material

   b) to use the Material at your own risk

   c) to maintain a master repository of the Material which includes a copy of this agreement

   d) to acknowledge Citicus' ownership of the Material appropriately in each work in which it appears (for example, by incorporating the words "Internal use only" and either "Copyright © Citicus Limited. All rights reserved." or "Original material reproduced courtesy Citicus Limited." in its footer or Properties page).

7. You agree not to:

   a) use, copy or distribute the Material without acknowledgement

   b) permit use of the material for any purpose other than that stated in Clause 5 or by any parties other than employees of your Organization or contractors acting on its behalf

   c) distribute the Material in its original or modified form, either by itself or as part of any work, product or service, outside of your Organization

   d) incorporate the Material in works that could be considered improper or offensive.

8. This Licence shall be subject to the non-exclusive jurisdiction of the English Courts and shall be governed by and be interpreted in accordance with English Law.

9. This agreement is between Citicus Limited, a company registered in England number 4111746 with offices at Holborn Gate, 330 High Holborn, London WC1V 7QT, England, and your Organization.