RMA GUIDANCE NOTE #1

RISK AND CONTROL
SELF ASSESSMENT

March 2013
Operational Risk Appetite | RMA Guidance Note #1 | 2

CONTENTS

Foreword .............................................................................................................................................................................................................................3
1. Introduction ...............................................................................................................................................................................................................4
2. Background ...............................................................................................................................................................................................................5
3. Demonstrating the Value of RCSA ..................................................................................................................................................................6
4. The RCSA Process .................................................................................................................................................................................................. 7
5. RCSA Guiding Principles .................................................................................................................................................................................................. 9
   – Preparing for an RCSA ..................................................................................................................................................................................9
   – Risk Identification and Assessment ..............................................................................................................................................................11
   – Scoring ...............................................................................................................................................................................................................12
   – Response ..........................................................................................................................................................................................................13
   – Aggregation .....................................................................................................................................................................................................13
   – Reporting ..........................................................................................................................................................................................................14
   – Monitoring and Review .............................................................................................................................................................................14

Appendices

Appendix A: Acknowledgements ...................................................................................................................................................................16
Appendix B: List of Guiding Principles .......................................................................................................................................................17
Appendix C: Glossary ..........................................................................................................................................................................................18
Appendix D: Workshop Dates & Locations ..............................................................................................................................................20

Version Number Date Issued Summary of Changes

1.0 Final and approved version

© 2014 Risk Management Association Inc (Vic), ABN 95 057 024 197
PO Box 20468, World Square, NSW 2002 Phone: 0403 170 792 Email secretariat@rmaaustralia.org
www.rmaaustralia.org

Disclaimer

The Guidance Note does not intend to prescribe a way of conducting a Risk and Control Self-Assessment (RCSA) process, the information contained in this
document is intended only to provide some suggestions based on industry experience, and considerations that should be given in implementation of this
management tool. It is not intended to be comprehensive. It does not constitute, nor should it be treated as, legal advice or opinions. Users are encouraged to
obtain professional advice about the application of any legislation or standard relevant to their particular circumstances and to exercise their own skill and care in
relation to any material contained in this guide.

The RMA Australia accepts no liability for any loss suffered as a result of reliance on this publication. This document has been published without prejudice.
The information contained herein is current as at the date of this document.

You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within
your organisation.
We continue to read major news headlines on business shocks and scandals such as mis-selling of consumer products, data breaches, major systems outage, and money laundering. This comes at a time when Boards and Senior Management strive to maintain and enhance shareholder returns through improved business performance, which can be significantly undermined by these material operational risk losses.

The need to ensure that an operational risk management framework is implemented both effectively and efficiently has never been more critical for organisations across the financial services industry. Practices continue to evolve and practitioners today endure many challenges in implementing these processes.

An Interbank Forum was established in 2005 by operational risk leaders amongst Australia’s largest banks. The primary objective of this Forum was to create a medium for sharing and learning from each other. This coincided with our plans to embark on implementing a framework that would qualify for Advanced Measurement Approach status.

More recently the Interbank Forum agreed on the need to work together to formulate industry guidance for practitioners, both current and future. We agreed that a guidance note relating to the ‘Risk and Control Self Assessment’ (RCSA) process was an important place to start. Irrespective of whether you were using advanced techniques for the measurement of operational risk capital, RCSA was deemed a foundation element of operational risk management that has strong linkages to other operational risk management processes.

This Guidance Note does not intend to prescribe a way of conducting an RCSA process, but merely provides some suggestions based on industry experience, and considerations that should be given in implementation of this management tool. Some areas go into more detail than others reflecting the maturity of key components relative to others. Additionally, this Guidance Note is not exhaustive, with the Operational Risk Forum considering development and release of further guidance notes addressing challenges of a more technical nature, such as those relating to the use of the traditional likelihood vs. consequence matrices.

I’m pleased that we have been able to bring together 13 banks and form a collective industry view on key principles. It has been rewarding to be part of discussions across such a diverse range of banks and to witness Australia’s financial services industry take greater ownership in enhancing operational risk practices.

More importantly, this initiative has enabled our operational risk practitioners to come together, share practices, learn from each other, discuss challenges, network, and identify guidance points they would effectively provide to an individual either having just started or even considering a career in operational risk management.

Finally, I’d like to personally extend my thanks to RMA Australia for their sponsorship of this initiative, Ernst & Young Australia for their facilitation and guidance, and each of the peer banks (and their representatives) for their commitment and contribution to development of this Guidance Note.

Regards

Tony Petkovski
Chair RMA Operational Risk Forum
The Risk and Control Self Assessment Guidance Note (this Guidance Note) outlines a set of guiding principles for implementing a risk and control self assessment (RCSA) process for an Australian financial services organisation. This Guidance Note has been formulated and agreed by an established industry working group (Working Group) operating under the Operational Risk Management Interbank Forum of the Risk Management Association (RMA) Australia. Development of this Guidance Note has included input from a number of representative banks, with facilitation by Ernst & Young Australia. Refer to Appendix A for acknowledgements.

It is understood that the implementation of the RCSA process will vary given the nature, size and complexity of each organisation. This Guidance Note:

• intends to outline guiding principles for practically applying the RCSA process; and

• is supplemented with helpful hints to overcome potential challenges associated with the process in the areas where it was felt there was sufficient consensus as to what worked well, what to be aware of, and what to avoid.

It should be noted that this Guidance Note has not been designed to document a detailed end-to-end RCSA process.
The Operational Risk Management Interbank Forum, under the sponsorship of the RMA Australia, established an inaugural Working Group in June 2012. The Working Group was tasked to define a value statement and address challenges and issues associated with implementing an RCSA process.

RCSAs are an important component of an organisation’s Operational Risk Management Framework (ORMF). They can demand a significant commitment of resources and hence should be implemented in a way that is meaningful and adds value to the business. To ensure the importance of the RCSA process is instilled throughout an organisation, there should be sufficient tone at the top with support and communication from executive and senior management.

Using the collective knowledge and experience of the Working Group, the purpose of this Guidance Note is to provide guidance on overcoming key challenges and issues identified by the Group, including:

- **demonstrating the value of RCSA**: articulating the value proposition for the RCSA process, with particular emphasis on effective ways to implement the RCSA to the business; and

- **identifying RCSA guiding principles**: establishing industry consensus on the key principles for implementing the RCSA process.

The Working Group acknowledges that RCSA is one component of an ORMF. This Guidance Note focuses only on RCSA and will not cover other elements of the ORMF.
Clear articulation of how the RCSA process adds value to the business is a common challenge for many financial services organisations. To gain maximum benefit from the RCSA process, participants need to develop an understanding of the reasons for conducting the RCSA, and derive meaningful benefit from it themselves. The more value perceived by the business, the more time and effort is given, resulting in greater quality information to drive better risk outcomes.

An organisation should articulate its own expectations and values associated with the RCSA process such as its use in day-to-day operational activities. This will vary with an organisation’s nature, scale and complexity. As a starting point, organisations may wish to consider the value proposition outlined below.

**Linkage with strategic plan**
Because of its linkage with, and alignment to, the business strategy and objectives, the RCSA process provides the ability to highlight areas of potential focus for the business so that its strategic plan can be met.

**Facilitation of management prioritisation**
The output of the RCSA process supports prioritisation of decision making, including the optimal allocation of resources. This is an important factor in an environment of increasing cost pressures, marginal growth, and demand for competitive advantage. It can be used to manage the business responsibly and is a single source of risk and control information.

**Enablement of governance**
The RCSA process provides structure to management thinking and can increase the transparency of decision making. Further, it can be used as a reference to meet external stakeholders’ expectations as well as identifying uncertainties both in a business-as-usual and change environment.

Once the value proposition has been articulated for the organisation, this needs to be underpinned by appropriate education and communication. Support by senior management for the value proposition of the RCSA throughout the organisation is critical.

The following guiding principles aim to draw some high level guidance for common application. Refer to Appendix B for a full list of guiding principles.
The process for identifying, assessing, monitoring and managing risks is known as the RCSA. The output of the RCSA process is documented in a risk register or illustrated on a risk heat map. The Bank of International Settlement's publication, Sound Practices for the Management and Supervision of Operational Risk, describes the RCSA process as an internally driven process to “identify the strengths and weaknesses of the operational risk environment” 1. Principle 4 of the publication states that “Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems”.

The RCSA should:

- assess vulnerability to known or past events;
- identify and assess events that may not have occurred; and
- monitor the business environment and internal control factors (BEICFs) including identifying and assessing key changes to the business.

The RCSA process is an element of an ORMF and links into the organisation’s risk governance structure, its risk appetite and has documented standards and processes. It is an integral part of the organisation’s operations such as the strategic planning process. RCSA is complemented by other ORMF elements within the framework for managing and measuring operational risk.

Ownership

The owners of the RCSA process and its output (across the organisation) are the business stakeholders. They should determine how the RCSA process will be executed, with support and challenge from the risk management function.

Frequency

As shown in the diagram below, the RCSA process is an ongoing activity. The frequency of review of RCSA outcomes should be risk-driven, responsive to business change and consider any regulatory or organisation specific requirements. Organisations should consider reviewing their RCSA outcomes at least annually, with a more frequent review depending on the size and complexity of the business.

---

1 Basel Committee on Banking Supervision, 2003
Approach
The RCSA can be conducted at a functional level or through an end-to-end process. There is no clear rule on which method is more practical or efficient. Certain elements of each will align, or be more valuable, depending on the organisation. Where one approach is adopted, the other may be used when challenging or providing oversight.

Level of RCSA
The level of the organisation at which the RCSA is completed is dependent on the structure, changes in the business, external environment, local regulatory requirements, financial independence of business units, and organisation requirements. The lowest level of the organisation at which the RCSA is completed is dependent on the materiality of the risks, with materiality defined by factors such as complexity of operations, scale and size of transactions and volumes. It is recommended that the RCSA process is performed at multiple levels of the organisation, and a top-down and bottom-up view applied to identify any gaps or trends across the whole organisation.

Figure 1: A typical RCSA process
The Working Group has developed 11 guiding principles across the RCSA process. These are outlined below.

**PREPARING FOR AN RCSA**

**PRINCIPLE 1:** Ensure preparation and delivery of the RCSA is completed within the context of the business, its strategies and objectives, and current risk environment. RCSAs should be preceded by engagement with key stakeholders and subject matter experts, as well as collection and preparation of relevant business and risk information (both internal and external).

Preparation involves collation of risk data, identification of attendees and gathering of the assessment material (including workshop material where appropriate). This role requires analytical and organisational skills. The role also involves taking minutes/notes (including the capture of rationale and justification for assessments) during the meeting and reflecting the results in the RCSA output.

Establishing a clear understanding of the following will assist with preparing for RCSA:

- business strategy and objectives, including key priorities for the business;
- risk appetite supporting the business strategy and objectives;
- any changes to the operating environment from previous assessments; and
- core processes central to the delivery of the business strategy and objectives.

In addition to this, the following should be considered:

- the operating environment that could influence the achievement of those strategies and objectives (either positively or negatively);
- forming a view of the nature, scale and complexity of the business, and its ability to meet its strategies and objectives; and
- ensuring the workshop participants have a common view (both retrospective and forward) of the business to assist them in identifying and assessing their operational risks.

Areas to consider when collating information about the business, its strategies, objectives and environment in which it is operating include (but are not limited to):

- risk appetite;
- previous risk registers, operational risk profiles, RCSA reports;
- emerging risks (e.g. social, economic and geopolitical factors);
- internal and external loss data, including near misses;
- breach registers;
- key risk indicators;
- control test data;
- technology (associated performance measures, age, level of support, interconnectivity of systems);
- Internal/External audit reports;
- approach to business continuity management;
- regulatory items and environment including upcoming regulatory change and possible increased scrutiny;
- fraud reports;
- documented processes (understanding degree of automation, manual processing, handovers, sharing of critical processes between areas);
• people/HR data (e.g. skills and knowledge of staff, resource levels, levels of engagement staff turnover, recruitment timeframes);
• customer profile – internal and external (e.g. customer segments, customer goodwill);
• reliance on internal and/or external third parties (e.g. scope of services, criticality of service);
• scope and reach of the business (e.g. offshore offices/branches, centralised processing areas);
• products and services (e.g. complexity); and
• change (e.g. level of changes initiated by the business and by other internal areas that will impact the business).

Note: not all areas above may apply to all business units or products.

Identifying the full business process through either the end-to-end or functional view gives a greater level of confidence on the completeness of RCSA outputs. Identifying all of the inputs and outputs of both up and downstream channels ensures that all aspects of a business profile are understood prior to implementing the RCSA process. This aids in the identification of controls, control owners and any potential weaknesses or exposures in the business.

HELPFUL HINT
Developing an understanding of the business environment cannot be undertaken in isolation and requires the knowledge of subject matter experts from the business and senior business leaders.

HELPFUL HINT
Set clear expectations regarding the pre-work required by business participants and outcomes (e.g. final deliverables and owners of those deliverables) of the meeting.

PRINCIPLE 2:
There are three distinct roles within the RCSA process:
• ownership (of the outcome);
• facilitation; and
• challenge and oversight.

While the roles can be performed by the same individual, the facilitation and challenge roles should be separate where possible.

Ownership of the RCSA process and outcome, and therefore the assessments, must be in place to ensure buy-in and accountability for risks and controls within a business. The owner should be a senior business leader or have adequate expertise in the business. The owner should ensure workshop participants have sufficient knowledge of the business to participate effectively, are engaged, and feel comfortable challenging and contributing to assessments.

Facilitation involves chairing the meeting from a neutral position with an objective to let all participants contribute to the discussion and maintain the momentum. The role requires good communication and observation skills as well as strong people skills. A facilitator should:
• understand the ORMF and RCSA process;
• understand the business strategy and challenges;
• keep the session on track;
• ensure the discussion is objective;
• elicit information and gain consensus from all participants; and
• summarise the discussion.

HELPFUL HINT
Senior business leaders should be present to give the introduction to the workshop (including articulation of business strategic objectives) supporting the importance of the RCSA as a business rather than a compliance exercise.

Challenge and oversight involves ensuring that all material operational risks are considered and the various attributes are reflected (e.g. relevant internal loss incidents and audit findings) to inform the RCSA outcome. The key requirements for this role are analytical skills, critical thinking, as well as strong communication skills. A critical competency is the confidence to challenge the business on the risks, controls and corresponding assessments. The role also requires strong business/product knowledge and understanding of the internal/external environment in which the business operates.

A more robust outcome may be derived in allocating the roles amongst different individuals. In mature organisations, facilitation of the assessments should be conducted by the business with oversight and challenge provided by the risk management function.
RISK IDENTIFICATION AND ASSESSMENT

PRINCIPLE 3:
Using knowledge of the business environment, identify risks that would prevent the business from achieving its objectives. Risks should be captured in a language that is meaningful to the business to ensure they can be easily understood and managed.

Risks should be clearly defined and articulated in simple terms that the business area concerned understands and agrees with, to avoid misinterpretation. The RCSA should capture risks that impact the business strategy and objectives. These risks should then be assessed, scored and managed in accordance with the ORMF.

Brainstorming sessions may identify numerous risks and it is recommended that these are again reviewed and filtered down to a sustainable and manageable level. There is no finite number of risks; the number per RCSA should be dependent on the organisation’s judgement of the business. Care must be taken to ensure causes and consequences are discussed and detailed and that these are not captured as risks themselves.

HELPFUL HINT
Where possible, encourage convergence in the assessment of compliance and operational risks to avoid duplication. That is, where potential non-compliance with internal policy and external regulatory requirements represents an operational risk to the business, it should be captured in the operational risk assessment process. This should include details of controls and be aligned with controls captured in compliance plans where held separately.

HELPFUL HINT
Libraries and standard categories of risks may be used to guide risk definitions, to aid in the risk identification process and for summarisation purposes.

The use of a risk library is considered useful to assist in articulating risks and in guiding terminology. In addition, standard definitions can promote easier comparisons between business areas and the business can gain value and insights into their risks on a relative basis.

PRINCIPLE 4:
Risk should be assessed on a residual and inherent basis.

Residual risk should be assessed by taking into account key controls (and the results of control assurance activities when performed), incident data and the overall business context, such as the views of subject matter experts in the area.

Whilst there is recognition of the industry definition for inherent risk, for practical purposes, it is defined here as the risk exposure given the removal (or failure) of identified controls. It is important that the inherent risk assessment is realistic and reflects the potential loss if there is a breakdown/removal in the control environment. This can then be used to prioritise resources and focus on the areas of highest potential exposure.

HELPFUL HINT
Assessing residual risk before inherent risk may improve the accuracy of the risk assessment and can provide a more natural flow for business participants. However, the ordering of the assessment is at the discretion of the facilitator, who should determine the sequence based on the workshop participants.

HELPFUL HINT
The focus of the inherent assessment is more clearly placed on the removal of identified controls, rather than if there is no control environment at all.

The Risk Rating Matrix should be used to calculate the overall risk rating based on the likelihood and consequence of the risk occurring. The same criteria should be used to determine the residual and inherent risk.

PRINCIPLE 5:
Control identification should consider the processes, systems, and activities that the business places most reliance on to manage the risk. They should be assessed on design and performance and take into account the business’ risk tolerance.

RCSA should identify a manageable list of controls which are considered to significantly reduce the likelihood and/or impact of a risk occurring. They should be named and defined in a succinct and meaningful manner and evaluated taking into account the reporting needs of the organisation. This is an important stage of RCSA as it helps the business understand the internal control environment, identifying any weaknesses, gaps or opportunities for improvement.
Controls should be:

- classified as preventative, detective or corrective. There may be additional benefit in further classifications e.g. manual vs. Automatic;
- categorised in terms of the importance or their effect on the inherent risk (e.g. key controls). Key controls are those which have the most impact on reducing the likelihood and/or the consequence of the risk occurring; and
- assigned a clear control owner.

Both the design (Design effectiveness) and performance (Operating effectiveness) of a control should be assessed separately and then combined to an overall assessment.

- Design effectiveness aims to assess the controls identified to ensure that they adequately address the risks. When assessing design effectiveness, the tolerance for the risk is taken into account i.e. the control design is effective if the control mitigates the risk so that the risk is within the business’ risk tolerance. As such, controls are designed to be effective in mitigating a given risk, the result of which is alignment between residual risk and risk appetite.
- Operating effectiveness determines whether the control is performing as intended.

The assessment should incorporate inputs, such as control assurance results, audit findings, recent incidents, key indicators etc. Materiality thresholds should be developed in line with the level at which RCSA is being performed e.g. Divisional materiality for Divisional RCSA, Group materiality for Group RCSA.

Accountability for ensuring the effectiveness and testing of key controls should rest primarily with the business however this may vary with the maturity of risk management practices.

HELPFUL HINT
Control assessment should not be confused with risk acceptance, i.e. there may be controls assessed as ‘Not Effective’, but management may have accepted the risk. Such a risk acceptance decision does not make a control ‘Effective’.

### SCORING

**PRINCIPLE 6:**
Risk assessment rating scales should be proportionate to the size of the business to which they are applied.

The most common industry approach for assessing inherent and residual risk is using likelihood and consequence scales. Generally this tends to be in the form of a risk heat map or matrix. The risk heat map is a tool used to visualise the outcome of an RCSA and helps the business compare and contrast risks.

HELPFUL HINT
Careful consideration should be given when using a risk heat map as the categorisation of likelihood and consequence can anchor thinking and produce biases. It can be helpful to ask participants to articulate the consequences and likelihood of a risk in practical terms without looking at the matrix first, and then referring them to the matrix to align their thinking to a category. This can assist to avoid the selection of categories based on emotive responses to category titles (e.g. catastrophic) or applying a literal definition of a criteria rather than the category term (e.g. “there is a 1:10 chance of the issue occurring” rather than “possible”).

HELPFUL HINT
Consequence should consider financial and non-financial impacts. Categories may include:
- financial;
- regulatory/legal;
- customer/partner;
- reputational;
- people/Staff/Work Health and Safety (WHS); and
- management effort/business operation productivity.
As risks are assessed at different levels of the organisation, there may also be a need for different consequence measurement scales in different business units or geographical areas, in particular, consideration of impacts from a financial perspective. Smaller business units or geographies may need a smaller consequence scale than the division or organisation level scale. Note, not all consequence measures should have different scales. Measures such as customer impact or reputation may be best measured consistently across the organisation. Likelihood should be assessed consistently across the organisation and typically takes the form of X times in a year or 1 in Y years.

RESPONSE

PRINCIPLE 7:
There must be a conscious assessment of residual risk, followed by a decision to accept or not accept the risk. The acceptance decision is done in the context of risk appetite and must be escalated and approved by the relevant governance committee. Where not accepted, there must be an action plan in place to remediate the risk back to within appetite. The action owner must be a senior business leader. Governance and independent oversight should be in place for risk acceptance and action tracking.

The business owner must decide on an appropriate risk treatment for each risk assessed in the RCSA. Management should either:

- Reduce the risk: Develop action plans to mitigate the risk exposure to an acceptable level; or
- Accept the risk: Document the rationale for accepting the risk, establish a review cycle, and ensure it is appropriately authorised by management. This applies where an organisation’s risk governance framework allows the business to accept risk exposures outside of risk appetite;
- Avoid the risk: Agree to remove or cease activities to avoid the risk exposure altogether; or
- Transfer the risk: Develop a plan to transfer the risk exposure to another party (e.g. an insurer), thereby minimising the exposure.

Where management wish to accept a risk that is deemed to be outside of risk appetite, or there are cases where business agrees that the risk appetite and tolerance require amending, the decision should be escalated in line with the organisation’s governance framework. The risk exposures and associated action plans or risk acceptance should be reported to an appropriate management level in the organisation in accordance with its risk governance framework. Appropriate oversight (for example from the Risk Management function), validation, escalation paths, and monitoring and review should be in place. It is important that risks that have been previously ‘risk accepted’ are reviewed on a regular basis (for example, at a minimum every year).

Each action plan should have an owner (possibly a separate rectification manager depending on the complexity of the plan), a due date, and clearly identify what steps/activities are going to be performed to remediate the risk. It is critical that action owners are held to account, that there is Risk Management oversight and an escalation path in place.

Action plans need to be reported regularly (at a minimum quarterly) to the risk owner’s respective management committee/forum. If possible, it should be a standing agenda item in an existing meeting, and be incorporated within the existing operations of the business.

The forum should have an agreed escalation process to deal with action plans that are not completed by the agreed due date, or that do not address the risk appropriately.

AGGREGATION

PRINCIPLE 8:
Businesses should manage and report risk exposures at multiple levels within the organisation. Top-down assessments should focus on risk appetite and decision-making, whereas bottom-up assessments should centre on the collection of information and recommendations to senior management.

The management and reporting of risk at multiple levels of the organisation is likely to require the results of risk assessments at the business unit level to be re-assessed at the divisional level. This is generally best accomplished through a combination of re-assessing risk within the context of the higher organisational level, its appetite, risk measurement scales and expected outcome from aggregation.

To achieve a comprehensive reassessment, a combined bottom-up and top-down approach is recommended. The bottom-up approach takes the risk assessments of the subordinate businesses as inputs and reassesses them within the context of the higher level business. Where risks appear in more than one business they are assessed to identify cumulative impacts and risks which are material to the higher level business’ objectives.

The top-down approach allows for risks identified at executive level to be cascaded down throughout the business, with appropriate actions being captured within lower levels of the organisation and responsibilities assigned to individuals for delivering and monitoring them.
REPORTING

PRINCIPLE 9:

RCSA reporting should be relevant, timely and useable for the business, taking into consideration the purpose and intended audience. It should cover areas of key risks and uncertainties for consideration, in order to provide the business with insight and drive informed decision-making. RCSA reporting should be written in the context of the business, avoiding risk jargon and acronyms where possible.

All reporting should highlight any areas of concern or uncertainty to the business (including the internal and external risk and control environment). It should be transparent, generate active discussion and drive decision making. It should be regular to maintain momentum and derive continued value from the RCSA.

The audience for RCSA reporting should be driven by the governance arrangements and organisational structure (including Board, relevant committees and senior management). Whatever the level of the audience, emphasis should be placed on keeping the reporting simple and user friendly.

Generally, less detail should be reported to the more senior audience, focussing on the significant areas of risk and/or control weakness that have the greatest potential to damage the business and prevent it from meeting its objectives.

Where reporting is targeted to the particular business unit, more detail can be included to provide insight into key/material risks, an understanding of the effectiveness of the control environment and detail key actions (including the owners of the treatments).

Reports can be in many formats, with some suggestions below:

- risk heat maps/traffic lights;
- dashboards;
- scorecards; and
- narrative reports.

RCSA reporting should:

- highlight concerns and uncertainties;
- provide clarity around known concerns and remediate issues through appropriate actions;
- be transparent around prioritisation;
- provide metrics;
- include status updates on treatments/changes to risk rating;
- be simple and user-friendly, avoiding risk jargon and acronyms;
- be reported frequently to ensure the assessments are current;
- highlight risks outside of the risk appetite (and continue to maintain visibility of these risks);
- highlight any emerging trends/risks; and
- drive decision making.

Suggested forums for discussion of RCSA reporting include (but are not limited to):

- business unit team meetings;
- discussions between group/divisional risk functions and business units;
- business unit management meetings;
- strategic meetings;
- Operational Risk Committee (or similar) meetings;
- Board Risk Committee (or similar) meetings; and
- Board meetings.

The RCSA should be only one element of risk reporting. It needs to be viewed with other risk commentary and metrics from the ORMF. This includes issue management and key risk indicators. These should be considered in light of the operating environment, both internal and external, to inform the operational risk profile of the organisation and should be integrated into business and risk reporting.

MONITORING AND REVIEW

PRINCIPLE 10:

RCSAs should be embedded into the business process and not as a standalone activity. Trigger events must be monitored by the business and Risk Management to ensure the RCSA outcome remains current.

The RCSA process needs to be regularly performed to ensure the RCSA outcome reflects the current risk and control environment of the business. The RCSA outcome should be reviewed and updated at least annually.

Changes to business environment could be a result of internal or external events. These trigger events should be assessed to determine if new risks or controls need to be added, or if the existing risks or controls need to be revised. Examples of trigger events may include (but are not limited to):

- major external events;
- significant regulatory change;
- significant internal loss events or regulatory breaches;
- major control breakdowns (that may or may not result in a loss);
- new products or major initiatives; and
- significant organisational restructures.
The business needs a mechanism in place to capture and monitor the trigger events using sources such as internal loss data, external loss databases and other business data such as control testing results.

Trigger events should be monitored continuously and RCSA outcomes should be updated to reflect trigger events at least quarterly or at the next annual review (whichever is sooner). The significance of trigger events (e.g. size, complexity, relevance), will determine the type of RCSA refresh performed. For example, a trigger event of great significance may warrant a formal re-assessment to be held. Less important triggers may require a less formal approach, i.e. desktop review or discussions. Regardless of the significance, businesses should ensure thematic discussions are embedded as part of business management.

**PRINCIPLE 11:**
Implementing an independent quality assurance process ensures transparency and integrity over the RCSA process, so that outcomes can be relied upon for decision making.

Given the RCSA process is subjective and dependent on the application of experience and judgement; there is a need for an independent quality assurance process to ensure the quality and consistency of the RCSA outcomes. Independent quality assurance refers to the internal or external validation of the process. Internal assurance should be performed by a party that is independent of the assessment process. This can be Risk Management teams, business unit or Group Operational Risk.

These independent quality assurance activities should focus on:

- identifying deficiencies or potential efficiencies arising from the RCSA process, including any systemic issues or trends for the organisation/divisions;
- assessing the consistency of the RCSA process across various business units within the organisation, including review and challenge of assessment rationale;
- assessing the extent RCSA is used to inform business decisions; and
- assessing the reliability of management’s assertion of their risks and controls by reviewing previous RCSA outputs against subsequent losses and incidents.

The results of independent quality assurance activities should be used to:

- validate and inform the aggregation process;
- form a view of the adequacy of resources and capability of management to manage risks effectively within their business units; and
- feed into management’s performance measures in order to drive an appropriate behaviour and culture for the organisation.
APPENDIX A: ACKNOWLEDGEMENTS

Acknowledgements for the development of the RCSA Guidance Note are outlined below.

- **Risk Management Association** for establishing and sponsoring the RCSA Working Group.
- **Commonwealth Bank of Australia** for coordinating development of the RCSA Guidance Note.
- **Ernst & Young Australia** for facilitation and coordination of the RCSA workshops and Guidance Note.

The following industry representatives contributed to the development of the RCSA Guidance Note.

- **Eugene Ee** – Risk Management, Investec Bank
- **Elizabeth Edwards** – Vice President, Head of Risk Management, State Street
- **Graeme Alexander** – Senior Manager, Operational Risk, Rabobank
- **Heather Witschge** – Head of Operational Risk, Bankwest Operations, Enterprise Services, Bankwest
- **Ibro Makhmudov** – RMG Operational Risk, Macquarie
- **Isabelle Testa** – Senior Risk Enablement Manager, Divisional Risk and Governance Team, ANZ
- **Jillian Coulam** – Risk Advisor, Suncorp Bank
- **Jonathan Mogg** – Partner, Financial Services Risk, Ernst & Young
- **Karen Gilbert** – Risk Manager, Vice President, Enterprise Risk Management, State Street
- **Kent Wong** – Senior Manager, Financial Services, Ernst & Young
- **Kirsten Allen** – Executive Manager, Business Risk & Credit Strategy, Westpac
- **Kirsty Whyte** – Senior Manager Operational Risk, GE Capital
- **Krista Franklin** – Senior Risk Business Partner, Bendigo and Adelaide Bank
- **Linh Chau** – Senior Manager Governance and Framework, Group Services Risk, Westpac
- **Luke Haworth-Booth** – Senior Manager Risk, Advice, BT Financial Group
- **Michael Hogan** – Head of Risk, Policy & Procedures, Banking & Payment Services, NAB
- **Michael Nasr** – Executive Manager Operational Risk, CBA
- **Oliver Leung** – Head of Group Operational Risk & Insurance, Westpac
- **Paul Curtis** – Senior Manager, Technology Risk Group Operational Risk and Compliance, ANZ
- **Paul Molloy** – Senior Manager, Group Finance Risk and Compliance, Westpac, Westpac
- **Rachel Solosy** – Senior Manager Risk and Compliance Practices, CBA
- **Richard Michael** – Manager Operational Risk & Internal Control, HSBC
- **Thalia Smith** – Risk Advisor Operational Risk Group Function, CBA
- **Tony Petkovski** – General Manager Operational Risk Group Function, CBA
- **Tuck Lau** – Senior Manager Operational Risk, NAB
- **Vicki Montesano** – National Manager Operational Risk, ME Bank
### Principle 1
Ensure preparation and delivery of the RCSA is completed within the context of the business, its strategies and objectives, and current risk environment.

RCSAs should be preceded by engagement with key stakeholders and subject matter experts, as well as collection and preparation of relevant business and risk information (both internal and external).

### Principle 2
There are three distinct roles within the RCSA process: ownership (of the outcome); facilitation; and challenge and oversight.

While the roles can be performed by the same individual, the facilitation and challenge roles should be separate where possible.

### Principle 3
Using knowledge of the business environment, identify risks that would prevent the business from achieving its objectives.

Risks should be captured in a language that is meaningful to the business to ensure they can be easily understood and managed.

### Principle 4
Risks should be assessed on a residual and inherent basis.

### Principle 5
Control identification should consider the processes, systems, and activities that the business places most reliance on to manage the risk. They should be assessed on design and performance and take into account the business’ risk tolerance.

### Principle 6
Risk assessment rating scales should be proportionate to the size of the business to which they are applied.

### Principle 7
There must be a conscious assessment of residual risk, followed by a decision to accept or not accept the risk. The acceptance decision is done in the context of risk appetite and must be escalated and approved by the relevant governance committee.

Where not accepted, there must be an action plan in place to remediate the risk back to within appetite. The action owner must be a senior business leader. Governance and independent oversight should be in place for risk acceptance and action tracking.

### Principle 8
Businesses should manage and report risk exposures at multiple levels within the organisation. Top-down assessments should focus on risk appetite and decision-making, whereas bottom-up assessments should centre on the collection of information and recommendations to senior management.

### Principle 9
RCSA reporting should be relevant, timely and useable for the business, taking into consideration the purpose and intended audience. It should cover areas of key risks and uncertainties for consideration, in order to provide the business with insight and drive informed decision-making. RCSA reporting should be written in the context of the business, avoiding risk jargon and acronyms where possible.

### Principle 10
RCSAs should be embedded into the business process and not as a standalone activity. Trigger events must be monitored by the business and Risk Management to ensure the RCSA outcome remains current.

### Principle 11
Implementing an independent quality assurance process ensures transparency and integrity over the RCSA process, so that outcomes can be relied upon for decision making.
### APPENDIX C: GLOSSARY

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADI</td>
<td>Authorised Deposit-taking Institution.</td>
</tr>
<tr>
<td>APRA</td>
<td>Australian Prudential Regulation Authority.</td>
</tr>
<tr>
<td>Corrective control</td>
<td>Controls designed to reduce the consequences or damage arising from an individual incident or a significant number of undesirable transactions, errors, events or incidents, after the risk has occurred.</td>
</tr>
<tr>
<td>Detective control</td>
<td>A control designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded.</td>
</tr>
<tr>
<td>End-to-end</td>
<td>Processes across the value chain of an organisation.</td>
</tr>
<tr>
<td>Functional</td>
<td>Processes that follow the organisational hierarchy.</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>The risk to an entity in the absence of any actions management might take to alter either the risk’s likelihood or impact.</td>
</tr>
<tr>
<td>Issue</td>
<td>Identified weaknesses or gaps in the control environment, or business improvements. These are remediated through appropriate action plans.</td>
</tr>
<tr>
<td>Key control</td>
<td>Controls which have the most impact on reducing the likelihood and/or the impact of the risk occurring.</td>
</tr>
<tr>
<td>Operational risk</td>
<td>The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.</td>
</tr>
<tr>
<td>Operational risk profile</td>
<td>Collective summary of all elements in the operational risk management framework containing information such as the RCSA output, internal and external loss data, key risk indicators and audit findings.</td>
</tr>
<tr>
<td>ORMF</td>
<td>Operational Risk Management Framework</td>
</tr>
<tr>
<td>Preventative control</td>
<td>A control designed to avoid an unintended event or result.</td>
</tr>
<tr>
<td>RCSA</td>
<td>Risk and Control Self Assessment – the process of identifying, assessing, monitoring and managing risks and controls.</td>
</tr>
<tr>
<td>RCSA reporting</td>
<td>The report that is produced out of RCSA process, noting specific insights from the data. This may include the ‘risk register’ and ‘risk heat map’.</td>
</tr>
<tr>
<td>Residual risk</td>
<td>The risk that remains after management’s response to inherent risk.</td>
</tr>
<tr>
<td>Term/Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk</td>
<td>The possibility that an event will occur and adversely affect the achievement of objectives.</td>
</tr>
<tr>
<td>Risk appetite</td>
<td>A clear statement of the degree of risk the organisation is willing (and able) to take in pursuit of its goals.</td>
</tr>
<tr>
<td>Risk heat map/matrix</td>
<td>A tool used to visualise the outcome of an RCSA.</td>
</tr>
<tr>
<td>Risk register</td>
<td>The list of risks generated by the RCSA process (often also containing controls).</td>
</tr>
<tr>
<td>Trigger event</td>
<td>Changes to the businesses’ operating model and environment or additional information (i.e. information not considered at the time of the last assessment) that indicates the current RCSA has shifted or changed.</td>
</tr>
</tbody>
</table>

Note: Common industry definitions have been leveraged where appropriate.
## APPENDIX D: WORKSHOP DATES & LOCATIONS

<table>
<thead>
<tr>
<th>Date</th>
<th>Host Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 June 2012</td>
<td><strong>Commonwealth Bank of Australia</strong>&lt;br&gt;Commonwealth Bank Place, South Building&lt;br&gt;11 Harbour Street, Sydney</td>
</tr>
<tr>
<td>8 August 2012</td>
<td><strong>GE Capital</strong>&lt;br&gt;572 Swan Street Richmond, Melbourne</td>
</tr>
<tr>
<td>22 November 2012</td>
<td><strong>Rabobank</strong>&lt;br&gt;Darling Park 3&lt;br&gt;201 Sussex Street, Sydney</td>
</tr>
</tbody>
</table>