HM TREASURY

Assurance frameworks

December 2012

HM TREASURY

Assurance frameworks

December 2012

Official versions of this document are printed on 100% recycled paper. When you have finished with it please recycle it again.

If using an electronic version of the document, please consider the environment and only print the pages which you need and recycle them when you have finished.

Any queries regarding this publication should be sent to us at: public.enquiries@hm-treasury.gov.uk.

ISBN 978-1-84532-974-7
PU1410

Contents

1 Introduction

Purpose

1.1 As expectations of organisations increase and available resources become more restricted, so do the constraints under which they operate and the risks that they face. This guidance advises on how assurance can best support Accounting Officers and Boards in central government departments and their arm's length bodies in the leadership of their organisations and in meeting their corporate governance obligations. It illustrates how risk and assurance arrangements can be directed to meet the delivery and accountability needs of the Accounting Officer and Board, providing evidence-based assurances on the management of risks that threaten the successful achievement of public service delivery objectives and, in turn, report on these to Parliament and other stakeholders.

1.2 It is essential that there is an effective and efficient framework in place to give sufficient, continuous and reliable assurance on organisational stewardship and the management of the major risks to organisational success and delivery of improved, cost effective, public services.

1.3 This assurance framework should be structured and provide reliable evidence to underpin the assessment of the risk and control environment for the annual Governance Statement, supported by independent appraisal from the internal audit service.

1.4 The Governance Statement is a key feature of the organisation's annual report and accounts. It covers the organisation's corporate governance, risk management and internal control arrangements. The statement should incorporate an evaluation on how well the arrangements have operated in practice, based upon the ongoing assessment processes.

1.5 There are many sources of assurance in an organisation that can be harnessed to provide the body of evidence required to support the continuous assessment of the effectiveness of the management of risk and internal control. Understanding the sources of assurance and their scope means internal audit can focus most effectively on the riskier areas. The structured mapping of assurances is one of the fundamental steps in building an assurance framework. This guidance sets out some key steps for both introducing arrangements for mapping and for monitoring assurances throughout the year.

1.6 Further detail can be found in Chapter 2, including definitions of terms used.

Responsibility

1.7 The Accounting Officer, supported by the Board, is responsible for ensuring that there are robust governance, risk management and internal control arrangements across the whole organisation, including any sponsored bodies. Authority, in terms of accountability and respective delegations, needs to be appropriately and clearly established and monitored. This responsibility includes the Accounting Officer demonstrating to Parliament that he/she has maintained a sound system of risk management and internal control in stewardship of the organisation's resources, which is affirmed in his/her signature of the Governance Statement.

1.8 Advice on and scrutiny of key risks is a matter for the Board. The Board will routinely monitor the mitigation of certain strategic risks. These will include risks of a sufficient magnitude to threaten organisational success and reputation, or a scenario of combined risks that would have a similarly devastating impact. This supports the Accounting Officer in ensuring that there is regular and timely assurance on the things that are important to organisational success; in particular, the proportionate management of risks that threaten the successful achievement of business outcomes and objectives.

1.9 Whilst the Board will most closely monitor its key risks, it will otherwise delegate the monitoring of assurance to an Audit and Risk Assurance Committee (ARAC), or appropriate equivalent body in the organisation, made up of independent Non Executive Directors. This is not a substitute for management's responsibility for the mitigation of risks. On behalf of the Board, the ARAC will examine the arrangements in place to provide comprehensive and reliable assurance. This involves identifying the assurance need, how it will be met, whether there are any assurance gaps or overlaps, how these can best be filled and whether this will provide the sufficient, relevant, reliable assurance that it needs. These arrangements should be monitored throughout the year to ensure that sufficient assurance is being planned and delivered to avoid surprises and to enable early decisions and action to be taken on risk and control issues. This will help to routinely validate assurance. A good framework is required to support the governance process.

Benefits

1.10 There are significant benefits to improved co-ordination of assurance. Fundamental to these is the provision of streamlined and synchronised information on organisational performance and the management of associated risks, helping the organisation to operate efficiently and effectively and to report to parliament accurately, meaningfully and without misleading.

1.11 More specifically, an effective assurance framework:

- Provides timely and reliable information on the effectiveness of the management of major strategic risks and significant control issues;
- Facilitates escalation of risk and control issues requiring visibility and attention by senior management, by providing a cohesive and comprehensive view of assurance across the risk environment;
- Provides an opportunity to identify gaps in assurance needs that are vital to the organisation, and to plug them (including using internal audit) in a timely, efficient and effective manner;
- Can be used to raise organisational understanding of its risk profile, and strengthen accountability and clarity of ownership of controls and assurance thereon, avoiding duplication or overlap;
- Provides critical supporting evidence for the production of the Governance Statement;
- Can clarify, rationalise and consolidate multiple assurance inputs, providing greater oversight of assurance activities for the Board/Audit & Risk Assurance Committee in line with the risk appetite; and
- Facilitates better use of assurance skills and resources.

2 Key principles and concepts

Principles

2.1 There are many mechanisms within an organisation that can help to provide information on how well performance and the associated risks to delivery are being managed. An assurance framework is a good mechanism for managing this in a structured, visible format, ensuring that the disparate assurance mechanisms are harnessed and focused to provide the best results in a proportionate and effective manner. Pre-requisites for successful creation of an assurance framework include:

- Support and direction from the Accounting Officer and ownership for the framework at Board level;
- Clarity on what you want it to achieve (particularly encompassing Board and Accounting Officer needs);
- Building the framework first within a manageable boundary (beginning with the high level strategic and key process risks);
- Simplicity – don't try to cover too much in a single assurance map (some organisations have different maps at different levels or separate maps for planning and evaluation); and
- Avoid technical jargon; processes should aim to foster a common clearly understood language.

2.2 The assurance framework should be owned by the Accounting Officer and used to assist him/her in meeting his/her personal obligations to Parliament to maintain a sound system of risk management and internal control, which is affirmed in the Governance Statement. The Board will usually take on oversight and may delegate the regular monitoring of assurance to the Audit and Risk Assurance Committee. The framework should be a core part of an organisation's arrangements for managing risk, rather than a separate exercise and should be integral to the risk management framework used for the effective delivery of the organisation's outcomes and objectives.

2.3 There are different types of assurance that may have different strengths and may be best used in different ways. The Audit and Risk Assurance Committee can therefore play a key role in seeking an optimum mix of assurance. The Three Lines of Defence model (below) can help in this respect.

2.4 Management will already have several sources of assurance over the key risks and an assurance framework is designed to bring these assurances together so that they are obtained more efficiently and effectively. The work will require collaborative input from the relevant parts of the organisation, with designated support to establish and maintain the associated frameworks and individual assurance maps. Risk managers and internal auditors are well placed to advise on structures and to provide content to update the maps, but ownership and compilation best resides within the management chain. Arrangements could vary depending on organisational structure but this could, for example, reside with a strategic or governance function, particularly where associated support is provided to the Board or Audit and Risk

Assurance Committee. The important point is that the arrangements are owned by the Board and management.

Concepts

Assurance frameworks

2.5 Assurance is defined[1] as "...an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization." An assurance framework is a structured means of identifying and mapping the main sources of assurance in an organisation, and co-ordinating them to best effect.

Assurance mapping

2.6 Assurance mapping is a mechanism for linking assurances from various sources to the risks that threaten the achievement of an organisation's outcomes and objectives. They can be at various levels, dependent upon the scope of the mapping. An overview of the process is provided at Annex A.

Three Lines of Defence

2.7 Assurance can come from many sources within an organisation. A concept for helping to identify and understand the different contributions the various sources can provide is the Three Lines of Defence model. By defining the sources of assurance in three broad categories, it helps to understand how each contributes to the overall level of assurance provided and how best they can be integrated and mutually supportive. For example, management assurances could be harnessed to provide coverage of routine operations, with internal audit activity targeted at riskier or more complex areas.

2.8 It is likely to be helpful to adopt a common assurance "language" or set of definitions across the three lines to ease understanding, for example, in defining what is an acceptable level of control or a significant control weakness.

First line

2.9 Within the 'front-line' or business operational areas, there will be many arrangements established that can be used to derive assurance on how well objectives are being met and risks managed; for example, good policy and performance data, monitoring statistics, risk registers, reports on the routine system controls and other management information.

Nature of assurance

2.10 This comes direct from those responsible for delivering specific objectives or operation; it provides assurance that performance is monitored, risks identified and addressed and objectives are being achieved. This type of assurance may lack independence and objectivity, but its value is that it comes from those who know the business, culture and day-to-day challenges.

Second line

2.11 This work is associated with oversight of management activity. It is separate from those responsible for delivery, but not independent of the organisation's management chain. This could typically include compliance assessments or reviews carried out to determine that policy or

[1] Institute of Internal Auditors Practice Advisory 2050-2

quality arrangements are being met in line with expectations for specific areas of risk across the organisation; for example, purchase to pay systems, health and safety, information assurance, security and the delivery of key strategic objectives.

2.12 The developing discipline of Portfolio Management may be of particular use in supporting the second line regarding the assurance of major business change. Portfolio Management aims to provide a co-ordinated approach to enable the most effective balance of organisational change and business as usual. It seeks to take a strategic viewpoint, focused on key issues, to build on and better co-ordinate existing processes such as strategic planning, investment appraisal and project and programme management.

Nature of assurance

2.13 The assurance provides valuable management insight into how well work is being carried out in line with set expectations and policy or regulatory considerations. It will be distinct from and more objective than first line assurance.

Third line

2.14 This relates to independent and more objective assurance and focuses on the role of internal audit, which carries out a programme of work specifically designed to provide the Accounting Officer with an independent and objective opinion on the framework of governance, risk management and control. Internal audit will place reliance upon assurance mechanisms in the first and second lines of defence, where possible, to enable it to direct its resources most effectively, on areas of highest risk or where there are gaps or weaknesses in other assurance arrangements. It may also take assurance from other independent assurance providers operating in the third line, such as those provided by independent regulators, for example.

2.15 Other sources of independent assurance available include Major Projects Authority Integrated Assurance Reviews, external system accreditation reviews/certification (e.g. ISO/Risk Management Accreditation Document Sets), European Commission/European Court of Auditors and Treasury/Cabinet Office/Parliamentary scrutiny processes.

2.16 As an additional line of assurance, sitting outside of the internal assurance framework and the Three Lines of Defence model, are external auditors, chiefly the NAO[2], who are external to the organisation with a statutory responsibility for certification audit of the financial statements. It is important that internal audit and external audit work effectively together to the maximum benefit of the organisation and in line with international standards[3].

Nature of assurance

2.17 Independent of the first and second lines of defence. Internal audit operates to professional and ethical standards in carrying out its work, independent of the management line and associated responsibilities. External audit operates similarly and reports mainly to Parliament.

[2] Some executive NDPBs may have private sector external auditors (either appointed by the relevant Secretary of State or by the Body's Executive) with a reporting line directly to the Secretary of State or to the body rather than through NAO to Parliament.
[3] International Standards on Auditing ISA 610 and 315.

3 Getting started

Assurance mapping

3.1 When first embarking on an assurance mapping exercise, to define an assurance framework, it is best to start simply, by identifying and mapping the assurance over key risks areas. The mapping is likely to be driven by the structures adopted for individual organisational risk registers, but could include strategic risks, significant operational risks, key processes and significant change programmes. Mapping initially at the strategic level, then extending the approach to cover other organisational areas, is likely to assist in reducing the complexity of the activity.

3.2 Much of the necessary information about the risks, who the primary owners are, risk ratings and identified controls/mitigating actions (and their owners), should already have been captured within risk registers and elsewhere. To this should be added the various sources of assurance and the frequency and timing of such activities. It helps to categorise these, using the Three Lines of Defence model, to evaluate and assess the assurance need, especially regarding key operational processes and systems, which may either come from the first or second line (see Chapter 2). This approach can be supplemented by the use of process flowcharts and similar documents, especially where these capture key risk and control points, which may not be included in risk registers.

3.3 A well structured assurance map will highlight where there are gaps in the assurances over significant risk areas. Equally, duplicated or potentially burdensome assurance processes may be identified. This provides useful information to challenge proposed assurances and to question whether the right type of assurance activity is being targeted at the right area of risks and whether this is efficient and prioritised. Delivery of the associated assurance can be reviewed, monitored and tracked throughout the year, helping to strengthen the risk management and control environment and as a consequence ease the task of collating the evidence supporting the annual Governance Statement. As the approach to assurance mapping develops and matures organisations should ensure that their frameworks and maps continue to provide the required breadth of coverage of their overall risk portfolio.

3.4 Assurance mapping is an emerging area of activity and therefore practical examples are continually evolving. The example assurance maps at Annex B are therefore provided as a snapshot and amalgamation of current good practice.

3.5 The assurance map examples recommend a two stage process. The first stage identifies sources of assurance and potential gaps or duplications. Two complementary approaches are suggested: to identify assurance providers against key areas of risk, linked to strategic business objectives; or in relation to key business systems/processes. Both approaches are valid and each is likely to give a different perspective to the assurance environment. Assurance providers are aligned to their position within the Three Lines of Defence model. The example risks, processes and assurance providers are not intended to be comprehensive, rather to give an indication of matters needing to be considered.

3.6 The second stage then maps the risks, systems/processes and assurances identified against the controls currently in place. An evaluation of the adequacy, in breadth and depth, of

assurance coverage is then required, to ensure that there is sufficient evidence available to ascertain whether controls are effective, efficient and comprehensive. This is combined with an assessment of current assurances on the effectiveness of current controls in the mitigation of the organisation's risks to ensure that these are adequate, efficient and comprehensive. Both of these assessments need to be in proportion to the risk exposures concerned, for example, by cross referencing to the assessments within departmental risk registers.

Key involvement in the process

3.7 Assurance mapping requires good engagement across the business, including senior managers, risk owners and/or functional heads and should therefore not just be in the domain of risk and assurance practitioners. The mapping outputs need to be useful and be seen to be so, for example, in driving efficiencies in assurance activities and helping to focus management attention on areas of risk or control requiring specific intervention to ensure delivery of key business strategies.

3.8 Mapping outputs will also help with the early identification of issues that might need to be addressed, or reflected within the Governance Statement, and also to provide specific examples of effective control and well managed risk for inclusion. This can place the Audit and Risk Assurance Committee in a good position to determine whether the Governance Statement represents a fair and balanced assessment and is underpinned by sufficient evidence.

4 Regular reporting on assurance and risk

4.1 The Accounting Officer and the Board will need to ensure that they are receiving sufficient and timely assurance information on the management of risk to enable them to exercise good oversight. This activity may take the form of reporting against a co-ordinated Assurance Plan or Programme. Information provided should include routine reporting on assurance arrangements and the body of evidence that supports this, together with any key points needing to be escalated to the Board. A particular focus should be on the key strategic risks directly owned by the Board but any major "routine" system and process risks should also be included.

4.2 A key component of the information required by the Board will include reports from the Audit and Risk Assurance Committee. This group can use assurance maps, their associated reports and other outputs to routinely monitor the assurance environment and challenge the build-up of assurance on the management of key risks across the year. This will ensure that the Accounting Officer and Board are sighted on significant issues in a timely fashion. From time to time, this may call for intervention to re-focus attention and implement corrective action when necessary.

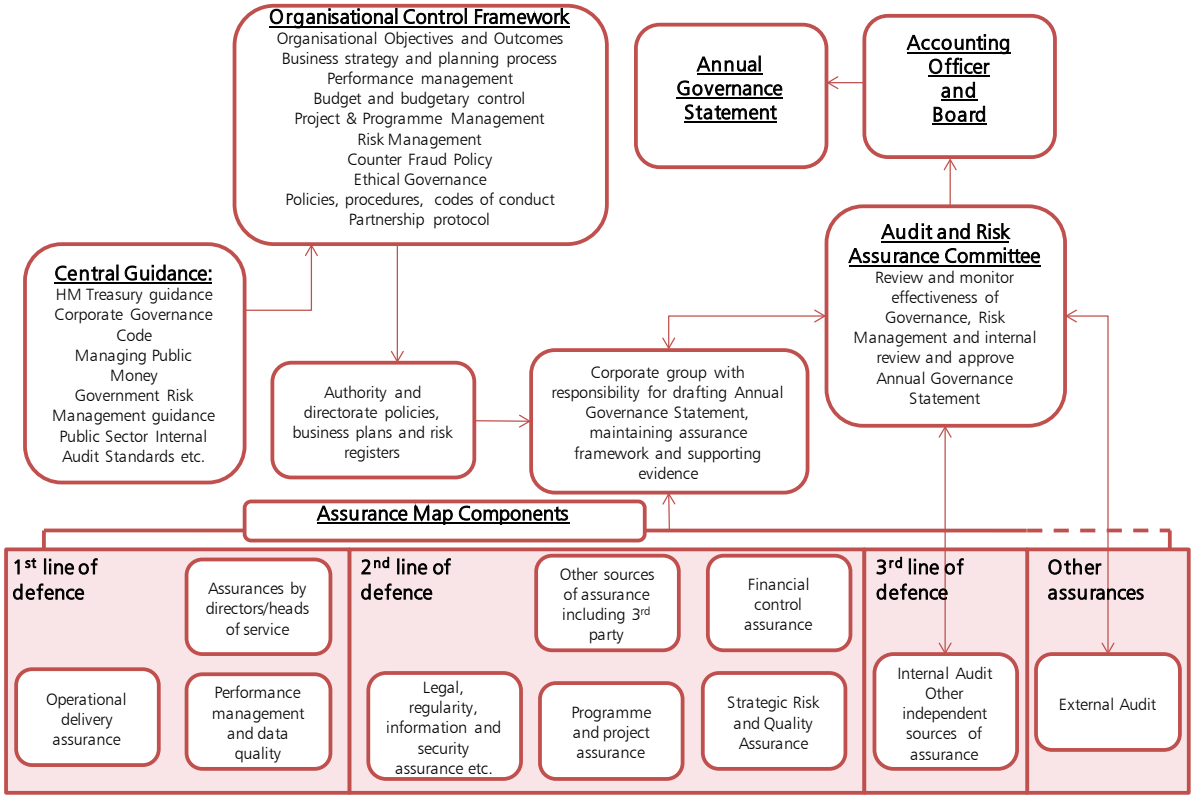
4.3 Both first and second line assurances provide valuable information that informs directors' assurance/stewardship reporting. When drawn together with the third line assurances and, in particular, the Head of Internal Audit's opinion on governance, risk and control, they provide the main information to support the Accounting Officer's Governance Statement. Where the Accounting Officer, Board, or Audit and Risk Assurance Committee identify that assurance information is conflicting, or out of line with the organisation's risk appetite, performance or risk assessment information, they should investigate further. Such action will benefit from direct discussion with senior managers and key assurance providers. The production of interim Governance Statements during the year helps to validate the process and gives time to remedy any issues identified.

4.4 Where significant areas of responsibility and/or funds flow are handled by an arm's length body, or other delivery partner, the associated risks should also feature at a high level in the departmental assurance map, with linkages to more detailed risk and assurance mapping in the related body. The related body or delivery partner should in turn be encouraged to follow the guidance within this document. Similar governance and control arrangements, proportionate to managing the delegated risks, should operate by nature of local risk and assurance frameworks, with suitable reporting and escalation processes in place. This should be reviewed as part of the sponsorship and other oversight arrangements put in place on behalf of the Accounting Officer and Board.

4.5 Similar and proportionate oversight and assurance reporting arrangements should be put in place in respect of services outsourced to external suppliers, including shared service arrangements.

A Process overview

Chart A.1: Example assurance framework arrangements



B Example mapping

Step 1 – Identify sources of assurance

(The example risks, processes and assurance providers are not intended to be comprehensive, rather to give an indication of matters needing to be considered).			Assurance Providers																
			Business Management (First Line) Identifying risks and improvement actions. Implementing controls. Reporting on progress. Management Assurance						Corporate Oversight (Second Line) Designing policies. Setting direction. Ensuring compliance. Assurance oversight						Independent Assurance (Third Line) Independent challenge, audit. Reporting on assurance. Audit of assurance providers. Entity level assurance.				
			Strategies & Business Plans	MI: Performance Management	MI: Financial Management & Reporting	Core Financial System etc. controls (e.g. Accounts Payable)	Core Procurement etc. System controls (e.g. Invoice reconciliations)	Management Self Assessments and Declarations (e.g. CRSA)	Governance Structures & Processes (e.g. Board reports and mitigating actions)	Functional Compliance Reviews (e.g. Finance, Information Security)	Quality Control Checks	Internal Business Change stage/gate reviews	Customer Satisfaction Surveys/Complains	Corporate Risk Management/ Assurance	External Project/Programme Reviews (e.g. MPA Integrated Assurance Reviews)	Adjudicators/ Tribunals	External Accreditation/Certification (e.g. RMADS)	Strategic Partners Assurance Reports	Internal Audit Engagements
Risk	**Risk Owner**	**Strategic Objective/ Priority**																	
Service Delivery																			
Programme & Project delivery																			
Efficiency & Value for Money																			
People and Skills																			
Implementation of Change																			
Management Information accuracy																			
IT Service: Reliability & Availability																			
Information Security																			
Supply Chain resilience																			
Legal/Regulatory compliance																			
Fraud and Error																			

(The example risks, processes and assurance providers are not intended to be comprehensive, rather to give an indication of matters needing to be considered).			Assurance Providers																
			Business Management (First Line) Identifying risks and improvement actions. Implementing controls. Reporting on progress. Management Assurance						Corporate Oversight (Second Line) Designing policies. Setting direction. Ensuring compliance. Assurance oversight						Independent Assurance (Third Line) Independent challenge, audit. Reporting on assurance. Audit of assurance providers. Entity level assurance.				
			Strategies & Business Plans	MI: Performance Management	MI: Financial Management & Reporting	Core Financial System etc. controls (e.g. Accounts Payable)	Core Procurement etc. System controls (e.g. Invoice reconciliations)	Management Self Assessments and Declarations (e.g. CRSA)	Governance Structures & Processes (e.g. Board reports and mitigating actions)	Functional Compliance Reviews (e.g. Finance, Information Security)	Quality Control Checks	Internal Business Change stage/gate reviews	Customer Satisfaction Surveys/Complains	Corporate Risk Management/ Assurance	External Project/Programme Reviews (e.g. MPA Integrated Assurance Reviews)	Adjudicators/ Tribunals	External Accreditation/Certification (e.g. RMADS)	Strategic Partners Assurance Reports	Internal Audit Engagements
Core Systems/Processes																			
System/Process	**Functional Head**	**Strategic Objective/ Priority**																	
Organisational Governance																			
Strategic & Business Planning																			
Performance Management & MI																			
Funding, Grants & Awards																			
Financial Processes & Reporting																			
Procurement & Contract Management																			
HR																			
Health & Safety																			
IT Systems																			
Estates & Infrastructure																			
Physical & Information Security																			
Legal & Regulatory Compliance																			
Projects, Programme & Change Management																			
Communications																			

Step 2 – Assess sources of assurance

(The example risks, processes and assurance providers are not intended to be comprehensive, rather to give an indication of matters needing to be considered)

				Assurance Providers				Assessment		
				Business Management (First Line)	Corporate Oversight (Second Line)	Independent Assurance (Third Line)				
				Identifying risks and improvement actions. Implementing controls. Reporting on progress. Management Assurance	Designing policies. Setting direction. Ensuring compliance. Assurance oversight	Independent challenge, audit. Reporting on assurance. Audit of assurance providers. Entity level assurance.		Control RAG Rating (See Key)	Assurance Sufficient? Y/N	Improvement Actions
Risk	Risk Owner	Strategic Objective/ Priority	Controls			Internal Audit	Other Independent Sources of Assurance			
Fraud and Error		Deliver demonstrable value for money for the taxpayer	Operating Procedures Training programmes System reports on specific areas of potential fraud Internal Quality Control checks Whistle blowing policy	Management reports on targeted fraud and error reduction action plans Active use of Managing Risks of Financial Loss toolkit	National Quality Control Checks Counter fraud policy compliance checks	Internal Audit review of counter fraud policy and implementation	Adjudicators/ Tribunals NAO audits	G	Y	
Customer Service		Deliver reliable, modern and affordable customer service	Operating Procedures Training programmes Internal Quality Control checks Monitoring intake levels & balancing of resources	MI: Performance Management reports Internal Quality Control checks	Intake and capacity reviews Governance Structures: e.g. Board Customer satisfaction surveys & Complaints			A	N	Consider need for independent assurance reviews - e.g. Performance MI quality
Programme & Project delivery		Improve our business by driving efficiency and service modernisation	Project management processes Project Boards New system testing processes Internal "approval to proceed" reviews	Project Management delivery reports	Programme Office reviews Programme and main Board reviews Corporate Risk Management/ Assurance reviews Internal "approval to proceed" project stage reviews	Internal audit reviews of project management and project risk management	OGC/MPA Gateway reviews	A	Y	Ensure effective integration of internal audit and MPA assurance reviews Review change implementation processes
Core Systems/Processes										
System/ Process	**Functional Head**	**Strategic Objective/ Priority**	**Controls**							
Financial Processes		Deliver demonstrable value for money for the taxpayer	Finance Manual Delegated authority processes Finance control reports (IT & manual)	MI: Financial Management & Reporting Active use of Managing Risks of Financial Loss toolkit	Finance team compliance checks	Internal Audit financial system reviews	NAO audits	A	Y	Ensure effective integration of internal audit and NAO reviews. Review assurances on shared services. Increase systemisation of finance control checks
Information Security		Deliver high standards of integrity and reliability in our data management	IS policy, guidance & training DPA policy, guidance & training Incident reporting	Management Reporting Structures Management Assurance Incident reporting	Information Security Compliance Reviews Incident reviews		Information Commissioner's Office reviews External Accreditation (e.g. RMADS)	A	N	Consider need for additional internal audit activity - e.g. DPA compliance
Supply Chain management		Improve our business by driving efficiency and service modernisation	Supplier contracts & SLAs Supplier performance reviews Contract management processes Business Continuity Plans	MI: Performance Management reports - internal Supplier performance reports Internal Quality Control checks	Contract management reviews Board etc. reporting			A	N	Consider options for Strategic Partner assurance reports. Consider need for independent assurance reviews

Key:	**RAG rating on the effectiveness of controls from assurance work undertaken**
	Low: Significant concerns over the adequacy/effectiveness of the controls in place in proportion to the risks
	Medium: Some areas of concern over the adequacy/effectiveness of the controls in place in proportion to the risks
	High: Controls in place assessed as adequate/effective and in proportion to the risks
	Insufficient information at present to judge the adequacy/effectiveness of controls

HM Treasury contacts

This document can be found in full on our website: http://www.hm-treasury.gov.uk

If you require this information in another language, format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

E-mail: public.enquiries@hm-treasury.gov.uk

ISBN 978-1-84532-974-7