Cabinet Office

Guidance for General Grants

Minimum Requirement Seven: Risk, Controls and Assurance

Version: 1.2

Date Issued: 30 June 2020

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, although guidance for the latter grant will be developed in the future. 'Managing Public Money' and local guidance within organisations will continue to apply until then.
- 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 in the following document: ***'Grant Scheme Readiness: a guide to designing and developing a new government grant scheme'***, available online through the 'Grants Centre of Excellence (GCOE)'. 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

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 framework involving risk management, controls and assurance including undertaking appropriate counter fraud and due diligence activities. An effective control framework will significantly reduce the risk of failure of a grant scheme to achieve its objectives and will help to support effective risk management, which also includes the requirement to assess and manage risks to national security, wherever applicable.

Grants Functional Standard: Key References

Mandatory expectations ('shall') for management of grants related to this minimum requirement have been extracted from the 'Grants Functional Standard' which can be accessed here on gov.uk. *Please note that in some cases the information has been paraphrased for conciseness - refer to the standard itself for the full version.*

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 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	12
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 factor into wider assurance and governance.	6.1 Risk and issue management	17
Supporting practices: *Counter fraud*	*A counter fraud strategy **shall** be developed appropriate to the identified risks.* *The risk of fraud **shall** be considered in relation to grant awarding and management activities.*		*6.2 Counter fraud*	*17*
Governance: Roles and responsibilities	The senior officer accountable for an organisation's grants is responsible for ensuring that the financial requirements for grant 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 SOA for the organisation's grants plays a key role in ensuring an acceptable level of risk is considered in grants management.	4.4.4 Senior officer accountable for an organisations grants	8

Overview

1. Departments and arm's length bodies (ALBs) should have an appropriate framework covering risk, controls, and assurance to manage their grant activity. This document provides detail on what should be included in such a framework.
2. The framework is linked to the requirement for the Senior Officer Responsible for a grant (SOR) to retain oversight of their grants and also support the Accounting Officer and the Principle Accounting Officer in discharging their responsibilities, as set out in Managing Public Money. The Senior Officer Accountable for an organisation's grants (SOA) is responsible 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 consider the minimum requirements for risk management, controls and assurance focused on:
    - systems to manage grants in departments and grant making ALBs;
    - management of individual grant schemes and awards; and,
    - incorporating the content of an earlier version of this document – *minimum standard seven* - which covered only due diligence and fraud.

Risk Management

4. Risk management within grant management processes and systems should be undertaken as part of department and ALB risk management systems and processes. Basic principles related to risk management are contained in the Orange Book.
5. Where grant making is a significant part of business objectives, departments and ALBs should decide how effective their grant management processes and systems need to be to deliver their core objectives and this should include an overall risk profile. This will inform the organisation's risk appetite. An immature grant management capability represents acceptance by the department or ALB of a higher degree of risk related to grant making.
6. Departments and ALBs should have an agreed appetite in relation to grant risk and should communicate that risk appetite to all involved in grant management – this includes departments communicating risk appetite to their grant making ALBs. The risk appetite should outline the principal risks that the organisation is both exposed to, and is willing to take, to achieve its objectives. Awareness of the risk appetite in departments and ALBs will support any subsequent escalation of significant risks and issues to senior management, ensuring only risks which exceed the agreed tolerance are escalated. Consideration of risk appetite should include the risk of fraud and loss of public money.
7. Significant events may change the risk appetite of the department, for example, the Public Accounts Committee inquiry into the Kids Company. In these cases, risk appetite should be re-set and re-communicated within the department and its grant making ALBs. More generally, departments and ALBs should regularly review the approach taken to approving their risk tolerance in order to keep pace with the changing types of risks faced.
8. Aspects of risk tolerance / appetite to be considered in relation to grants may also include factors such as the amount of expected fraud, compliance with the General Data Protection Regulation (GDPR) to protect personal information, ensuring that

value for money can be demonstrated, or where applicable, covering risks to national security, for example through knowledge transfer or data use as a result of funded research, etc.

9. Types of risk relevant to the grant management system include:

- central arrangements to manage grant making are not effective;
- the overall control framework is not effective or efficient;
- no process exists to escalate significant grant risks or issues;
- national security risks have not been considered or mitigated where it is necessary, for example in relation to sensitive research with dual military or civilian uses or where grant awards may be diverted to fund extremism;
- insufficient guidance and advice is made available for colleagues across departments to enable consistent and effective grant making;
- the limited capacity and capability of those involved in managing the grant making process;
- the extent to which grants are subject to competition;
- ministerial requests to make direct awards that may contravene Managing Public Money;
- insufficient focus on responsible grant making by grant recipients, resulting in reputational damage;
- second line assurance activity is not sufficient or effective; and,
- grant systems do not support prompt or efficient payment.

Risk management in grant making

10. As required by the Functional Standard risk management shall be a core component of every stage of the grant management process, from design and development to final evaluation.

11. Broad risk areas relevant to individual grant schemes and awards – aligned with Accounting Officer tests on propriety, regularity, value for money, and feasibility include:

- poor value for money secured, or value for money not assessed, due to poor delivery of the output;
- risk of fraud, or loss of public money;
- insufficient due diligence to ensure grant recipient is solvent and an appropriate organisation to receive funding;
- failure to pay a grant recipient promptly and accurately;
- non-conformance to the GDPR, leading to increased risk related to the storage of personal information relating to the grant recipient;
- non-compliance with legal frameworks such as: Export Controls, the Academic Technology Approval Scheme (ATAS), the UK money laundering regulations and the UK Sanctions Regime;
- grant expenditure leads to questions related to State Aid compliance and possible referral to competition authorities by a third party;
- activity is outside the ambit of the department, or is novel, contentious and repercussive, or carries a potential risk to national security; and,
- reputational damage, arising from any of the above.

12. Departments and ALBs setting up grant schemes in the fields of research, innovation, technology and infrastructure should consider the following:

    - National security risk: the risk of a threat to UK national security arising from an Organisation's failure to protect intellectual property, classified information or sensitive or dual use technology emerging from a grant award (further advice is available at https://www.cpni.gov.uk/trusted-research-guidance);
    - Export control risk: the outputs from some grant awards can, in some circumstances, give rise to a risk of breaching export controls on sensitive or dual use technology. Early engagement with the Export Control Joint Unit can help mitigate such risks. Further advice is available at: https://www.gov.uk/guidance/export-military-or-dual-use-goodsservices-or-technology-special-rules;
    - Organisational security risk: the risk of a threat to the security of an organisation, its personnel or its own or other's intellectual property arising from that organisation's failure to protect sensitive information emerging from a grant award; and
    - The correct categorisation and application of tax relief on research and development according to the HM Treasury Consolidating Budget Guide.

13. Department and ALB risk registers shall include very high and high rated risks to significant grant scheme and awards.

14. Risk registers shall be held by those teams managing significant grant schemes and awards. These shall be used to consider if additional controls are needed to reduce the impact or likelihood of grant risks. They also support ongoing assessment on whether current risks are outside of the department's or ALB's risk tolerance / appetite and, therefore should be escalated.

15. Approaches to managing risks can be characterised as:

    - **Treated**: controls applied to reduce the likelihood and impact;
    - **Tolerated**: risk and issues are accepted;
    - **Transferred**: responsibility for the grant may be transferred to another business area better suited to manage the risk; and
    - **Terminated**: the grant scheme or award is withdrawn.

16. Where a business area decides to accept – *tolerate* - a significant risk or issue, it should document the management decision and the rationale. Fraud risk assessments (FRA) shall also be held for significant grant schemes and maintained through the life of the scheme to ensure there is continuing focus on fraud prevention. The FRA should identify specific fraud risks within schemes and examine the associated controls, including an assessment of their effectiveness. This includes a consideration of how fraud could still occur despite the controls - *residual risk*. The purpose of the FRA is to facilitate discussion and enable decision making by considering whether the levels of controls are appropriate, and whether the residual risk is tolerated.

17. A similar risk management approach can be applied to grant schemes and awards that carry potential *national security risks*, including documenting the assessment process and instigating regular reviews to assess residual risk and ensure that risk mitigation measures remain appropriate.

18. Departments and ALBs can use the following broad tiers to identify grant schemes and awards that may require additional, more in-depth risk management, including risk registers and FRAs.

    Tier 1: below £100k and low risk – a risk register would not typically be held for these grants, however a basic fraud risk assessments should be held.

    Tier 2: £100k - £5m, or high risk - (related to novel, contentious or repercussive grants) – a risk register and FRA shall be held for these grants.

    Tier 3: £5m plus – a risk register and detailed, regularly reviewed FRA shall be held for these grants.

Effective risk management in grant management

19. The following are positive attributes related to the use of grant risk registers:

- risks are focused on achievement of the objectives;
- includes consideration of the department and ALB risk appetite in relation to grants;
- the risk register is regularly discussed and is used as an important tool to support good grant management;
- risk management processes are not burdensome, for example the risk register does not require significant effort to maintain and only focuses on the top risks - typically no more than six depending on the grant scheme or award;
- awareness of the distinction between risks and issues; and
- mitigating action should be detailed to reduce the likelihood or impact of the risk within the department's risk tolerance.

Resources: the Grants Centre of Excellence website contains several examples of risk templates and risk appetite statements and also hosts an FRA template.

20. Departments and ALBs should have a process in place to escalate significant grant risks within the organisation and also to escalate from the ALB to the department, if the risk is significant. Department and ALB risk registers shall include high-rated risks to significant schemes and awards. Significant risks, including those related to fraud, shall be discussed at departmental governance boards and audit committees, as part of an embedded risk review process.

Risk management in the grant making / management process

21. Risk management shall be undertaken at every stage of the grant management process:

a. **Design and development**: to ensure risks are considered when designing grant schemes:

- conduct early options and risk analysis, including rating the risks for each option;
- determine the right structure of the design to minimise risks and optimise delivery of objectives;
- secure business case and efficiency control approvals and seek advice from the New Grants Advice Panel (NGAP), where applicable, (see '*Minimum Requirement Three: NGAP*' for more information);
- engage with appropriate teams including finance, commercial and legal, to ensure related risks are considered; and
- undertake a FRA, and where appropriate ensure that *national security risks* are also assessed - apply the appropriate legal frameworks, such as export controls.

b. **Market engagement**: to ensure risks related to market engagement are reduced:

- prepare the requirement, application documents and evaluation strategy with regard to the department's risk appetite;
- application assessment - to ensure the organisation considers the risks when selecting the grant recipient; and
- conduct due diligence - in the context of the risk indicators outlined below;

c. **Application assessment**: to ensure the organisation considers the risks when selecting the grant recipient:

- conduct due diligence - in the context of the risk indicators outlined below;
- rank the applications, including estimating the level of recipient risk and consider if additional controls are needed as a result; and,
- review risk registers submitted by grant recipients – applicable to significant grants.

Note: when developing general grant models and assessing individuals and/ or organisations for an award, consideration should be given to risk indicators, which may include the following:

- financial stability of the applicant e.g. grant to revenue ratio;
- ownership or control structure of the organisation;
- the applicant's previous experience, if any, in managing grant awards;
- whether the applicant has adequate internal, fiscal and administrative controls;
- the applicant's performance under other government grant awards;
- any adverse information regarding the applicant's officials or key employees that calls into question the applicant's ability to perform satisfactorily;
- any adverse information on the applicant's international collaboration partners, whose links to research, institutions or authoritarian states may present *national security risks* or reputational risks to the organisation and recipient;

- website and web presence (via a search engine);
- the length of grant period, including whether it has been renewed over several years;
- grant value;
- type of recipient i.e. individuals, organisations (public sector, private sector), new recipients;
- turnover of board members;
- late financial reporting; and,
- address search, use of a Post Office (PO) box.

d. **Grant award**: to ensure that appropriate assurance requirements are established to monitor risk mitigation:

- approve grant applications and notify the recipient; and
- plan proportionate risk mitigation actions, for example:
  - increasing the frequency or scope of monitoring;
  - providing targeted technical assistance;
  - requiring additional progress reporting;
  - detailing the requirement for internal audits; and
  - applying special conditions.

e. **Performance monitoring:** to ensure delivery risks are managed:

- monitor the recipient's performance and assess if risks are being managed effectively; and
- undertake action to reduce the risk, as required.

f. **Final evaluation:** to consider if there are lessons to improve risk management of similar grants:

- document recipient performance against delivery of the agreed output and/ or financial outturn; and
- document lessons learnt. (See also '*Minimum Requirement Eight: Performance and Monitoring*' for further guidance on evaluation).

Risk matrix

22. Departments and ALBs should use their own processes to rate their risks, based on a *probability versus impact* model. This will result in an overall score for each risk. A suggest risk matrix format is set out below. Risk ratings - Very High, High, Medium, or Low - shall be recorded in the appropriate field on the GGIS database to support the identification and review.

Table: Risk Matrix

			Impact (Negative)			
			Minor	**Moderate**	**Major**	**Critical**
			1	**2**	**3**	**4**
Probability	**4**	**Almost certain**	Medium (4)	High (8)	Very High (12)	Very High (16)
	3	**Likely**	Medium (3)	High (6)	High (9)	Very High (12)
	2	**Possible**	Low (2)	Medium (4)	High (6)	High (8)
	1	**Unlikely**	Low (1)	Low (2)	Medium (3)	Medium (4)

Basic illustrative examples of the impact for each risk rating are:

Critical: grant objectives will not be substantially met and there is likely to be a significant reputational impact on the department or ALB, including:

- loss of personal information by the grant recipient;
- loss of sensitive information impacting on national security;
- significant likelihood of referral to competition authorities due to State Aid questions;
- the team has no capacity to monitor and manage grant funds in line with the Functional Standard; and
- funding is diverted by the grant recipient to fund criminal or terrorist activities.

Major: grant objectives will not be substantially met:

- significant risk of fraud, impacting a large proportion of the grant funding;
- non-compliance to State Aid regulations;
- due diligence issues related to the grant recipient causing reputational damage;
- team capacity to monitor and manage funds is very limited;
- a team member has an undeclared conflict of interest that is likely to cause reputational damage and
- payments are not made promptly or accurately to the grant recipient.

Moderate: some grant objectives will not be met:

- some risk of fraud affecting a low proportion of the grant funding;
- grant funding not used within the year, resulting in clawback of the funding to the funding organisation; and
- team capacity to monitor and manage grants is limited.

Minor: Some slight impact on delivery of the full business objectives and a small risk of fraud.

Risk rating definitions

23. The following provide basic definitions of overall risk ratings. Grants loaded onto GGIS shall have a risk rating ascribed to them.

Very high or high risk: grants rated very high or high risk may include several risk factors in combination, leading to a greater level of uncertainty in delivery terms. For example, a high value grant awarded to an organisation which does not have a long track record of delivery in government grants, and/ or where a grant is focused in a policy area which is new to the department or highly innovative. Novel and contentious grants and those that are awarded as a result of a ministerial direction, should also be considered for a high-risk rating. These grants have a significant impact on the department's strategy or operational activities and significant stakeholder concern in the event of the risk materialising.

Medium risk: grants rated medium risk may be lower value than high risk grants and will usually be in policy areas familiar to the department, but perhaps where the department is seeking to break new ground or innovate. They may also include those which are awarded to organisations considered slightly higher risk in terms of credibility or financial viability due to a lack of alternative options in the market. These grants have a moderate impact on the department's strategy or operational activities and moderate stakeholder concern in the event of the risk materialising.

Low risk: grants rated low risk consist of low value, routine or repeat grants in policy areas familiar to the department, awarded to recipients with a proven track record of successful delivery in the public and/ or private sector. These grants have a low impact on the department's strategy or operational activities and low stakeholder concern in the event of the risk materialising.

Controls

24. 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.

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

26. Where grants administration is part of ALB activity departments should ensure that any Framework Document, Memorandum of Understanding, and other governance documents that govern the relationship between the department and the ALB contain appropriate reference to supporting a control framework related to grant making and that they provide assurance, via an agreed format, that the framework is operating effectively.

27. The existence and effectiveness of controls should be considered during every stage of the grant making process. They should typically entail a range of preventative, directive and detective controls for every stage of the process as described below:

Preventative controls include:

- appropriate segregation of duties when setting up and paying grant recipients;
- involvement of finance and commercial in setting up grant schemes and making awards;
- procedures to identify and prevent conflicts of interest
- effective risk management; and
- fraud risk assessments and counter fraud strategy.

Directive controls include:

- delegation letters to SROs;
- guidance and defined procedures on how grants are to be set up and managed;
- detailed grant agreements;
- setting and agreement of risk tolerance; and
- requirement for those involved to undertake training.

Detective controls include:

- regular due diligence checks;
- reviews of payments against invoices;
- internal fraud landscape reviews and internal audits; and
- compliance checks by internal control teams.

Controls to support departmental and ALB grant management

28. Departments and grant making ALBs should ensure that controls to manage and monitor grant administration are effective and efficient - core controls include:

- an effective Senior Functional Lead to manage and direct the grant making;
- ensuring that those involved in managing the grant activity have sufficient capability and capacity, whether undertaken in a central team or a more disbursed one;
- appropriate systems to store grant management information in a consistent way and to enable analysis and provide management information and reporting;
- risk management, including fraud risk assessment - and where necessary national security risk assessments - is effectively embedded within grant management processes;
- compliance with the Cabinet Office grant standards;
- compliance with elements of other standards that may apply, such as Finance, Fraud, Commercial and Analysis, and also with the finance Global Process Design Principles for grants, the Data Protection Act and/ or the General Data Protection Regulation;
- processes to ensure there is strong awareness of the need to seek ministerial direction where the Accounting Officer considers the scheme is novel, contentious or repercussive;
- payment systems conforming to the finance Global Process Design Principles support prompt and accurate payments to grant recipients; and
- procedures to identity and address conflicts of interest.

Controls placed on grant recipients

29. Departments and grant making ALBs should consider the controls that they place on grant recipients during the initial development stages. The *grant agreement* will detail those controls - they may include:
    - categories of eligible and ineligible expenditure;
    - regular reporting of progress- monthly or quarterly- to the department and ALB on progress against the objectives of the grant;
    - regular reporting of expenditure, within eligible categories, and reconciliation of spend to invoices;
    - retention of financial records evidencing all grant spend for future audit;
    - retaining the right of the department or ALB to audit the activities of the grant recipient related to the use of the grant; and
    - requiring the grant recipient to nominate an Accountable Officer to sign off the accounts and formally confirm the funding was spent only on eligible expenditure.

30. Departments and grant making ALBs should consider the impact of any controls placed on the grant recipients to ensure that collectively they do not create a disproportionate burden - an excessive control regime may actually reduce compliance with key controls.

Controls placed on local public bodies and charitable organisations

31. Departments and grant making ALBs should consider the controls needed when grants are awarded to other public bodies (such as police authorities) or to charities.

32. There should not be a presumption that fewer controls are needed because the grant recipient is a public orientated or worthy body such as a charity. Specific controls include those provided to manage other grant recipients, set out above. Additional controls may also include:
    - confirmation that funding used to fund staff is being spent on those specific posts, rather than other posts and activities;
    - assurance from local audit teams that funding is being used effectively and only for eligible expenditure;
    - fraud risk assessments, and where necessary *national security risk assessments*, should still be undertaken; and
    - there should be an assessment as to whether the funding constitutes the majority of the organisation's total funding and whether that is appropriate. In that respect exit plans may need to be agreed with the organisation, for instance to increase other funding sources and reduce reliance on government support.

33. There are specific arrangements related to controls over grant monies issued to public entities such as Local Authorities and certain Local Enterprise Partnerships. Departments should comply with guidance issued by MHCLG on grants to these entities.

Controls to prevent grant fraud

34. The key intention of controls is to reduce the likelihood and impact of fraud and other similar risks such as conflicts of interest. Controls to reduce fraud should form part of the thinking throughout the lifecycle of a grant scheme, from fraud risk assessments at the design and development stage, through to checks that should be undertaken at the final evaluation stage.

35. Grant fraud is defined as '*deliberately obtaining grant funding that a person or organisation would not be entitled to, by making a false declaration or failing to report material changes*.'

36. Common grant fraud risk scenarios include:

- falsifying information in grant applications or contract proposals;
- charging personal expenses as business expenses against the grant;
- charging for costs which have not been incurred or are not attributable to the grant;
- charging for inflated labour costs or hours, or categories of labour which have not been incurred, for example fictitious employees, contractors or consultants;
- grant application from a fictitious or '*shell'* company;[1]
- billing more than one grant or contract for the same work;
- falsifying test results or other data;
- substituting approved materials with unauthorised products; and
- misrepresenting a project's status to continue receiving government funds.

37. Basic controls to reduce the risk of fraud include:

- taking a proportionate approach to managing the risk of fraud within grants as part of the organisation's *Counter Fraud, Bribery and Corruption Strategy*;
- training, education, and awareness of all staff on fraud risks and the appropriate action to take if fraud is suspected;
- actively designing fraud out of the grant process at the initial development stages;
- considering the fraud risk assessment at intervals throughout the life of the scheme, for tier 2 and 3 grants;
- undertaking proportionate due diligence at the initial award stage and also at intervals during the delivery period;
- the use of data analytics to proactively look for potential fraud;
- ensuring organisations have appropriate whistleblowing arrangements to support the reporting of fraud or other related issues; and
- site visits for high-value and high-risk grants.

[1] A *shell* company is defined as an inactive company used as a vehicle for various financial manoeuvres, or kept dormant for future use in some other capacity.

Controls to support due diligence

38. Due diligence refers to a process, or set of processes, to appraise:

- performance;
- eligibility;
- basic financial checks;
- past track record; and
- background of the potential grant recipient.

39. These are part of initial checks performed during the assessment of applications, but may be refreshed during the lifecycle of the grant if proportionate. Robust due diligence processes help to mitigate reputational risks, potential fraud, potential national security risks, errors and the loss of grant funding.

40. Due diligence is important to:

- confirm that a grant recipient understands and can manage the risks associated with grants and that they are working with organisations, entities, or institutions that are likely to assist them with successfully achieving their objectives;
- identify potential early warning signs and avoid bad decisions; and
- support information gathering, which is useful for ensuring all checks are completed prior to the application proceeding to the next stage of the grant making process.

41. Departments 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 departments - departments 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;
- for complex and contentious grants or those above £100,000, consider using staff with specialist skills, for example accountants, fraud investigators, lawyers, etc.; and
- there is no prescription on the seniority of those conducting due diligence checks, but those involved should have the powers and authority to carry out due diligence in full and the SOR be able to confidently sign-off on the findings from due diligence checks.

42. Departments and their grant making ALBs should develop due diligence models based on best practice and guidance that are proportionate to the value of the grant, as demonstrated in the table below - mandatory due diligence checks to reflect spend and risk:

Below £100k and Low Risk	£100k - £5milion and/ or High Risk	Above £5million
Checks to be conducted by the grant or policy team with support from finance.	Due diligence conducted by internal finance professionals.	Due diligence to be compliant with HMT guidelines and to be conducted by finance professionals with support from external experts if required.
Specific requirements: • Check if the individual or organisation has received another source of government funding (GGIS). • Evaluate feedback, if it is a previous grant recipient (GGIS). • Individual legal entity checks (Charities Commission). • Financial viability checks. • Basic fraud risk assessment.	Further requirements: • ***Financial***: cash flow and reserves- consider the impact of the recipient taking on outcome-based grant. • ***Commercial***: consider the impact on competitors or the market (State Aid). • ***Operational***: investigate if the grant recipient has the people, processes and products required for delivery – a site visit advisable • ***Governance***: is the governance structure robust.	Further requirements: • A mandatory site visit and detailed analysis of financial accounts. • It is recommended that a non-executive member sits on the programme board. • Quarterly reviews of performance.

43. The following due diligence checks should be considered:

- the short and medium-term financial viability of the applicant organisation, including the extent of reliance on grant and other government funding;
- capability, track record and credibility;
- use of the Government Grants Information System (GGIS) and other sources of data such as 360Giving and the EU's Financial Transparency System to assess performance track record and the risk of overlapping funding;
- verification of identity and/ or legal status via legal teams including checks against Companies House and the Charities Commission as well as checks of legal documentation such as certificates of incorporation or articles of association, where applicable;
- bank account verification prior to any payments being made – including location, where a UK based account is specified;
- checks to establish the *beneficial ownership* in relation to the potential recipient organisation to ensure that departments and grant making ALBs know who has significant control over an organisation;
- whether the disclosed directors or trustees have links to other grant recipients and whether there is any risk associated with those shared directorships;

- the track record of the directors associated with the applicant organisation and whether historical poor performance is indicative of a higher risk of misuse of the funding;
- research to investigate specific areas of risks, for example conflicts of interest, anti-money laundering (AML), countering terrorist financing (CTF), bribery and other criminal activities associated with the activity being funded - in particular when working with vulnerable adults or children; and
- an assessment of any *national security, export control or organisational security* risks.

44. For grants in the fields of research, innovation, technology and infrastructure, the following checks should be considered - whether:

    - the applicant intends to collaborate, or has a history of collaboration, with foreign organisations of potential *national security* concern, for example, those that are subject to export restrictions or thought to conduct research on behalf of the military or intelligence agencies of hostile foreign states;
    - the applicant has proportionate measures in place to protect sensitive information or technology arising from the grant award, for example, physical, personnel, and cyber security policies;
    - the organisation is itself or has directors or owner that are subject to the UK or international sanctions regimes;
    - the Export Control Joint Unit should be consulted; and
    - the institution is compliant with the Academic Technology Approval Scheme.

    Each of these has its own conditions and complying with one will not satisfy the conditions of the others. Failure to comply with legislation may expose the grant recipient to criminal investigation.

45. The three potential outcomes from the due diligence process are:

    Fully approved: a recommendation to proceed with the award.

    Partially approved: depending on the concerns raised a variety of options are available such as a reduction in grant value to lessen the department's exposure, further enhanced due diligence steps and considering funding in tranches with enhanced monitoring.

    Not approved: a recommendation not to proceed with the award.

Assurance

Governance processes

46. Departments and grant making ALBs should obtain appropriate assurance over the effectiveness of risk management and controls, as part of 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, size and type of grants and the impact on business objectives. Ultimately this will inform the end of year reporting process.

Assurance framework related to grants

47. Departments and grant making ALBs with significant grants expenditure should map out the *three lines of defence* (see below) to support effective risk and control management in relation to grants. Further detail on ensuring the department or ALB has an effective and efficient assurance framework is detailed in the HM Treasury assurance frameworks guidance. Mapping out the *three lines of defence* supports the identification of weaknesses and gaps in assurance, such as whether second line assurance activity is sufficient. The Government Internal Audit Agency (GIAA) can provide further advice on how best to undertake this exercise.

48. Departments and grant making ALBs should ensure that assurances are obtained as part of ongoing governance processes from those operating in the *three lines of defence.*

Reporting of assurances related to grants

49. Departments and grant making ALBs shall have a process to ensure that important assurance reports are shared with their senior governance boards and audit committee for review and comment - this includes:

- Cabinet Office led grant maturity assessments, which provide an important source of assurance by issuing an assessment of grant making in the department. The scores shall be discussed by the department's boards and audit committee, along with any action plans to improve the scores;
- Internal audit reports and assurances on grant management; and
- Infrastructure and Project Authority (IPA) work.

50. 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.

51. End of year governance statements shall include an assessment of the effectiveness of the control framework related to grant management, where it is material to the department and ALB's business objectives.

52. Principal Accounting Officers remain accountable for grant funding issued to ALBs. As a result, with respect to grant funding Accounting Officers should:

- seek assurance that ALBs are complying with the Functional Standard and associated minimum requirements for general grants and have an appropriate assurance framework;
- ensure that ALB framework and governance documents include a reference to the requirement to comply with the Functional Standard - review of the efficacy of governance documents should be undertaken at an appropriate point;
- ensure there is a process to escalate risks from the ALB to the department; and,
- accurately outline responsibilities related to grant management within their AOSS.

Use of research funding which may pose a risk to national security or breach export controls

Protecting research

53. 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. All materials can be found here: https://www.cpni.gov.uk/trusted-research-guidance

54. The expectation is that grant making departments and ALBs shall ensure grant recipients provide a commitment that Intellectual Property (IP) generated from taxpayer funded research will be of benefit to UK prosperity.

Understanding the risk

55. 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.

56. Dual use technology, which may be subject to export control, could be adapted by a foreign state's military against UK interests. Good due diligence should include a consideration of potential *national security* concerns surrounding the award of a grant. 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.

Further Resources

57. In adhering to this minimum requirement and additional guidance, and in addition to the references and resources highlighted earlier in this document, organisations may want to consider the following in particular:
    - The HM Treasury Orange Book: Management of Risk – Principles and Concepts.
    - Each government organisation's internal guidance on risk management, controls and assurance, particularly where it details arrangements related to grant risk appetite and management of related risks and controls.
    - The Centre for the Protection of National Infrastructure (CPNI) and National Cyber Security Centre (NCSC) Trusted Research guidance, which can be found here: https://www.cpni.gov.uk/trusted-research.

58. Organisations should also make full use of wider resources available through the Grants Centre of Excellence and the Government Grants Academy.