December 2021

Risk, Compliance & Assurance

Version 2.0

Money & Pensions Service

Purpose & Overview

Purpose

This Money & Pensions Service (MaPS) Risk Management Framework (RMF) is designed to be a documented structured process for identifying potential threats, our strategy for eliminating or minimising the impact of these risks and the mechanisms to effectively monitor and evaluate this strategy. The RMF is one of the three pillars of our Risk Management Approach (RMA). This framework ensures we have an agreed and documented process for effectively identifying, measuring, mitigating, reviewing, monitoring and reporting the risks we face in line with corporate governance and best practice standards. It also provides assurance to the MaPS Board that the Accounting Officer has appropriate systems and structures in place to manage risks to the organisation achieving its objectives.

Principles & Benefits

For the RMF to be effective the following principles should be applied;

- Risk management is an essential part of governance and leadership and fundamental to decision making within the organisation at all levels
- Risk management is an integral part of all organisational activities to support decision making in pursuit of objectives
- Risk management should be collaborative and informed by the best available information and expertise
- Risk management processes should be structured to include;
  - Risk identification, assessment and measurement to determine and prioritise how the risk should be managed;
  - A planning process for determining how to treat the risk and ensure it is managed within appetite
  - The design and operation of integrated, and informative risk monitoring;
  - Timely, accurate and useful risk reporting to enhance the quality of decision-making to support management and oversight bodies in meeting their responsibilities

Risk management should be subject to continued improvement to take into consideration learning and experience.

Risk Management Approach

As set out in the MaPS RMA, detailed in Appendix A, the RMF is one of three pillars that set out how MaPS will manage risk in pursuit of our objectives. A Compliance Framework, detailing what rules and regulations MaPS needs to be compliant with and how MaPS should fulfil these obligations is the second pillar. Likewise, an Assurance Framework, which is designed to provide assurance to the executive and non-executive members of the Board, the Accounting Officer, key external stakeholders, the Chief Risk Officer (CRO) and other Executive officers of MaPS that the organisation has in place effective risk management procedures, robust and comprehensive controls plus a positive culture with regards to compliance is the third pillar.

It is vital these three frameworks operate in parallel with the shared objective of enabling MaPS to achieve it's strategic, functional and change objectives. Transparency and availability of information between the three pillars is crucial to ensure risks identified through Compliance and Assurance activity is measured, monitored and reported. The RMF, through risk reporting, will guide Compliance and Assurance activity based on areas of concern in the MaPS risk profile.

Three Lines of Defence

MaPS has adopted the Three Lines of Defence model in its approach to risk management.

Everyone at MaPS has some responsibility for risk management. The Three Lines of Defence model provides a simple and effective way to help, define, delegate and coordinate risk management roles and responsibilities within and across the organisation. The illustration below helps demonstrate the relationship between each line of defence and external bodies.

The Board and accounting Officer have overall accountability and responsibility for the management of risk within MaPS. The Audit, Risk & Assurance Committee (ARAC) takes the lead in focusing on this responsibility for the Board.

First Line of Defence (1LoD)

The First Line of defence (1LoD) is responsible for the day-to-day management of risk and quality assurance within the organisation.

The 1LoD are the primary owners of risks at MaPS, with responsibility for identifying, measuring and managing risk.

The 1LoD are responsible for executing the response to identified risks on a day-to-day basis, through the planning and implementation of internal controls and mitigating actions. There should be adequate monitoring controls in place to ensure controls are managing the risks as anticipated, highlighting any control weakness or inadequate processes and unexpected events.

Second Line of Defence (2LoD)

The Second Line of Defence (2LoD) provides objective review, monitoring and appropriate challenge to the 1LoD. It should work collaboratively with the 1LoD whilst maintaining its independence when assessing risk exposure.

The 2LoD are made up of functions and activities that monitor and facilitate the implementation of effective risk management practices and facilitate the reporting of adequate risk related information up and down the organisation to enable informed decision making.

The 2LoD will support management and risk owners by bringing expertise, best practice, and monitoring alongside the first line to help ensure that risks are effectively managed at MaPS.

The 2LoD are responsible for developing the policies, frameworks and tools that will enable effective risk management at MaPS.

Third Line of Defence (3LoD)

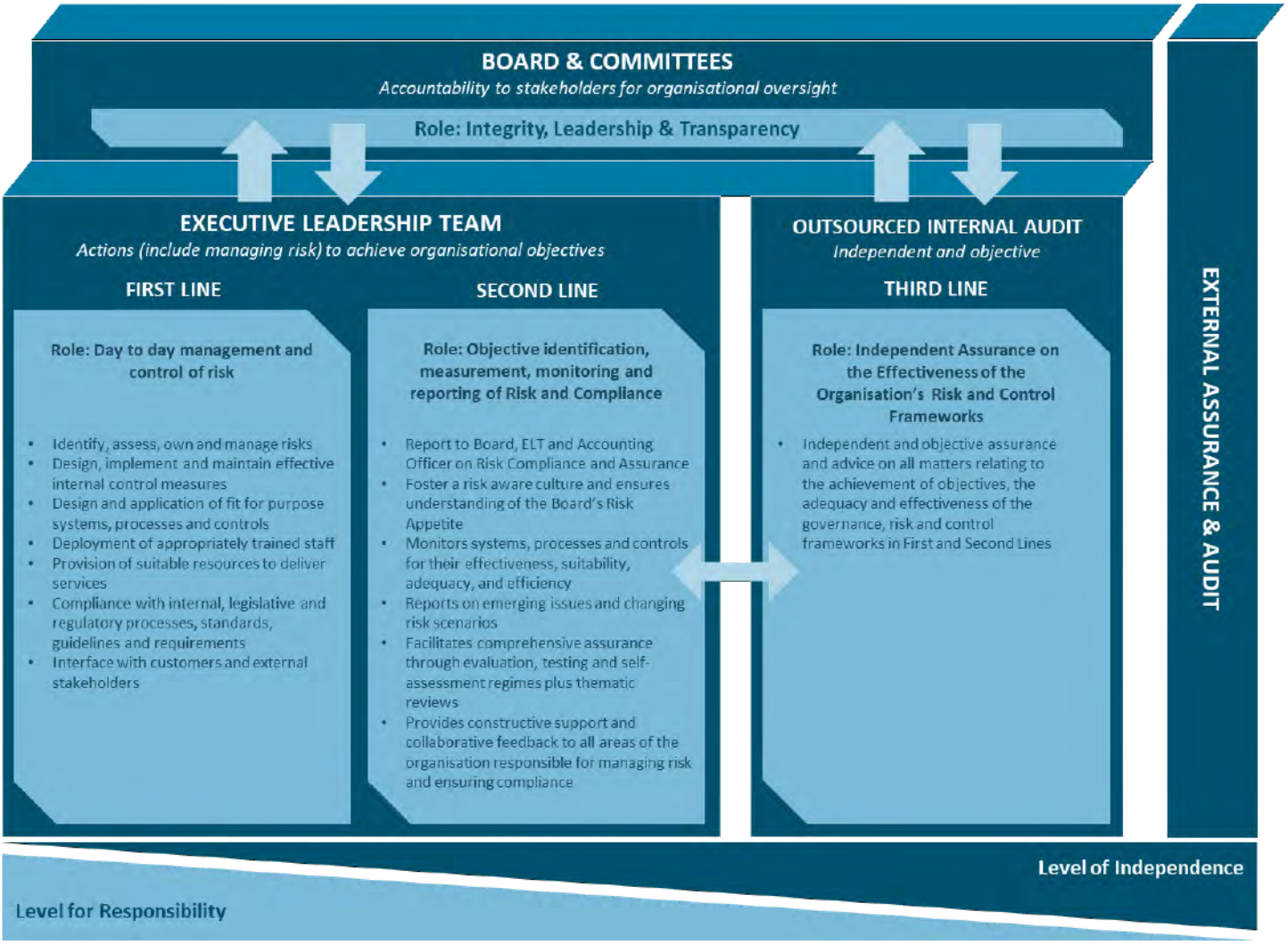
Through a risk-based approach to its work, the Third Line of Defence (3LoD) provides independent assurance on the design and operation of the control environment including the activities performed by both the 1LoD and 2LoD. It will provide an objective evaluation of how effectively MaPS assesses and manages its risks. MaPS' Third Line of Defence is performed by its Internal Audit function, which is outsourced.

The 3LoD reports its findings into the ARAC but is managed on a day-to-day basis by the CRO, who must therefore pay particular attention to ensuring that the 3LoD can maintain its independence in bringing its findings to the ARAC.

Collaboration

The lines of defence have a common objective: to help the organisation achieve its objectives with effective management of risk, illustrating the importance of MaPS' positive and constructive risk culture, underpinning the risk management process and approach.

The Three Lines of Defence model is also designed to ensure that the Board can receive independent reports or a second perspective from the CRO. Thus, while the role holder reports into the CEO / Accounting Officer, it is also very important that this position can have direct access to the Chair of the ARAC and, if necessary, the Chair of the Board.



Risk Appetite

Her Majesty's Treasury defines 'risk appetite' as 'the amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time. It is measured according to a rising scale of appetite from averse to hungry as defined below. The definitions used by MaPS are consistent with those in the HM Treasury guidance:

- **Averse**: Avoidance of risk and uncertainty is a key objective
- **Minimalist**: Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited reward
- **Cautious**: Preference for safe options that have a low degree of residual risk and may only have limited potential for reward
- **Open**: Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward
- **Hungry**: Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risk)

These definitions are then applied to categories of risk that MaPS could be exposed to in the delivery of its objectives. These categories are defined in a Risk Taxonomy. This is detailed in the Board's Risk Appetite Statement which is reviewed on an annual basis, ideally in line with the Business Planning cycle. However, they can be reviewed and modified by the Board in the event that the organisation's objectives and strategy change.

The Risk Appetite Statement is owned by and should reflect the Board's appetite for risk as the organisation seeks to meet its objectives. However, it is the responsibility of management to apply the statement to day-to-day management of risk. Thus, it is very important that the Executive team embrace and cascade the contents of the Risk Appetite Statement and that the Risk, Compliance and Assurance Directorate takes steps to increase awareness and understanding of it at all levels in the organisation.

Sometimes it is not easy to apply the definitions of appetite and category of risk to each and every situation. At executive level the CRO should take responsibility for interpreting the Board's Risk Appetite but should always defer to the Board's view when expressed or seek further guidance via the Board ARAC if challenged or where there is ambiguity.

On a regular basis, the MaPS CRO should report to the Board or Board ARAC the organisation's exposure to risk relative to the Board's appetite and as soon as practical if in the CRO's view, MaPS is outside of the Board's Risk Appetite for one of the high-level categories of risk in the Risk Appetite Statement.

There are **seven** categories of risk within the Risk Taxonomy, with a further 33 sub-categories. These sub-categories of risk enable clearer, more meaningful risk reporting. The seven high-level categories are;

- Reputation & Credibility
- Operational Delivery
- Financial
- People & Culture
- Legal / Regulatory
- Information Security
- Strategy

The full Risk Appetite Statement (with the sub-categories detailed) can be found in Appendix B.

Risk Management Process

Overview

As set out in the MaPS RMA document, 'Risk' is defined as '**an uncertain event or set of events that, should it / they occur, will have an effect on the achievement of objectives.**"

Some risk-taking is inevitable if an organisation is to achieve its objectives and effective risk management is likely to improve performance against objectives.

The risk management process consists of five key components:

1. **Identify** - The purpose of identifying risks is to gain a full understanding of any risk that might threaten MaPS' pursuit of its strategic objectives.
2. **Measure** - Once risks have been identified, it is important to measure those risks to help explain the significance of the risks that MaPS faces in pursuits of its strategic objectives
3. **Manage** - It is not enough to just identify and measure risks; they need to be mitigated through some form of proactive management
4. **Monitor** - Risks change, priorities change, actions get completed, risk responses that were once effective can become less effective, etc. It is, therefore, important to continue to monitor and review risks and the effectiveness of their controls and measures.
5. **Report** - It is essential that periodic risk reports are provided to key stakeholders via committees and Boards, but also flexibly when there are significant changes in circumstances or key decisions to take

Guidance on how to complete each step in the risk management process is provided in the following section, with examples of best practice, tools and methodologies to enable all colleagues to exercise their responsibilities in risk management effectively.

A crucial component of effective risk management is a positive and constructive risk culture with values and behaviours embedded throughout all levels of MaPS and everyone taking personal responsibility to manage risk in everything they do. Raising awareness will ensure consistency and best practice is being adopted across the organisation enabling MaPS to operate within its risk appetite. To achieve a positive risk management culture, it is vital that senior management encourage and embrace a transparent risk culture in decision making and references the Board's Risk Appetite Statement in day-to-day management of risk.

MaPS seeks to promote a culture of risk awareness and as such, all employees should have the ability to identify key risks. The risks themselves will remain the responsibility of the relevant owner in the business. Appendix E provides further detail on roles and responsibilities in relation to the risk management and reporting process.

Requirments for Each Component

The objective of the RMF is to ensure MaPS takes all reasonable steps in the identification and control of risks that prevent MaPS from ensuring everyone can make the most of their money and pensions.

It applies to all MaPS employees, Risk Owners, All Directorates/ Functions, ELT, ARAC and Board. More information can be found on each stage in the risk management process throughout this section, including the tools and methodologies that can be employed. The table below illustrates the minimum standards for each;

Component	Requirements

Identify	• Proactively take steps to identify risks
	• Clearly articulate risks;
	  Risk description
	  Causes of risk
	  Impacts of risk event occurring
	• Assign a Risk Owner
	• Capture on either Pentana (risk system) or Change risk registers

Measure	• Risk assessment completed • Inherent risk score assigned
Manage	• Respond to the risk event (Avoid, Reduce, Transfer, Accept) • Identify appropriate measures to reduce the likelihood and impact of the risk event occurring • Assign owners to mitigating measures/ controls • Assign review dates to mitigating measures/ controls • Update risk assessment with residual risk score assigned
Monitor	• Provide timely updates to measures and risk • Update risk assessment based on a point in time and the effectiveness of control measures • Current risk score assigned
Report	• Ensure accurate and timely information captured on either Pentana (risk system) or Change risk registers to enable onward risk reporting

ELT are responsible for their Directorate's adherence with the RMF.

Internal Audit will provide independent assurance of requirements' implementation across the organisation, reported to ELT, ARAC and Board.

1 - IDENTIFY – The purpose of identifying risks is to gain a full understanding of any risk that might threaten MaPS' pursuit of its strategic objectives.

There are a variety of techniques and methodologies that can be used to identify risks. Listed below are some examples of activity that can be utilised to support the identification of risk;

- Day to day activity and risk management
- Risk Identification Workshops
- Risks captured as part of Projects & Programme Risk, Assumption, Issue & Dependency logs (RAID)
- Risk assessments
- Reviews of Objectives
- Committee reporting and minutes
- Strength, Weakness, Opportunity & Threat (SWOT) Analysis
- Political, Economic, Social, Technological, Legal, Environmental (PESTLE) Analysis
- Risk identified through Horizon Scanning
- Constraints & Dependencies (Operational Planning)
- Risk identified through Internal Audit Reports
- Emerging risks identified through Key Risk Indicator reporting
- Lessons learned
- Assurance Maps
- Compliance Monitoring

Consideration should be given to all types of risk. The Board's risk appetite statement defines the risk categories and sub-categories of risk that MaPS faces as an Arms-Length Body (ALB) and is contained within the Risk Appetite Statement, found in Appendix B. Associated levels of Board Risk Appetite can also be found there.

Identifying risks should not be limited to pre-defined risk reviews and should be an ongoing, continuous and dynamic activity. All MaPS colleagues are encouraged to and have the ability to identify new and emerging risks when carrying out their day-to-day duties. Risk identification happens at all Lines of Defence and is not the responsibility of any given group.

Once risks have been identified, it is also important to articulate them in a way that is understandable to the wider organisation. It is important to ensure risk descriptions are brief but fully communicate the risk in question.

The following wording groups are often used to begin the process of articulating risk;

- Increase in...
- Failure to...
- Potential to...
- Disruption to...
- Lack of...
- Inability to...

Risk descriptions should contain: a Description of the risk event/ the cause(s) of that event and the impact(s) of the event occurring. All risks should be assigned an appropriate Owner as well as being mapped to the risk taxonomy and associated appetite.

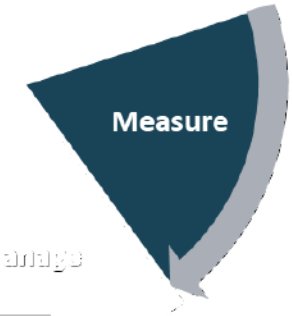
Identified risks are captured on Risk Registers. There are three types of risk register used at MaPS depending on the types of risk; a Strategic Risk Register, the Functional Risk Registers & Programme/

Example of a risk description

There is a risk that a lack of controls and / or failure to adequately follow or check that data protection principles apply to MaPS' specific activities carried out by internal colleagues and / or third parties. Such non-compliance could lead to a fine, complaint(s) to the ICO and / or reputational damage

Project Risk Registers. More information on each can be found in the Resources section of the RMF, including a breakdown of the information that should be captured.

2 - MEASURE - Once risks have been identified, it is important to measure those them to help explain the significance of the risks that MaPS faces in pursuits of its strategic objectives.



Risks should be assessed against two main dimensions: their impact and likelihood of occurring. These are defined as:

- **Impact** - the estimated effect on one or more objectives of a particular event (threat or opportunity) actually occurring;

And;

- **Likelihood** - the likelihood of a particular event (threat or opportunity) actually occurring

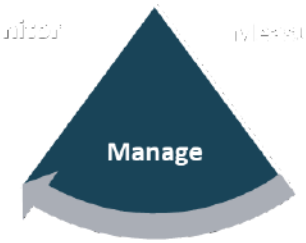
When assessing the likelihood and impact of identified risks, **the risk scoring framework**, in Appendix C, provides consistency across MaPS and is a tool for understanding the size of the risk the organisation faces. Scores are given to both the impact and the likelihood, and when multiplied together, result in a risk score for each identified risk. The score is then mapped to the Board's Risk Appetite for that category of risk to determine whether it is in or outside Risk Appetite. The risk appetite statement can be found in Appendix B and will illustrate the acceptable risk scores for each category of risk. The table below demonstrates the scores applicable to Cautious Risk Appetite.

Risk profile Impact x Likelihood						
Impact score	Severe	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Insignificant	1	1	2	3	4	5
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost certain
			Likelihood score				

It is the responsibility of the risk owner to measure their risks and it is best practice to involve a number of stakeholders from across the organisation to accurately capture the risk position. The risk owner should be someone with knowledge of the risk area and of enough seniority to ensure response actions are implemented.

At this stage of the risk management process, identified risks will have their inherent risk measured, which represents the amount of risk that exists in the absence of controls or mitigating actions.

3 - MANAGE - It is not enough to just identify and measure risks; they need to be mitigated through some form of proactive management.



Risk response planning or risk treatment should be documented for all risks but balanced against where the risk is relative to the Board's Risk Appetite for that type or category of Risk. The aim of managing risks is to bring each one to within a level of residual risk within the Board's appetite for that category. This is defined as the level of exposure after action has been taken to manage it and assuming that the action is effective.

The four risk response strategies that can be utilised in managing risks are;

1. **Accept** – choosing to accept the likelihood and impact of the risk crystallising in delivery of objectives. This requires Accounting Officer approval
2. **Avoid** – developing controls and mitigating actions to reduce the likelihood of the risk to zero
3. **Reduce** – developing controls and mitigating actions to reduce the likelihood of the risk to within appetite
4. **Transfer** – transfer all or part of the risk to a Third Party, for example, through insurance

Risk responses are an important part of the risk management process which help inform how to plan and then execute for each identified risk.

It is the responsibility of the risk owner to ensure each risk is managed effectively. Managing risk is an ongoing activity and should continue until the risk has reached its residual position. Capturing controls and mitigating action should be completed once the risk has been measured. It is important to **assign owners** to the measures identified in the risk response, with realistic completion dates. Controls and mitigating actions should identify;

- **Who** will be carrying out the activity
- **What** will be done and **when**
- **How** it manages the identified risk

When considering what action is required to effectively mitigate risk, it is best practice to work collaboratively with colleagues in the 2nd Line of Defence. If proposed responses are not adequately challenged by the appropriate people, risk owners run the risk of investing in something that does not effectively reduce the risk to the required level.

At this stage of the risk management process, identified risks will have their residual risk measured. If the proposed measures, once completed, do not bring the risk within Board Risk Appetite, consideration should be given to additional measures that would bring the risk to an acceptable level. Escalation to Executive Leadership Team (ELT) and / or ARAC might be required to discuss / agree next steps.

4 - MONITOR - Risks change, priorities change, actions get completed, risk responses that were once effective can become less effective, etc. It is therefore important to continue to monitor and review risks and the effectiveness of their controls and measures.

Risk management is not a one-off process, and all risk owners should ensure it is continuous and dynamic. Through frequent risk reviews and consideration of the proximity of the risk crystallising, risk owners should review and assess the current risk score, the progress and effectiveness of the measures in place to mitigate the risk, as well as identifying new controls or measures that will need to be implemented.

Monitoring risks also acts as an escalation point for risk owners should the planned measures not bring the risk to an acceptable level. Risk owners and the 1st Line of Defence (1LoD) should work constructively and collaboratively with the 2nd Line of Defence (2LoD) in reviewing the current measures

At this stage in the risk management process, risk owners are responsible for updating their current and residual risk assessments. Current risk scores illustrate level of exposure faced at a point in time and consider progress being made on each of the measures that reduce the likelihood / impact of the risk and help illustrate the trend.

The 2LoD also plays an important role in the monitoring of the organisation's risk profile. They are responsible for providing oversight, support and challenge on the progress of the measures in place and will provide independent, objective assessments to risk owners, ELT, ARAC and Board on where the organisation is operating in relation to its risk appetite.

Risk Registers are extremely useful in a relatively new or changing organisation to help identify where risk lies. As an organisation matures, new risk identification should become less frequent and a Risk and Control Self-Assessment becomes more relevant. Here the emphasis is on assessing the effectiveness of controls put in place to manage identified risks and the resource allocated to the controls is calibrated against the Board's Risk Appetite. Over time, it is the aspiration of MaPS to transition from managing functional risk registers to a Risk & Control Self-Assessment (RCSA) process for monitoring risks, facilitated by the 2LoD. There is a recognition that there is a need to continue to embed the RMF and supporting processes and methodologies to enable this to happen effectively. This will be further supported by the development of Key Risk Indicators (see section 5. Report for more detail).

Risk & Control Self-Assessment

Risk and control self-assessment (RCSA) is a process through which risks and the effectiveness of their controls are assessed and examined by the 1st Line. The objective is to provide reasonable assurance that all business objectives will be met.

RCSA take two primary forms; a facilitated workshop with risk owners or structured questionnaires where risk owners identify and assess risks and controls in their respective Directorates. A facilitated RCSA can:

- Increase awareness of Directorates objectives and the role of internal control in achieving goals and objectives.
- Support the design and implementation of control and processes
- Highlight and help prioritise mitigation activity for each Directorate, aligned to the Board's Risk Appetite
- Develop action plans to address situations where directorates are exposed to risk positions that are outside of appetite

Strategic Risk Register (SRR)

It is important that the SRR represents a 'top down' view of the most material risks to MaPS achieving its objectives. Risks captured on the SRR are owned by members of the Executive Leadership Team (ELT), which is facilitated by the Head of Enterprise Risk. The SRR is held on Pentana, where updates are provided enabling accurate reporting.

The SRR includes information on;

- Risk description
- Risk Causes
- Risk Impacts
- Risk assessment – Inherent, Residual and Current
- Associated risk taxonomy and level of Board appetite
- Controls and mitigation strategies

The SRR illustrates where MaPS is operating, at Strategic level, in relation to the Board's Risk Appetite. Risk mitigation plans to bring the risk position within appetite should be documented against each entry.

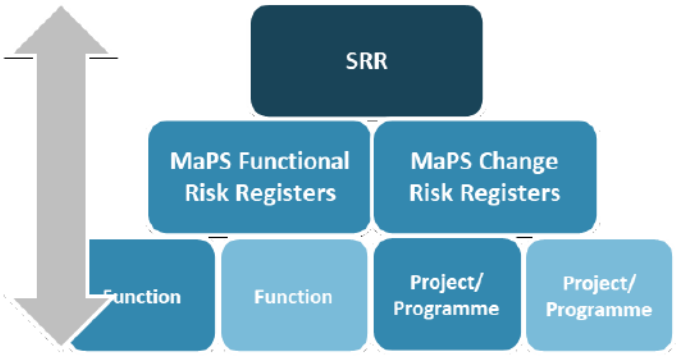
Functional Risk Registers

Functional Risk Registers are held by each function at MaPS and all feed into an overarching MaPS Functional Risk Register. Functional Risk Registers are used to capture risks that would impact the achievement of functional objectives. They are held on Pentana and act as a repository for risk information, including;

- Risk description
- Risk Causes
- Risk Impacts
- Risk assessments – Inherent, Residual and Current
- Associated risk category and level of Board appetite
- Controls and mitigation strategies

Risk owners are expected to provide timely progress updates and risk assessments to their risks within the pre-defined period of time. Functional Risk Registers are used to illustrate where MaPS is operating in relation to their risk appetite and helps management understand the key events that will impact our ability in achieving our objectives. Functional Risk management information is presented to ELT, ARAC and Board.

The relationship between the Strategic Risk Registers and the functional risk register is illustrated below;



At present, monthly meetings between 1Lod and 2LoD take place to review all functional risk registers. In addition, the 1LoD and 2LoD will maintain open communication channels and work collaboratively with each other to provide ongoing support to the 1loD on matters and events that occur that may impact functional risks or existing control measures plus ensure timely escalation of risk reporting as issues and events occur.
The SRR is reviewed with 2LoD and risk owners every other month to align with the risk reporting schedule, detailed in Appendix E.
Functional risks are escalated to SRR as and when appropriate based on the materiality of their impact on MaPS' strategic objectives and direction.

Project and Programme Risk Registers

Project and Programme risk registers capture and monitor risks that have potential to impact the ability of achieving the project deliverables and milestones. They are also held on Pentana and, where appropriate, reported through the Portfolio Group for escalation. Managing and monitoring project and programme risk gives Project/ Programme Managers early indication for challenges that their change

activity may encounter and enable sufficient time to respond to the risk accordingly.

Systems

Risk Management software and tools are an important component of risk management frameworks. Currently, MaPS uses Pentana, which has the capability to act as a central repository of risks across the organisation and from all areas of the risk taxonomy, capturing;

- Risks
- Risk descriptions, causes and impacts
- Risk owners
- Risk assessments
- Risk updates
- Controls and mitigating actions
- Controls owners
- Control updates

Pentana enables timely and accurate reporting of the organisation's risk position and has the capability to build bespoke reports for different areas of risk or different directorates. Access and training to Pentana are available on request from the Risk, Compliance & Assurance Directorate (RC&A). Currently, risk and control owners, Risk Champions and the RC&A Directorate have access to Pentana and are responsible for providing timely updates and assessment to risks, dictated by review dates on either. The RCA will undertake an annual review of the use of risk management software to ensure the needs of MaPS are sufficiently being met. More information on Pentana can be found in Appendix D.

5 - REPORT - It is essential that periodic risk reports are provided to key stakeholders via committees and boards, but also flexibly when there are significant changes in circumstances or key decisions to take.

It is the responsibility of the 2nd Line of Defence to report **objectively** and **independently** on the risk profile of the organisation. The key committees are;

- Board
- Audit, Risk and Assurance Committee (ARAC)
- Executive Leadership Team (ELT)
- Strategic Risk Committee (SRC)
- Senior Management Team (SMT)

There are other key committees and meetings across MaPS that will provide useful information for the reporting and oversight of risk management activity. They include; Compliance Steering Group, Portfolio Group, Project and Programme Boards

The risk reporting structure can be found in Appendix E.

It is therefore important that risk owners ensure they provide timely updates to their risks through regular reviews with the Risk Team or the use of Pentana/Change risk registers to enable accurate reporting.

Key Risk Indicators (KRIs) & Enterprise Risk Data Points

MaPS will develop a suite of key data points from across the organisation that will act as indicators to help Board and ELT understand the organisation's risk profile in relation to its risk appetite.

KRIs provide an early indication of increasing risk exposures across all forms of risk captured. At MaPS, KRIs give an early warning to identify potential events that may harm continuity in pursuit of MaPS' strategic objectives. KRIs enable MaPS to report holistically by each area of its risk taxonomy, providing an evidence-based assessment of whether the organisation is operating within risk appetite.

KRIs will be reported, as part of the RMF, to ELT, ARAC and Board, inviting comment from each on where MaPS is operating (as a trend, not a point in time assessment) and the effectiveness of MaPS' control environment.

Ownership of the different data points will sit across the organisation and responsibility for producing the KRIs sits with the RC&A directorate. It is the responsibility of the data owners and providers to supply the RC&A with the data in a timely manner, as detailed in the KRI procedure notes.

Whilst KRIs are mostly quantitative, MaPS also has a suite of qualitative measures that can be used to inform an objective assessment of the risk profile. These measures include, but are not limited to; risk registers, stakeholder engagement reporting, Internal Audit Reports/recommendations, Annual Assurance Assessment, Compliance Monitoring and Corporate Strategy. These measures provide an important overlay to our KRIs in the holistic assessment of our risk taxonomies and their performance in relation to our appetite and strategic deliverables.

Risk Culture & Awareness

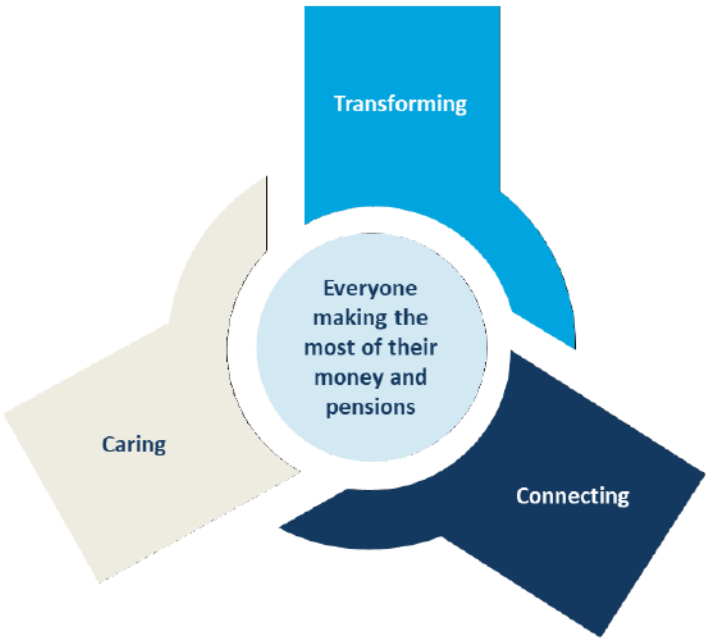
Risk Culture & Awareness

A crucial component to effective risk management is a **positive** and **constructive risk culture** with values and behaviours embedded throughout all levels of MaPS and everyone taking personal responsibility to manage risk in everything they do whilst being careful not to create a 'blame culture'. Raising awareness will ensure consistency and best practice is being adopted across the organisation enabling MaPS to operate within its risk appetite. To achieve a positive risk management culture, it is vital that senior management encourage and embrace a transparent risk culture in decision making and references the Board's Risk Appetite Statement in day-to-day management of risk.

Evidence of an effective risk management culture includes:

- Commonality of purpose
- Universal adoption and application
- Learning and continuously improving organisation
- Transparent, prompt and honest communications
- Understanding of the value of effective risk management
- Individual and collective responsibility
- Expectation of constructive challenge

The Risk, Compliance & Assurance Directorate will facilitate activity throughout the year to increase awareness and understanding of risk management processes at MaPS for all three key components of the RMA. Parallel to that, every year, all colleagues at MaPS will be required to complete a mandatory e-learning Risk Management module, demonstrating the importance risk management plays in the pursuit of organisational objectives. Members of the ELT and a number of the SMT will be required to attend additional training.



Roles & Responsibilities

Business Case Risk Management

As detailed in the Business Case User Guide, for all projects where public money will be spent, endorsement sign-off is mandatory from a number of teams across the organisation.

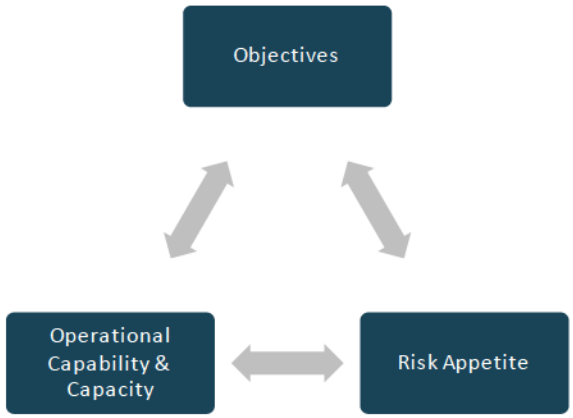
The 1LoD and Business Case owners are responsible for identifying and measuring the risks associated with their business case using the risk scoring framework, making linkages to the Risk Appetite Statement, as detailed in the Business Case template.

The RC&A Directorate will assess that the risks identified, and subsequent risk scores are valid and proportional. Acting in a 2LoD capacity, the Risk, Compliance & Assurance Directorate will also provide an objective and independent view of the Business Case proposal in the context of MaPS' objectives.

In order to do this accurately and effectively, the Risk, Compliance & Assurance team will need at least **72 hours** to provide an assessment of its endorsement. Turnaround times are dependent on the complexity of the business case.

Business Planning & Corporate Strategy

As detailed in the RMA, MaPS' Business Planning takes place in an annual cycle. Where possible, it is considered best practice to involve the Risk, Compliance and Assurance Directorate in the business planning process. This is in order to provide a 2LoD viewpoint on the risks to achieving objectives within the plan. This can best be described as a triangulation in the following Figure:



Business Planning Triangulation

An organisation that sets stretching objectives when it has limited operational capability and capacity is likely to breach the Board's Risk Appetite in the delivery of those objectives unless the Board has a high tolerance for risk in achieving them. Alternatively, a Board that has a very low tolerance for risk in meeting its objectives, may set relatively conservative objectives or wish to receive a high degree of assurance that the organisation's operational capability and capacity is sufficient to meet those objectives.

It should be the responsibility of the Risk, Compliance and Assurance Directorate to inform the Board of the alignment between its objectives, appetite for risk and the organisation's operational capability and capacity.

Incident Reporting

Incidents are inevitable. Having the opportunity to understand why they occur and their impact can lead to better risk management processes and control improvements. MaPS has developed a central reporting mechanism where incidents can be recorded from across the organisation, providing better visibility of incidents and their impact. It is envisaged that a central reporting process will enable better insight and provide more robust assurance to ELT, ARAC and Board on the organisation's control environment. Incident reporting can capture the impact of incidents, mapped

to the risk scoring framework, root cause analysis and remedial actions taken, as well as an independent and objective 2LoD assessment of the event. Incident reporting will provide an important data point in the reporting of risk at MaPS as part of the RMF.

Continuous Improvement

MaPS will carry out annual reviews of the RAS and the RMF. These reviews will be carried out collaboratively with the executive before sign off and approval is requested by our ARAC and Board. The effectiveness and embedding of the RAS and RMF will remain under close review outside of the annual review cycle by the Risk, Compliance & Assurance Directorate.

Resources

Throughout the RMF, there has been reference to a number of risk management resources that are utilised by MaPS to support the effective management of risk, including;

- Risk Appetite
- Risk Taxonomy and sub-categories
- Strategic Risk Register
- Functional Risk Registers
- Programme/ Project Risk Registers
- Risk Scoring Framework
- Key Risk Indicators
- Risk Response Strategies
- Pentana

More information on each of these resources can be found throughout the RMF and in the Appendices. Alternatively, please contact the RC&A Directorate for more information and guidance.

Board and Risk Management

The Accounting Officer is responsible for Risk management within the organisation wth both the first and second lines of defence reporting into her/him.

The Board is responsible for risk oversight and the approval and ownership of the policies and procedures that underpin risk management at MaPS.

The Board and Accounting Officer have responsibility to ensure risk management is factored in as a crucial part of strategy and decision making to enable the efficient day-to-day management of the organisation.

Glossary

Term	Definition
Assurance	An evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework
Audit, Risk & Assurance Committee	A committee appointed to support the Board in monitoring the corporate governance and control systems in the organisation
Compliance	MaPS and our funded delivery partners adherence with the MaPS standards, external regulation, legislation (including the requirements of the Financial Guidance and Claims Act 2018), guidelines and specifications (e.g., Managing Public Money), as well as internal policies and contract management
Internal Control	Any action, originating within the organisation, taken to manage risk. These actions may be taken to manage either the impact if the risk is realised, or the frequency of the realisation of the risk
Inherent Risk	The exposure arising from a specific risk before any action has been taken to manage it
Functional Risk	Failure to achieve business / organisational objectives due to human error, system failures and / or adequate procedure and controls
Opportunity	An uncertain event that would have a favourable impact on objectives or benefits if it was to materialise
Programme Risk	Risks concerned with transforming high-level strategy into new ways of working to deliver benefits to the organisation
Project Risk	Risks concerned with the successful completion of the project's objectives
Residual Risk	The exposure arising from a specific risk after action has been taken to manage it and assuming that the action is effective
Risk	Uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance
Risk Appetite	The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time
Risk Assessment	The evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised
Risk Management	All processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress
Risk Profile	The documented and prioritised overall assessment of the range of specific risks faced by the organisation
Strategic Risk	Risk concerned with where the organisation wants to go, how it plans to get there, and how it can ensure survival

Appendices

Links can be found below to appendices referenced throughout the RMF.

Appendix A : Risk Management Approach

Appendix B : Risk Appetite Statement

Appendix C :Risk Scoring Framework

Appendix D : Risk Management Software

Appendix E : Risk Reporting Structure

Appendix F : Incident Reporting Form

Governance

Version Control

Version Control			
Version	**Date**	**Author**	**Summary of Changes**
0.1	23/11/2020	E. Cecil/ S. Pinchin	First draft of RMF
1.0	15/12/2020	E. Cecil/ S. Pinchin	Minor edits following ARAC approval
1.1	15/11/2020	E.Cecil/ S.Pinchin/ R.Golbourn/ O.Higginbottom	Updates made by Risk Team during annual review of RMF, pre-ARAC Dec 2021.

Version number	1.1
Effective date	**/11/2021
Document Owner/ Primary Approver	Head of Enterprise Risk
Secondary Approver	Chief Risk Officer