RAC Group
Enterprise Risk Management Framework
Guidance & Procedures

Contents

Enterprise Risk Management Framework - Guidance & Procedures

1. Risk & Risk Management – Overview

What is Risk?

Risk can be described as "uncertainty of outcome – whether positive opportunity or negative threat". In all types of business, including RAC, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

RAC is exposed to various types of risks which can relate to:

- Internal factors – systems issues, ineffective operating processes, risks associated with third parties, loss of key colleagues etc
- External factors – regulatory and legal changes, risks arising from our competitor's strategy, and the economic environment etc

What is Enterprise Risk Management ("ERM")?

Risk management can be described as the "process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure." Risk management is not all about threats – it is about maximising opportunities (upside) and not just about things going wrong (downside). Risk management should be viewed as risk and opportunity management.

RAC takes an enterprise-wide approach to managing risk across the Group – this means that the risk framework is focused on identifying and managing all risks affecting RAC's ability to meet its strategic objectives, regardless of the types of risks being considered.

Why does RAC need to manage risk?

There are a number of reasons why it is important that RAC manages risks, which include:

- To ensure our customers receive good outcomes from their dealings with RAC (avoiding "conduct" issues and the associated financial loss / brand/reputational damage these may bring).
- To help us to successfully execute our RAC 2025 strategy and our divisional objectives – managing the risks to the execution of the strategy and ensuring that we exploit the opportunities that we are presented with.
- To protect the overall enterprise value of RAC and ensure that our investors are progressing towards an eventual successful "exit" of their investment.
- To ensure that we operate in line with the detailed FCA / PRA rules & guidance on risk management, compliance and governance that apply to us.
- To ensure we operate in line with other corporate governance requirements that apply to all medium/large private companies (Financial Reporting Council etc).

What are the benefits of effective risk management?

The benefits or "upside" gained from effectively managing risk include:

Improved strategic management

- Greater ability to deliver against objectives and targets
- Improved decision making
- Allowing RAC to seize opportunities which are denied to our competitors because we are able to gain a better-informed view of how a particular risk should be managed
- Increasing the probability of our success and reducing the possibility of failure and the uncertainty of achieving RAC's objectives
- Helping us achieve a positive outcome from a situation that could have gone wrong, without good judgement and effective risk management

Improved operational management

- Reduction in managerial time spent dealing with the consequences of the risk event having occurred
- Improved service delivery to RAC's customers
- Fewer disruptions to our operations and greater operational efficiency

Improved financial management

- Better informed financial decision making
- Greater financial control
- Minimising waste and poor value for money

Improved customer service

- Minimal service disruption to customers and projecting a positive external image as a result of all of the above

2. RAC Group - Enterprise Risk Management Framework (ERMF)

Introduction

The purpose of this document is to describe the Enterprise Risk Management Framework (ERMF) in place across the RAC Group. The ERMF applies across all the RAC Group of companies, including the three regulated entities; RAC Motoring Services, RAC Financial Services Limited, and RAC Insurance Limited.

Overall Aim of RAC Group ERMF

The RAC Group ERMF is designed to enable the Board to set an appropriate risk strategy for the business. The Framework ensures that a strong culture of risk control and management is embedded across the RAC Group and aims to ensure that a 'holistic' view of risk is taken.

The ERMF aims to facilitate the identification and mitigation of risks throughout the organisation. The framework is designed to cover both the management of "hazard" risks, as well as risks associated with opportunities and to enable RAC to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. This comprehensive enterprise-wide approach to risk management aims to assist RAC in benefitting from the 'upside of risk'.

Risk Architecture

The 'Three Lines of Defence' Risk Governance Model

In common with many FCA/PRA regulated firms, RAC has a 'Three Lines of Defence' ("3LOD") risk management model in place. The 3LOD risk management model aims to ensure that sufficient oversight and challenge exists to provide assurance that the business is operating in accordance with regulatory requirements and that risks are being effectively identified and mitigated.

The high-level risk management responsibilities within the 3LOD model are:

- **1st line (Day to Day Management & Control)** - **Business Management** - Board, Exec, Business Units/Functions (HR, IT, Finance, Sales, Operations etc) Primary responsibility for risk identification and management. The 1st Line are Risk & Control owners;
- **2nd line Oversight, Policy & Methodology** - **Risk & Compliance Teams** - Support for and challenge on the completeness and accuracy of risk assessment, risk reporting and adequacy of mitigation plans;
- **3rd line** - **Independent Assurance** - **Internal Audit** - Independent and objective assurance on the robustness of the risk management framework and the appropriateness and effectiveness of internal control

The following table summarises the high-level role of each line of defence.

1st Line of Defence Day to day management	2nd Line of Defence Oversight	3rd Line of Defence Independent Assurance
Management in the business is accountable for: › Risk taking & managing those risks, including risks to good customer outcomes › Implementing the risk framework › Embedding a risk culture › Implementing controls and ensuring that they are operating effectively › Ensuring risks are identified and managed during projects › Ensuring outsourced activity is managed and controlled to an acceptable level	The Risk Function is accountable for: › Oversight and challenge of key risks › Ensuring compliance with risk limits › Developing the risk framework, methods and tools › Being a centre of excellence for risk management expertise › Being able to influence and objectively challenge all key material business decisions	Internal Audit is accountable for: › Providing independent assurance of the robustness of the framework and systems and controls managed and overseen by the 1st and 2nd lines, reporting to the Risk, Audit & Compliance Committee

Key Roles & Responsibilities

The table below outlines the key roles of the different groups of colleagues within the risk management framework:

Board Risk & Audit Committee	› Reviewing reports and other information from the Executive Risk, Audit & Compliance Committee and the Risk Function › Reviewing the adequacy and effectiveness of the Group's internal financial controls and internal control and risk management systems; › Reviewing, as appropriate, the design and implementation of the risk management framework and assessing the effectiveness of the company's management of risk and regulatory compliance; › Assessing whether issues of a risk management or control nature are being appropriately addressed by management in a timely manner; › Reviewing and approving the Group's risk appetite and risk profile, and providing assurance to the Board that the risk profile is consistent with the Group's risk appetite and risk policies and making recommendations to the Board as appropriate;
Executive Risk, Audit & Compliance Committee	› Reviewing the overall design and implementation of the risk management framework › Assessing whether issues of a risk management or control nature are appropriately addressed by management in a timely manner, including the evaluation of potential emerging or new risk issues and their potential impact; › ensuring that the Group Key Risks are captured and articulated to the Board Risk & Audit Committee; › Keeping under review the risk appetite and risk profile to apply
Executive	› Ensuring that risks within their Business Division/Function are identified and that appropriate mitigating actions and controls are in place; › Preparing and keeping up to date the divisional risk registers;

	- Reporting material risks to the Executive and Board risk committees;
Senior Leadership Team	- Understanding, accepting and implementing the risk management process; - Supporting their Exec member in the identification and management of risks within their area responsibility
All Colleagues	- Understanding, accepting and implementing the risk management process; - Identifying and managing the risks faced in relation to the core activities and processes under their control and stewardship;
Risk Function	- Providing oversight of the risk management activity taking place in the 1st line of the business and challenging management in their assessment of risk; - Ensure that the importance of effective risk management is understood by 1st line colleagues and management; - Preparing reports and other management information for the Executive, Board and risk committees in order to provide them with details of key risks, mitigating actions and controls, and to enable them to assess the overall effectiveness of the risk management framework;
Internal Audit Function	- Providing independent assurance of the robustness of the framework and systems and controls managed and overseen by the 1st and 2nd lines, reporting to the Board Risk & Audit Committee

Please refer to the Risk Management & Internal Control Policy which provides full details of roles and responsibilities.

Risk Committee Responsibilities

RAC has in place a framework of committees with risk management responsibilities which assist the business in ensuring that risk is effectively managed. The committee structure is deemed to be appropriate for the size and complexity of the RAC Group.

The responsibilities of each of these committees are documented in the detailed Terms of Reference for the committee. Key responsibilities are shown below.

Board Risk & Audit Committee

Key responsibilities:

- Reviewing the Group's Financial Statements prior to approval on behalf of the Board and reviewing the external auditor's reports thereon;
- Establishing procedures to ensure that the Group monitors and evaluates risks appropriately;
- Ensuring that RAC has a culture of delivering good customer outcomes and identifying any risks to those outcomes is embedded consistently across the business;
- Reviewing internal controls and approving the internal audit plan to monitor the effectiveness of those controls;
- Considering the consistency of accounting policies across the Group and the accounting for any significant or unusual transactions where judgement has to be applied;

Executive Risk, Audit & Compliance Committee

Key responsibilities:

- Reviewing the risk registers from the business areas to ensure that key risks are captured and that appropriate mitigating actions are in place. Ensuring the Group key risks are captured and articulated to the Board Risk & Audit Committee;

- Review the design and implementation of the risk management framework and assessing the effectiveness of the RAC Group's management of risk and of regulatory compliance, including the specific risk appetite for strategic, operational, financial, regulatory and conduct risk;
- Assessing whether issues of a risk management or control nature are appropriately addressed by management in a timely manner;
- Keeping under review the risk appetite and risk profile to apply, providing assurance to the Committee that such appetite and policies are consistent with and aligned to the RAC Group's appetite and profile and making recommendations to the Committee; and
- Reviewing and assessing the approach taken by the RAC business to ensure fair outcomes to customers. Reviewing Conduct Risk MI to ensure it is fit for purpose and identify any trends which may cause concern and suggesting and overseeing mitigating actions and controls, where appropriate

Conduct Risk Committee

Key responsibilities:

Conduct Risk Management and Monitoring:

- Providing oversight of Conduct Risk across the business and its adherence with the Conduct Risk appetite
- Monitoring business output to identify potential Conduct Risks, suggesting and overseeing mitigating actions where appropriate
- Introducing cross functional and departmental Conduct Risk reviews (where appropriate)

Conduct Risk Reporting:

- Reviewing the Conduct Risk MI and providing appropriate challenge and direction
- Reviewing the Conduct elements of the business Risk Register and providing appropriate challenge and direction
- Reporting to the Board, through the Risk and Audit Committee, 3 times per year, the Conduct Risk MI and appropriate updates

Conduct Risk Strategy:

- Reviewing and providing comment on the Conduct Risk strategy
- Reviewing and providing oversight of the Product Governance cycle, including the review and approval of new products

Risk Reporting

Risk Reporting & Monitoring

RAC Risk Universe

RAC's "Risk Universe" consists of all the risks identified across the Group – within Business Functions, by specialist governance teams (Data Protection, InfoSec etc) and at Group Key Risk level.

The following section describes the key risk information that will be recorded and reported on an ongoing basis.

Group Key Risks

RAC has a Group Key Risk Register in place to capture key risks to the business. These represent the "principal" or "top tier" risks to the group. Each risk is allocated an Executive level risk owner(s) in order to ensure clear ownership and ongoing focus on monitoring the risk and ensuring that mitigating actions and controls remain appropriate.

The Group Key Risk Register will be compiled by the Risk Team with consideration being given to the risks disclosed by the business areas on their Key Risk Registers and any aggregation of risks across different risk registers which may occur. The 'top risks' will also be identified. These are risks which, if not well controlled, will result in the most significant impact to RAC and where further action is needed to mitigate them.

The Group Key Risk Register will be updated regularly and will be approved by the Executive Risk, Audit & Compliance Committee and reviewed by the Board Risk & Audit Committee.

Business Division Risk Registers

Each Business Division will maintain a risk register capturing all key risks. The key risk register for each area will be reviewed on a regular basis to ensure that it remains a true reflection of the current key risks in that area and that mitigating actions and controls remain appropriate, via the Risk & Control Self-Assessment Process.

Individual members of the Executive team are responsible for ensuring that material risks within their area are identified and mitigated, and reported via their Business Division Risk Registers.

Emerging Risks

RAC defines emerging risks as being "newly developing or changing risks which are in the process of being understood and quantified, and which may have a major impact on RAC".

Emerging or "horizon" risks will be those where some of the aspects needed to evaluate the risk (risk cause, events, likelihood, consequence, etc) have not yet been determined and the full evaluation process cannot be performed. This means that these risks are not identifiable in a sufficiently clear articulation or definition, but nevertheless exist and pose a threat to RAC.

RAC will use the following sources of information to identify emerging risks:

External Sources

- Media / Daily news
- Third Party Reports / Other research
- External loss events experienced by other companies

Internal Resources

- Major change initiatives
- Operational risk tools – risk events / output of the RCSA process undertaken by each business area
- Meetings with 1st line risk and control owners
- Input from RAC's Executive Team and Board Risk & Audit Committee

Emerging risks should be captured, closely monitored, and escalated to the appropriate risk register(s) (if required). RAC also maintains a Group Emerging Risk Register and this will be populated to show any material emerging risks at Group level.

Operational Risk Management

RAC defines operational risk as being "risks resulting from inadequate or failed internal processes, people, and systems, or from external events."

Operational risk is one of the key risk categories of risk that RAC uses to classify risks within its overall risk management system (the others being; Strategic, Financial, Regulatory/Legal and Conduct).

Examples of operational risks include:

- Internal Fraud – misappropriation of customer premiums, other funds, bribery.
- External Fraud – theft of information, hacking damage, third-party theft.
- Employment Practices and Workplace Safety – employee health and safety, discrimination, workers compensation, talent / organisational restructuring.
- Clients, Products, and Business Practice – products not meeting customer needs, regulatory rules not being followed, outsourcing.

- Damage to Physical Assets – theft, accidental damage, weather events.
- Business Disruption and Systems Failures – disruptions to utilities (electricity, water etc), software failures, hardware failures.
- Execution, Delivery, and Process Management – data entry errors, accounting errors, failed mandatory reporting, failed business change programmes.

Operational risks will be recorded on the risk registers which RAC has in place for each of its 8 key Business Divisions. Each risk register is owned by the member of the Executive team with responsibility for the area. Mitigating actions and controls will be implemented to ensure that the profile of the risk is reduced to an acceptable level.

In addition, RAC maintains a Group Key Risk register. Any Operational risks which were deemed to be key risks would be recorded on this risk register and allocated an Executive owner in order to ensure that the risk is closely monitored and is effectively mitigated. The Group Key Risk register is reviewed regularly with RAC's Executive Team and also by our Board / Executive Risk, Audit & Compliance Committees.

RAC also has Risk Appetite Framework & Statements in place which include a specific statement in relation to Operational risk.

Third Party Risk Management

RAC engages with a range of third party firms to provide us with goods or services. These can include:

- IT services or system providers (systems, "cloud" data storage etc).
- European Breakdown Cover providers, Breakdown contractors.
- Key parts suppliers (parts, batteries, other consumables etc).
- Outsourced Contact Centre providers.
- Claims handling service providers.
- HR services (payroll, screening checks etc).

Many of these services will be critical to RAC's business operations and the services it delivers to customers.

RAC has, in effect, extended its enterprise into the third party company and any issue with a third party supplier could result in disruption to RAC's business operations, adverse customer outcomes, financial loss, and/or brand/reputational damage.

It is therefore vital that we:

- Only engage will third parties that we are confident have the appropriate competence and capability and that we undertake robust due diligence on them.
- Ensure that appropriate oversight arrangements are in place.
- Specifically, in terms of risk management, ensure:
    - We are clear on the risks involved in the arrangement and that we undertake a robust risk assessment (initial and ongoing).
    - We only partner with third party firms that we are confident have effective risk management processes in place and that we seek regular assurance relating to these processes.

Specific FCA/PRA rules and guidance apply to "Material Outsourcing" arrangements. RAC has a Material Outsourcing & Key Supplier Policy in place which sets out the requirements in this area should be referred to.

RAC Insurance Limited – Material Risks

RAC Insurance Limited ("RACIL"), as a PRA authorised insurer, is subject to rules relating to the Solvency II Directive. These rules include the requirement to perform an Own Risk & Solvency Assessment ("ORSA") annually. The process for the identification and assessment of material risks to the solvency of RACIL, or to policyholders, is detailed in the ORSA Policy. Material risks to the solvency of RACIL will be recorded in the RACIL Material Risk Register, which will form the basis of the annual ORSA report.

Climate Change Risk

RAC is required to have a robust framework in place to identify, measure, monitor, manage and report on its exposure to climate risks against a well-defined risk appetite that considers the current balance sheet and business model risk.

The key PRA requirements, taken from their July 2020 'Dear CEO' letter, are summarised as follows:

- Risk identification and measurement - firms must be able to quantify their exposure to climate-related financial risks and develop risk metrics that indicate potential financial loss.
- Risk monitoring - firms must develop risk management tools that support decision-making and allow them to monitor progress against their climate-related strategic aims and risk appetite.
- The PRA expect firms to use risk management tools, which are appropriate for the speed of change that is necessary (e.g. early-warning indicators to engender prompt action where appropriate, or metrics to track a plan to pivot a firm's business model gradually over a number of years).
- Risk management and mitigation - firms to have conversations with clients and counterparties about potential current and future impacts of the physical and transition risk factors.
- Risk reporting and management information - Firms to provide the board & relevant sub committees with MI on their exposure - based on scenario analysis and mitigating actions / associated timeframe. This MI should enable the board / committee to discuss, challenge and take decisions relating to the risks.

Business Climate Change Risk Assessment

RAC's climate-related risks are identified using the following approach.

- RAC's Executive team will perform a 'top down' annual assessment of the material climate change risks to RAC Group with the output of this being recorded on an overall Group Climate Change Risk Register. These risks will be reported to our Board ESG Committee annually.
- The Exec member with responsibility for each area will be able to validate the overall assessment and to suggest risks that are particularly relevant to their areas, as well as seeking input from their teams, if appropriate. As well as recording any material risks on the overall Group Climate Change Risk Register, risks can also be recorded on individual business division risk registers, if appropriate.

The risk framework includes a Climate Change risk category which means that there is the capability for risks to be captured on business division risk registers, if needed.

It is considered that the most effective means of identifying material climate change risks to RAC is to focus on a 'top down' assessment by the Exec / Board. RAC will adjust this approach in future i.e. if performing a more detailed business division climate risk assessment is deemed to be required.

In addition:

- Any risks from climate change that are deemed to be material to the overall Group will be captured in the Group Key Risk Register which is reported into the Exec Risk, Audit & Compliance Committee and Board Risk & Audit Committee.
- Any material risks from climate change which could specifically impact on RAC Insurance Limited will be included in the annual Own Risk & Solvency Assessment ('ORSA').
- Material risks from climate change will be disclosed within the Group Annual Report & Accounts if these are deemed to represent 'Principal Risks' to the performance, future prospects or reputation of the Group.

RAC's Group Risk Appetite Statements include an ESG statement which covers our risk appetite in respect of the risks from climate change. The Group Risk Appetite Statements will be reviewed annually.

As our understanding of the risks that climate change presents to our business increases, further FCA or PRA regulatory output is released setting out their expectations of firms, and as we learn from the actions being taken by other comparable businesses, our approach to managing the risks from climate change will evolve.

Risk Ownership

Group Key Risks

All Group Key Risks will be allocated an Executive level risk owner with responsibility for managing the risk in line with agreed risk appetite, ensuring that mitigating actions and controls remain appropriate, and reporting on progress / changes in the risk profile to the relevant committees.

Business Area Risks

The Executive member with accountability for each business area will be responsible for the identification and management of risks in their area, via the Risk & Control Self-Assessment Process. Responsibility for monitoring and managing the risk can be delegated to other colleagues but will remain the ultimate responsibility of the Executive risk owner.

Risk Appetite & Standards

Risk appetite is termed as the "amount and type of risk that an organisation is prepared to seek, accept or tolerate". RAC has Risk Appetite Framework & Statements in place which ensure that risk appetite is set by the Board, cascaded throughout RAC, used in decision making, and regularly reviewed to ensure the statements reflect the current risk appetite of the business.

Group Risk Appetite Statements

The Group Risk Appetite Statements are aligned to the main categories of risk in RAC's risk management framework.

Conduct Risk Appetite Statements

RAC has implemented a Conduct Risk Appetite Framework & Statements in line with FCA requirements and current best practice. The statements are designed to articulate the Board's specific appetite and tolerance for conduct risk in order that this can be communicated to all colleagues. The RAC risk appetite statements have been developed to incorporate a high-level statement and to cover the customer "lifecycle" (Culture & Governance, Product Design & Governance, Sales Processes & Post Sales Service).

The Risk Appetite Statements should be considered in all business decisions, which should be taken in line with them. The Risk Appetite Statements will be reviewed on a regular basis or following changes in overall strategy, in order to ensure that they remain appropriate.

Please refer to the Risk Appetite Framework & Statements document for full details.

ERM Policies, Standards & Guidance

The following are key documents within the ERM framework:

- Risk Management Strategy
- Risk Management & Internal Control Policy
- Risk Appetite Framework & Statements
- Risk Management Guidance & Procedures
- ORSA Policy

Risk Management Governance & Assurance

The Board of RAC is responsible for overseeing the group's risk management and internal control systems, which management is responsible for implementing. The Board aims to deliver clear guidance to the business on matters relating to risk management and internal control. The Executive Risk, Audit & Compliance Committee and Board Risk & Audit Committee support a strong risk governance framework. These committees monitor and review the effectiveness of all risk management activities and, in particular, monitor adherence to agreed risk limits.

The Risk & Compliance Team provides effective challenge to risk owners and co-ordinates the reporting of information to the risk committees. In addition, the RAC Internal Audit function gives assurance to the Board and risk committees as to the overall effectiveness of risk management arrangements

RAC's external auditors (Deloitte) may review the effectiveness of the ERMF as part of their annual audit. From time to time RAC may engage external consultants to review the overall governance arrangements for the business, including the ERMF.

Risk Management Culture

The Board of the RAC is committed to ensuring that a risk aware culture exists, with clear accountability for risk related decisions, and that the importance of risk management is driven from the 'top down'.

Review of the RAC ERMF

The RAC Group ERM Strategy and Framework will be reviewed annually or following any significant changes in business strategy in order to ensure that it remains fit for purpose and improvements will be made, if required.

Appendix 1 - Risk & Control Self-Assessment Methodology & Procedures

Risk & Control Self-Assessment ("RCSA") is the process by which each Business Division or Group Function reviews their material risks and the controls in place to mitigate these.

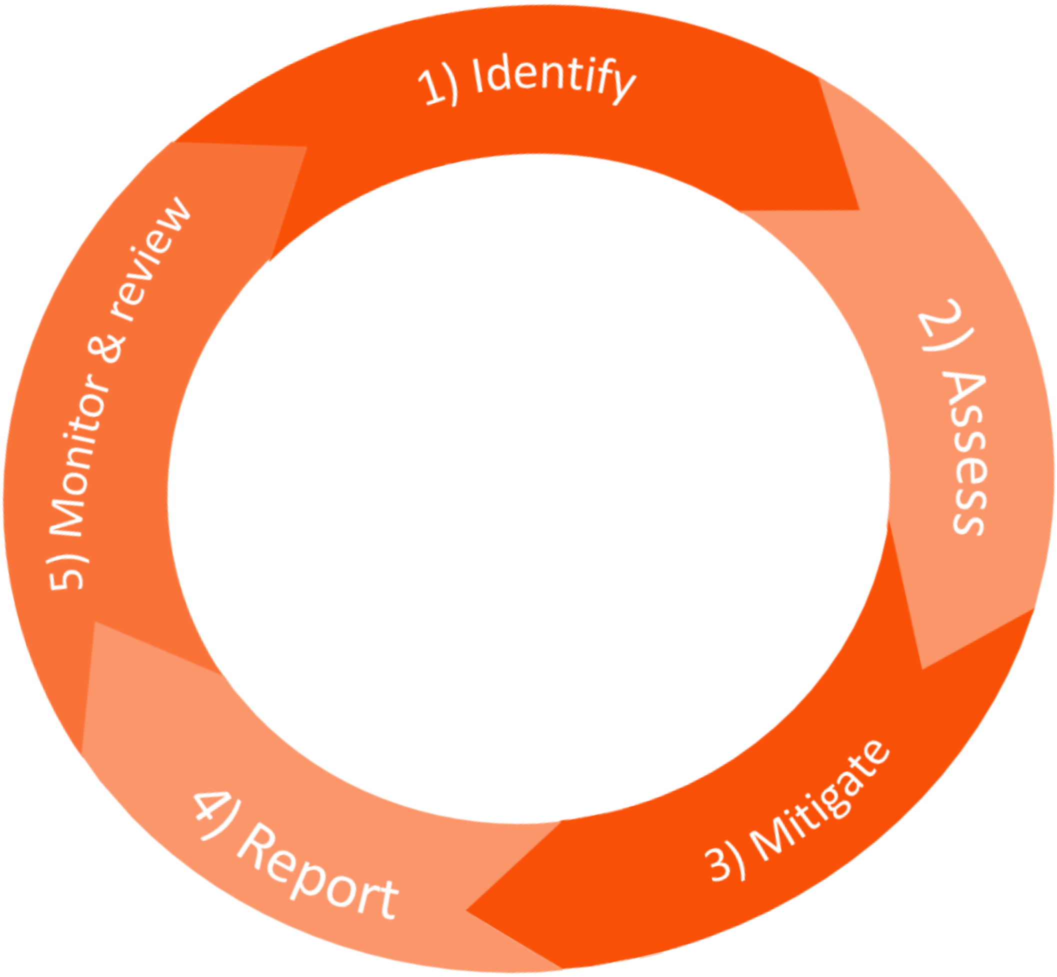
This section outlines RAC's Risk & Control Self-Assessment methodology and procedures, which aim to ensure that a consistent approach is taken.

RAC Enterprise Risk Management Process

RAC uses a risk management process with 5 key stages, which are as follows:

1. Identify Risks
2. Assess & Prioritise Risks
3. Mitigate Risks
4. Report on Risks and Mitigation Status
5. Monitor & Review the Level of Risk Exposure & Mitigation Status

The 5 key stages are part of an ongoing "cycle". Risk management should be a dynamic process and, in view of this, the identification phase needs to be carried out continuously.



The following section describes each stage of this process in more detail.

1) Risk Identification

Identify
Assess
Mitigate
Report
Monitor & Review

The exercise of identifying and assessing risk is a key part of "Risk & Control Self-Assessment" (RCSA).

Risk identification can be described as the process of finding, recognising and describing risks.

This process should be completed 3x per year, in line with reporting to the Exec Risk, Audit & Compliance Committee.

The aim of risk identification is to identify RAC's exposure to uncertainty and help us decide how we want to manage it. Risk identification will be conducted using a 'top down' (identification of key strategic risks) and 'bottom up' (identification of more granular risks within individual business areas) approach.

The Exec and SLT of each Business Division to ensure that the risk register captures all material risks in each business area. Risk Team to assist with facilitation of this exercise, if required.

Risk identification will consider:

- External factors - regulatory/legal change, competitor strategies, economic factors etc
- Internal factors - such as system malfunctions, ineffective operating processes, loss of key colleagues etc

Risks can also fall into the following categories:

- Strategic risks - those impacting on RAC's mission and strategic objectives.
- Financial risks - those risks impacting on the solvency or financial performance of the business.
- Operational risks – risks that could result from inadequate or failed internal processes, people and systems or from external events.
- Conduct / Customer Outcome risks - risk of RAC's behaviour resulting in poor outcomes for customers.
- Regulatory/Legal risks - those arising from the potential failure to comply with the various laws and regulations, or that changes to existing laws and regulations could impact on RAC's strategy, business model or on specific aspects of our operations.

Which risks should be captured on a Business Division Risk Register?

The Business Division Risk Register should contain a focused list of all material risks within each Business Division. Whilst there are no specific parameters for the risks that should be captured, examples (not exhaustive) include:

- Risks which could have a material impact on customer outcomes (these will generally be systemic issues – those which could affect multiple customers).
- Risks which could result in significant financial loss to the Business Division and/or the wider RAC Group.
- Risks which could impact on the ability of each Business Division to achieve its objectives and/or impact on RAC's overall ability to achieve its strategic objectives.
- Operational risks (risks resulting from inadequate or failed internal processes, people, systems or external events) which could impact on our ability to provide services to customers.
- Any material risks that exist for a period of time but may then fall away for example those arising from key projects (these are often termed "transitional risks").

Further risks or events which may inform us of material risks / areas where our controls require improvement include:

- Regulatory Breaches, Key Data Risks or Data Breaches (inc material risks highlighted in Data Protection Impact Assessments ("DPIAs"))
- Risk Events – where a material loss event or near miss has occurred;
- Internal Audit reports – where material risks have been identified which are not currently recorded on the risk register;
- Material Third Party risks – even if we have outsourced key activities, these may still present risks to RAC's operations / customer outcomes.

Risks to the successful execution of our strategy (overall Group strategy / Business Division strategy) should be a particular consideration in the risk assessment.

Discussion should take place within the SLT of each area to discuss potential risks, determine whether risks should be added to the risk register, and generally "sense check" the assessment.

All material risks should be captured, even if the mitigating actions and controls in place are deemed to be sufficient.

We also need to ensure that any emerging risks are captured, so that we ensure our assessment is more forward-looking and help us spot potential risks before they turn into issues.

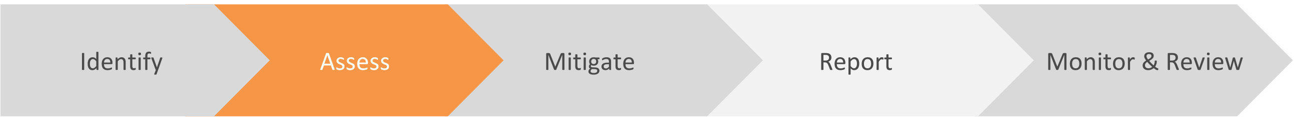
In summary, whilst it is clearly not practical to capture every risk within RAC Group, we want to ensure that each Business Division continues to consider whether it has captured all its material risks.

Own Risk & Solvency Assessment ("ORSA") – RAC Insurance Limited

The risk assessment process will consider whether any of the risks arising from the individual business areas of RAC Group, as well as Group Key Strategic & Operational Risks, have the potential to have a material impact on the solvency of RAC Insurance Limited ("RACIL"), or on the delivery of services to RACIL policyholders. These risks will be included in the periodic assessment and reporting of risks relating to RACIL to the RACIL Board and will be included in the annual ORSA process and report, if appropriate.

Please refer to **Appendix 2** for further guidance on RCSA.

2) Risk Assessment



Risk Assessment includes the process of Risk Analysis - the process of understanding the nature of the risk and determining the level of risk (level is a combination of likelihood and consequences) and Risk Evaluation - the process of comparing the results of risk analysis with risk criteria (risk appetite – see section below) to determine whether the risk and its magnitude is acceptable and tolerable.

Risks assessed using the Probability and Impact matrix including impact guidance (Customer impact, financial impact and operational impact). The assessment should consider what the Inherent risk is (pre-control) and also what the Residual risk position is now (the position now considering the mitigating actions and controls that are in place). The status of each risk to also be assessed versus RAC's Group Risk Appetite Statements. The Risk Team will calibrate risk ratings.

Please refer to **Appendix 2** for further guidance on RCSA.

3) Risk Control

Risk Control (also referred to as Risk Mitigation or Treatment) is the process of selecting and measuring appropriate mitigating actions and controls to modify the risk, including those required to bring the risk back within risk appetite.

In order to respond to risks, one of the following types of responses are generally selected:

- Tolerate (accept/retain) – the risk and its likely impact
- Treat (control/reduce) – the risk to reduce the likely impact or exposure
- Transfer (insurance/contract] – the risk to a third party i.e. by conventional insurance, or by paying a third party to take the risk in another way
- Terminate (avoid/eliminate) – the activity generating the risk

A range of controls may be used to manage risks, for example; preventative, corrective, directive controls.

Most risks can be managed, either by minimising the likelihood of the risks occurring and / or reducing the severity of the consequences should the risk occur. Relatively few risks have to be avoided or transferred. Risk owners must judge the most appropriate course of mitigating action to address each of the risks that have been identified.

The cost/benefit of each control action must be assessed. The benefits will not always be solely financial. Risk owners need to use their own professional knowledge and experience to judge whether the financial cost of risk control is justified in terms of non-financial benefit to RAC. On occasion, risk owners may conclude that the cost of the control action may outweigh the benefits which will accrue as a result of the action being taken. In such instances, all or an element of the risk is retained. However, no regulatory rules or policies should be breached when making this decision.

Any Planned Actions (also termed "Key Risk Actions") that are required should be recorded, including who will be responsible for delivering them and when are we aiming to get them in place.

The mitigating actions and controls selected should be reviewed regularly in order to ensure that they remain appropriate and are operating as intended. Clear ownership should be attributed to all mitigating actions and controls.

When documenting controls we should focus on articulating the "control framework" that helps us to mitigate each risk on an ongoing basis. This could be separate documented processes, governance forums/other meetings, management information/formal review of this with action promptly taken etc.

Risk Acceptance

Any risk acceptance taking place should be considered (including making reference to the Group Risk Appetite statements). Risk acceptance should also be formally documented and referred to the appropriate level of management for approval. Reference should also be made to other RAC risk acceptance processes, if appropriate. For example, those described in the Group Delivery Framework or within Technology Change Management / Project closure proceses.

Please refer to **Appendix 2** for further guidance on RCSA.

4) Risk Reporting

Identify
Assess
Mitigate
Report
Monitor & Review

Risk reporting is the process of recording and reporting details of material risks within each business area.

Risks are captured on the Risk Register and reported to the Executive Risk, Audit & Compliance Committee via the Risk Management & Internal Control Summary.

The Risk Management & Internal Control Summary records details of key risks, the risk rating and details of the actions being taken to mitigate the risk.

5) Risk Monitoring

Identify
Assess
Mitigate
Report
Monitor & Review

Risk monitoring is a vital component of the ongoing risk management cycle and is the process of monitoring the status of risks, including the probability and impact, effectiveness of mitigating actions and controls, as well as the profile of the risk compared to our risk appetite.

Monitoring will include review of:

- The implementation of any agreed risk control action plan
- The effectiveness of these actions in controlling the risk; and
- How the risk has changed over time

Risk owners must monitor the implementation of the risk mitigating actions and controls in order to ensure that responsibilities and deadlines do not slip.

Risk monitoring is owned by the Executive Team member with responsibility for the Business Area / Function and should be undertaken on a regular basis. The risk register should be maintained as a "live" document which is actively used to manage/track key risks. The frequency of the monitoring required will be dependent on the nature of the risk and the assessment of its probability and impact. For example, risks which would have a potentially severe impact may require 'close and continuous' monitoring, whereas periodic monitoring of risks which have a less severe potential impact may be more appropriate.

Any accepted risks should also be monitored / revisited periodically to ensure any mitigating actions are effective and that no further action is required.

Risk Categorisation/Classification

RAC categorises risks into five high-level categories (also known as "key risk drivers"). The process of categorising risks helps us to identify any accumulations of risks and aggregate them, which also assists us in establishing our overall risk profile. The categories are described below.

- Strategic – risks impacting on RAC's mission and strategic objectives
- Operational – risks resulting from inadequate or failed internal processes, people, and systems, or from external events
- Financial – risks impacting on the solvency or financial performance of the business
- Regulatory/Legal – risks arising from failure to comply with applicable laws and regulations
- Conduct / Customer Outcome – risks of RAC's behaviour resulting in poor outcomes for customers

Underneath the high-level risk categories sit a number of sub-categories of risks which are shown in the following table.

Risk Category **(Level 1)**	**Strategic**	**Operational**	**Financial**	**Regulatory/ Legal**	**Conduct / Customer Outcome**
Risk Category (Level 2)	Bids Client Relationship Mergers / Acquisitions Investments Capital Structure	Process Information Security/Cyber People Assets & Liabilities MI Technology Facilities Change Service Delivery Third Party/Outsourcing Climate Change / ESG Data Governance Business Continuity / Disaster Recovery	Market Liquidity Credit Solvency Underwriting / Reserving Investment Reinsurance Income / Expense Assets & Liabilities Reporting Tax Procurement	Regulatory Legal Governance Health & Safety	Customer Outcome risk: Product & Service Price & Value Customer Support Customer Understanding Incentive/Remuneration Internal Fraud External Fraud: Third party supplier fraud Customer fraud

In addition, risks can be described as Emerging or Horizon risks. Please see the Emerging Risk guidance in Section 2.

Risk Probability, Impact & Status

Once risks have been identified they need to be assessed. This process requires risk owners to assess the level of risk by considering:

- The probability of an event occurring – "likelihood"
- The potential severity of the consequences should such an event occur – "impact"

In common with many companies, RAC uses a probability and impact matrix to assess individual risks. This helps us to ensure that a consistent approach to the assessment of risk is adopted across the group and assists with the reporting of risks. This should be used for the "Inherent" ("gross") assessment and for the "Residual" ("net") assessment.

Risk Probability

Each risk is assessed using the following probability guidance and a score allocated based on the likelihood of occurrence:

		Guidance	Weighting
High	Very Likely	>70% probability of occurrence within one year	4
Medium (High)	Likely	>45% & <70% probability of occurrence within one year	3
Medium (Low)	Possible	>20% & <45% probability of occurrence within one year	2
Low	Remote	<20% probability of occurrence within one year	1

Risk Impact

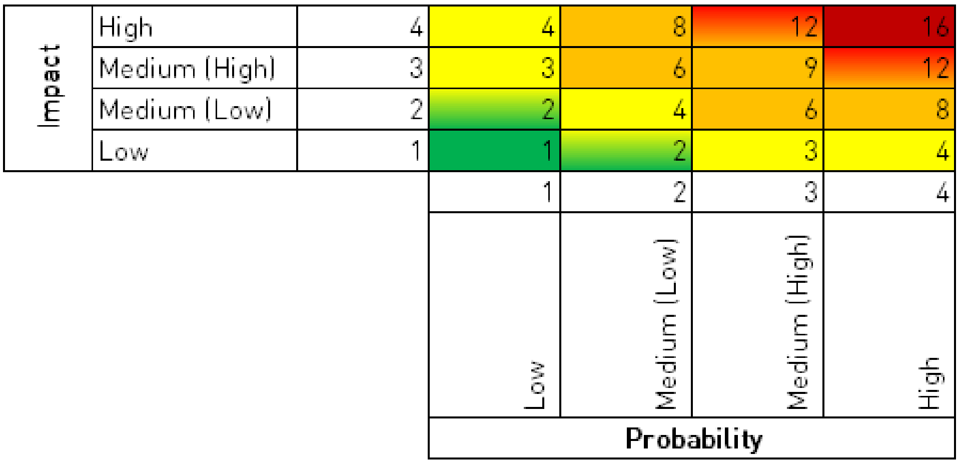
Each risk will then be assessed in line with the following impact guidance and an inherent and residual score allocated based on potential impact:

		Guidance	Weighting
High	Critical	Major financial loss, operational disruption or impact on customer outcomes.	4
Medium (High)	Significant	Significant financial loss, operational disruption or impact on customer outcomes.	3
Medium (Low)	Important	Financial loss, impact on operational effectiveness or some impact on customer outcomes	2
Low	Moderate	May lead to disruption / financial loss / minor impact on customer outcomes	1

Output Matrix

The risk matrix shown below is then used to produce an overall rating for each risk. In common with many companies, RAC uses a "4 x 4" output matrix for assessing probability and impact.

The output is a 'RAYG' rating for each risk. This assists us in prioritising and ranking risks and to identify our aggregate/total risk exposure and allows the benchmarking of risks across all RAC business functions.



Impact	High	4	4	8	12	16
	Medium (High)	3	3	6	9	12
	Medium (Low)	2	2	4	6	8
	Low	1	1	2	3	4
			1	2	3	4
			Low	Medium (Low)	Medium (High)	High
			Probability			

Following the assessment exercise, actions required will be prioritised as follows:

- Red risks – will be given priority and will require an immediate action plan.
- Amber risks – will require an action plan and/or the risk will need to be closely monitored.
- Yellow risks – can generally be accepted but may require an action plan. These risks will need to be monitored to ensure that the status does not deteriorate.
- Green risks – can be accepted and will not require action plans. These risks will need to be monitored to ensure that the status does not deteriorate.

Risk Status

The status of individual risks can be described as follows:

- Inherent Risk – the risk that an activity could pose if no controls or other mitigating actions were in place. Essentially, the risk if were to 'do nothing'. This is sometimes termed the "pre control risk"
- Residual Risk – describes where the risk sits today considering any controls or mitigating actions which have already been implemented.
- Target Level (risk appetite) – the level of risk an organisation is willing to take – where the level of risk needs to be, if it is not there already

Our assessment and reporting of risk should consider the Residual risk which exists at the time of the assessment. The Inherent risk position will also be assessed and recorded.

Emerging Risks

Emerging risks will be those where some of the aspects needed to evaluate the risk (risk cause, events, likelihood, consequence, etc) have not yet been determined and the full evaluation process cannot be performed. This means that these risks are not identifiable in a sufficiently clear articulation or definition, but nevertheless exist and pose a threat to RAC.

Emerging risks will be captured, closely monitored, and escalated to the appropriate risk register(s) (if required).

Risk Appetite & Tolerance

The assessment of each risk should consider the Board approved Group Risk Appetite Statements and Conduct Risk Appetite Statements. Where risks are deemed to be out of appetite immediate action should be taken to reduce the level of risk to within appetite. Please refer to the Risk Appetite Framework & Statements document for further information.

Appendix 2 - Risk & Control Self-Assessment – Additional Guidance

Risk & Control Self Assessment ("RCSA") is the process by which each Business Division or Group Function reviews their material risks and the controls in place to mitigate these.

This should be completed as:

- A Full assessment (3x per year).
- An Interim assessment (in between formal 3x per year updates).

Further guidance on the key points to consider when undertaking Full and Interim assessments is provided below.

Full Assessment

The Full assessment should be completed 3x per year with the key risks reported to the Exec Risk, Audit & Compliance Committee.

Risk and control owners should be asking the questions in the following checklist when completing this assessment:

Area	Key points to consider
Key Risks	What are the key risks within each area that would have a significant operational, financial, strategic or customer impact if they are were to occur (including third party risks). Have we missed anything? Are there any new projects or other business initiatives that might mean we need to acknowledge new risks?
Risk Rating	Have the risks been rated appropriately (using the guidance provided) so that we are focusing our efforts on mitigating and tracking the key risks?
Risk Events	Have there been any 'Risk Events' (loss events / regulatory breaches) / other issues which might mean we need to strengthen our controls and to acknowledge new risks?
Emerging Risks	Are there any emerging risks that need to be captured and tracked at Business Division level?
Existing Controls	Is each risk being mitigated effectively? Are we sure we know what the controls are? Are these controls robust? Do they make sense and do they actually work? Have they been documented and tested? Is ownership clear?
Additional Actions/Controls	Are there any additional actions we need to take or controls we need to implement? Is ownership clear and are we tracking these additional controls through to completion?

This assessment will allow each area to form a view as to the sufficiency of the controls in place and to determine whether the risk is "Under-controlled", has "Appropriate controls" in place, or is "Over-controlled". If the outcome of the assessment is that the risk is "Under-controlled" or "Over-controlled", this would then drive an action plan to either implement further controls or to remove controls.

Interim Assessment

In between the Full assessments the Business Division of Group Function should undertake an interim review of the register, focused on the key risks.

Risk and control owners should be asking the questions in the following checklist when completing this assessment:

Area	Key points to consider
"Top" Risks &	What are the "Top" (3 approx) risks? Are we doing enough to address these risks? Is there enough urgency in our efforts to mitigate them and what do we need to do to accelerate

Mitigation	this?
New Risk Events	Since the last full review, have there been any new 'risk events' (loss events / regulatory breaches) / other issues which might mean we need to strengthen our controls and acknowledge new risks on the risk register?
Additional Actions/Controls	Where we have committed to implementing additional controls (on any of our risks), have these now been implemented? What do we need to do to drive these actions forward to completion?

Revision History

Version	Date	Author	Remarks
1.0	01/03/2016	A.Catleugh	Document Creation
2.0	26/10/2018	A.Catleugh	General update
3.0	28/03/2019	A.Catleugh	Major update. Numerous changes made.
4.0	18/09/2019	M.Andrews	Updated Output Matrix and impact/probability guidelines.
5.0	16/09/2020	M.Andrews	Updated formatting
6.0	20/05/2021	A.Catleugh	Major update. Additional guidance added to Appendix 1. Appendix 2 added.
7.0	04/03/2022	A.Catleugh	New 'Climate Change Risk' section inserted. Due to the evolving nature of climate change risk this section will need to be subject to a detailed review in Q4 2022. Further information added to Group Key Risks and Emerging Risks sections.
8.0	08/07/2022	A.Catleugh	Wording in Climate Change Risk section updated
9.0	12/05/2023	A.Catleugh	Review undertaken in connection with Consumer Duty implementation to ensure that the importance of identifying risks to good customer outcomes is clearly explained. Various changes made to wording. In addition, changes made to description of committees (names/responsibilities) to align these with the description in other documents.