Government
Finance
Function

Good Practice Guide: Risk Reporting

August 2021
V1.0

Contents

1. Introduction

1.1 The Orange Book – Management of Risk, Principles and Concepts (2020) advises that processes shall be structured to include 'timely, accurate and useful risk reporting to enhance the quality of decision-making and support management and oversight bodies in meeting their responsibilities'. Risk reporting is a key component of the risk management framework (Figure 1), providing insight and confidence to both internal and external stakeholders. Good risk reporting offers an integrated perspective, which draws on and complements planning and performance frameworks and insights in assuring the effectiveness of the risk management approach, and highlighting areas where intervention is required.

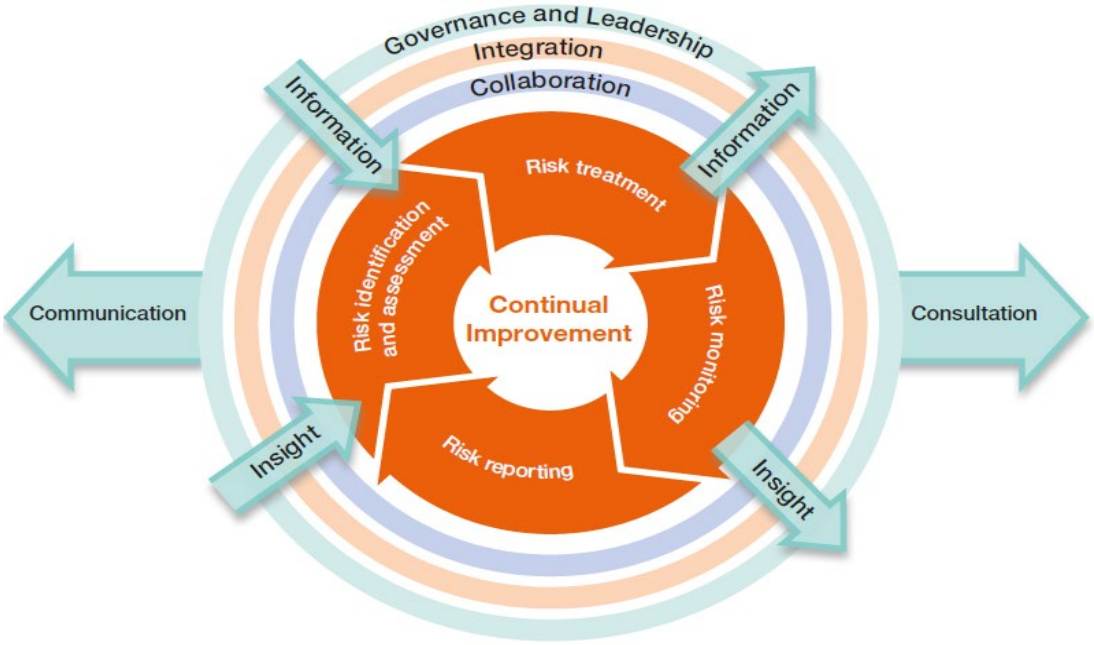

Figure 1.

1.2 The Orange Book (A6) also states that regular reports to the board should provide a balanced assessment of the principal risks and the effectiveness of risk management. The accounting officer, supported by the Audit and Risk Assurance Committee, should monitor the quality of the information they receive and ensure that it is sufficient to allow effective decision-making.

1.3 This guidance outlines principles and key considerations for organisations to apply when designing and developing risk reports. The principles detailed in this guide are based on best practice developed and refined within the Civil Service risk management community. It is intended for both risk professionals and senior leaders responsible for managing risks and prioritising resource allocation.

1.4 This guidance is tailored to support the effective reporting of principal and emerging risks in an enterprise risk management context. It should be considered alongside the Orange Book and other associated good practice guides. These documents can be accessed via Gov.uk or OneFinance.

1.5 Whilst this guidance may be of interest in a programme or project management context, it is not intended to supersede or replace other specific guidance, including project delivery information issued by the Infrastructure and Projects Authority, or risk reporting requirements outlined by the Cabinet Office to support Planning and Spending Review processes.

1.6 The Government Finance Function is grateful to all involved in the production of this guide. A full list of contributors is provided in the acknowledgements section at Annex C.

2. Assumptions

2.1. This guide has been developed to support the implementation of the concepts and principles outlined in the Orange Book, and is framed around the assumption that an organisation's risk framework aligns with these requirements. Accurate, timely and insightful risk reporting is predicated on the establishment of effective risk management practices, which facilitate clear communication and information exchanges.

2.2. To maximise the benefits of this guidance, organisations should recognise that risk reporting will best enhance decision making when:

- Objective, priorities and delivery outcomes are clearly understood across the organisation
- Effective partnership working arrangements are in place between departments, arm's length bodies and other delivery bodies
- Risk identification processes are in place to capture new and emerging risks
- Risk management is an integral element of day-to-day activities underpinned by good governance and leadership
- Risk management is conducted as a collaborative process integrated with other key governance and oversight mechanisms, including but not limited to planning and performance processes
- Risk management reporting is considered through formal governance mechanisms on a regular basis
- Robust risk analysis takes place to ensure risk causes and consequences are properly understood, and control activity is directed effectively
- The organisation has set and understands its risk appetite
- The risk culture embraces openness and clear communication, supports transparency, welcomes constructive challenge and promotes collaboration, consultation and co-operation
- There are processes in place to enable the aggregation and escalation of risks to the appropriate management level

2.3. When developing a risk reporting approach, principal risk reporting, risk professionals should adapt this guidance as required in response to the size, complexity and needs of their organisation. Other factors to consider include the phasing and

interconnectivity of governance arrangements, the operating environment, stakeholder needs and organisational culture.

2.4. The principles outlined in this guide may be applied to inform the development and delivery of risk reporting across all organisational levels.

3. What is Risk Reporting?

3.1. A good risk management framework anticipates, detects, acknowledges and responds to changes and events in an appropriate and timely manner. Risk reporting provides a regular mechanism to direct updates to key stakeholders, ensuring the right information is given to the right people, at the right level, at the right time. As a minimum this is delivered by enterprise risk management teams on a quarterly basis to support an ongoing narrative of information. In doing so risk reporting enhances the quality of organisational decision-making, informs prioritisation of activity, and strengthens organisational oversight.

3.2. The benefits of regular risk reporting include:

- Embedding a consistent understanding of principal and emerging risks, thereby reducing the uncertainty of outcomes within an organisation
- Monitoring progress in achieving or maintaining tolerable or optimal risk appetite positions across an organisation,
- Enabling an organisation to understand the effectiveness of internal controls and take direct, timely and informed interventions as required
- Integrating risk, planning, performance and prioritisation discussions to enable informed consequence-based decisions
- Providing assurance to stakeholders, including oversight bodies, that risks are understood and being effectively managed
- Providing oversight of business activities, enabling a dynamic response to unplanned events threatening delivery of priorities and strategic objectives

4. Developing Risk Reporting

4.1. As set out in the Orange Book, the board, supported by the Audit and Risk Assurance Committee, should specify the nature, source, format and frequency of the information that it requires. This information should support the board to:

- Assess whether any changes are required to strategy and objectives
- Assess whether decisions are being made within its risk appetite to successfully achieve objectives
- Review the adequacy and effectiveness of internal controls
- Revisit or change policies, reprioritise resources, improve controls, and/or alter their risk appetite

Enterprise risk teams should therefore develop and deliver clear, informative and useful reports or dashboards highlighting key information enabling effective management. This information should provide visibility against each principal risk, compare results against key performance/risk indicators, indicate whether these are within risk appetite, assess the effectiveness of key management actions and

summarise the assurance information available. Reports should include qualitative and quantitative information where appropriate, show trends and support early warning indicators. Understanding and decision-making should be supported through the presentation of information in summary form and the use of graphics and visualisation.

4.2. **Scope:** Risk reporting should provide analysis and insight on the strength and effectiveness of risk management activities, supporting of an Orange Book compliant risk management framework. Risk reports should be framed around requirements set out by the commissioning parties. These commissions may include direction on the:

- Cost, frequency and timeliness of reporting
- Integration with other matters, including planning and performance management processes
- Links to organisational objectives, priorities and decision-making
- Method and format of reporting
- Scope of principal risk updates
- Stakeholder requirements

4.3. Commissioning bodies should scope reporting requirements that best support delivery of their roles and responsibilities. Expectations should be scaled against organisational maturity, and developed and improved over time, in line with the capacity and capability within the risk team.

4.4. To support oversight and governance arrangements, risk reports should also reflect pertinent information relating to arm's length bodies (ALBs). Effective relationships and partnership working between departments, ALBs and other delivery partners ensure a proportionate approach to monitoring and reporting risks.

4.5. **Purpose:** Risk reporting should be focused on supporting organisational needs and will typically present updates to enable:

- an assessment on the nature, status and trends across the risk profile
- areas of concern across the organisation, which may impair the delivery of objectives or priorities
- consideration of factors which impact on or may be impacted by principal and emerging risks
- the review of information relating to interdependencies or macro environmental concerns
- necessary decision-making and prioritisation activity
- the identification and management of potential areas for improvements within risk management activities
- progress updates in achieving optimal or tolerable risk positions
- an overview of risk management activities and outcomes across the organisation

- the transmission of useful information that informs interaction with stakeholders, including those with responsibility and accountability for risk management activities

4.6. Optimally, risk reporting should be delivered as an integrated product complementing pertinent planning and performance data. Integrated reporting better supports organisational governance, oversight and informed decision-making. Care should be taken not to duplicate information from other governance reporting; rather this should be signposted and aligned in risk reporting.

4.7. **Report Types:** Risk reporting should provide a balanced assessment of principal and emerging risks and the effectiveness of enterprise risk management activities. Organisations should consider how best to achieve this within governance arrangements, ensuring the appropriate information is provided to relevant parties. This may take the form of one risk report, which is updated for consideration at various fora, or through the delivery of a suite of different but aligned products. The following four reporting types are in common use to support the scrutiny and management of principal risks (Annex A provides information to support risk professionals in developing local reporting).

I. **Principal risk report:** This type of report is commissioned to provide an overview of principal and emerging risks within an organisation. Commonly, this reporting is considered by governance forums on a quarterly basis to provide assurance on the risk management approach, and review progress in achieving an optimal or tolerable risk position compared to the risk appetite. This report supports informed decision making, including the prioritisation of resources.

II. **Deep Dive Report:** This type of report is commonly commissioned to facilitate a detailed assessment of the nature and management of an area of or specific risk. It is often commissioned on a cyclical basis against an organisation's most significant principal risks or informed by the outcome of consideration of principal risk reporting. It may be used to support directed management intervention where there are concerns about risk management activities, such as the effectiveness of internal controls or where a risk has moved away from a tolerable risk appetite position. This type of report may also be used to assess the suitability of a risk for closure, de-escalation or merger into another principal risk. By enabling in depth scrutiny, the deep dive process allows senior leaders to assure themselves of the risk management approach and provide informed management direction.

III. **Risk Radar:** This type of report is commissioned by governance forums to highlight and summarise emerging risks or wider environmental factors that may have a significant impact on the delivery of organisational objectives or priorities. Risks which do not meet the threshold for formal escalation can be

monitored using a risk radar. Similarly, a risk radar may be utilised to monitor risks with either a high likelihood and/or high impact (e.g. business continuity/business resilience threats).

IV. **Risk Moderation:** This type of report is submitted to governance forums to moderate changes recommended to the principal risk portfolio. It should be used to provide senior leaders with a rationale to support changes proposed to the principal risk portfolio, which may include closure, escalation, merger or de-escalation of risks. This report outlines the information required to enable senior leaders to make informed decisions on changes to the principal risk portfolio, and provides assurance that strategic discussions remain appropriately focused. This report type is especially useful in facilitating the escalation of risks, as risks can crystallise quickly, and it provides assurance to the board and Audit and Risk Assurance Committee that there are clear processes for bringing significant issues to its attention rapidly when required, with agreed triggers for doing so as a part of risk reporting.

4.8. Good risk reporting should ensure the right information is presented to the right people at the right time. The four key elements which enable this are aggregation, analysis, visualisation, and review and improvement. The principles and good practice outlined below will support the completion of the report types highlighted above.

4.9. **Risk Aggregation:** Risk aggregation describes the process of summing up and developing an overall risk position within an organisation's delivery chain. In doing so, risk aggregation enables the identification and management of several risks, which may be assessed as manageable when considered in isolation but require enhanced management at the principal level when considered as a whole. Risk aggregation is a necessary element of risk reporting as it provides organisations with an accurate perspective on the levels of risks and their interdependencies. It can be used to support informed decision making and assess where additional actions may be required in the pursuit of objectives.

4.10. Risk aggregation is usually conducted within a risk function, as risk professionals are uniquely placed to maintain oversight of the whole risk portfolio. Risk professionals should develop an approach to aggregating risk which is appropriate for organisational needs and requirements. This approach should be applied consistently, to support the development of analysis and trend information around aggregate risks. Risks may be aggregated across a number of elements, delivery objectives, risk appetite areas or risk categories, and direction should be sought from senior leaders regarding their preferred approach.

4.11. Risk aggregation may result in the development of new cross cutting risks or may be used to inform and influence the assessment of an existing principal or emerging risk. Regardless of how the aggregate perspective is reported, it is important that it is

subject to refresh at the same intervals as principal risks to ensure it remains timely and accurate.

4.12. **Risk Analysis:** Risk analysis should provide insight on the principal risk portfolio, which delivers a clear understanding of the status of principal risks, including the effectiveness of risk management activity, commentary on trends and emerging concerns, progress in achieving the optimal appetite position and recommendations where action would realise improvements. Risk reporting should not provide an isolated update, but rather it should form a continuous narrative, building on previous updates to support the development of organisational awareness and insight.

4.13. This information should be tailored to the reporting requirements set out by the commissioning party and be supported by an evidential base. Risk analysis should draw from relevant management information and expertise, including planning and performance data and the work of assurance providers, to provide the reader with a considered assessment of organisational risks. This assessment may reference qualitative or quantitative information.

4.14. Risk professionals should develop an analysis approach which is appropriate to organisational needs, taking into consideration the expertise, datasets and information available. Where analysis has been developed on the basis of limited, partial or unverified data, this should be clearly noted in reporting to ensure this is handled appropriately when informing decision making and prioritisation activity.

4.15. The designated individual responsible for leading the organisation's overall approach to risk management should include their assessment of the outcomes of this analysis in reporting. This may form an overarching statement or may be provided against each principal risk. The assessment should highlight areas of concern requiring intervention, support delivery of an integrated governance approach, and inform organisational prioritisation and spending decisions.

4.16. **Risk Visualisation:** Good risk reporting should make appropriate use of visualisation, infographics, tables and diagrams to illustrate points and insight. In addition to improving user engagement with reporting, visualisation techniques enable risk professionals to present complex information in a concise and compelling format. When used appropriately, visualisation enhances the narrative of risk reporting, and provides supporting evidence to the analysis presented. Care should be taken to ensure infographics present relevant and useful information to senior leaders, and risk reporting is not overwhelmed by visual elements. Risk professionals should develop visualisation tools tailored to organisational requirements and remain mindful of accessibility concerns when doing so.

4.17. **Review and improvement:** Risk professionals should regularly review risk reporting to ensure it remains fit for purpose:

- Stakeholders should be engaged regularly to support the review and optimisation of reporting, to ensure it continues to meet their needs by delivering organisational insight and business needs
- Reporting should also be reviewed in response to changes to the operating environment, shifts in the risk culture or changes to organisational risk maturity, or other events which provide opportunities to develop and embed the delivery of quality products supporting informed decision-making and organisational oversight.

The risk reporting checklist provided in Annex B may be used as a self-assessment tool to assist in this process.

4.18. The board, supported by the Audit and Risk Assurance Committee, should periodically review the quality of reporting, and provide feedback on the scope, purpose and content of reports. This may form part of an annual governance review and will enable risk professionals to optimise reporting and ensure that it supports effective decision-making.

5. Further information

5.1. The latest updates on Orange Book Good Practice Guides can be found on via the Risk Management Centre of Excellence on OneFinance. Please refer to the Heads of Risk Network page for the latest news.

5.2. For more information, or to provide feedback on this guidance, please email GovFinance@hmtreasury.gov.uk.

Annex A – Risk reporting

As set out in the Orange Book, the board, supported by the Audit and Risk Assurance Committee, should specify the nature, source, format and frequency of the information that it requires. When designing reporting, risk professionals must ensure risk reporting meets organisational needs, and adds value to strategic conversation. All reporting must be clear, informative, useful, and support the board to discharge their responsibilities, which include:

- Assessing whether decisions are being made within its risk appetite, and communicating if any additional activity is required
- Reviewing the adequacy and effectiveness of internal controls
- Monitoring performance and delivery
- Ensuring value for money
- Refreshing strategies, objectives and policies.
- Informing the prioritisation of resources
- Reviewing and amending the risk appetite, and communicating that to those responsible for managing the risks

The information provided below will aid risk professionals in developing the four following products.

The information detailed below must be considered alongside local requirements to ensure each reporting type meets organisational needs. It should be noted that there is no requirement to maintain separate reporting to cover each update area, where appropriate these updates may be presented in a composite document. Risk professionals should consult with senior leaders to design an approach best suited to local needs.

Across all reporting types, risk professionals should ensure the content and layout of the report is tailored to ensure appropriate, useful and relevant information is presented to the audience. Updates should include qualitative and quantitative information, and where appropriate the use of visualisation and infographics is encouraged to illustrate points and provide insight.

Annex A – I. Principal risk report: This type of report is commissioned to provide an overview of principal and emerging risks within an organisation, and is subject to regular governance consideration. This report may be delivered in various formats, including PowerPoint updates, written reports, dashboards or a combined approach. The following headline areas should be considered for inclusion:

Background: this section should outline the scope and purpose of the report, including:

- Contributing parties, e.g. performance team, arm's length bodies and other delivery partners
- Outline of the risks covered within the report, highlighting new or closed risks
- Period of time covered by the reporting

Risk analysis: this section should provide a summary report against each principal risk managed within the organisation. This may be arranged according to risk category, severity, proximity or likelihood of risks. These updates should provide both qualitative and quantitative updates to illustrate the status of each risk, and may include:

- Changes or emerging changes to the operating environment impacting on risks and management activity
- Changes to the risk profile, including trends, achievements and significant or emerging concerns or opportunities, progress towards achieving optimal and tolerable risk appetite positions, and impact on key performance indicators. This section also references the consequence of these changes, such as the impact on priority outcomes or the financial position
- Data and information summarised in infographics to support the report narrative
- Summary of the risk, including key information relating to risk owner, main impact areas, links to strategic objectives, proximity and relevant corporate context / dependencies.
- Update on contingency arrangements (where appropriate)

Head of Risk / Chief Risk Officer assessment: The designated individual responsible for leading the organisation's overall approach to risk management should:

- Provide an independent assessment on risk management activities
- Recommend interventions to support improvements to risk management activities, risk culture and risk maturity
- Highlight areas within the risk portfolio for senior leader scrutiny
- Inform organisational prioritisation and spending decisions

Next steps: This section should summarise the following:

- Notable activities or events which may impact on risk management activity
- Planned activities designed to support organisational risk culture and maturity
- Proposed actions in the next quarter to improve performance

Annexe A – II. Risk deep dive report: This type of report is commonly commissioned to facilitate a detailed assessment of the nature and management of risks. The following headline areas should be considered for inclusion:

Scope / purpose: This section should outline what will be covered within the report, for example a thematic or specific risk review, and why the report was commissioned. This may relate to a regular review cycle, or an extraordinary commission resulting from:

- Completion of risk management actions / changes in the operating environment
- Early warning indicators (EWI) or triggers
- Regular or ad-hoc review or audit scrutiny and adverse findings

Principal risk summary: This section should support an informed assessment of the risk by providing useful details and context, such as:

- Risk description(s)
- Date of adoption / duration of active management
- Corporate context - Links to strategic objectives and outcomes
- Optimal and tolerable risk appetite positions / current level of exposure.
- Summary of management plans
- Projected closure / completion date

The inclusion of infographics, such as risk dashboards, and continuous monitoring tools, such as flight paths which summarise trends and forecast future outcomes, support the reader to develop an in-depth understanding of the information presented.

Progress summary: This section should summarise progress to-date in the management of the risk(s). This may include:

- Metrics demonstrating direction of travel, including achievements and EWIs
- Delays / threats to delivery of plans, such as changes in the operating environment

Risk owner assessment: This section should present the risk owner's assessment on risk management activity, detailing achievements, future concerns and current issues which are barriers to control and mitigation activity. This may include:

- Confidence in risk management plans and key controls
- Confidence in systems of internal controls impacting on the risk
- Reflections on the appropriateness of the optimal and tolerable risk appetite

Recommendations: Corrective actions and / or interventions requested from senior leaders on the basis of the risk owner's assessment. This may include:

- Amendment of optimal and / or tolerable risk appetite position
- Additional funding to support control and management activity
- De-escalation of the risk

This type of report would benefit from infographics to support the reader to develop an in-depth understanding. This may include risk dashboard and continuous monitoring tools such as flight paths which summarise trends and forecast future outcomes.

Annexe A – III. Risk radar report: This type of report is commissioned by governance forums to highlight and summarise emerging risks or environmental factors that may have a significant impact on the delivery of organisational objectives or priorities. Visualisation techniques are important tools in developing meaningful and impactive risk radar reporting. Commissioning bodies should provide clear direction on the risks where a watching brief should be monitored. When developing risk radar reporting, risk professionals should consider the following areas for inclusion:

Scope: this section should outline the scope of the report for the reader. For example, will this report provide exception reporting against monitored risks, where notable changes have occurred? Does it provide a retrospective or forward-looking perspective? What informed the perspective provided in this report, for example horizon scanning activity, or open source research? This may include reference to the National Risk Assessment, or data provided by GO Science.

Radar analysis: this section should be used to provide an overview of each risk, in accordance with senior leader requirements. This may include:

- Summary of risks subject to radar monitoring, including links to corporate priorities.
- Proximity and severity of risks
- Changes to risk status, and associated consequences relating to principal risks / strategic objectives / delivery outcomes
- EWIs triggered during the reporting period

In addition to providing a corporate perspective on risks, this section may also be used to

- Highlight changes to the macro environment which may impact on strategic outcomes and delivery objectives
- Summarise contingency arrangements in place to respond to risk materialisation

Recommendations: this section should be used to provide recommendations around risks subject to monitoring. This may include recommendations relating to the modification of risks subject to radar reporting, such as formally adopting or discarding risks.

Annexe A – IV. Risk moderation report: This type of report is submitted to governance fora to moderate changes recommended to the principal risk portfolio, recommended outside of governance oversight mechanisms. This is achieved by outlining the information required to assure senior leaders that proposed changes are appropriate and justified. The following headline areas should be considered for inclusion in this type of report.

Purpose / recommendation: This section should summarise the purpose of the report and summarise recommended changes to the risk portfolio. This may include:

- Closure
- De-escalation
- Escalation
- Merger

Each recommendation should also include reference to the senior leader / governance body sponsoring this change.

Each risk subject to a recommendation should then be supported by the following information:

Risk summary: This section should provide a high-level summary of the uncertain events or conditions which require active management by the organisation. This should include

- Risk description, including causes and impacts
- Risk owner
- Current risk rating and risk trend projections
- Optimal and tolerable risk appetite position

Management activity to-date: This section should include an assessment of the current risk status against the optimal or tolerable risk position and should briefly summarise activity in train to support the management of the risk. This should be tailored according to the purpose of the report, for example escalation proposals should summarise actions and controls implemented to prevent risk materialisation and de-escalation / closure proposals should summarise outcomes realised through risk management actions and controls.

Rationale: This section should be used to provide supporting evidence for recommended changes. As risks should be managed at the lowest appropriate level, this reporting should focus on the benefits of the proposed action. This may include reference to:

- Internal and External Dependencies and / or cross-cutting impacts
- Investment and change requirements
- Key achievements, issues or opportunities.
- Risk management plans and controls
- Significant potential impacts projected across the short, medium and long-term
- Strategic priorities and delivery objectives

Annexe B - Risk reporting checklist

The following principles may aid risk professionals in reviewing and optimising their risk reporting approach in line with best practice.

☐ **Collaborative:**
Is the risk reporting aligned and informed across the organisation, its partners and its stakeholders?

☐ **Evidence-based:**
Is the risk reporting evidence based, making good use of the management information and expertise available?
Does it contain the information required by the reader to make decisions or participate in productive discussions?

☐ **Focused on the delivery of objectives:**
Does the risk reporting support informed decision-making and prioritisation activity?

☐ **Informative and insightful:**
Does the risk reporting promote:

- A clear understanding of risks?
- Provide a confidence assessment in the treatment of risks?
- Prompt corrective actions?
- Support informed decision making?

☐ **Integrated:**
Is the risk reporting integrated with other governance discussions and processes, including but not limited to planning and performance management and the insights provided across the “lines of defence”?

☐ **Scope:**
Does the risk reporting a suitable context to support the robust assessment of an organisation’s principal risks, by providing an accurate:

- Internal perspective,
- System-wide perspective
- Update on current macro-environmental concerns, and
- Horizon scanning information?

Does reporting build an informed perspective supporting continuous improvement?

☐ **Tailored:**
Is the risk reporting tailored to provide the information required by customers?
Does the reporting provide a clear summary and confidence assessment of the risks to the organisation?

Annexe C - Acknowledgements

The Government Finance Function extends thanks to colleagues from the following organisations who were instrumental in compiling this guide.

ALARM embrace risk

CPS

Department for Education

Department for Environment Food & Rural Affairs

Department for International Trade

Foreign, Commonwealth & Development Office

Government Internal Audit Agency

Government Legal Department

Ministry of Housing, Communities & Local Government

NAO National Audit Office

NDA

Ministry of Justice

Rural Payments Agency

This page is left blank

This page is left blank

Produced by Mark Ripley, Government Finance Function