Risk and Control Self Assessment

Operational Risk Sound Practice Guidance

SWORD GRC

VLERICK BUSINESS SCHOOL

THE INSTITUTE OF OPERATIONAL RISK

An IRM Group Company

Foreword

The Institute of Operational Risk (IOR) was created in January 2004 and became part of the Institute of Risk Management in 2019. The IOR's mission is to promote the development of operational risk as a profession and to develop and disseminate sound practice for the management of operational risk.

The need for effective operational risk management is more acute than ever. Events such as the global financial crisis or the COVID-19 pandemic highlight the far-reaching impacts of operational risk and the consequences of management failure. In the light of these and numerous event organisations must ensure that their policies, procedures, and processes for the management of operational risk meet the needs of their stakeholders.

This guidance is designed to complement existing standards and codes for risk management (e.g. ISO31000). The aim is to provide guidance that is both focused on the management of operational risk and practical in its application. In so doing, this is a guide for operational risk management professionals, to help them improve the practice of operational risk in organisations. Readers looking for a general understanding of the fundamentals of operational risk management should start with the IOR's Certificate in Operational Risk Management.

Not all the guidance in this document will be relevant for every organisation or sector. However, it has been written with the widest possible range of organisations and sectors in mind. Readers should decide for themselves what is relevant for their current situation. What matters is gradual, but continuous improvement.

The Institute of Operational Risk Sound Practice Guidance

Although there is no one-size-fits-all approach to the management of operational risk, it is important that organisations benchmark and improve their practice on a regular basis. This is one of a series of papers, which provides practical guidance on a range of important topics that span the discipline of operational risk management. The objectives of these papers are to:

- explain how to design and implement a 'sound' (robust and effective) operational risk management framework
- demonstrate the value of operational risk management
- reflect the experiences of risk professionals, including the challenges involved in developing operational risk management frameworks.

Contents

1. Introduction

The Risk and Control Self Assessment (RCSA) is an integral part of most operational risk management frameworks. RCSAs provide a structured mechanism for estimating operational exposures and the effectiveness of controls. In so doing RCSAs help organisations to prioritise risk exposures, identify control weaknesses and gaps, and monitor the actions taken to address any weaknesses or gaps.

A well designed and implemented RCSA can help to embed operational risk management across an organisation, improving management attitudes towards operational risk management and enhancing the overall risk culture. In contrast, an inefficient or unnecessarily complex RCSA can damage the reputation of the (operational) risk function and reinforce the perception that operational risk management is a bureaucratic, compliance-focused, exercise that does not support the achievement of organisational objectives.

It cannot be emphasised enough that an effective RCSA is much more than a technical exercise. Though RCSAs can, and should, be used to help assess, even quantify where necessary, operational risk exposures. They are equally important as a mechanism for promoting open discussions about operational risk. Many operational risks are hard to identify, let alone quantify, this is because of a lack of accurate loss data and because new risks emerge on a regular basis. Equally the effectiveness of specific controls can be hard to assess accurately. However, despite these difficulties, operational risks and their associated controls must not be ignored. Organisations that discuss, openly, their operational risks and the effectiveness of their associated controls should be better prepared for what the future holds, improving the proactivity of their operational risk management activities.

An effective RCSA can also help support the governance and compliance activities of an organisation. The results of an RCSA provide assurance to the governing body and regulators that an organisation has in place a sound system for the management of operational risks. Equally, RCSAs can support the work of internal and external auditors helping them to prioritise audit attention and structure audit reports.

Finally, RCSAs can help to improve business efficiency. Weaknesses or gaps in controls can increase the chance of system and process failures and the impact of external events, increasing costs and the potential for disruption. In contrast, an excessive level of control can slow down systems and processes unnecessarily.

2. RCSA Fundamentals

There are many ways to approach the design and implementation of an RCSA. Organisations should take time to review the options and select the approach that works best for the nature, scale, and complexity of its activities, as well as its risk culture.

Despite this variety, many fundamental decisions need to be made. These fundamentals are discussed below.

2.1. Application and scope

The first key decision is whether to require RCSAs for some or all of the operational risks to which an organisation is exposed.

The common default option is to require that all identified operational risks should be subject to a RCSA. This ensures that the results of the RCSA are as comprehensive and complete as possible. However, given that the number of discrete operational risk exposures may number in the 100's or 1000's across an organisation it can be very time consuming and expensive.

Alternative options include:

1. Limiting the granularity of the RCSA. Organisations that categorise their operational risks may, for example, decide that they need only be completed for the 'level 1' risks in their categorisation (see the IOR Sound Practice Guidance Paper on Operational Risk Categorisation). This ensures that RCSAs are completed for all categories of operational risk but ensures that the number of assessments is limited. The downside of this approach is that it may lack sufficient detail for some users of RCSA information (e.g. internal audit, department management, etc.)
2. Limiting the focus to the significant operational risk exposures that threaten the achievement of an organisation's objectives. Such an approach will provide the information required by the governing body and senior management, but it will not help the department or divisional management to manage their local operational risks effectively.
3. Limiting the focus to the significant operational risk exposures that threaten the achievement of department or function objectives. This ensures that department and divisional managers get the information they need to manage local risk exposures. In addition, an escalation process may be implemented to ensure that risks, significant enough to threaten the whole organisation, are reported to the governing body/senior management.

Combinations of the above three approaches may be used to further refine the application and scope of a RCSA. For example, option 2 might be conducted using the level 1 risks in a categorisation, option 3 the level 2 risks to increase granularity.

As in any risk management activity, the costs and benefits of a more or less comprehensive RCSA approach must be considered. A fully comprehensive approach is not necessarily best, especially if it results in information overload and requires excessive amounts of time and effort to complete. RCSAs should only be used where they are value-adding, meaning that the benefits must exceed the costs.

2.2. Process or event focus

Most operational RCSAs are conducted on an event basis. This means that they are linked to specific risk events such as fire, fraud, injury, hacking attack, power failures, etc. For more on the nature and categorisation of risk events please refer to the IOR's guidance paper on operational risk categorisation.

An alternative is the process basis. This approach involves mapping organisational processes and identifying potential points of failure within these processes (e.g. the potential for human error or systems failure). A process focus increases alignment between operational risk management and the day-to-day operations of an organisation. In so doing it may be perceived as more relevant to my management and can be used to link effective operational risk management to business process efficiency.

The downside of a process approach is the time required to map processes. The greater the detail, the more comprehensive will be the set of identified operational risk exposures. However detailed process maps can take a considerable amount of time and expertise to complete accurately.

Where an organisation has detailed process maps in place already it is recommended that these are used as the basis for identifying operational risks for RCSA. However, where such maps are not in place, the costs involved in creating them are likely to be excessive.

2.3. Roles and responsibilities

Usually, the RCSA process will be 'owned' by the (operational) risk function. This means that the (operational) risk function will be responsible for the design of the RCSA and for overseeing its implementation to ensure that the tool is used correctly. This may include documenting the RCSA process, providing coaching and training on how to conduct RCSAs, and facilitating RCSA workshops (see 4.1.4 below).

Table 1 summarises the other roles and responsibilities concerning RCSAs. For more on roles and responsibilities for operational risk please refer to the IOR's guidance on Operational Risk Governance.

Role	Responsibility
Governing body	Ensuring that an appropriate system of internal control is in place. This may include receiving assurance on the effectiveness of the RSCA approach and reviewing the results of RSCAs for significant operational risk exposures.
Senior management	Responsible for supporting the work of the board. This includes ensuring that an effective RCSA approach is in place. Where present the Chief Risk Officer (CRO) will have primary responsibility for overseeing the design and implementation of the RCSA.
Risk owner	Responsible for the completion of RCSAs, ensuring that exposures are within appetite/tolerance and that there are no significant weaknesses or gaps in controls. Risk owners may either complete the RCSA themselves or delegate the responsibility to suitably qualified individuals. Risk owners must also oversee the completion of any actions required to address control weaknesses or gaps.

Control owner	Responsible for the design, implementation, and maintenance of effective controls. Should provide information to risk owners on any weaknesses or gaps in controls. Should also ensure that action is taken to address any identified weaknesses in the controls they own.
Data owner	Responsible for providing data to risk and control owners to enable them to complete the RCSA.
Control owner	Ensure the design and implementation of the RCSA to senior management and the governing body.

Table 1: Other roles and responsibilities for RCSAs

Roles and role terminology may differ in organisations. Some may not use terms like risk, control, or data owner. Where this is the case it will be important to identify individuals responsible for the following:

- The production of timely, accurate and complete RCSAs
- The identification of control weaknesses or gaps
- Providing the data required to complete effective RCSAs
- Overseeing actions to address control weaknesses or gaps

2.4. Frequency and timing

Once completed for the first time RCSAs should be reviewed regularly to ensure that they remain up-to-date. An annual review and update is the most common frequency. But frequencies ranging from one month to one year are normal.

The frequency chosen by an organisation will depend on the dynamics of its operational risk exposures. The more frequently they change the more frequently RCSAs must be reviewed.

Organisations may complement a full annual review with ad-hoc updates for risks that change significantly within a year. That way RCSAs may be kept up-to-date while keeping completion costs to a minimum.

Ideally, RCSAs should be updated before annual reviews of organisational or departmental/ divisional objectives and budgets. That way information from RCSAs can be feed into performance and budgetary reviews, helping to embed operational risk management within the strategic activities of an organisation.

3. Designing an RCSA

The design of an RCSA influences its success or failure. Key is weighing the costs and benefits of additional comprehensiveness or complexity. The more elements that are added to an RCSA the longer it will take to complete, requiring more time and resources.

3.1. Common elements of an RCSA

Common elements of an RCSA are outlined below. Each of these elements represents a different aspect of an organisation's operational risk exposures. Not all RCSAs will contain every element. As mentioned above it is important to balance the benefits of an RCSA with the costs of completion, especially if they are updated regularly.

3.1.1. Risk (probability and impact) matrix

Most RCSAs include a qualitative assessment of risk exposure use an ordinal scale for probability and impact, then combine these into a simple risk matrix. These scales typically range from 1-3 (Low, Medium, and High) up to 1-5. But any numerical range is possible. These are commonly referred to as 3x3, 4x4 or 5x5 risk matrices.

The key point about an ordinal scale is that data is shown in order of magnitude only, meaning that 2 is larger than 1. With an ordinal scale, it is not possible to determine how much bigger 2 is than 1 because there is no standard of measurement for the differences between these two values. Sporting leagues are another example of ordinal scales. It is possible to say that the team at the top is the best team, but not how much better this team is relative to the others in the league. Table 2 illustrates a simple 3x3 ordinal scale risk matrix for probability and impact.

Probability		Impact	
1	Rare	1	Low
2	Possible	2	Medium
3	Frequent	4	High

Probability	Impact			
		1	2	3
	1	1	2	3
	2	2	4	6
	3	3	6	9

Table 2: Example ordinal scale 3x3 risk matrix

To assist in the use of ordinal scales, points of reference should be provided to help users decide on the scale of probability and impact. A simple example is provided in Table 3.

Probability		Impact	
Rare	Chance of occurrence not expected to exceed once every 5 to 10 years	Low	The financial loss not expected to exceed 1% of cash flows and can be easily absorbed into day to day running costs
Possible	Chance of occurrence not expected to exceed once every 1 to 5 years	Medium	Financial loss between 1% to 5% of cash flows and may require moderate cost-cutting
Frequent	Chance of occurrence expected to exceed once per year	High	Financial loss exceeds 5% of cash flows and may require major cost-cutting or the cancellation of strategic projects.

Table 3: Example points of reference for qualitative exposure assessments

Organisations should always determine their points of reference for impact. These should be linked to the size of the organisation (especially in terms of cash flows and assets and its strategic objectives. In terms of size, a loss of £1million may be significant for a small organisation, but insignificant for a large organisation with a strong balance sheet.

In terms of probability it is normal to link this to either probability ranges (e.g. 0.8-1 for high, 0.5-0.79 for medium, etc.) or temporal frequency, in terms of the number of events every year or number of years. Table 3 provides an example which may be used as a starting point. Most people that use risk matrices tend to prefer temporal ranges for probability, as they are less technical.

3.1.2. Inherent risk exposure

Inherent risk refers to the level of risk exposure with no controls applied. It is also known as gross risk.

An assessment of inherent risk within a RCSA provides a baseline exposure score for the risk in question. One advantage is that it highlights the significance of any risk should no controls be applied. A low level of inherent exposure suggests that the risk in question is of low significance and should require little management attention. In contrast, a high inherent exposure suggests that time and effort should be devoted to controlling the risk.

Organisations may decide that risks with a low level of inherent exposure do not require a full RCSA. There is little point spending time and resources assessing control effectiveness or identifying control gaps if inherent exposure is very low. Better to invest this time and resources on risks with higher inherent exposure scores.

The main problem with including inherent risk is how to determine inherent exposure. It is rare for risks to exist in an environment of zero control. Hence inherent assessments can be very conceptual and judgmental, increasing the potential for over or underestimates of inherent exposure.

3.1.3. Residual risk exposure

Residual risk is an assessment of the level of risk exposure with controls in place. It is also known as net risk.

An assessment of residual risk considers the number, type and effectiveness of the controls that are in place. In theory, a well-designed mix of effective controls should reduce residual risk exposure. The difference between the level of inherent and residual risk illustrating the contribution that the relevant controls are making to reducing exposure.

Residual risk is easier to assess because it reflects the actual level of exposure given the controls that are in place. Hence it should be a realistic assessment that is supported by actual experience in managing the risk, including, where available, historical loss data. It is hard to imagine how an RCSA could work without an assessment of residual risk exposure.

3.1.4. Causes

Operational risks are typically categorised on an event basis (see IOR guidance on Operational Risk Categorisation). This means that inherent and residual risk assessments usually refer to an organisation's exposure to specific operational risk events (e.g. the probability and impact of an IT systems failure).

However, events rarely occur in isolation and may be caused by a range of factors. For example, an IT systems failure may be the result of a power cut, a hacking attempt, or a faulty update, or a combination of all three.

Hence some RCSAs include information on the causes of risk events. This helps to provide further information to assist in probability assessments. It can also be used to help link controls to specific causes of risk events, and to check that controls are in place to address all of the most significant causes.

By linking events and especially controls to causes RCSAs can be made more prospective, helping organisations to better prevent future operational risk events. By collecting information on causes it can also be possible to link events, thus identifying how a particular cause or control failure concerning a specific cause may precipitate a chain of operational risk events.

3.1.5. Effects

At the other end of the cause-event-effect chain are the effects of operational risk events. Operational risk events have a range of effects (e.g. financial, business disruption, reputational and physical). Equally the size of these effects can vary. For example, a small fire, contained to a limited area, compared to one that destroys a whole building or site.

Certain controls are designed to reduce the effects of operational risk events. Hence some RCSAs collect information on effects to help link the relevant controls to these effects. For example, a sprinkler system will reduce the effect of a fire, but only if the system is well designed and maintained. Equally the establishment of an IT contingency site can help to reduce the effect of system failures. But only if the site is well maintained and tested regularly.

By collecting information on effects, it is possible to determine whether an appropriate mix of controls is in place to address them, or whether there are gaps that need to be filled, for example, effects for which no controls are currently in place.

3.1.6. Control effectiveness (individual)

By definition, a RCSA must include an assessment of the controls put in place to address the causes and effects of operational risk events. Ineffective controls will have little to no effect on an organisation's exposure to operational risk. Worse they may create a false sense of security, resulting in an underestimate of exposure.

There are two main ways to assess control effectiveness: a subjective assessment versus objective controls testing.

Subjective assessments of control effectiveness use an ordinal scale similar to those used for probability and impact. The simplest is a two-point scale: 'effective' or 'ineffective', but scales of 3 or more as common. Table 4 provides an example of a 3-point scale.

	Control Effectiveness	Description
3	Substantial	Control is fully effective and working as intended
2	Adequate	Control is mostly effective, but there are minor flaws in its operation
1	Requires improvement	Control is defective, there are significant flaws in its operation

Table 4: Example control effectiveness scale

Subjective assessments rely on management judgement, but it is recommended that they are supported by any available information, such as reported loss events or near misses (which may have been the result of a control failure) and internal audit reports.

Objective controls testing requires the identification and monitoring of control effectiveness indicators, usually referred to as 'control indicators' or 'key control indicators'. Examples of these indicators include:

1. The frequency with which business continuity plans are tested and updated, including whether tests or updates are overdue.
2. The results of IT security penetration tests.
3. Results of Portable Appliance Testing, and whether tests are overdue.
4. Identified breaches of policies and procedures.

Hence indicators may either be related directly to the operation of a control or the frequency and reliability of any reviews conducted to test effectiveness.

For more on the use of risk indicators in general please refer to the IOR's guidance on Key Risk Indicators.

3.1.7. Control effectiveness (overall)

It is rare for operational risks to have only one control. Typically, a variety of controls are required, some causal controls, designed to prevent the event from occurring, others effect based, designed to detect, and mitigate the damaging effects of operational risk events. This range of cause and effect-based controls are typically referred to as a risk event's 'control environment'.

Estimates of the overall effectiveness of the control environment for a particular operational risk event are less common than the assessment of specific controls but provide valuable insight into whether a risk is over or under controlled. The identification of over or under controlled

operational risk events is an important benefit of an effective RCSA, so the inclusion of an overall effectiveness assessment is strongly recommended.

Usually, assessments of overall control effectiveness are subjective and rely on a three point scale:

1. Risk is under controlled, meaning that there are gaps in the control environment that need to be filled.
2. The overall level of control is appropriate, meaning that the control environment contains an appropriate mix of controls.
3. Risk is over-controlled, meaning that some controls are unnecessary, and it may be possible to remove them.

Loss event and near-miss data, coupled with internal audit reports can provide valuable information on the overall effectiveness of the control environment. They may both highlight potential gaps in the control environment, while internal audits may sometimes identify obsolete controls.

3.1.8. Action plan

Most RCSAs will include fields to capture information on agreed action plans. Typically, these plans will address either deficiency in existing controls, the implementation of new controls or the removal of obsolete or excessive controls.

Agreed actions must be: Specific, Measurable, Achievable, Realistic and Timebound (SMART) (see Table 5). This should ensure that actions are completed on time. It is also important to assign actions to an owner, usually, the owner will be a manager with the necessary seniority to ensure the action is completed, preferably the controlling owner.

Specifc	Set a specific target or goal for the action
Measurable	By setting an action that is measurable it is possible to demonstrate in an objective manner that it is complete
Achievable	Actions must be achievable to ensure that they are completed in a timely and effective manner
Realistic	Controls and control environments are rarely 100% effective. Minor flaws may be considered tolerable, especially when the costs associated with increasing the level of control are high.
Achievable	Actions must be assigned an end date to ensure that they are completed in a timely manner

Table 5: SMART Actions

3.1.9. Other

The above elements are the most common in RCSAs, but that does not mean that they are the only ones. For example, some organisations may include information on:

- Organisational objectives, to link specific operational risk events to objectives
- Risk descriptions, to add detail and context to the identified risk events

- Risk, control, and performance indicators
- Loss event and near-miss data
- Identified internal audit issues and actions

Care should be taken when adding new elements – at all times it is important to weigh the costs and benefits. The more detailed and complex an RCSA is, the longer it will take to complete.

3.2. Designing the template

Two main options are available:

1. Spreadsheet
2. IT system

Most organisations start by using a spreadsheet. An example is provided in Appendix A.

It is recommended that organisations use a spreadsheet approach for a few years before moving to a system. This will allow them to refine the design of the RCSA to ensure it is appropriate for the nature, scale, and complexity of their activities, along with their risk culture.

It is not recommended that organisations purchase 'off the peg' RCSA systems that pre-determine the design of the RCSA approach. Such systems may not be compatible with the organisation or its risk culture. It is important that any system can be customised, as fully as possible.

3.3. Top-Down and Bottom-Up

RCSA may be designed for top-down or bottom-up completion.

Top-down completion refers to RCSAs that are typically completed by senior management, including the executive. A top-down RCSA will usually focus on strategic level operational risks that may threaten the achievement of organisational objectives. Such risks are likely to have a significant financial, regulatory, or reputational impact on an organisation, and are usually organisational wide, though they may sometimes be specific to a department, division, or function.

Bottom-up RCSAs focus on departmental or functional level operational risks. They are primarily designed to be a local management tool, to help prevent/mitigate loss events and near misses and or improve the system and process efficiency.

Most organisations will design top-down and bottom-up RCSAs. The advantage of a top-down approach is that strategic level risks can be cascaded down, and aligned to the risks, controls and actions identified in departments, divisions, or function assessments. This can help to improve operational risk governance and ensure that organisation-wide and local priorities are aligned.

The advantage of a bottom-up assessment is that local managers can focus on the risks and controls that are relevant to their area. Equally significant local risks may be escalated for top-level consideration, as may significant correlations between local level risks in different areas.

Top-down and bottom-up RCSA templates must be consistent, using similar elements and terminology. This will facilitate the cascade of operational risk information up and down the organisation. However, given the time-limitations of senior managers, it may be appropriate to develop a shorter, less complex template for them to complete.

4. Completing an RCSA: Approaches and Techniques

It is not recommended that RCSAs are completed by one person – such as the risk owner, or their delegate. The judgemental nature of most RCSAs means that subjective bias is very likely. Such bias may result in an over or under assessment of exposure and control effectiveness. In either case, this will result in inaccurate information and wasted resources.

The best way to address bias is to improve the number of individuals in the RCSA process. That way the problem of individual biases should be mitigated, where the group can challenge them effectively. A further advantage of involving many individuals is to increase the range of expertise and experience involved. It is rare for anyone individual to have all the information required to complete an RCSA effectively.

4.1. Workshop approach

A workshop approach to RCSA completion ensures human interaction and enables guidance to be provided by a risk professional during the process (see: 4.1.4). Although it can be more time consuming than the alternatives, the quality of the information generated by a workshop approach can be considerable. This is because of the range of skills, experience and expertise that should be present.

A workshop is a mechanism to get people engaged in talking about their risks, controls, and any necessary improvements. Further potential benefits of a workshop approach include:

- Raising awareness of operational risks and their associated controls
- Enabling the assessment and improvement of 'softer', hard to measure, control mechanisms e.g. communications, training, and accountability
- Providing an opportunity for the transfer of risk management skills across the organisation

4.1.1. Planning

Preparation is key to ensure a successful RCSA workshop. Guidance should be provided to the 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.

Table 6 summarises common actions that should be taken to plan for a successful RCSA workshop.

Topic	Action required
Get executive support	Risk committee or equivalent should communicate its support for the workshops to risk and control owners. Relevant executive or senior manager for the area asked to attend the first 5 minutes of the workshop to communicate its importance. If attendance is not possible, ask them to contact the attendees via phone or e-mail or produce a short introductory video.
Identify priority areas	Some departments or functions may have a more urgent need for workshops. This can be determined through the review of loss and near miss data, internal audit reports or the identification of inherently high-risk areas.

Secure local support for the RCSA	Contact local management to ensure that they understand the process and benefits of an RCSA and address any concerns they may have. In particular secure their support for ensuring that any identified actions will be completed within the agreed timescales.
Review area processes and activities	Identity the key activities and processes performed by the area. It is important to understand the operations of an area to ensure that the right participants are selected. Where available review existing operational risk assessments and any loss or near miss data.
Identify and invite participants	Determine who should attend the workshop (see 4.1.2) and confirm their attendance. If key attendees find that they are no longer available they should be asked to nominate a delegate.
Workshop scope and objectives	Agree the scope and objectives of the workshop with the participants. For example, it may be that only a specific category of operational risks will be considered (e.g. IT risks) or specific operational processes (e.g. customer processes). Sometimes risks are identified as part of the RCSA process. This means that the workshop will begin by identifying the relevant risks. However, it is recommended that the primary categories of risk (e.g. the relevant level 1 categories) are identified in advance. This will help to save time during the workshop.
Supply standard documentation (RCSA process and workshop agenda)	Ensure attendees understand what an RCSA is, the information required, and how the workshop will be performed.
Organise a facilitator	Workshops will require an expert facilitator skilled in RCSA. The facilitator should be impartial and may be a member of the (operational) risk function, a risk expert from another part of the organisation, or an external consultant.

Figure 6: Planning topics and actions for a RCSA workshop

4.1.2. Attendees

The selection of attendees will depend on the scope of the workshop (e.g. risk categories to be covered, processes and activities under review, etc.). As a general rule, the following should attend:

- A local management representative, including, where specified, the relevant risk owner(s)
- Where specified, all relevant control owners
- Where not represented by the relevant control owners, subject matter experts, covering key control areas like IT systems and security, customer relations, marketing, human resources, finance, etc.
- An independent observer, such as a member of the risk function or a risk owner from another part of the organisation

As a general rule around 6-8 attendees is optimal, with 12 as a maximum. As workshops increase in size, facilitation becomes harder and there will be insufficient time to ensure that all voices are heard.

The role of the independent observer is to look for potential bias. The observer should only speak if they are concerned that a risk exposure or control effectiveness assessment is being over or underestimated.

Care should be taken when inviting managers to workshops. Often they need to attend because they are the relevant risk or control owners. However, there is a danger that they may dominate the discussion and or discourage others from raising concerns. Here the role of the facilitator is key, along with the independent observer. They should be of sufficient seniority to ensure that management does not take over a workshop or use it to pursue a particular political agenda.

4.1.3. Structure and duration of the workshop

RCSAs can take several days to complete, especially when covering the full range of operational risks for the area in question. This presents challenges for the structure and timetabling of workshops. Even with regular breaks, sessions longer than 2-3 hours can result in fatigue, reducing focus and leading to inaccurate assessments.

To help maintain focus it is recommended that workshops are structured into distinct sections or modules. These modules may take place within one workshop or timetabled sequentially over a number of days.

Module 1 - Describing the risks to be assessed and assessing inherent risk.

Module 2 - Control identification and effectiveness and the assessment and residual risk exposure.

Module 3 - Action planning and next steps.

By focusing discussion at the workshops on these core aspects (i.e. risks, controls and action planning), other additional requirements such as control testing, agreeing on action due dates, or allocating and amending risk and control ownership, can be finalised outside of the workshops.

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 local management. A workshop is merely a tool designed to assist them in discharging that responsibility effectively.

4.1.4. Facilitation

The use of a skilled facilitator helps to reduce subjectivity and bias and identify potential conflicts of interest and political manoeuvring (e.g. over or understating a risk to influence resource budgets).

Some organisations prefer to facilitate their own internal RCSAs, others will use external facilitators. When using internal facilitators, it is permissible to use experts from the risk or audit functions, providing it is made clear that ownership of the assessment and its outcomes rests fully with local management (e.g. the relevant risk and control owners).

The role of the facilitator requires a specific skill set as outlined in table 7.

Role	Skills
Maintain momentum and ensure the agenda is followed	Active listening
Ensure that the RCSA process is followed	Create a safe space for discussion, ensure that all perspectives are valued
Challenge potential bias or conflicts of interest	Assert authority and control to maintain discipline
Involve all attendees in the discussion	Summarise discussions clearly and accurately and set priorities
Ensure a balanced discussion	Detailed knowledge and experience of the RCSA process
Ensure that decisions, actions, and any disagreements are recorded (may use a note taken to support this)	

Table 7: Role of a facilitator

4.1.5. Validation

To help combat subjective bias it is recommended that the output from similar workshops are compared. This should help to reveal significant outliers in terms of responses. Usually, this work should be completed by the (operational) risk function.

For example, it should be possible to compare risk and control assessments for similar risks across departments and functions. Where an assessment of a particular risk or type of control differs significantly, a discussion should be had with the relevant managers to confirm whether there are good reasons for these differences.

Note that care should be taken when asking for amendments to RCSAs. The risk function must, at all times, ensure that RCSAs are owned by the managers responsible for them. This may sometimes require tolerance of assessments that are slightly biased. But a flag should be placed on such assessments to ensure that this is signalled, especially when reporting RCSA output to senior management.

4.2. Questionnaires

Questionnaires can be used to collect some or all of the information required for an RCSA. Questionnaires may be used as a substitute for a workshop, to help save time and resources. But they are most effective when combined with workshops. Here the initial thoughts of workshop participants can be collected via the use of a questionnaire and a workshop can be used to discuss the findings.

It is also possible to use questionnaires to reach a wider audience than the few who may be invited to a workshop. This should reduce the chance that risks or controls are omitted and help to control individual biases.

4.2.1. Questionnaire scope

Questionnaires may be designed for specific categories of operational risk (e.g. fraud or IT risks) or they may attempt to capture information on all risks. There are advantages and disadvantages to both. A more focused questionnaire will be shorter and take less time to complete, reducing the risk of respondent fatigue and increasing the accuracy of responses. However, where many focused questionnaires are required to complete a RCSA it is recommended that the are spaced over several months to prevent complaints about questionnaire overload. Alternatively, different focused questionnaires can be sent to different samples of respondents. This can be especially effective where each sample is selected based on subject expertise (e.g. IT risks survey is sent to the relevant IT experts and the main IT system users, etc.).

Equally, questionnaires may be exploratory (e.g. using open questions to identify new risks or controls) or confirmatory. Usually, questionnaires are confirmatory, meaning that they start with a particular set of risks and controls in mind.

For confirmatory questionnaires, it is recommended that a consistent operational risk categorisation is used across the organisation (see IOR guidance on Operational Risk Categorisation) and that standardised list of controls are produced for the organisation. Preferably linking each risk category to a specific sub-set of these standardised controls. This will provide a consistent structure for the questionnaire and allow responses to be compared easily.

4.2.2. Questionnaire content

At a minimum, a questionnaire should ask questions on the following:

1. Estimated level of inherent risk
2. Estimated control effectiveness (individual and the overall environment if this is part of the RCSA)
3. Estimated level of residual risk
4. Recommended actions to improve control effectiveness

The questionnaire should be kept as short as possible. The longer the questionnaire the greater the chance that respondents will either give up answering or provide random responses.

Socio-demographic questions (e.g. age, gender, etc.) are not usually necessary so should be omitted to reduce the length of the questionnaire. The only potentially relevant questions are the department or function in which individual works and their level of seniority.

4.2.3. Designing a questionnaire

Questions can be standard or non-standard:

- Standard questions are written centrally, usually by the operational risk function. These will address the minimum content identified above
- Non-standard questions are written locally by the relevant management to address specific operational risk and control issues or concerns

Where management buy-in remains a concern, it may be better to adopt a non-standard approach, giving greater ownership of the questionnaire design to local management. However, this will make it harder to aggregate and compare responses. Ideally, local managers should be asked to include many standard questions and then be given the freedom to add further questions if they wish.

Closed questions should be structured so they can be answered using either an even-numbered Likert type agree or not agree scale (e.g. 1 for Strongly Agree, 4 for Strongly Disagree) or a binary Yes or No. This will ensure that respondents do not 'sit on the fence' and provide the middle value for most responses (e.g. 3 for a 5-point scale).

Use of a 'Not Applicable' option is permissible, but only when respondents can justify this with an explanation (e.g. a particular control is not currently used in their area).

Open questions are encouraged, especially to justify choices like 'Not Applicable' or No. Open questions might also be used to help add context, for example, to explain why control is believed to be effective or not effective.

4.3. Questionnaire content

Workshops and questionnaire are the most common techniques, but there are others which may be considered. Table 8 summarises 3 alternative options.

Role	Skills
Structured what if technique	Structured what-if technique (SWIFT) is a systematic team-oriented technique most commonly used for the assessment of health and safety and environmental related risks and controls in areas like chemical processing and manufacturing, but it can be applied in many other ways. The technique uses a series of structured 'what-if' and 'how-could' type questions to consider how deviations from the normal operation of systems, processes and controls may result in risk events. Brainstorming is supported by checklists to help focus the discussion. SWIFT relies on expert input and the use of a 'SWIFT leader' to structure the discussion. The SWIFT recorder keeps an on-line record of the discussion on a standard log sheet. There is no single standard approach to SWIFT - one of its strengths is that it is flexible and can be modified to suit each application. SWIFT is an expensive technique to use, because of the time and people involved. But it is more likely to address all relevant risk events and controls. This is why it is most commonly used in hazardous sectors like chemical processing or nuclear power generation.
Delphi technique	The Delphi technique is an information-gathering tool that is used as a way to reach a consensus of experts on a subject, in this case, the completion of RCSAs. Each expert participates anonymously, and a facilitator uses a questionnaire to solicit ideas about the important points related to the subject. The responses are summarised and re-circulated to the experts for further comment. Consensus may be reached in a few rounds of this process. Concerning RCSA, the Delphi technique helps reduce bias and keeps any one person from having undue influence on the assessment. A range of experts can be used including risk management specialists, other functional specialists (IT, HR, governance, etc.) and department and functional management (e.g. operations managers, accountants, etc.). Anonymity is key because it encourages experts to be as honest and open as possible. Studies have shown that the technique can be very effective at predicting future outcomes, but it also very time consuming, especially if consensus is hard to reach.

Root cause analysis	Root cause analysis assumes that operational risk events have multiple causes. For example, a fire risk event needs: material to burn, a spark and oxygen before it can cause damage. Root cause analysis adds depth to an RCSA thought an exploration of how and why an event may occur. The emphasis is on future prevention by improving existing controls or adding new ones to address previously unforeseen causes. Root cause analysis approaches vary, but most are based on four principles: 1. Identify the causes of an event 2. Establish the timeline from normal operations to a risk event 3. Distinguish between root causes and more immediate causes 4. Use the results to help assess exposure and control effectiveness Often the causes of an event, as well as the order in which the causes may arise, are identified using the 'five whys' technique. This asks why questions such as: 1. Why did a fire occur? Because combustible material started to burn 2. Why did the material burn? Because a spark caught the material alight 3. Why did the spark occur? Because an electrical fault occurred in the building's wiring 4. Why did the electrical fault occur? Because the wiring was old 5. Why was the wiring old? Because the wiring had not been safety inspected More or less why questions than five may be used to get to the root cause, but usually it is possible to get to the underlying process failure in 5 questions. Further questions could still be used in this example to identify why a safety inspection has not been carried out, for example. Root cause analysis is time-consuming and it is rarely practical or cost-effective to use it for all RCSAs, but it is a good technique to use when assessing the most significant operational risks across an organisation.

Table 8: Other RCSA data collection approaches

5. Integrating an RCSA into the Operational Risk Management Framework

RCSA is not a stand-alone process. To be effective it must be integrated into the wider operational risk management framework. This means using other elements of the framework to provide information to support the completion of RCSAs. It also involves using the output from RCSAs to support other elements, notably operational risk reporting.

5.1. Linking to internal and external loss data

External and internal operational loss data can be used to support RCSAs in two ways:

- To support the assessment of residual risk and control effectiveness
- To validate residual risk and control effectiveness assessments

The size and frequency of actual loss events indicates what may occur in the future, assuming current trends remain the same. Equally, operational loss events can often be linked to specific control failures or gaps in the control environment, providing information on control effectiveness.

Where RCSA results differ significantly from the available internal or external loss data additional validation work may be required. This work should consider both the accuracy of the RCSA output and the effectiveness of loss of data collection. For example, it may be that a high level of predicted residual exposure, relative to reported loss events, is the result of assessment bias, or it could be that the loss data is incomplete.

5.2. Scenario analysis

Significant control weaknesses and risk exposures 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 the identification of operational risk exposures and control weaknesses not currently captured within the RCSA.

Scenario analysis can be especially helpful when assessing inherent risk, where captured. By considering the potential causes and consequences of major control failures a structured approach to the analysis of scenarios can result in more robust inherent risk exposure estimates.

It is rarely practical or cost effective to use scenario analysis for every inherent risk assessment. But it can be a useful tool for validating especially high inherent risk scores.

For more information see the IOR guidance paper on Operational Risk Scenarios.

5.3. Reporting RCSA results

There are various ways to report the results of RCSAs. Usually, a combination of different formats will be required – according to the audience for the report:

- Narrative reports (descriptions of the various risk exposures and any control weaknesses, may be presented in the form of a risk register)
- Heat Maps/Traffic Light Reports (see Appendix b)
- Dashboards (risk, control effectiveness and performance indicators, usually presented using trend diagrams, pie charts, etc.)
- Benefits log (a log of any improvements made to the control environment, such as enhanced control effectiveness, removal of obsolete controls, etc., and the effects of these in terms of reduced operating costs, improved efficiency, etc.)

As a general rule, less detail should be reported the more senior (high level) the audience. For the governing body and senior management, the focus should be on the most significant areas of risk/control weakness that have the greatest potential to damage the organisation and prevent it from achieving its 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 detailed monitoring of the progress of action plans against agreed milestones and deliverables. Also, whatever the level of the audience, emphasis should be placed on keeping it pertinent and relevant to the audience for which it is intended.

The maintenance of a benefits log is highly recommended. These logs can be used to improve buy-in across the organisation, thus improving the timeliness and accuracy of RCSAs. Such a log provides a tangible record of why RCSAs is a worthwhile exercise that can add value to the business.

5.4. Action planning

RCSA outputs are a valuable source of information for the development of operational risk action plans. Such plans might include improving the effectiveness of existing controls, removing obsolete controls, or introducing new controls to address gaps in the control environment.

Actions must always be justified on cost/benefit grounds, just because a control could be made more 'effective' or a new control added, does not mean that the time and effort required to achieve this is necessary. 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. Equally, it must always be remembered that increasing the level of control can reduce the efficiency of systems and processes and may even result in unforeseen new risks. For example, significantly increasing the frequency of password changes for IT access may result in staff writing down and then losing their passwords.

When deciding on the nature of an action plan it is helpful to remember the four common responses to risk exposures:

- Acceptance – no further action is taken, either because the residual risk exposure is within appetite or the cost of additional control is excessive relative to the benefits earned
- Mitigation – which will involve enhancing the level of control (improving control effectiveness or introducing new controls) to reduce the likelihood (loss prevention) and/or the impact of the risk (loss reduction)
- Transfer – which may involve financial risk transfer to an insurer, or the physical transfer of risk to an external service provider[1]
- Avoidance - where changes are made to an activity, process, or system to reduce inherent risk exposure

All action plans must specify what is to be done, by whom and by when. Progress against completing action plans should be monitored until completion. Depending on the significance of the action, progress may be monitored by the governing body, a board delegated committee, the (operational) risk function or local management.

[1] In some sectors, such as financial services, organisations are not able to fully transfer certain risks to external service providers and must remain accountable to any operational loss events that occur and the effectiveness of a service providers operational risk framework. It is recommended that readers check their local requirements before attempting to use service providers for operational risk transfer purposes.

5.5. Internal audit planning and reporting

The use of RCSA output by the internal audit can confer a number of advantages:

- By taking on more responsibility for the maintenance of the control environment auditees should better understand the purpose of operational risk management and the benefits of effective assessment and control
- Providing additional information to support audit work (e.g. the validation of control effectiveness estimates)
- Exposure assessments can be used to support a risk-based approach to internal audit

It is also recommended that the internal audit function should review, periodically, the effectiveness of the RCSA to ensure that it remains effective and proportionate.

6. Conclusion

An effective RCSA approach is an important part of most operational risk management frameworks. However, if poorly designed and implemented the outputs can do more harm than good. Like any operational risk management tool, an effective RCSA must be value-adding, not a bureaucratic, compliance-oriented, box-ticking exercise. Excessive complexity or prescription can result in a process where the costs exceed the benefits. At all times operational risk professionals should remember that RCSAs must support business decision making.

Appendix A: Example RCSA templates

Examples of RCSA templates are provided below.

1. Example Excel based template (simple)

ID	Risk Description	Risk Owner	Inherent Risk	Key Controls	Control Owner(s)	Residual Risk	Within Appetite?	Action Required?
12c	Significant disruption to normal business operating environment	M Smith	High	• Business Continuity plans in place • Plans tested and updated annually • Telephone call cascade tested quarterly	J Brown	Medium	No	Yes
13a	Breach of client data confidentiality	F Jones	High	• Data Security policy in place and regularly reviewed • Independent monitoring of adherence to Policy • Escalation of non-compliance • Breach register	S Thomas	Low	Yes	No

More fields may be added, see 3.1 above.

2. Example RCSA action plan

ID	Risk Description	Residual Risk	Action Required	Action Owner	Target Date	Expected Residual Risk
Outside Appetite						
12c	Significant disruption to normal business operating environment	Medium	Introduce desktop walkthrough exercises twice a year	J Brown	30/09/20	Low

3. Example questionnaire excerpt

Example extract taken from questionnaire examining access controls within an IT admin function. The comments section may be used to provide a rationale for the response provided, including any tangible evidence.

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?			

4. Example RCSA end to end process assessment template

Example extract taken from questionnaire examining access controls within an IT admin function.

The comments section may be used to provide a rationale for the response provided, including any tangible evidence.

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.*

Appendix B: Example RCSA heatmap report for senior management

A TYPICAL KEY TO AN OPERATIONAL RISK PROBABILITY AND IMPACT ASSESSMENT

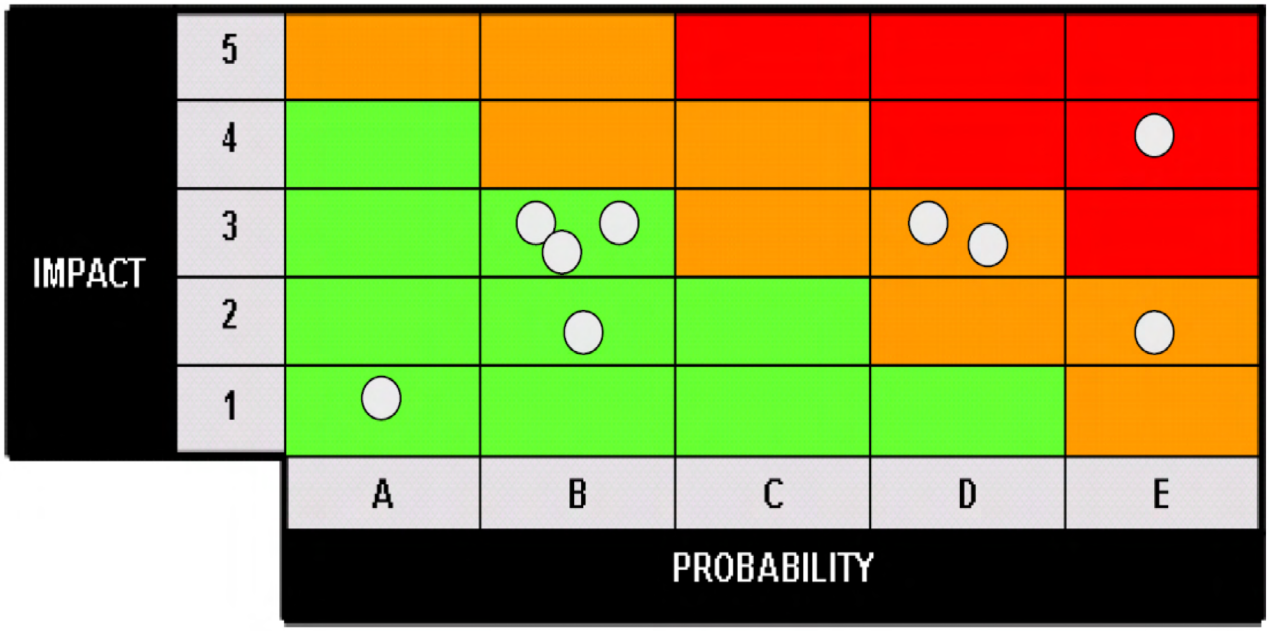
This is an example but calibration of scales must be proportional to the assessment point concerned.

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 year)

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



www.theirm.org

irm

Developing risk professionals