Cabinet Office

Guidance for General Grants

Minimum Requirement Seven: Risk, Controls and Assurance

Version: 2.6

Date Issued: September 2024

Important note

- This guidance applies only to general grants made by departments and their arm's length bodies (ALBs) using Exchequer funding. It does not apply to formula grants or grant in aid. Managing Public Money and local guidance within government grant making organisations is applicable to those categories.

- Organisations' primary concern when administering grants is to have due regard to the 'Grants Functional Standard' (GovS 015) and the key documents referred to within it including 'Managing Public Money'. Nothing in this guidance is intended to contradict or supersede these. Furthermore, this guidance is not intended to be an additional spending control - departments retain accountability for decisions on all grant expenditure.

- This guidance should be read in conjunction with the wider set of 'Minimum Requirements' guidance documents (including the Introduction). Further information about how to apply this guidance can be found online through the 'grants Centre of Excellence (CoE)'. Further references and resources are highlighted throughout. It should also be read alongside organisations' internal guidance, where available, which will provide the departmental policy context.

- This guidance should be approached on a 'comply or explain' basis. It is important to consider flexibility and proportionality in adhering to the minimum requirements. As such there may be some specific instances where the requirements may not be met in full. In these instances, appropriate justification should be recorded within the business case or equivalent approval documents.

Contents

Minimum Requirement **4**
Purpose **4**
Grants Functional Standard: Key References **5**
Overview **7**
Risk **7**
Risk Appetite 7
Engagement **Error! Bookmark not defined.**
Risk Registers 8
Risk Rating 9
Fraud Risk Assessment (FRA) 9
National Security and Economic Crime 10
Controls **12**
Due Diligence **13**
Table: due diligence checks 14
Assurance **16**
Governance processes 16
Assurance framework related to grants 16
Reporting of assurances related to grants 17
Accounting Officers 17
Further Resources **18**

Minimum Requirement

All government grants shall be subject to **timely and proportionate due diligence**, **assurance** and **fraud risk assessment**.

Purpose

Minimum Requirement Seven: risks, controls and assurance provides detail on the creation and maintenance of a risk, controls and assurance management framework, including the management of national security and economic crime threats. An effective risk, controls and assurance framework is designed to reduce the risk of grant schemes failing to achieve their objectives and will support efficiency and the achievement of value for money, helping to minimise the misuse of public money.

Grants Functional Standard: Key References

Mandatory requirements are defined by the word 'shall' in the Grants Functional Standard, which can be accessed on GOV.UK. The 'shalls' for the management of grants related to this minimum requirement have been extracted from the 'Grants Functional Standard' and are set out below. **Please note**; in some cases the information has been paraphrased for conciseness – refer to the standard itself for the full text.

Area	Requirement(s)	Context	Reference	Page
Grant Life Cycle: General grants life cycle	When developing general grant models and criteria for assessing individuals and organisations for a grant award, consideration **shall** be given to combinations of risk and fraud risk indicators, which could affect the value of the award, or whether the grant should be awarded at all.	Early identification and mitigation of risk is critical.	5.2.1 Design and development	13
Supporting practices: Risk and issue management	Organisations **shall** ensure effective risk management is established in their assurance and governance processes.	Risk management practices and procedures will be part of overall assurance and governance.	6.1 Risk and issue management	18
Supporting practices: Counter fraud	An assessment of fraud risk **shall** be undertaken for every scheme proportionate to the value, sector and required activity of the scheme, and supported by mitigating actions appropriate to the identified risks. When managing and planning counter fraud activities, Functional Standard GovS013: Counter Fraud **shall** be followed.	This approach is to ensure that government grant funding in respect of policy delivery and the purchase or improvement of assets is awarded safely and used for its intended purpose.	6.2 Counter fraud	19

Governance: Roles and accountabilities	The senior officer accountable for an organisation's grants is accountable to the senior officer accountable for finance. They are responsible for ensuring that the financial requirements for grants schemes and awards are implemented, in full, within the department and its arm's length bodies (if any) and depending on the management arrangements in place. In particular: - ensuring the required outcomes from grant-making activities are realised, at an acceptable level of risk and cost.	The senior officer accountable for the organisation's grants plays a key role in ensuring an acceptable level of risk is considered in grants management.	4.4.5 Senior officer accountable for an organisation's grants	12

Overview

1. Departments and arm's length bodies (ALBs) shall have an appropriate framework covering risk, controls, and assurance to manage their grant activity. This document provides detail on what should be included.

2. The Senior Officer Responsible for a grant (SOR) shall retain oversight of their grant schemes and also support the Accounting Officer and the Principal Accounting Officer in discharging their responsibilities, as set out in HMT's Managing Public Money. The Senior Officer Accountable (SOA) for an organisation's grants portfolio is accountable for ensuring the required outcomes from grant-making activities are realised at an acceptable level of risk and cost.

3. The following sections of this document considers the minimum requirements for risk management, controls and assurance, focussing on:

    - Systems to manage grants in departments and grant-making ALBs.
    - Management of individual grant schemes and awards.

4. Risk management, fraud risk assessments (FRAs), due diligence, controls, and assurance are essential to the grant-making process and shall be continuously monitored throughout the grant's lifecycle.

Risk

5. Risk management shall be included in department and ALB grant management processes. Basic principles and guidance related to risk management are contained in the Orange Book.

6. The Grants Functional Standard covers risk management, which shall be a core component of every stage of the grant management process, from design and development to final evaluation.

7. Departments and ALBs should use their own decision-making tools and guidance to rate their scheme level risks, based on a likelihood versus impact model. The MR7 supporting guidance on the grants Centre of Excellence (CoE) provides more information on this model and includes an example risk matrix. **Very high** or **high**-rated grant risks should be highlighted and explained in the scheme's business case, along with mitigating actions and controls.

8. Transparent identification and management of principal risks within business and financial plans will support delivery confidence.

Risk Appetite

9. Departments and ALBs should have a defined and agreed appetite in relation to risk, approved by the Senior Officer Accountable for Finance (also known as the Finance Director). This should be communicated to all staff involved in the design,

development and administration of grants, via guidance. Awareness of the risk appetite in departments and ALBs will support subsequent escalation of risks and issues to senior management, ensuring risks and issues which exceed the agreed tolerance are escalated.

10. The risk appetite of departments and ALBs should be reviewed on a regular basis, in order to keep pace with the changing types of risk faced, and in the light of significant events, which may impact the risk landscape. For example, the COVID Business Support Scheme significantly raised the risk of fraud and misuse in grant making during the pandemic. In these cases, risk appetite should be reassessed and reset if appropriate and re-communicated within the department and its ALBs.

11. Documented processes should be in place to enable grant managers to escalate risks to appropriate boards/levels as they materialise. Grant managers should follow internal risk management policy for risk escalation.

Risk Registers

12. Department and ALB risk registers shall include **very high** and **high** rated risks, related to significant grant schemes and awards, as a minimum. These risks and issues shall be discussed at departmental governance boards and audit committees, as part of an embedded risk review process. The assessment of what constitutes a significant scheme should consider a range of factors and at a minimum should include level-1[1] schemes and those that meet the mandatory CGAP referral criteria (as detailed in MR3).

13. Detailed risk registers shall be developed and owned by all SORs who manage significant grant schemes and awards. The creation and maintenance of a proportionate, high-level risk register is considered good practice for all grant schemes, regardless of value. These shall be used to consider if additional controls are needed to reduce the impact or likelihood of risks being realised. They also support ongoing assessment of whether current risks are outside of the organisation's risk appetite and, therefore, should be escalated to the department's SOA (see paragraph 2).

14. Grant scheme risk registers should ensure the following:

- risks are focused on achievement of the grant objectives and outcomes, with full consideration of the principles set out in Managing Public Money;
- Orange Book risk categories (**Annex 4**) are fully considered and applied, where appropriate, when identifying risks;
- the residual risk profile is compared with the department's or ALB's risk appetite and any risks outside that appetite should be escalated to the SOA;
- the risk register is regularly discussed, including at every stage of the lifecycle of the grant, and is used as an active tool to support good grant management;

[1] Level-1 grant schemes have a minimum value of £20 million and are defined in the Grants Pipeline Control Supporting Guidance, which is available to download from the grants Centre of Excellence.

- related controls are documented and are subject to regular assurance (see assurance section at paragraph 49), appropriate to the severity of the risks being mitigated;
- departments and ALBs have a process in place for rating their risks, based on a likelihood versus impact model (see paragraph 7)
- materialised **very high** and **high** risks are recorded as issues and are subject to documented action plans, which are regularly updated proportionate to their materiality to the department or ALB.

15. Approaches to managing risks can be characterised under the following categories.

- **Treat**: controls applied to reduce the likelihood and impact.
- **Tolerate**: risk and issues are accepted.
- **Transfer**: responsibility for the risk may be transferred to another organisation better suited to manage it.
- **Terminate**: the grant scheme or award is withdrawn or the scheme is redesigned to eliminate one or more specific risks.

16. Where a business area decides to accept – tolerate – a **significant risk** or **issue**, which is outside of the department's or ALB's risk appetite, it should document the management decision and the rationale. Such treatment should be approved by the SOA and should be recorded within the department's or ALB's existing risk reporting.

GGIS Risk Rating

17. Departments and ALBs shall assign an overall risk rating to each grant scheme at the business case stage. The initial rating shall be recorded on the GGIS in the **scheme risk profile** field. This rating should be reviewed, and updated if appropriate, at each stage of the grant's lifecycle. More information on this field is on page 26 of the grants data standard, which can be found on the grants CoE. The ratings - **high**, **medium** and **low** are defined on page 111 of the same document.

18. The MR7 supporting guidance on the grants CoE provides some details on what factors might contribute to the application of each of the risk ratings.

Fraud Risk Assessment (FRA)

19. Every grant scheme shall have a documented assessment of their fraud risk, which should be proportionate to the size and perceived risk of the grant scheme within the organisation and align to the requirements of GovS013 Counter Fraud.

20. All grant schemes should consider the impact of fraud over and above financial loss. This may include: reputational damage; the impairment of the achievement of government policy objectives; physical or societal harm; environmental impacts; as well as risks to national security, including terrorist financing, hostile state actors and organised crime.

21. In addition to fraud, broader risks should be considered – the Initial Fraud Impact assessment (IFIA), detailed within the Government Counter Fraud Professional Standards and Guidance, sets out a methodology for this.

22. The IFIA should be completed early on in the lifecycle, prior to spending approval, and is required for all new major spend activity. The PSFA defines major spend activities as those which are large, complex or innovative, with many 'breaking new ground'. More information can be found on page 47 of the Government Counter Fraud Professional Standards and Guidance.

23. A detailed Fraud Risk Assessment (FRA) should be developed for all schemes. This should be done prior to funding being approved where possible. More information on fraud risk assessments can be found in the Government Counter Fraud Professional Standards and Guidance. Supporting information in Managing Public Money places emphasis on FRA in relation to assessing vulnerability to fraud, evaluating the scale of fraud risk and responding to fraud risk.

24. As a minimum, all grant schemes should consider common fraud risks including: falsified eligibility; misuse of grant funding; hijacked identities; inflated costs; claims for work not performed; duplicate funding; deliberate claims for excessive funding; collusion between the applicant and an internal actor; changing bank details to a fraudster's account (mandate fraud); and claims from entities which do not exist or are not operating. This list is not exhaustive, departments and ALBs should consider a full range of fraud risks appropriate to individual schemes.

25. A detailed FRA should be maintained through the life of the scheme to reflect changes to risk, controls and risk tolerance to ensure there is continuing focus on fraud prevention, detection and recovery.

26. It is important for the organisation's Counter Fraud Function to have an overview of all its grant schemes, from a fraud risk perspective, as set out in the Government Counter Fraud Professional Standards and Guidance, which provides further detail on how to do high-level and intermediate fraud risk assessments. This should inform the organisation's counter fraud strategy.

27. Where there is a lack of capacity or no dedicated counter fraud function to support, the Public Sector Fraud Authority (PSFA) can provide fraud risk services via the Risk, Threat and Prevention accessible Tactical Support team (mailbox: psfa-rtp-services@cabinetoffice.gov.uk).

National Security and Economic Crime

28. Grants schemes are vulnerable to actors who may wish to undermine the UK's national and economic security. It is important that grant makers are aware of these potential risks to their schemes. The type of threats they pose can be distinguished into two areas.

- **Opportunistic threats:** These occur when actors discover and exploit vulnerabilities within processes or systems during regular grant activities. They usually require little planning and are often carried out for immediate gain.

- **Targeted threats:** These are deliberate attacks aimed at specific schemes for a variety of purposes such as theft of funds or intellectual property, or to disrupt or influence government policies. These threats are typically premeditated, involve extensive planning and take longer to implement than opportunistic threats.

29. Hostile actors can include terrorists, extremists, individual criminals, organised crime groups, political or pressure groups, delinquent businesses, and even other states or state-sponsored entities. The purpose of their illicit activities can also range in scope; from simple financial gain, through to accessing innovative technology, facilities or networks. For example, hostile states have used intermediary businesses to gain access to intellectual property (IP) that has dual civilian and military use.

30. Some schemes may be subject to regulatory or legislative controls that require consideration of specific National Security / Economic Crime risks. One overarching example of this is the requirement within the UK sanctions regime not to issue funds to sanctioned individuals or entities. Another more policy specific example covers the potential impact of Martyn's Law, where funds are used to improve the security of venues and public spaces to protect those who use those spaces, or where grant funding is for wider development of public spaces where the owners or operators may owe a similar duty of care. Under these circumstances, please check the relevant regulations or laws and any associated guidance to ensure compliance wherever necessary. In the above example with public infrastructure development, the Publicly accessible locations (PALs) guidance provides detail on what to consider and mitigations (some of which may prove useful even in instances that go beyond the strict requirements laid out in the regulations).

31. The Grants Threat Handbook (available on the Standard Documents page of the grants Centre of Excellence) sets out key risk indicators (from page 18) grants schemes should consider across a number of national security and economic crime areas. Examples include risks around fraud and corruption that are addressed elsewhere in this document, as well as covering espionage, theft, market abuse, cyber-crime and money laundering.

32. Where risk indicators are identified, or where a grant falls into the threat parameters outlined in paragraph 28, advice should be sought from subject matter experts to identify whether a national security or economic crime risk is present within a scheme. In the first instance, contact your department or ALB's security team or contact the GGMF National Security and Risk Unit nsru.commissions@cabinetoffice.gov.uk

Research Funding

33. There is a risk that technology developed as part of an international research collaboration could be misused by a foreign state to control or repress their population.

34. Dual use technology, which may be subject to export control, could be adapted by a foreign state's military against UK interests. In such cases, failure to protect IP and a lack of due diligence into collaborators could result in sensitive technology being transferred to and misused by a hostile foreign state. The loss of sensitive IP and technology has the potential to damage the prosperity of the UK.

35. The Centre for the Protection of National Infrastructure has launched Trusted Research, a new campaign to support the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector. If you manage research and innovation grants please familiarise yourself with the aims and objectives of the campaign and promote it to your grant recipients as appropriate.

36. Grant making departments and ALBs shall ensure grant recipients provide a commitment that IP generated from taxpayer funded research will be of benefit to UK prosperity.

Engagement

37. Departments should consider the engagement standards set out in the UK Government's Engagement Principles, when providing external engagement or funding.

38. The Government's Engagement Principles combine best practice guidance for engagement, with a set of standards against which officials can make carefully considered judgements about who to engage with and provide funding to. The engagement principles and accompanying guidance are designed to help officials feel more confident in the engagement decisions they take and to engage more widely – thereby increasing the quality and consistency of government's engagement.

Controls

39. Departments and ALBs should ensure that there are proportionate, risk based, efficient and effective controls in place to manage the risks identified at every stage of the grant administration process. Effective risk management and controls for the whole grant management system is a specific responsibility of the department's SOA supported by the SOR for individual schemes and awards.

40. Controls are any action taken by management, the board and other accountable parties to manage risk and increase the likelihood that identified objectives will be achieved. They should typically entail a range of preventative, directive, deterrent, detective and corrective controls.

41. Where a residual risk, logged on the risk register, is deemed to be outside the tolerance of the department's risk appetite, additional controls should be identified and implemented to bring the risk within appetite. Exceptions to this should be documented and approved by the SOA.

42. When ALBs are responsible for grant administration, departments should ensure that governance documents, (for example - memorandum of understanding (MoU), framework documents) contain appropriate reference to a control framework supporting grant making. These documents should provide assurance that the control framework is operating effectively.

Due Diligence

43. The GGMF Grants Due Diligence Guidance (available to download from the grants CoE), sets out the steps departments and ALBs should consider taking across the grants lifecycle. This ensures public money is awarded to appropriate entities and helps address potential risks related to governance, legal, financial, security, operational and reputational concerns. It also addresses risks relating to economic crime - including but not limited to fraud, money laundering, sanctions evasion and bribery and corruption – as well as national security - including but not limited to state activity, cyber-attacks, dis and misinformation, extremism and terrorism - and serious and organised crime and terrorist financing.

44. The objective of due diligence checks is to identify and evaluate potential risks and threats involved in the grant assessment award process, and ensure that grant funding is awarded efficiently to eligible recipients, in order to deliver better value for money and outcomes.

45. Due diligence, proportionate to the scheme value and risk level should be performed during the assessment of applications. Due diligence is an ongoing process, and initial assessments should be reviewed and updated as part of monitoring and post-award assurance. Robust due diligence processes help to mitigate reputational risks, potential fraud, potential national security risks, errors and financial loss.

46. Grant making departments and ALBs should consider the resources to be allocated for due diligence, in line with the following principles:

- resources allocated to the due diligence process are at the discretion of funding organisations, which are free to conduct due diligence themselves, or outsource as appropriate;
- ensure that the right people with the right skills are assigned to the task and consider the resource allocation, based on the thresholds of grants outlined in the diagram below, for example, for grants with a value of less than £100,000 the due diligence checks can be undertaken by the grant or policy team with support from finance and commercial when needed;
- for complex and contentious grants, or those above £100,000, consider using staff with specialist skills as appropriate, for example, accountants, fraud investigators, lawyers, etc.; and

- there is no prescription for individuals conducting due diligence checks, but those involved should have the powers, authority, knowledge and experience to carry out due diligence in full, and the SOR should be able to confidently approve the findings and recommendations from due diligence checks.

47. Grant making departments and ALBs should develop due diligence models, based on best practice and guidance that are proportional to the value of the grant, as illustrated in the table below.

Table: mandatory due diligence checks

Due diligence checks on business and non-profit entities		
Grants award below £100k and Low Risk	**Grant awards £100k - £5milion and/ or High Risk**	**Grant awards above £5million**
Basic Mandatory Requirements **Eligibility** Check if the individual or entity meets the eligibility criteria. ● Identity (for example, entity is who they say they are). ● Legal Structure and Status of an organisation (e.g. the organisation is trading/active, this can usually be found on Companies House and Charities Commission. ● Day-to-day activities of the organisation are in line with the grant purpose. **Operational** ● Past experience in managing grant awards. ● Performance under other government grant awards/contracts.	**Further requirements in addition to the previous column:** **Operational**: investigate if the grant recipient has the people, processes and products required for delivery **Financial** • Unrestricted reserves held by the organisation are in line with their own financial policies, controls and procedures. • There are sufficient unrestricted reserves to pay any creditors falling within one year. **Governance**: Their internal policy documents include: financial controls; risk management; safeguarding.	**Further requirements in addition to the previous two columns:** ● A site visit is advisable ● Detailed analysis of financial accounts. ● Quarterly reviews of performance. ● Consider that a non-executive member sits on the programme board.

Financial ● Up to date financial reporting (for example, no overdue accounts). ● What is the percentage of grant funding sought in relation to the turnover listed in latest set of financial accounts. Look for signs of reliance on grants funding. ● Does the applicant have a credible case for assistance (need for grant) and is the grant amount requested the minimum necessary for the project to go ahead? ● Bank Account verification (for example, name/bank account details match). **Governance** ● Registration history (how long has the organisation been registered)? ● Ownership and corporate control of the organisation. ● Directors/trustees are active. ● Director/trustee conviction/disqualification. ● Conflicts of interest Where a non-UK based organisation or non-British Director/trustee is identified within the ownership structure, checks should be made to verify if they are subject to UK or international sanctions regimes, or hold a high profile political or public role (Politically Exposed Person). **Reputation**		

Perform adverse media checks. Departments should consider carrying out checks against the engagement standards set out in the UK Government's Engagement Principles.		

48. Below are three potential outcomes from the due diligence process.

- **Fully approved:** a recommendation to proceed with the award.
- **Partially approved:** depending on the concerns raised, a variety of options are available such as: requiring a guarantor; reduction in grant value to lessen the department's exposure; further enhanced due diligence checks; and considering funding in tranches with enhanced monitoring.
- **Not approved:** a recommendation not to proceed with the award.

Assurance

Governance processes

49. Grant-making departments and ALBs should obtain appropriate assurance against the effectiveness of their risk management and controls, as part of internal governance processes. This can be achieved through internal audits, internal reviews and other assurance mechanisms. The level and range of assurance depends on the departmental risk appetite, the size and type of grants administered and the impact on business objectives. Ultimately this will inform the end of year reporting process.

50. A comprehensive assurance framework will provide confidence that control measures are operating, effective and aligned with organisational policies. It will also help identify any areas where controls may be lacking.

Assurance framework related to grants

51. Departments and grant making ALBs should develop an assurance framework in line with the **three lines of defence model**. This should be completed at both organisational and scheme level, considering risk and proportionality. Departments and ALBs should periodically review the effectiveness of the implementation of controls designed to mitigate key risks to acceptable level.

52. HMT's guidance on assurance frameworks provides further details and provides templates to conduct the assurance mapping exercise. This process will help identify gaps in assurance arrangements and enable departments to strengthen controls where needed.

53. Where schemes present significant financial, delivery, strategic or reputational risks, SORs may benefit from additional assurance activity. Departments and ALBs should

consult with Government Internal Audit Agency (GIAA) or internal auditors. This could include probative testing to confirm the eligibility of expenditure claimed, grant conditions have been complied with and value for money has been achieved.

54. The GIAA Grant Specialism Team can provide advice and guidance on matters relating to compliance with the Grants Functional Standard and can undertake bespoke assurance activities to assess the adequacy of assurance frameworks. This includes the development of testing methodologies to assess the effectiveness of the implementation of grant management and control arrangements. All enquiries can be directed to: GrantSpecialism@GIAA.gov.uk.

Reporting of assurances related to grants

55. Grant making departments and ALBs shall have a process to ensure that assurance reports are shared with their senior governance boards and audit committee for review and comment.

    This could include:

    - internal audit reports and assurance on grant management and control arrangements;
    - validated Statements of Grant Usage from grant recipients;
    - value for money assessments at the business case and evaluation stages; and
    - Infrastructure and Project Authority (IPA) assessment, findings and recommendations.

    And shall include:

    - the biennial continuous improvement assessments (previously the 'maturity assessment') - scores shall be discussed by the organisation's boards and audit committee, along with any action plans to improve the scores.

Accounting Officers

56. As required by HM Treasury guidance, responsibilities related to grant management shall be clearly defined in departments' annual Accounting Officer System Statement (AOSS) – the '7th Section' of the guidance sets out the requirements for grants. The AOSS provides visibility against required assurances from those with responsibility for the management of the department's grants portfolio.

57. Principal Accounting Officers remain accountable for grant funding issued to ALBs. With respect to grant funding, Accounting Officers should:

    - seek assurance that ALBs sponsored by their department are compliant with the grants functional standard and associated minimum requirements for general grants and have an appropriate assurance framework;
    - ensure that associated ALB framework and governance documents include a reference to the requirement to comply with the grants functional standard - a

review of the efficacy of governance documents should be undertaken periodically, at an appropriate point;
- ensure there is a process to escalate risks from the ALB to the department; and,
- accurately define responsibilities related to grant management within their AOSS.

Further Resources

58. To meet these requirements, departments and ALBs should consider the following resources:

    - The HM Treasury Orange Book: Management of Risk – Principles and Concepts.
    - Internal guidance on risk management, controls and assurance, particularly related to grant risk appetite and management.
    - The Centre for the Protection of National Infrastructure (CPNI) and National Cyber Security Centre (NCSC) Trusted Research guidance.

59. Each central government department has a Grants Champion, whose role is to act as a single point of contact between the department and the GGMF. This includes sharing and providing access to information, across their organisation and their grant making ALBs. If you do not know who your Grants Champion is, please access the Grants Champion page on the grants CoE.

60. Departments and ALBs should also utilise wider resources available through the grants CoE – including the MR7 Supporting Guidance and GGMF Guide to Due Diligence for Grants.