Organisation of Certified Risk Managers

Fundamentals of Risk Management

Unit 1

1, Overview

It is a matter of definition that organisations exist for a purpose – perhaps to deliver a service, or to achieve particular outcomes. In the private sector the primary purpose of an organisation is generally concerned with the enhancement of shareholder value; in the central government sector the purpose is generally concerned with the delivery of service or with the delivery of a beneficial outcome in the public interest. Whatever the purpose of the organisation may be, the delivery of its objectives is surrounded by uncertainty which both poses threats to success and offers opportunity for increasing success.

Risk is defined as an uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks (the "inherent risks") and then responding to them.

The resources available for managing risk are finite and so the aim is to achieve an optimum response to risk, prioritised in accordance with an evaluation of the risks. Risk is unavoidable, and every organisation needs to take action to manage risk in a way which it can justify to a level which is tolerable. The amount of risk which is judged to be tolerable and justifiable is the "risk appetite".

Response, which is initiated within the organisation, to risk is called "internal control" and may involve one or more of the following:

- tolerating the risk
- treating the risk in an appropriate way to constrain the risk to an acceptable level or actively taking advantage, regarding the uncertainty as an opportunity to gain a benefit
- transferring the risk
- terminating the activity giving rise to the risk.

In any of these cases the issue of opportunity arising from the uncertainty should be considered.

The level of risk remaining after internal control has been exercised (the "residual risk") is the exposure in respect of that risk, and should be acceptable and justifiable – it should be within the risk appetite.

None of this takes place in a vacuum. Every organisation functions within an environment which both influences the risks faced and provides a context within which risk has to be managed. Further, every organisation has partners on which it depends in the delivery of its

objectives whether they be simply suppliers of goods which the organisation requires or direct partners in the delivery of objectives. Effective risk management needs to give full consideration to the context in which the organisation functions and to the risk priorities of partner organisations.

The management of risk at strategic, programme and operational levels needs to be integrated so that the levels of activity support each other. In this way the risk management strategy of the organisation will be led from the top and embedded in the normal working routines and activities of the organisation. All staff should be aware of the relevance of risk to the achievement of their objectives and training to support staff in risk management should be available.

Hierarchy of risk

Source: SU report Risk: improving government's capability to handle risk and uncertainty, Nov 2002

Managers at each level therefore need to be equipped with appropriate skills which will allow them to manage risk effectively and the organisation as a whole needs a means of being assured that risk management is being implemented in an appropriate way at each level. Every organisation should have a risk management strategy, designed to achieve its objectives. The application of that strategy should be embedded into the organisation's business systems, including strategy and policy setting processes, to ensure that risk management is an intrinsic part of the way business is conducted.

This course aims to provide an introduction to the range of considerations which apply in risk management, all of which can be applied at various levels ranging from the development of a strategic, organisation-wide risk policy through to management of a particular project or

operation. It is important to note that this course is *not* a detailed instruction manual for how to manage risk – its aim is simply to draw attention to the range of issues which are involved and to offer some general direction to help the reader think about how these issues may be addressed in the specific circumstances of their own organisation.

This course establishes *principles* of risk management. Organisations may choose to adopt particular standards (for example, the "Risk Management Standard" produced jointly by IRM, ALARM and AIRMIC in the UK, the Australian standard, CoSo, ISO 3100 or the Canadian government sector standard). More important than compliance with any particular Standard is ability to demonstrate that risk is managed in the particular organisation, in its particular circumstances, in a way which effectively supports the delivery of its objectives.

2, Identifying Risks

In order to manage risks, an organisation needs to know what risks it faces. Identifying risks is the first step in building the organisation's risk profile. There is no single right way to document an organisation's risk profile, but documentation is critical to effective management of risk.

The identification of risk can be separated into two distinct phases. There is:

- initial risk identification (for an organisation which has not previously identified its risks in a structured way, or for a new organisation, or perhaps for a new project or activity within an organisation), and there is;
- continuous risk identification which is necessary to identify new risks which did not previously arise, changes in existing risks, or risks which did exist ceasing to be relevant to the organisation (this should be a routine element of the conduct of business).

In either case risks should be related to objectives. Risks can only be assessed and prioritised in relation to objectives (and this can be done at any level of objective from personal objectives to organisational objectives). Care should be taken to identify generic risks which will impact on business objectives but might not always be immediately apparent in thinking about the particular business objective. When a risk is identified it may be relevant to more than one of the organisation's objectives, its potential impact may vary in relation to different objectives, and the best way of addressing the risk may be different in relation to different objectives (although it is also possible that a single treatment may adequately address the risk in relation to more than one objective). In stating risks, care should be taken to avoid stating impacts which may arise as being the risks themselves, and to avoid stating risks which do not impact on objectives; equally care should be taken to avoid defining risks with statements which are simply the converse of the objectives. A statement of a risk should encompass the cause of the impact, and the impact to the objective ("cause and consequence) which might arise.

Objective – to travel by train from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	**X** this is simply the converse of the objective
Being late and missing the meeting	**X** This is a statement of the impact of the risk, not the risk itself
There is no buffet on the train so I get hungry	**X** this does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	This is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	This is a risk which I cannot control, but against which I can make a contingency plan

The individual risks which an organisation identifies will not be independent of each other; rather they will typically form natural groupings. For instance, there may be a number of risks which can be grouped together as "resources" and further risks which can be grouped together as "environmental". Some risks will be relevant to several of the organisation's objectives. These groupings of risks will incorporate related risks at strategic, programme and operational levels. It is important not to confuse a grouping of risks with the risks themselves. Risks should be identified at a level where a specific impact can be identified and a specific action or actions to address the risk can be identified.

All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed; the risk owner may not be the person who actually takes the action to address the risk.

It is necessary to adopt an appropriate approach or tool for the identification of risk. Two of the most commonly used approaches are:

- Commissioning a risk review: A designated team is established (either in- house or contracted in) to consider all the operations and activities of the organisation in relation to its objectives and to identify the associated risks. The team should work by conducting a series of interviews with key staff at all levels of the organisation to build a risk profile for the whole range of activities (but it is important that the use of this approach should not undermine line management's understanding of their responsibility for managing the risks which are relevant to their objectives);

- Risk self-assessment: An approach by which each level and part of the organisation is invited to review its activities and to contribute its diagnosis of the risks it faces. This may be done through a documentation approach (with a framework for diagnosis set out through questionnaires), but is often more effectively conducted through a facilitated workshop approach (with facilitators with appropriate skills helping groups of staff to work out the risks affecting their objectives). A particular strength of this approach is that better ownership of risk tends to be established when the owners themselves identify the risks.

These approaches are not mutually exclusive, and a combination of approaches to the risk identification process is desirable – this sometimes exposes significant differences in risk perception within the organisation. These differences in perception need to be addressed to achieve effective integration of risk management at the various levels of the organisation.

3. Assessing Risks

There are three important principles for assessing risk:

- ensure that there is a clearly structured process in which both likelihood and impact are considered for each risk;
- record the assessment of risk in a way which facilitates monitoring and the identification of risk priorities;
- be clear about the difference between, inherent and residual risk.

Some types of risk lend themselves to a numerical diagnosis - particularly financial risk. For other risks - for example reputational risk - a much more subjective view is all that is possible. In this sense risk assessment is more of an art than a science. It will be necessary, however, to develop some framework for assessing risks. The assessment should draw as much as possible on unbiased independent evidence, consider the perspectives of the whole range of stakeholders affected by the risk, and avoid confusing objective assessment of the risk with judgement about the acceptability of the risk.

This assessment needs to be done by evaluating both the likelihood of the risk being realised, and of the impact if the risk is realised. A categorisation of high / medium / low in respect of each may be sufficient, and should be the minimum level of categorisation – this results in a "3x3" risk matrix. A more detailed analytical scale may be appropriate, especially if clear quantitative evaluation can be applied to the particular risk - "5x5" matrix is often used, with impact on a scale of "insignificant / minor / moderate/ major/ catastrophic" and likelihood on a scale of "rare / unlikely / possible / likely / almost certain". There is no absolute standard for the scale of risk matrix - the organisation should reach a judgement about the level of analysis that it finds most practicable for its circumstances. Colour ("Traffic Lights") can be used to further clarify the significance of risks.

	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	11	16	20	23	25
Likely	7	12 2	17	21 2	24
Possible	4	8	13 1	18 1	22 2
Unlikely	2	5 1	9	14	19 5
Rare	1	3	6	10	15 1

At the organisational level risk appetite can become complicated, but at the level of a specific risk it is more likely that a level of exposure which is acceptable can be defined in terms of both a tolerable impact if a risk is realised, and tolerable frequency of that impact. It is against this that the residual risk has to be compared to decide whether or not further action is required. Tolerability may be informed by the value of assets lost or wasted in the event of an adverse impact, stakeholder perception of an impact, the balance of the cost of control and the extent of exposure, and the balance of potential benefit to be gained or losses to be withstood.

Thinking about risk frequently focuses on residual risk (ie- the risk after control has been applied which, assuming control is effective, will be the actual exposure of the organisation. Residual risk, of course, will often have to be re-assessed – for example, if control is adjusted. Assessment of the *anticipated* residual risk is necessary for the evaluation of proposed control actions.

Care should also be taken to capture information about the *inherent* risk. If this is not done the organisation will not know what its exposure will be if control should fail. Knowledge about the inherent risk also allows better consideration of whether there is over-control in place – if the inherent risk is within the risk appetite, resources may not need to be expended on controlling that risk. This need to have knowledge about both inherent and residual risk means that the assessment of risk is a stage in the risk management process which cannot be separated from addressing risk; the extent to which the risk needs to be addressed is informed by the inherent risk whereas the adequacy of the means chosen to address the risk can only be considered when the residual risk has been assessed.

Risk assessment should be documented in a way which records the stages of the assessment. Documenting risk assessment creates a *risk profile* for the organisation which:

- facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves);
- captures the reasons for decisions made about what is and is not tolerable exposure;
- facilitates recording of the way in which it is decided to address risk;
- allows all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it;
- facilitates review and monitoring of risks.

Once risks have been assessed, the risk priorities for the organisation will emerge. The less acceptable the exposure in respect of a risk, the higher the priority which should be given to addressing it. The highest priority risks (the key risks) should be given regular attention at the highest level of the organisation, and should consequently be considered regularly by the Board. The specific risk priorities will change over time as specific risks are addressed and prioritisation consequently changes.

4, Risk Appetite

The concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk (the uncertainty) being considered is a threat or an opportunity:

- When considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure becomes a reality and finding an acceptable balance;
- When considering opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

It should be noted that some risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example many organisations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases the organisation needs to make *contingency plans.*

In either case the risk appetite will best be expressed as a series of boundaries, appropriately authorised by management, which give each level of the organisation clear guidance on the limits of risk which they can take, whether their consideration is of a threat and the cost of control, or of an opportunity and the costs of trying to exploit it. This means that risk appetite will be expressed in the same terms as those used in assessing risk. An organisation's risk appetite is not necessarily static; in particular the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time.

The concept of risk appetite can be further analysed into three categories:

Corporate Risk Appetite

Corporate risk appetite is the overall amount of risk judged appropriate for an organisation to tolerate, agreed at board level. This may not be just one statement: OGC, for example, look at 5 key risk areas (policy/guidance risk; people and internal systems risk; propriety, regularity, finance and accountability risk; reputation risk; external risk) and make a statement on risk appetite for each. The Board and senior managers should judge the tolerable range of exposure for the organisation and identify general boundaries for unacceptable risk

(or at least for risks that should always be referred to/ escalated up to the Board for discussion and decision when they arise.

Delegated Risk Appetite

The agreed corporate risk appetite can then be used as a starting point for cascading levels of tolerance down the organisation, agreeing risk appetite in different levels of the organisation. The effect of this is that what is considered a high level of risk at one level will be a lower level of risk to a higher level of management. This facilitates both a risk escalation process for the taking of risk decisions when delegated boundaries are met , and empowers people to innovate within their delegations;

Project Risk Appetite

Projects that fall outside of day-to-day business of an organisation might need their own statement of risk appetite. Different types of projects might also require different levels of risk appetite, for example an organisation may be prepared to accept a higher level of risk for a project that would bring substantial reward.

Different types of project could be:

- Speculative (akin to venture capitalism in the corporate sector): with high risks but potentially high rewards, e.g. Invest to Save Budget projects; Pilot projects. It may be that the bulk of these projects are unsuccessful but important lessons are learnt.
- Standard development projects: for example IT, procurement, construction, etc.
- Mission critical' projects: where organisations need to be sure of success.
- The level of risk appetite will obviously vary, with a speculative project prepared to take on higher levels of risk than a "Mission Critical" project.

Effective management and application of delegated risk appetite requires escalation processes. It is possible to set 'trigger points' where risks can be escalated to the next level of management as they approach or exceed their agreed risk appetite levels. The next level up in the hierarchy would then take appropriate action, which may mean managing the risk directly, or could mean adjusting the level of risk that they are happy for the level below to manage. It is also often the case that a higher level of management, with a wider portfolio of risk to manage, has more scope to accept higher risks in particular areas as they can offset them against other lower risks in their portfolio.

Further applications of the concept of risk appetite include:

Resource allocation

Once the risk appetite level is set, it is possible to review if resources are targeted appropriately. If a risk does not correspond to the agreed risk appetite, resources could be focused on bringing it to within the tolerance level. Risks which are already within the agreed tolerance level could be reviewed to see if resources could be moved to more risky areas without negative effects.

Project initiation

When taking the decision whether to initiate a new project, and when undertaking, risk appetite can be used as a course on whether to proceed with the project and also to help identify and manage risks which may impede the success of the project.

5, Addressing Risks

The purpose of addressing risks is to turn uncertainty to the organisation's benefit by constraining threats and taking advantage of opportunities. Any action that is taken by the organisation to address a risk forms part of what is known as "internal control". There are five key aspects of addressing risk:

Tolerate

The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

Treat

By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk, action (control) is taken constrain the risk to an acceptable level. Such controls can be further sub-divided according to their particular.

Transfer

For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organisation or because another organisation is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk.

Terminate

Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can

be achieved. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

Take the Opportunity

This option is not an alternative to those above; rather it is an option which should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats, an opportunity arises to exploit positive impact. For example, if a large sum of capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be re-deployed.

The option of "treat" in addressing risk can be further analysed into four different types of controls:

Preventive Controls

These controls are designed to limit the possibility of an undesirable outcome being realised. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls. The majority of controls implemented in organisations tend to belong to this category. Examples of preventive controls include separation of duty, whereby no one person has authority to act without the consent of another (such as the person who authorises payment of an invoice being separate from the person who ordered goods prevents one person securing goods at compnay expense for their own benefit), or limitation of action to authorised persons (such as only those suitably trained and authorised being permitted to handle media enquiries prevents inappropriate comment being made to the press).

Corrective Controls

These controls are designed to correct undesirable outcomes which have been realised. They provide a route of recourse to achieve some recovery against loss or damage. An example of this would be design of contract terms to allow recovery of overpayment. Insurance can also be regarded as a form of corrective control as it facilitates financial recovery against the realisation of a risk. Contingency planning is an important element of corrective control as it is the means by which organisations plan for business continuity / recovery after events which they could not control.

Directive Controls

These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided - typically associated with Health and Safety or with security. Examples of this type of control would be to include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.

Detective Controls

These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, "after the event" so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks (which detect whether stocks or assets have been removed without authorisation), reconciliation (which can detect unauthorised transactions), "Post Implementation Reviews" which detect lessons to be learnt from projects for application in future work, and monitoring activities which detect changes that should be responded to.

In designing control, it is important that the control put in place is proportional to the risk. Apart from the most extreme undesirable outcome (such as loss of human life) it is normally sufficient to design control to give a *reasonable assurance* of confining likely loss within the risk appetite of the organisation. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to constrain risk rather than to eliminate it.

6, Reviewing and Reporting Risks

The management of risk has to be reviewed and reported on for two reasons:

- To monitor whether or not the risk profile is changing;
- To gain assurance that risk management is effective, and to identify when further action is necessary.

Processes should be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed, report significant changes which adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process should be subjected to regular review to deliver assurance that it remains appropriate and effective. Review of risks and review of the risk management process are distinct from each other and neither is a substitute for the other. The review processes should:

- ensure that all aspects of the risk management process are reviewed at least once a year.
- ensure that risks themselves are subjected to review with appropriate frequency (with appropriate provision for management's own review of risks and for independent review/audit);
- make provision for alerting the appropriate level of management to new risks or to changes in already identified risks so that the change can be appropriately addressed.

A number of tools and techniques are available to help with achieving the review process

- Risk Self Assessment (RSA) is a technique which has already been referred to in the identification of risk . The RSA process also contributes to the review process. The results of RSA are reported into the process for maintaining the organisation-wide risk profile. (This process is also sometimes referred to as CRSA "Control and Risk Self Assessment");

- "Stewardship Reporting" requires that designated managers at various levels of the organisation report upwards (usually at least annually at the financial year end, and often on a quarterly or half yearly interim basis) on the work they have done to keep risk and control procedures up to date and appropriate to circumstances within their particular area of responsibility. This process is compatible with RSA; managers may use RSA as a tool to inform the preparation of their Stewardship Report.

- The "Risk Management Maturity Model", produced by Investors in Risk Management and other risk management companies, provides a tool for evaluating the maturity of an organisation's risk management.

In addition to these formal tools, individuals, work groups and teams should constantly by considering the risk issues which they face in the work they are doing.

Internal Audit's work provides an important independent and objective assurance about the adequacy of risk management, control and governance. Internal audit may also be used by management as an expert internal consultant to assist with the development of a strategic risk management process for the organisation. It will have a wide ranging view of the whole range of activities which the organisation undertakes, and will already have undertaken some form of assessment to inform its planning of systems and processes to be audited. However it is important to note Internal Audit is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff who have executive responsibility for the achievement of organisational.

Many organisations have specialist review and assurance teams which have been established for a particular purpose (for example, Accounts Inspection Teams, or Compliance Review Teams). Their work contributes to the assurances available about the risk and control systems in use in the organisation. "Stewardship" assurance mechanisms, whereby line managers give account of their stewardship of their areas of responsibility, are also important, especially in organisations with highly devolved control structures.

The Audit Committee should be asked by the Accounting Officer /Board to:

- gain assurance that risk, and change in risk, is being monitored;
- receive the various assurances which are available about risk management and consequently delivering an overall opinion about risk management;
- comment on appropriateness of the risk management and assurance processes which are in place.

However it should be noted that the Audit Committee should not itself own or manage risks and is, as with internal audit, not a substitute for the proper role of management in managing risk.

Some organisations may establish a Risk Committee. The Board need to decide what role it wants to assign to the Risk Committee

7, Communication and Learning

Communication and learning is not a distinct stage in the management of risk; rather it is something which runs through the whole risk management process. There are a number of aspects of communication and learning which should be highlighted.

Communication within the organisation about risk issues is important:

- It is important to ensure that everybody understands, in a way appropriate to their role, what the organisation's risk strategy is, what the risk priorities are, and how their particular responsibilities in the organisation fit into that framework. If this is not achieved, appropriate and consistent embedding of risk management will not be achieved and risk priorities may not be consistently addressed;
- There is a need to ensure that transferable lessons are learned and communicated to those who can benefit from them. For example, if one part of the organisation encounters a new risk and devises an effective control to deal with it, that lesson should be communicated to all others who may also encounter that risk;
- There is a need to ensure that each level of management, including the Board, actively seeks and receives appropriate and regular assurance about the management of risk within their span of control. They need to be provided with sufficient information to allow them to plan action in respect of risks where the residual risk is not acceptable, as well as assurance about risks which are deemed to be acceptably under control. As well as routine communication of such assurance there should be a mechanism for escalating important risk issues which suddenly develop or emerge.

Communication with partner organisations about risk issues is also important, especially if the organisation is dependent on the other organisation not just for a particular contract but for direct delivery of a service on behalf of the organisation. Misunderstanding of respective risk priorities can cause serious problems – in particular leading to inappropriate levels of control being applied to specific risks, and failure to gain assurance about whether or not a partner organisation has implemented adequate risk management for itself can lead to dependence on a third party which may fail to deliver in an acceptable way.

It is important to communicate with stakeholders about the way in which the organisation is managing risk to give them assurance that the organisation will deliver in the way which they expect, and to manage stakeholder expectation of what the organisation can actually deliver.

Glossary of key terms

The glossary below provides definitions for commonly used risk management terminology.

- Permission to produce extracts from Vigilant Risk Manager is granted by the Vigilant Risk Manager.
- Text has been used from The Orange Book under Crown copyright.

The ISO 31000:2009 has been used as the primary source of definitions.
Where the Standard does not include a definition of a particular term, other sources have been used.

Communication and consultation
Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk

Consequence
Outcome of an event impacting objectives

Control
Measure that modifies risk

Control assessment
Systematic review to ensure that controls are still effective and appropriate

Enterprise-Wide Risk Management (ERM)
An integrated approach to assessing and addressing all risks that threaten the achievement of the organisation's strategic objectives; the purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks.

Establishing the context
Defining the external and internal parameters to be taken into account when managing risk and setting scope and risk criteria for the risk management policy

Event
Occurrence or change of a particular set of circumstances

Exposure
Extent to which an organisation and/or stakeholder is subject to an event

External context
External environment in which the organisation seeks to achieve its objectives

Frequency
Number of events or outcomes per defined unit of time

Hazard
A source of potential harm

Internal audit
Independent, objective assurance and consulting activity designed to add value and improve an organisation's operations…accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of: (1) Risk management (2) Control, and (3) Governance processes. (IIA Professional Practices Framework)

Internal context
Internal environment in which the organisation seeks to achieve its objectives

Key control indicator (KCI)
Measures or metrics that demonstrate a change in a specific control's effectiveness

Key performance indicators (KPIs)
Metrics or measures used to monitor changes in business performance in relation to specific business objectives (e.g. volumes of business, revenue etc.)

Key risk Indicators (KRI)
Measures and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of the risk occurring

Level of Risk
Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

Likelihood
Chance of something happening

Loss
Any negative consequence or adverse effect, financial or otherwise

Monitoring
Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

Probability
Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Residual risk
Risk remaining after risk treatment

Review
Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

Risk
Effect of uncertainty on objectives

Risk acceptance
Informed decision to take a particular risk

Risk aggregation
Combination of a number of risks into one risk to develop a more complete understanding of the overall risk

Risk analysis
Process to comprehend the nature of risk and to determine the level of risk

Risk appetite
Amount and type of risk that an organisation is willing to pursue or retain

Risk assessment
Overall process of risk identification, risk analysis and risk evaluation

Risk attitude
Organisation's approach to assess and eventually pursue, retain, take or turn away from risk

Risk aversion
Attitude to turn away from risk

Risk avoidance
Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

Risk criteria
Terms of reference against which the significance of risk is evaluated

Risk description
Structured statement of risk usually containing four elements:
sources, events, causes and consequences

Risk evaluation
Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk financing
Form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

Risk identification
Process of finding, recognising and describing risks

Risk management
Coordinated activities to direct and control an organisation with regard to risk

Risk management audit
Systematic, independent and documented process of obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework or any selected part of it is adequate and effective

Risk management framework
Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management plan
Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Risk management policy
Statement of the overall intentions and direction of an organisation related to risk management

Risk management process
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk matrix (or heat map)
Tool for ranking and displaying risks by defining ranges for consequence and likelihood

Risk mitigation
Measures taken to reduce an undesired consequence

Risk owner
Person or entity with the accountability and authority to manage a risk

Risk perception
Stakeholder's view on risk

Risk profile
Description of any set of risks

Risk reduction
Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk

Risk register
Record of Information about identified risks

Risk reporting
Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

Risk retention
Acceptance of the potential benefit of gain, or burden of loss, from a particular risk

Risk severity
A measure of the magnitude of a risk, based on a combination of the likelihood and consequence of a risk

Risk sharing
Form of risk treatment involving the agreed distribution of risk with other parties

Risk source
Element which alone or in combination has the intrinsic potential to give rise to risk

Risk tolerance
Organisation's or stakeholder's readiness to bear the risk, after treatment, in order to achieve its objectives

Risk treatment
Process to modify risk

Stakeholder
Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity