Institute of Operational Risk

Operational Risk Sound Practice Guidance

Risk Control Self Assessment

March 2010

The Institute of Operational Risk

Established in January 2004, the Institute of Operational Risk is a professional body dedicated to the **promotion of skills and standards** associated with Operational Risk Management.

Membership is available to Operational Risk practitioners at all levels and there are four grades of membership: Fellow, Professional Member, Member and Associate.

The Institute supports its members through the provision of:

- **High standards -** against which membership and professional competency is judged
- **External events -** for the promotion of ideas, ongoing professional development and networking
- **Research -** to assist the above and ensure the continual improvement of methods, techniques and knowledge
- **A Knowledge Centre** – the development of a robust and informative knowledge centre for operational risk management
- **Sound Practice Guidance** – the development of a series of Sound Practice Guidance papers providing the know-how for a variety of risk management practices

Members are located in the UK, Europe, Middle East, Nigeria, South Africa, Hong Kong, Australia and New Zealand**.**

To find out how membership can benefit you, visit our website: www.ior-institute.org

Sound Practice Guidance Papers

It is the intention of the Institute of Operational Risk that the Sound Practice Guidance papers be updated and improved from time to time. If any reader of any Sound Practice Guidance has any experience or opinions that they believe may enhance the guidance offered, they should email standards@ior-institute.org.

Table of Contents

Title: Risk Control Self Assessment	Date issued: 10 March 2010
	Version: 0.51
File name: IOR RCSA Final Version	Update date: 03 Jan 2010

1. The Development of RCSA

1.1. Origins

In September 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a four volume report entitled *Internal Control— Integrated Framework*. This report presented a common definition of internal control, providing a framework against which internal control systems could be assessed and improved and later became a standard that U.S. companies now use to evaluate their compliance with the Foreign Corrupt Practices Act (FCPA).

Around the same time in the UK, the Combined Code and Turnbull guidance was under development, requiring UK companies to demonstrate a sound system of internal control and risk management and to review the effectiveness of their internal controls, providing a meaningful disclosure within their annual accounts.

These two initiatives largely lead to the creation of Risk Control Self Assessment (RCSA) and have since become an integral element of a firm's overall operational risk management and control framework.

1.2. Overview

The aim of an operational risk framework is to identify, assess, control and mitigate operational risk and to champion effective reporting of risk and emerging risk issues.

RCSA forms an integral element of the overall operational risk framework, as it provides an excellent opportunity for a firm to integrate and co-ordinate its risk identification and risk management efforts and generally to improve the understanding, control and oversight of its operational risks.

RCSA provides a systematic means of identifying control gaps that threaten the achievement of defined business or process objectives and monitoring what management is actually doing to close these gaps. It is therefore an integral component of good operational risk management.

The findings from a RCSA can be used to formulate appropriate action plans to address identified control gaps, taking into account risk-reward (cost-benefit) considerations. With progress against these plans monitored as part of the overall operational risk management approach. In this respect RCSA promotes analysis and monitoring of factors that affect the level of operational risk exposure.

A further driving force behind the growth and emergence of RCSA is the fact that RCSA acts as a complementary audit and management tool, as well as being the generally accepted means to satisfy corporate governance and regulatory requirements.

1.3. Benefits / Value Add

A well designed and properly managed RCSA programme will offer significant insight into a firm's risk and control environment.

Specifically, it will provide:

- A mechanism to place front line responsibility for operational risk management and control directly with management (where it firmly belongs!);
- A common language and common set of values across the organisation;
- Clear and specific ownership of action plans;

- Open discussion of risk and control matters amongst staff and management, leading to better transparency and understanding of risk and its implications across the business; and
- Cultural change, helping operational risk management to become embedded at all levels of the organisation, with respect to both day to day activities and longer term business decision making.

However, the RCSA needs to be carefully designed, planned and executed to provide the maximum opportunity for success and achievement of its full range of benefit potential.

2. Generic Characteristics of an RCSA Approach

The core generic characteristics of a typical RCSA will consist of:

- The identification of business objectives, which can be defined either in terms of business targets or process delivery goals;
- The identification of risks that could threaten the achievement of those objectives and the activities and processes affected by the different risks identified;
- Identifying the controls in place intended to prevent the risks from crystallising;
- Determining where responsibility for performing those controls lies; and
- An assessment of the effectiveness of the controls in operation and the level of residual risk remaining after control.

It is often beneficial to consider structuring the RCSA in order to risk assess an entire process or business line from 'end to end' (as per the principles established by SOx 404), or to define the RCSA by specific location e.g. where a standard process may be operating in different geographic locations such as the account opening procedure within branches of a building society.

2.1. Risks

Operational risks are sometimes referred to as a firm's intrinsic or inherent potential exposure and in addition to the internal environment, should consider factors arising from the external environment including industry trends as well as taking into account any 'upstream' or newly emerging risks. New risks can emerge daily and may take on new dimensions, for example, consider how internet security, phishing, privacy and discrimination risks have escalated in recent years.

As a rule of thumb the term 'risk' is generally defined as something that has not yet caused a direct operational problem for the firm however there remains some degree of uncertainty concerning future outcomes. Whereas 'issues' or 'events' are more commonly referred to as actual problems, that have materialised within the work environment. When prompted to identify key business 'risks', most people have an almost natural inclination to identify 'issues' that they know are current problems in the workplace. Firms are thus well advised to provide some guidance to aid the internal understanding of the differences between risks, issues and events.

Also, some firms find it valuable to outline high level categories of operational risk in order to identify more specific risks linked to a particular activity, whilst others might use headings such as governance, reporting and compliance to facilitate their risk identification process.

For the purposes of self-assessment (and indeed throughout the whole operational risk framework), other ways of characterising and describing risks beyond specific event categories should also be considered. For example, examining cause and effect factors can provide major

insights into a firm's risk profile and are often useful in identifying the most effective risk management mitigation strategies (in terms of cost of correction and level of risk reduction).

Alternatively the identification of 'risk drivers' can be good indicators of how the risk profile of a firm is changing. Risk drivers tend by their very nature to be more forward looking and thus predictive of future issues. There are many 'risk driver' categories and a few of the more common ones may include people, customer satisfaction, transaction volumes, level of organisational change, and balance of manual vs. automated processing. These risk driver categories can be widely encompassing for example 'people' drivers can incorporate staffing levels, skills-sets and effectiveness measures. Also risk drivers need to take into consideration external factors in their measurement of risk. If a firm has not already defined its own internal operational risk classifications it may find it useful to adopt the classification defined by the Basel Committee in the Capital Requirements Directive.

Firms should also understand the distinction between inherent risks (risk environment before consideration of any existing controls); residual risks (after consideration of the effectiveness of controls currently in place); and issues / events (those risks that have crystallised into specific observable unintended consequences) and consider capturing these different aspects within the RCSA itself.

2.2. Controls

The capture of 'key' controls in the RCSA is critical in defining and understanding which controls the firm relies upon for effective operational risk management. The definition of 'key' controls being: those controls that provide the most defence against a particular risk.

Controls can be categorised, the most common being:

- Preventative – preventing a risk from happening, for example 'input of an incorrect postcode preventing the user from continuing the transaction'. This category of controls can also be called 'before the event' or 'ex-ante' controls;
- Detective – detects a risk that might or has happened, for example 'an exception report'. This category may also be called 'after the event' or 'ex-post' controls.

Examples of typical controls within both a financial and a non-financial services sector firm will include management oversight, segregation of duties, KPIs, policies and procedures, training, diversification, outsourcing, supply chain management and capacity management.

These are just a few common examples. Many more controls will be in place depending on the nature and operating environment of the firm.

2.3. Design and Operating Effectiveness

Once controls are defined they should be aligned to risks, which in turn are associated with business objectives or processes. Sometimes controls are inappropriate (i.e. not suited to the risk to be controlled) and so can hinder the accomplishment of business or process objectives. Alternatively, if there are unnecessary layers of controls in light of the nature and extent of the risk to be managed (over-control), this can introduce inefficiencies and even additional operational risk, in the case of performance errors.

An effective RCSA will facilitate the identification of:

- 'Over' or 'inappropriate' control, as well as areas of missing control (design effectiveness) and
- Poorly executed control (operating effectiveness).

To this end, it can be useful to rate each control or set of controls as either 'effective', 'defective' or 'excessive' (or 'strong', 'adequate', 'poor', where an evaluation of 'poor' could include excessive control). This may make it easier to identify where there is a need to modify controls and help shape the subsequent action plans resulting from the RCSA.

Risks assessed as insufficiently controlled i.e. posing an unacceptable level of risk exposure, should be subject to corrective or mitigating actions to bring the residual risk exposure to a more tolerable level. On the other hand, if there are risks that are identified from the RCSA as being over-controlled, then consideration should be given to reallocating control resources to risk areas that are inadequately managed.

It is important to record, track and measure the efficiency gains achieved through decisions taken as a direct result of RCSA to reduce over-control, e.g. full time equivalent (fte) savings in time spent on streamlining a specific activity or process, or the creation of a 'shared services' function centralising controls previously operating in multiple business areas. This helps to highlight the practical benefits of RCSA and thus increase management buy-in.

2.4. Verification of Control Assessments

RCSA can incorporate explicit verification of the effectiveness of controls e.g. one technique is to assign a control owner with responsibility for testing whether the controls are working in practice. The control owner will physically test the controls and report back. Where controls are deemed ineffective then consideration should be given to whether the controls are appropriately or adequately designed in the first instance or whether the problem is in the execution.

An RCSA that incorporates evidence of testing of controls is useful in support of Sarbanes Oxley (SOx) requirements, although a formal framework for the recording and testing of SOx 404 controls will need to be established where a firm has SOx 404 obligations.

2.5. Risk Assessment

RCSAs, by their nature, contain an element of assessment of operational risk exposure.

Some firms use inherent risk scoring (i.e. assessment of a risk before controls are put in place) and residual risk scoring (after existing controls have been applied) as an important part of the RCSA process. The expected outcome is that residual risk will be lower than inherent risk, depending upon the extent and effectiveness of the controls in place.

- In identifying a firm's inherent risk profile is should be noted that the techniques and disciplines of inherent risk estimation can be extremely subjective and difficult to quantify, although it can allow the firm to explicitly evaluate the benefit of controls by demonstrating the level of exposure in the absence of controls. This can be useful in justifying future 'spend' on improving controls.

Other firms may simply use the RCSA to assess the level of their current (residual) operational risk exposure as it stands given the controls already in place, without trying to imagine a situation of 'no' control. This approach recognises that an understanding of the inherent risk profile is **not** essential in order to identify improvements required to existing controls to manage the risk exposure to the desired level. Accordingly, an assessment approach on this basis is well suited to existing operational risk management activities and the identification of any current control gaps that are in need of remediation. It can also be supplemented by a firm's actual 'loss event' experience (where controls might be re-evaluated in the light of actual loss events).

Irrespective of the starting point (inherent risk or current risk profile), often a 'target' level, or score, is set by the business for residual risk exposure. If the 'target' level is lower than the current assessed residual risk level, the aim is to reduce the current residual risk down to a more

acceptable level (acting as an indication of the appetite for that particular risk in that particular activity). Once the required control improvements have been put in place, the residual risk level will be reassessed to determine whether the 'target' level has now been achieved, with further control enhancements made as necessary until this is the case.

3. RCSA Approaches and Techniques

There are essentially three key approaches to performing an RCSA, namely workshop, questionnaire or hybrid. However there is no 'right' or 'wrong' way to implementing RCSA. Each firm should select whichever approach, or combination of approaches, best suits its governance, culture, operating environment, size, complexity, structure and geographical dispersion. The respective sections below set out the key advantages of each approach.

However, experience shows that any approach can be successfully implemented in any type or size of firm, provided that there is sufficient commitment to the concept of RCSA from the top down (executive and senior management level), as well as across the lower levels of the firm.

3.1. Workshop Approach

A workshop approach to RCSA can help to bypass some of the more detailed paperwork sometimes associated with the process, although appropriate and relevant data capture is an important part of the exercise. A workshop is a mechanism to get people engaged in talking about their risks, controls and required improvements. They also bring 'events' into focus and can be run in conjunction with business process checklists and procedural reviews.

The benefits of a workshop approach include:

- Raising awareness of cross functional and hierarchical risks;
- Enabling the assessment and improvement of 'softer' control mechanisms e.g. communications, training and accountability; and
- Providing an opportunity for the transfer of risk management skills across the organisation.

3.1.1. Planning

It is probably self-evident that preparation is key to the successful outcome of any RCSA workshop.

As a broad indication the following areas provide some generic pre-requisite considerations that should be worked through prior to undertaking specific workshops.

Topic	Action required
Evaluate which business areas to address first	Interviews with participants Review of audit reports Identify high risk areas (take risk based approach) Review of internal loss events
Workshop objectives	Clearly define workshop objectives / process under evaluation
Getting Executive support	Set up Steering Group Request Line Executive to open workshop / attend selected parts
Detailed process / controls expertise	Invite Subject Matter Experts (SMEs) / specialists to workshops
Facilitator	Professionally trained RCSA facilitator who is impartial / could come from another business area or external consultant
Interlinking processes	Attendance by properly selected / empowered staff who have vested interest as part of 'end to end' process
Standardised workshop documentation	Pre-defined by Group Op Risk function / Internal Audit Use in all workshops to ensure a consistent approach
Getting corrective action	Ensure line management approval and ownership of workshop output including the documentation of action points and target dates
Key issues reporting	Ensure that a mechanism is in place for the upward reporting of key issues (e.g. a report to the Operational Risk Committee) & ongoing oversight by IA

It is also important to provide guidance to participants in advance of the workshop so that they fully understand the context and objectives of the exercise and indeed the contribution they are expected to make.

3.1.2. Who Should Attend

For a workshop to deliver an accurate assessment of risks and controls and indeed to avoid a silo approach to RCSA, it is important to include appropriate representation from all areas of the firm. This is particularly key if the process under review features controls that are carried out in different business areas; as the accuracy of the assessment reached could be materially impacted without input and experience from all relevant business areas.

For example, a workshop review of the product development area should invite representatives from Sales, Marketing, Research & Development, IT and Finance and should include subject matter experts and those in specialist roles, It is also recommended that the outputs from the whole RCSA programme be independently reviewed for both consistency of approach across different business areas and also to identify firm-wide themes that may require escalation. This activity is generally undertaken in larger firms by a 2nd or 3rd Line of Defence (LOD) function, for example a Group Risk or Internal Audit function.

3.1.3. Pros and Cons of Inviting Management

The decision on whether to include management within the workshops will most likely depend on the culture within the firm.

Whatever the decision, management's input to the discussions and workshop outputs should be sought at some stage. Indeed it is their 'sign up' and agreement to the outputs that is required in carrying conviction to deliver on the actions.

Some 'pros' of having Management attend a workshop are:

- They can help endorse or sanction the requirement to undergo the RCSA process and demonstrate management support for the process;
- It enables a manager-multi staff communication opportunity that may not otherwise exist; and
- It provides management with an opportunity to genuinely encourage and empower their staff to take responsibility.

Some 'cons' of having Management attend a workshop are:

- They may have conflicting views on what is said at the workshop and become defensive;
- Staff may not want to openly give their opinions in front of management; and
- Political or sensitive issues may not get aired.

The role of the facilitator is key at each workshop event and the ability to keep an open dialogue at all times between all participants, including management, is most important. It is not generally encouraged to hold separate meetings for management outside of the workshops, however there are opportunities for management to demonstrate their support for the overall process more publicly e.g. via senior management Town Hall meetings.

3.1.4. How Many Should Attend

There is no magic optimal number of participants. However groups of between 6 and 12 (at maximum), tend to work best.

3.1.5. Thematic Structure of Workshops

It is advisable to try to structure the workshop into distinct sections (which can take place in separate sessions), so as to help keep the discussion relevant and focussed and not to over-burden participants or lose momentum. Ideally, the coverage of the workshop can be broken down into a maximum of 3 modules as follows:

- Module 1 – risk identification and profiling of known risk issues;
- Module 2 – control identification and residual risk assessment;
- Module 3 – action planning and ownership.

By focussing discussion at the workshops on these core aspects (i.e. risks, controls and action planning), other additional requirements such as control testing, defining the ownership of risks and controls and determining control adequacy and effectiveness can be finalised post-workshop. In all cases, it is critical to remember that responsibility for, and ownership of, the business objectives, processes, risks and controls and their proper identification lies with the business. The workshop is merely a tool designed to assist them in discharging that responsibility effectively.

3.1.6. Terminology

Successful and effective RCSA workshops require the use of easily digestible language. Not everyone understands risk or audit speak so definitions of objectives, risks and controls should be simply articulated to ensure everyone understands what the workshop is aiming to achieve. Furthermore, where there is cross-functional participation, activity specific jargon should also be avoided.

For example consider articulating requirements around core concepts using illustrative language, like:

- Objectives – 'the reasons why the activity/function exists' e.g. to provide 1st class customer service information;
- Risks – 'things that can and sometimes do go wrong when trying to deliver the objective' e.g. lack of knowledge to be able to answer a customer's query; and
- Controls – 'things we must do and/or have in place to stop risks from happening' e.g. product training.

These types of articulation will be received far better than generic risk terminology, particularly for operational staff attending a risk workshop for the first time, thereby helping to engender engagement from the start.

3.1.7. Top Down and Bottom Up

To benefit from a comprehensive approach to RCSA throughout the firm a combined 'top down' and 'bottom up' approach works well. This allows for themes identified at Executive level to be cascaded down throughout the business, with appropriate actions being captured within lower level RCSA outputs and responsibilities assigned to individuals for delivering and monitoring them.

Equally themes identified at lower level RCSA workshops should have an escalation route up to senior management in order to provide visibility of potential newly emerging threats that may require Executive consideration. For this process to be effective the firm must have in place an appropriate means of monitoring operational risk e.g. Operational Risk (OR) Committees, OR Steering Groups who meet regularly and have oversight responsibility for managing operational risk.

As noted in Section 2 earlier, it can be beneficial to structure the RCSA approach so as to scope out 'end to end' processes or specific business lines, capturing key controls that operate across different areas of the business. (If a business area or function reviews only its own specific areas of control, sometimes key controls operating cross-functionally can be overlooked). This end to end type of approach to RCSA offers benefits through greater visibility to a wider audience and can lead to the identification of widespread improvements across entire processes, in addition to creating local departmental improvements, thus providing greater efficiencies to the overall operating effectiveness of the firm.

3.1.8. How Many Sessions Should Be Run

There is no predefined number of individual assessments that a firm should aim to produce from RCSA. However, in order to ensure all aspects of the operational risks that a firm may face are identified, it can be useful to start with an Executive RCSA workshop, often more strategic in nature, that the Executive Committee (ExCo) or equivalent agree to participate in. This should then be followed up with more specific workshops e.g. focusing in turn on each individual ExCo member's area of responsibility.

Further workshops can then be rolled out as required drilling down into the firm's hierarchy e.g. the next level might focus on the direct reports of each ExCo member and so on. How much lower this rollout goes within the firm is discretionary but should at the end of the day demonstrate that the process is sufficiently embedded to provide assurance that both operational risk and the associated control environment is being monitored effectively. Care should be taken so as not to create an industry from this type of approach but to generate the value added benefits that RCSA can provide.

3.1.9. How Long Should the Workshop Last

There is no set rule for how long a workshop should last as generally this depends on how much time managers and the other participants are willing to invest in the exercise.

However as a 'rule of thumb' sessions of 3 to 4 hours duration seem to work well in practice.

3.1.10. Ground Rules

It is always advisable to establish some core ground rules at the start of a workshop.

These can be as basic as the following:-

- Checking venue, seating, equipment;
- Agreeing/clarifying the agenda and objectives;
- Clarifying how outputs will be recorded, summarised & captured and by whom;
- Agreeing next steps.

It is also advisable to remind attendees that their participation is essential to the success of the workshop but to respect each other's contributions, for example by all means 'challenge' but respectfully. The facilitator should ensure that only one conversation at a time takes place, ask clarifying questions as necessary and seek group consensus. Participants should be encouraged **not** to bring blackberry or mobile phones into workshops wherever possible to allow them to focus fully on the task in hand, without the distraction of day to day operational matters.

3.1.10.1. Facilitation and Other Required Key Skills

The role of the facilitator is an important one with expert facilitation required not only for RCSA workshops but also for the validation and challenge of the RCSA outputs post-workshop, usually undertaken by other 2nd and 3rd Line of Defence (LOD) independent review functions such as Information Security and Internal Audit.

Some firms prefer to facilitate their own internal RCSA assessments whilst others will look to the support of Internal Audit or the Risk function to facilitate this activity on their behalf. Either approach is acceptable providing it is fully understood that ownership of the workshop outputs and any subsequent actions arising, belongs with the business.

The role of the facilitator requires a specific skill-set as outlined in the table below.

RCSA Facilitator	
Role of RCSA facilitator is to:- • Maintain the 'flow' during a workshop and ensure rules and procedures are adhered to • Maintain discipline • Help the group manage their time • Record decisions and actions • Act as devil's advocate • Engender group discipline • Ensure involvement of the entire group so everyone has the chance to have their say • Act as arbiter and ensure balanced input	**Basic skills-set required:-** • Active listening skills • Ability to clarify and check understanding by asking questions • Sort, prioritise and organise issues for discussion • Ability to assert authority and maintain control at all times • Problem solve • Accurately record outputs • Ability to maintain open dialogue with all members of the group

3.1.11. Data Collection

To aid the collation and consolidation of outputs from a workshop, it is strongly recommended that a laptop and overhead projector screen is used to capture information during the event.

It is generally advisable to use a facilitator's assistant to perform this task. Not only does it allow participants to see that their comments are being captured accurately and hence is more professional but it also requires much less 'post workshop' time and effort to deliver the results back to them for confirmation.

3.2. Questionnaire Approach

Some firm's have found benefits in establishing extensive, comprehensive standard questionnaires with questions allocated to respondents based upon the relevance of the activities under their responsibility. Others have developed overall conceptual frameworks for questionnaire based RCSAs, with each function setting its own questions with Corporate or Group Operational Risk functions overseeing the completeness of the questionnaires and responses.

Questionnaire based RCSAs can add value by demonstrating:

- An understanding of operational risk roles and responsibilities of each area of the organisation;
- Identification of the operational risks faced; and
- Evaluation of the residual, uncontrolled risk by a comparison of the actual controls that are in existence and their performance versus the optimal set of controls (or control standards).

3.2.1. Structuring the Questionnaire

The structure of an RCSA questionnaire should ensure complete coverage of a firm's operational risks and provide benchmark standards against which to evaluate how well these are being managed.

This can be delivered by:-

- Defining roles and responsibilities for managing operational risk across the firm.
- Defining risk/control objectives i.e. what the firm is trying to achieve in respect of the management of the different operational risks it faces by means of the controls in place;
- Determining the standard controls that should be performed around each risk/control objective and use the RCSA questionnaire to determine the extent to which those controls are in place (i.e. design effectiveness);
- Evaluation of the quality of actual control performance via questionnaire responses to determine the operating effectiveness of the controls in place;
- Reviewing the results of the questionnaire (both design and operating effectiveness) as the basis for estimating the residual operational risk profile after controls and use this to determine the nature and priority of any remediating actions that are necessary to address unacceptable levels of residual (uncontrolled) risk exposure.

3.2.2. Timing and Regularity

The recommended minimum frequency of performance is once a year, although twice a year or even more often may be appropriate depending on the compliance objectives of the RCSA. Timing and regularity should be determined by the purpose of the RCSA and any co-dependencies, for example SOx or other applicable regulatory reporting requirements.

In addition, there should be a mechanism in place for targeted ad hoc performance, if there is a significant change in the perceived risk profile, for example 'due to a change in the operating environment (internal or external)' *or* 'introduction of new business activities or new products'.

3.2.3. Effective Questions (Structure and Number)

Questions can be standard or non-standard:

- Standard questions are those written centrally, based on the nature of the risk being evaluated such that all functions responsible for managing that particular operational risk respond to the same standard question, making comparison and consolidation of results easier.
- Non-standard questions, on the other hand, would be written by each RCSA respondent function, such that similar operational risks across different parts of the organisation may have different questions, but those questions have more relevance to the responding function as they are written in the function's own terminology.

The choice between the two approaches will be influenced by the degree of maturity of the firm's operational risk management framework.

Where line buy-in remains a concern, it may be better to adopt a non-standard approach, giving greater ownership of the questionnaire definition to the respondent functions, with subsequent independent validation by the central operational risk management function.

Whether standard or non-standard, effective questions should be structured around the inherent risks of each function's activities (i.e. those operational risks that the function is responsible for managing on behalf of the firm).

Ideally questions should be structured so they can be answered *Yes* or *No* (or occasionally, *Not Applicable*), with *No* and *Not Applicable* answers subject to further explanation, to ensure responses have been provided for all risks and for ease of interpretation of results. The interpretation of a *Not Applicable* response is that the risk being evaluated by the question was not within the scope of responsibility of the respondent function in the period covered by the RCSA, for reasons that should be explained.

The number of questions should be limited to that necessary to understand whether the control standards applicable to each operational risk have been executed such that the risk/control objective has been met.

3.2.4. Effective Responses (Style, Respondent and Hierarchical Sign-off)

To be effective, a response should be explanatory, pertinent and corroborated.

Reasons should be provided for *Not Applicable* responses to help refine the questionnaire and ensure a clear understanding of the sub-set of risks and controls under the respondent's responsibility and where de facto management/execution responsibility lies (if not with the respondent). This in turn helps determine that there is management ownership of all operational risks of the organisation and whether the ownership is appropriate.

Whilst responses should be provided by those fairly close to the day to day management of the risk to provide an accurate picture, hierarchical sign-off is important to ensure that the significance of issues flagged up i.e. 'no responses' is put into proper perspective and any concentration of issues across respondents is identified.

Implementing a sign-off hierarchy gets around any strategic or 'big-picture' knowledge gaps of the questionnaire respondents. Further, hierarchical sign-off allows issues to become known throughout the management/governance structure, at levels of detail commensurate with the signatory's position in the hierarchical structure.

3.3. Hybrid Approach

Hybrid formats tend to be launched via an initial workshop approach followed in future periods by a questionnaire format for subsequent RCSA exercises, with a further workshop if a new activity or major trigger event occurs. A hybrid approach can often be successful in maintaining momentum / keeping the process alive over time without overburdening the participants (see also section 5 - Keeping it Alive).

4. Effective Use of RCSA within a Fully Integrated Operational Risk Management Framework

It is extremely informative to consider the individual findings from an RCSA exercise to help identify areas in need of improved control, clusters/concentrations of risk, duplication of controls or other forms of over-control and raise awareness of cross functional risks, through comparison of the results across different functions.

However, the results and findings from the RCSA can also be used in conjunction with other components of the operational risk framework (e.g. internal event data, external loss data and scenario analysis) to permit enhanced insight into the firm's operational risk profile.

The ability to provide a coherent, integrated view of the operational risk profile of the firm is not only highly desirable but a 'must' in today's regulatory environment. The more the individual components of the framework provide consistent indicators of where the risks of the firm lie and the likelihood of events and their severity, the more effective will be the design and the operation of the overall framework.

4.1. RCSA and Internal Loss Data

RCSA results can help to highlight areas that are susceptible to operational risk loss events in the future (e.g. via the identification of control gaps). Conversely, operational risk loss (or event) data tracking can supplement the management information provided by the RCSA by comparing the frequency and occurrence of actual events to the residual risk profile implied by the RCSA results. Where the incidence of event occurrences is consistent with the areas of exposure identified from the RCSA, this provides some reassurance as to both the quality of the RCSA and the data collection process.

If this is not the case, for example 'significant losses are being experienced in areas that the RCSA results suggest are not a cause for concern', the firm should look again at how the RCSA is being executed, to ensure the correct people are involved and that they have a proper understanding of the process and are executing it conscientiously. If the RCSA results predict a high risk of loss, but there are in fact no, or few, events occurring, the firm may want to look again at the data collection process, to check completeness of capture and also, as necessary, the execution of the RCSA.

In the banking sector, Basel 2 has been a key driver in encouraging firms to undertake root cause analysis of operational risk events, although for most this is an area where there remains scope for improvement. Root cause analysis can provide valuable information on observed risks and their drivers, which can be compared to those that have been identified through the RCSA process. As necessary, that is where relevant risks are not already captured in the RCSA, they should be incorporated into the process and subject to assessment.

4.2. RCSA and External Data

Firms may find it useful to use the RCSA results to identify areas of risk vulnerability where they may benefit from considering external data to fast-track their understanding of the potential impact of the weaknesses identified, drawing on the experiences of 3rd party organisations. Also external data can be a useful input towards ensuring that the firm has properly identified its inherent risks, by allowing it to expand the breadth of risks it considers beyond those of its own experience.

4.3. RCSA and Scenario Analysis

Control weaknesses and areas of risk exposure identified through the RCSA are a valuable source of input for scenario analysis. Similarly, the process of defining and assessing risk scenarios may lead to identification of risk factors not currently captured within the RCSA that should be.

4.4. Keeping It Alive (post RCSA exercise)

Focus on keeping the RCSA approach fresh and simple. Once senior management's buy-in has been obtained it is vitally important to maintain momentum and interest.

There are many additional ways of maintaining momentum and stakeholder 'buy-in' and 'keeping the process alive' within the firm, other than simply repeating the workshop approach, for example:

- Consider the creation of a 'benefits log' to capture the business improvements and efficiency savings defined by the initial RCSA exercise;
- Build RCSA into business as usual activities, as a regular feature on the agenda of management meetings, reinforcing business ownership of risks;
- Encourage Internal Audit to use RCSA outputs to support their focus of activity;
- Develop, measure and monitor Key Risk Indicators (KRIs) to better monitor the firm's RCSA risk profile and exposure; and
- Take the opportunity to complete a new RCSA exercise following any significant change in the firm's structure or external operating environment.

4.5. Central Risk Repository

Consider establishing a central operational risk repository (database) across the firm. Not only does this make refreshing of the RCSA output easier to establish but it also enforces consistency of data capture and can provide a central common risk event and key control library together with standardised risk reporting functionality for use both within individual business areas and also by a centrally led Group Operational Risk function.

4.6. Action Plans

Firms should take the opportunity to create Risk Mitigation Plans (RMPs) from RCSA outputs that are directly aligned to their strategic and business planning. That way, RCSA outputs will continue to maintain their relevance as they will always be a cross-reference to ongoing senior management strategic and operational activity.

The RMP should always be based on sound risk/reward judgements, such that proposed actions to address a risk or control gap are commensurate with the potential impact as a result of events resulting from that risk/control gap. For example, it is not worth spending £1 million to fix a control gap that is assessed as representing a risk of loss of £100,000. In such an example, the RMP should be appropriately scaled so that there is a sound cost-benefit trade-off.

4.7. Reporting and Follow-up

Where the value added from RCSA really comes into its own is through the ongoing monitoring of the operational risk profile and exposure via senior management at Operational Risk Committees, Steering Groups and senior business management team meetings, supported by regular reporting.

There are many different forms of reporting that the firm may find useful (see examples in section 7) and, in fact, it is likely that a combination of different formats will be required – according to the audience for the reporting:

- Narrative reports

- Scorecards
- Heat Maps/Traffic Light Reports
- Dashboards

As a general rule, less detail should be reported the more senior (high level) the audience. Rather, the focus should be on the more significant areas of risk/control weakness that have the greatest potential to damage the firm and prevent it from achieving its business and strategic objectives.

Conversely, reporting for line managers can contain more detail as the additional information may be helpful to them in determining the best course of action and for the purposes of detailed monitoring of progress of RMPs against agreed milestones and deliverables.

Also, whatever the level of the audience, emphasis should be placed on keeping it simple, (e.g. use simple rather than complex grading of risks and controls and do not include data that is not relevant).

4.8. Measurement of RCSA – Quantitative vs. Qualitative

Banks and other financial institutions acknowledge the importance of operational risk and of the requirement for proper risk measurement including allocation of economic capital for operational risk. Indeed the new Basel Accord has been much delayed in view of industry comments and feedback, indicating the need for further review and more quantitative impact studies – currently this debate is on-going. Whilst quantification is an essential ingredient of qualification for AMA banks in the context of calculating regulatory capital, it remains a very challenging area for smaller firms.

To consider the use of RCSA as a tool that provides a direct contribution to the evaluation of an operational risk capital charge may be tenuous, however, in the interim, Group Operational Risk functions continue to attempt to identify global hotspots within their respective firms through the use of RCSA and endeavour to make informed decisions through the consolidation of aggregated operational risks despite the fact that operational risk is inherently an empirical rather than a mathematical science.

4.9. RCSA and Internal Audit Engagement

The introduction of RCSA within a firm will provide a beneficial effect on the practice of Internal Audit by facilitating a more transparent and risk-focused approach to Internal Audit.

For example:-

- Through Management taking on more responsibility for the maintenance of the control environment allowing auditees to then understand the purpose of controls and risk management;
- Allowing auditors to accomplish better control assessment (RCSA becoming a mechanism to improve Internal Audit's efficiency and effectiveness);
- Internal Audit assisting the RCSA exercise by contributing to the validation of estimates (for example, effectiveness of controls);
- RCSA helping to drive the Internal Audit programme of scheduled reviews via a risk based perspective.

Thus each of the above striving to consolidate stronger collaboration, engendering the same risk language and agreement of 'high risk' areas across the organisation.

5. Appendices

5.1. Specimen Templates

5.1.1. Workshop Record Example No 1

RISK & CONTROL ASSESSMENT

Risk Ref	Risk Description	Key Controls	Control Owner	Residual Risk Rating	Within Appetite?	Further Action required to reduce exposure?
12c	Significant disruption to normal business operating environment	• Business Continuity plans in place and regularly reviewed • Plans tested annually • Telephone call cascade tested quarterly	AN Other	Amber	No	Yes
13a	Breach of client data confidentiality	• Data Security policy in place and regularly reviewed • Independent monitoring of adherence to Policy • Escalation of non-compliance • Breach register	JF Security	Green	Yes	No

5.1.2. Workshop Record Example No 2

ACTION PLAN IDENTIFIED

Risk Ref	Risk Description	Current Residual Risk Rating	Treatment Plan	Action Plan Owner	Target Date for Completion	Expected Residual Risk Rating Post Completed Action
Outside Risk Appetite						
12c	**Significant disruption to normal business operating environment**	**Amber**	**Introduce desktop walkthrough exercises twice a year**	AN Other	**x/x/2010**	**Green**

5.1.3. Heat Map Report

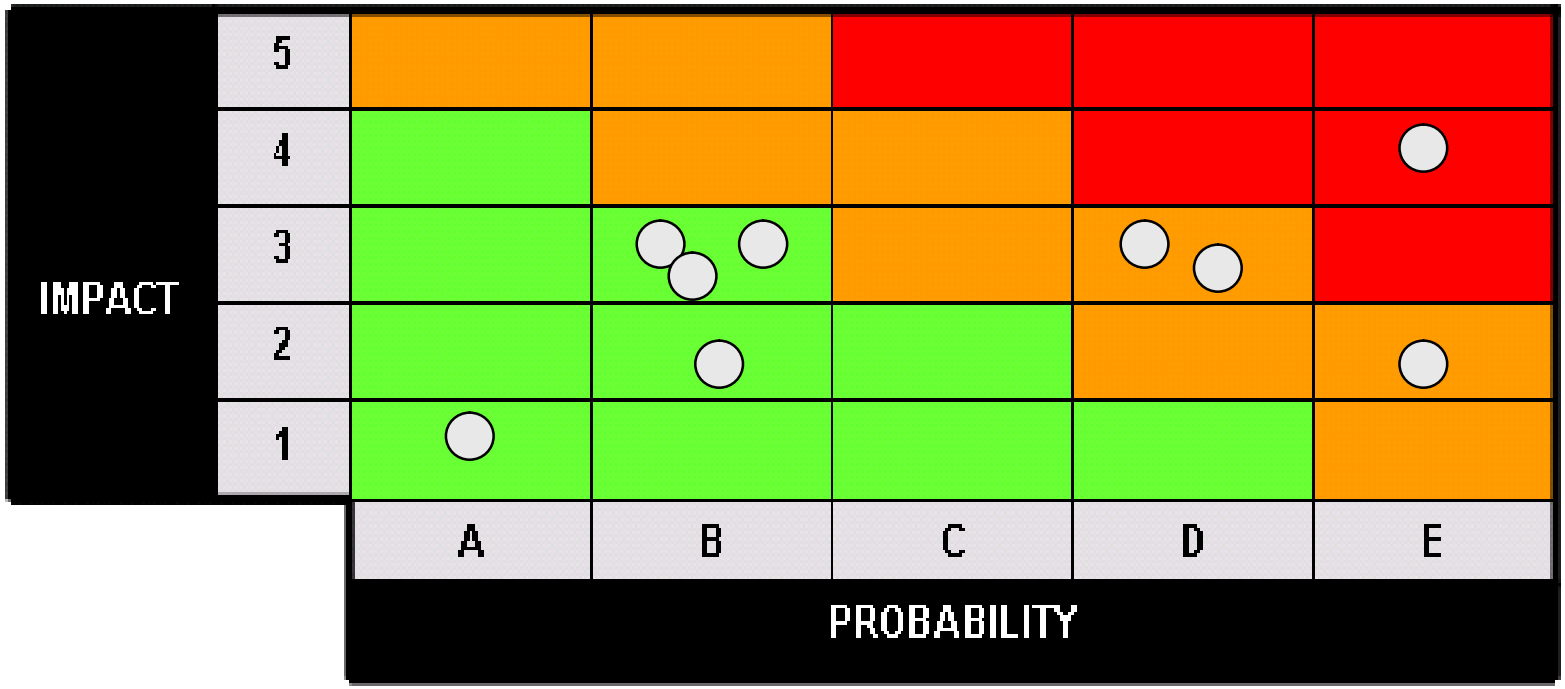
A TYPICAL KEY TO AN OPERATIONAL RISK PROBABILITY AND IMPACT ASSESSMENT

PROBABILITY (or likelihood of a risk crystallising over a certain time period)

A – Rare (10-25yr period) B – Unlikely (5-10yr period) C- Possible (1-5yr period) D – likely (once a year) E – Frequent (multiple times a yr)

IMPACT (measured here from a financial perspective but could equally be measured in terms of customer or reputational impact)

1= £10-100K 2 = £100K-1M 3 = £1-5M 4 = £5-10M 5 = >£10M



5.1.4. Example Questionnaire

EXAMPLE EXTRACT TAKEN FROM QUESTIONNAIRE EXAMINING ACCESS CONTROLS WITHIN AN IT ADMIN FUNCTION

	Question:	Yes	No or n/a	If No or n/a pls provide comment
1.	**ACCESS CONTROL**			
1.1	Are you satisfied that your Admin IT Hardware and Software is located as securely as possible and adequate security measures are taken to prevent theft (e.g. security marking of hardware)?			
1.2	Is written permission required before staff are allowed to take hardware or sensitive data off-site?			
1.3	Do you have a formal procedure to record, approve and regularly review computer access?			
1.4	Do the access levels awarded to members of staff only reflect what they need in order to carry out their work?			
1.5	Is your Admin Network purely internal to the establishment i.e. it does not have any external links (e.g. links to the internet or dial up facilities)?			
1.6	Are your Admin machines and your curriculum machines on separate networks?			
1.7	Are you satisfied that all reasonable security measures have been taken to prevent unauthorised access to your admin network (either internally or by external access)?			
1.8	Are staff instructed not to use Admin. IT equipment or software unless they are authorised to do so?			
1.9	Are staff given good practice guidance on password security (e.g. password length, change frequency etc.)?			
1.10	Are procedures in place that ensure visitors are appropriately escorted whilst on the premises?			

5.1.5. Example RCSA End to End Process Evaluation Assessment

Supplier & Location		
Supplier Contact		
Service being investigated		
	Risk *(Define the associated risk)*	**Pre-Production** *Pre-Production relates to activities that occur prior to the creation of the product or service being sourced at the Supplier.*
1	**Supplier failure to meet pre-contractual deliverables**	Does the Quality File include all specific required documents? *Refer to Supplier Requirements for list of documents, I.e. Design Review docs*
2		How does the supplier incorporate learning from field experiences into their engineering activity?
3		Does the Supplier have a well defined process flow chart?
4		Has Control Plan been submitted and accepted? *Check that last revision has been incorporated.*
5		Have bottlenecks been identified and addressed?
		Sub-Supplier Management
6	**Lack of adeqaute supplier contingency to ensure delivery**	Does the Supplier have a effective sub-supplier approval process? *Check the sub-supplier corrective action requests...*
7		Have all purchased components, materials and services from sub-suppliers been approved by the supplier through a formal process? *Check Initial Samples reports for each component and material*
8		In case of subcontracting, did the supplier audit the sub-supplier process, and does the sub-supplier deliver a Conformance Report to the supplier?
9		Does the supplier perform an Incoming Inspection? Is it according to the Control Plan? *Non-conformances effectively handled in corrective action sys tem?*
10		How does the supplier document the receipt of materials and services? *Receipts are in local business system and includes quantity, lot numbers, receipt date, …information that supports part traceability*
11		Is there a sub-supplier performance-Quality, Delivery, monitoring process defined and used for improvement? *Also check the criteria and responsiveness of sub-suppliers in case of customer complaints, Sub-supplier corrective action requests.*
		Production/Service Execution
12	**Lack of adequate 3rd party QA processes**	Are all special characteristics checked by a mistake proofing or process control methods like Statistical Process Control? *Applicable in case the component has special characteristics.* *If not controlled by mistake proofing, are containment plans and corrective actions in place? Is this documented in the Control Plan?*
13		Are customer approved master samples available at required workstations? *Applicable if this has been requested.*
14		Does the packaging used in production comply with safety requirements? Does it protect efficiently components and materials?
15		Is a disposal system in place for rejected material/components? *Check that bins are marked with a color code for easy identification*
16		How does the supplier monitor process effectiveness and implement changes for improvement?
		Logistics
17	**Inadequate Service Level Agreements or lack of specific Terms & Conditions**	Is the supplier able to receive and understand order releases and delivery dates? *Check EDI or web connections - Ask the supplier to review last release*
18		Are packaging and shipping instructions clearly posted at point of operations, and are they known by operators? *Check that they are in conformance with Product/Process Control Plan. Do they adequately detail how to perform the operations and what to inspect? Check for customer complaints/warranty claims from errors in packaging and shipment.*

