CCMS
Council for Catholic Maintained Schools

Council for Catholic Maintained Schools (CCMS)

Risk Management Framework

01.09.2021

Contents

Introduction

1. The Council for Catholic Maintained Schools (CCMS) is a Non-Departmental Public Body (NDPB). Its parent Department is the Department of Education for Northern Ireland.

2. As a public sector body CCMS operates within the framework of Managing Public Money Northern Ireland (MPMNI). MPMNI makes clear that: "*Embedded in each public sector organisation's internal systems there should be arrangements for recognising, managing and tracking its opportunities and risks"* (MPMNI 4.3)

What is Risk Management?

3. Risk Management is the process by which organisations seek to identify and control risks and to reduce their effects on the achievement of their objectives.

4. Risk can be defined as an uncertain event which should it occur would impact on the achievement of organisational objectives. In managing risk CCMS seeks to minimise (but not necessarily eliminate threats) and to maximise opportunities. Successful risk management involves:

    i. Identifying and assessing threats and opportunities;
    ii. Taking cost-effective action to anticipate or manage them; and
    iii. Monitoring risks on an ongoing basis and reviewing them to establish if they are still relevant and if further action is relevant.

5. This framework forms part of the overall governance approach followed by CCMS. It seeks to:

    i. Ensure that the process of risk management is managed in a consistent way across CCMS;
    ii. Ensure that risk identification, assessment and management operate in an effective way to support the achievement of agreed objectives;
    iii. Ensure that risks are regularly reviewed, assessed and prioritised;
    iv. Reduce the risk of fraud, financial loss, poor performance, poor information management, complaints, service disruption and adverse events;
    v. Enable the Chief Executive as Accounting Officer to demonstrate a robust system of risk management within CCMS; and
    vi. Promote an internal culture where staff are "risk aware" rather than "risk averse" by placing risk management in the context of a wider management framework

Purpose of the Risk Management Framework

6. This framework explains the CCMS approach to risk management and the main reporting procedures. It also documents, at Appendix A, the roles and responsibilities of the Accounting Officer, the CCMS Council, the CCMS Audit

and Risk Assurance Committee, the CCMS Senior Leadership Team (SLT), CCMS staff, and Internal and External Audit.

7. The use of this Framework should be an intrinsic part of the CCMS business planning and decision-making process. No change of direction or objectives should occur without first considering the potential risks involved.

Principles

8. The following key principles underline the CCMS approach to risk management:

    i. The CCMS approach is aligned as closely as possible to that of the Department of Education;
    ii. The CCMS Accounting Officer assumes responsibility for risk management across the organisation;
    iii. There is an open and receptive approach by the Council to discussing and addressing risk across the organisation;
    iv. The management of key organisational risks is a priority for the CCMS SLT;
    v. The CCMS risk management process is integrated with day-to-day management and informs the annual business planning cycle. In this way risk management links with overall management control to support the achievement of CCMS objectives.

The Internal Control Process

9. The Council has overall responsibility for ensuring that appropriate arrangements are in place to ensure effective risk management across CCMS. The Chief Executive and the SLT are responsible for managing risk with the active support and involvement of staff across the organisation. Roles and responsibilities are described in detail at Appendix A.

10. The key elements of the internal control process in CCMS are outlined below.

The Risk Management Framework

11. The Risk Management Framework is developed by the SLT. It sets out a framework for the identification, assessment and ongoing monitoring of risks that are considered to be significant to CCMS. The Audit and Risk Assurance Committee provides an independent and objective view to the Council of the risk management approach deployed by the organisation.

12. New risks will be added to the CCMS Risk Register with the approval of the Council and progress in relation to each risk captured in the Register will be monitored on a regular basis.

13. CCMS will use a variety of mechanisms to give the Accounting Officer adequate assurance that risk is being effectively managed. These include:

i. The maintenance of embedded risk management arrangements;
ii. Regular reporting on the status of risk and control;
iii. Regular use of assurance statements i.e. declarations on risk and control from management; and
iv. Use of internal audit to perform a combination of risk assurance, internal audit reviews and consultancy-based work.

Governance Statement

14. The Governance Statement (GS) is a public accountability document that describes the effectiveness of internal controls in an organisation. The CCMS GS is an integral part of the organisation's annual reporting process. It is signed by the Accounting Officer, presented with the Annual Report and Accounts and reviewed by the Northern Ireland Audit Office (NIAO) for consistency with other information in the financial statements. The GS focuses on providing assurance about performance and risk management.

15. CCMS is required to submit its Accounting Officer GS to the Department of Education as part of the wider accountability reporting process across the Education Sector.

Internal Audit Review

16. To provide independent assurance CMMS Internal Audit will perform a regular review of risk management, providing an opinion on the process and making recommendations for improvement if needed.

The Risk Management Process

17. Risk Management involves a series of well-defined steps that support better management decision-making. This provides greater clarity on risk management in an organisational context. The main steps are:

Step 1 - Clarifying Objectives

18. This means formulating clear aims, objectives and plans for delivery of outputs, services and longer-term outcomes. If objectives are unclear then the risk of under-performance or failing to meet objectives will also be unclear. CCMS objectives are set out in the organisation's Corporate Plan and its Annual Business Plan.

Step 2 – Identifying Risks

19. This is about recognising and identifying the key risks which are most likely to impede or enhance performance, the delivery of services and the achievement of objectives. Various categories of risk facing CCMS are included at Appendix C. Specific consideration of information and fraud risks is also required (see paragraphs 48-52 and 53-56). In seeking to identify risks management should consult widely throughout the organisation and seek the views of stakeholders.

20. The identification of a potential new risk should be considered each time a new objective or new key business activity is being considered. Risk assessment and management should be a routine element of CCMS management decision-making. Risks considered should include not only those which threaten the achievement of objectives but also the risks associated with failing to identify and exploit opportunities to do things differently or better (i.e. missed opportunities).

21. Identifying risk involves thinking about what could happen, why it could happen and how it could happen. It is important that risks are clearly articulated. If they are not, it is difficult to put in place effective mitigating actions and contingency plans. Description of risks should not simply describe the objective – e.g. living within budget. They should outline the specific nature of the risk including the cause and the effect. For example: *"Ineffective planning, monitoring of expenditure or resource constraints"* (cause) *"result in a balanced resource budget not being achieved by CCMS"* (effect). Identification of the specific cause makes it easier to match appropriate counter-measures to the potential threat..

22. It is also important to think about the impact. A risk register should therefore outline the potential consequences of a risk. Wherever possible management should seek to quantify potential impact – especially where resources are at risk.

Step 3 – Assessing Risks

23. In deciding how to handle a risk it is important to assess its significance. One of the aims in assessing a risk is to provide a consistent management framework to inform decisions on risk areas that need attention and the relative priority of each risk identified.

24. Risk assessment also takes into consideration the tolerability by management of individual risks. This is risk appetite. Risk appetite sits within a framework of set boundaries that guide the limit of risk which CCMS is prepared to carry for each category. Appendix C matches each risk category with a level or risk appetite.

25. Identified risks should also be analysed and evaluated to provide an overall assessment of their potential impact, and the timescale over which they need to be managed. The assessment of risk is based on rating each risk on two factors – its potential impact to the objective/outcome and the likelihood of its occurrence. Both factors use a rating of 1(lowest) to 5 (highest). A model and some examples to help the scoring of each of these factors is provided at Appendix D (for impact) and Appendix E (for likelihood)

26. When assessing risks, particular attention should be given to the potential impact on stakeholders and others groups including:

    i. Catholic Maintained Schools

ii. Pupils
iii. The Department
iv. The taxpayer.

27. The potential impact and likelihood scores should then be multiplied together to develop an overall risk score:

    Potential Impact x Likelihood of Adverse Outcome = Risk Score.

    Appendix F provides a Risk Assessment Matrix, which places the risk score within certain ranges. These ranges determine the level of action required to manage the risk.

28. While the scores are not intended to provide precise measurements of risk, they do provide a useful basis for identifying vulnerabilities and prioritising risks to ensure that highly rated risks get the necessary management attention. Scoring also provides a means of comparing different risks across CCMS.

29. Where the risk exists in its raw state (i.e. if there are not controls in place to manage the risk) this is described as the inherent risk. However, in most cases where there is ongoing management activity, there are already controls in place to reduce the level of risk. The residual risk is the level of risk outstanding after the controls are in place. By assessing both management can determine how effective the current controls are in managing the risk and whether further controls to manage the risk are needed.

Step 4 – Assigning Ownership

30. Each risk needs to be allocated an owner who will be responsible for, and who will lead on, the management of that risk. This is not the same as being responsible for carrying out any actions which may be needed to control the risk. However, without a named individual taking overall responsibility, it is unlikely that risk management actions will be followed through. Risk ownership should be delegated as far as possible, but the risk owner should be someone who has the authority to take action to address the risk.

31. Management of risk and an individual's responsibility for it should be considered in setting personal objectives, agreeing individual areas of work and reviewing personal performance.

Step 5 – Addressing Risk

32. Decisions on how to control and manage risk generally draw from the five standard responses outlined below. In choosing between them, relevant factors include cost, feasibility, probability and the potential impact.

Table: Addressing Risk

Action	Description
Terminate	A decision is made not to take the risk or cease the activity. Where the risk outweighs the possible benefits, terminate the risk by doing things differently and thus removing the risk, where it is feasible to do so. This is not always possible in the provision of public services or mandated or regulatory measures but the option of closing down an activity where the benefits are in doubt must be a real one
Tolerate	Accepting the risk. This may be where the risk is external and the ability to do anything about it is limited, or where the probability or impact is so low that the cost of managing it would be greater than the risk. This option may, however, be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.
Transfer	Where another party can take on some or all of the risk more economically or more effectively e.g. through another organisation directly undertaking the activity or through obtaining insurance. Some risks are not fully transferable – in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure the successful transfer of risk
Treat	Mitigating the risk. In practice, this is the most common response to risk. It is achieved by eliminating the risk or reducing it to an acceptable level by prevention or another control action. The option of “treat” in addressing risk can be further analysed into four different types of controls: Preventative Controls These controls are designed to limit the possibility of an undesirable outcome being realised. The majority of controls implemented in organisations tend to belong in this category. Directive Controls These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, for example, in a health and safety situation. Examples of this type of control would be to include a requirement that protective clothing must be worn during the performance of dangerous duties. Corrective Controls/Reversibility These controls are designed to correct undesirable outcomes which have been realised. Applied after the event, these may

	consist of contractual remedies to recover overpayments or obtain damage payments or may be a detailed contingency plan that will be triggered by the event (e.g. disaster recovery or business continuity plans) Detective Controls These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, "after the event" so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks, reconciliation (which can detect unauthorised transactions), Post Implementation Reviews which detect lessons learned from projects for application in future work, and monitoring activities which detect changes that should be responded to
Take the Opportunity	This option is not an alternative to those above; rather it is an option which should be considered whenever tolerating, transferring or treating a risk. It is for circumstances where the potential gain seems likely to outweigh the potential downside. There are two aspects to consider. The first is whether or not at the same time as mitigating threats an opportunity arises to exploit positive impact. For example, if a large sum of funding is to be put at risk on a project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be redeployed.

33. Selecting the most appropriate risk treatment option involves balancing the potential benefits associated with the achievement of objectives against the cost, effort or disadvantage of proposed actions.

34. When agreeing responses or actions to control risk, consideration should also be given as to whether the actions themselves introduce new risks or affect people in other ways which they need to be informed about.

Contingency Plans

35. Any risk could suddenly be realised, even those that have been assessed as having a relatively low likelihood. It is therefore important to consider in advance what action to take if a risk develops or a crisis occurs to help mitigate the risk. This is referred to as contingency planning and it is essential in creating an environment of "no surprises".
36. Contingency plans need to be developed for all risks which have been assessed as having a potentially high impact (impact score of 4 or 5) irrespective of the potential likelihood, or where risks are external and largely outside of the control of CCMS. Contingency plans also need to be tested.

The impact rating at the residual stage should usually only be reduced if a contingency plan has been developed which, in the event of the risk materialising, would lessen the risk's impact.

37. Business continuity plans must be prepared to help keep CCMS running during times of change or disruption. These plans outline how CCMS will cope with major disruption to activities and services and how it will deal with any health and wellbeing and communication problems that such events may cause.

Risk Escalation

38. In managing risk organisational context is an important factor. Some large organisations will have a layered risk management approach with risks managed at different levels in the organisational hierarchy. In this setting lower-level risks may change and be escalated to a higher level to be managed and vice versa.

39. CCMS is a relatively small, centralised organisation with 60 staff on the books. In these circumstances the organisation has determined that a single centralised risk register is the most appropriate and cost-effective way of managing risk.

40. At individual directorate level within CCMS the aims, objectives and risks associated with directorate activity will be considered and reviewed on a regular basis as part of normal business planning. Where a new risk is identified it will be considered and escalated for inclusion in CCMS risk register if appropriate.

41. The CCMS Register will be closely aligned with the Department's Corporate Risk Register insofar as is possible given the differing focus of the two organisations.

Step 6 – Reporting Risks

42. The CCMS risk management approach is recorded and documented in the organisation's risk register.

43. Each risk contains the following standard information which reflects the template at Appendix G

    i. Business objective linked to the risk;
    ii. Risk description;
    iii. Risk owner
    iv. Potential consequences if the risk was to materialise;
    v. Current management actions to manage the risk;
    vi. If required, an action plan for improvement, which is designed to reduce the residual risk score, with responsibilities and target dates assigned;

vii. If required, contingency action to counter the impact of risk in the event of it materialising; and
viii. An assessment of the inherent and residual impact and likelihood of the risk.

44. The CCMS Risk Register will be developed and maintained by SLT. The Register will be reviewed every quarter by the SLT or more frequently if circumstances require. The outcome of the review process shall be presented to the Audit and Risk Assurance Committee (ARAC). The Chair of the ARAC shall report to the Council with an independent view following each in-year review. Any changes to the CCMS Register will be subject to Council approval.

45. A formal review of the CCMS Risk Register will be undertaken by the SLT at the beginning of each financial year. The review outcome and a revised Risk Register shall be presented formally to the ARAC. The Chair of the ARAC shall report to the Council with an independent view following each annual review. Any changes to the CCMS Register will be subject to Council approval.

46. The reviews of the Risk Register outlined above provide an opportunity for the SLT to actively examine the CCMS approach to risk management. At each review the SLT should:

i. Discuss progress on actions identified to improve control of risks;

ii. Assess whether risks are being appropriately controlled and remain within the risk tolerance level or if further action needs to be taken;

iii. Consider whether management or contingency plans continue to be the most effective and best value for money response;

iv. Consider whether new risks have arisen which would impact on the fulfilment of business objectives and how these should be addressed; and

v. Document any agreed changes.

47. The approach outlined above will ensure that reports on the management of risk will be aligned with those on business planning, emphasising the linkages between the two and embedding risk management as an integral part of the strategic business planning cycle.

Information Risk

48. Information risk is sometimes not given the same prominence as other risks and as a consequence may not be managed as effectively. Information is a key CCMS asset and it is important that there is a strong culture throughout the organisation of information being carefully and securely managed and valued. Such a culture will help secure CCMS compliance with relevant legislation including the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

49. All information used for operational and reporting purposes needs to be captured and processed accurately. Personal data and other sensitive information require additional safeguards.

50. Information risk is explicitly covered in the CCMS Governance Statement completed by the Accounting Officer which forms part of the organisation's Annual Report and Accounts.

51. Major information risks can arise from:

    i. Inadequate information management policies and procedures;
    ii. Absence of senior level focus on risk management;
    iii. Poor understanding and control of information assets;
    iv. Inadequate staff training and awareness;
    v. Poor record management practices;
    vi. Ineffective reporting and management of data incidents;
    vii. Failure to consider information risk when developing new policies, processes and procedures – data protection impact assessments are a statutory requirement for projects involving the use of personal data;
    viii. Loss, destruction or unavailability of key information;

52. Given the importance of information risk management an information risk should always appear on the CCMS Risk Register.

Fraud Risk

53. All organisations face a range of fraud risks specific to their business from both internal and external sources. The consistent application of management controls is the most effective way of mitigating against fraud. It is therefore important that the organisational controls in place address potential fraud risks.

54. Typically, the risk of fraud is greatest where:

    i. Significant volumes or amounts of payments are processed;
    ii. Teams are in receipt of payments;
    iii. Information is held or produced, the receipt of which would be attractive to a third party
    iv. Significant amounts of goods are purchased for Team consumption;
    v. Cash is held within a Team.

55. Where a specific vulnerability to fraud exists, this should be identified and clearly documented. All fraud risks where the analysis has identified the risk as high (red) must be recorded in the CCMS Risk Register.

56. Consideration should also be given to the inclusion of fraud risks identified as medium (amber) in the CCMS Risk Register.

Further Information

57. Appendix H provides details of further reading on Risk Management.

CCMS Risk Management Framework – List of Appendices

Appendix A	**Risk Management – Roles and Responsibilities**
Appendix B	**Template for Team Discussion of Risk**
Appendix C	**Risk Categories and Risk Appetite**
Appendix D	**Risk Impact – Scoring Guide**
Appendix E	**Risk Likelihood – Scoring Guide**
Appendix F	**Risk Assessment Matrix**
Appendix G	**CCMS Risk Register Template**
Appendix H	**Further Reading**

Appendix A

RISK MANAGEMENT ROLES AND RESPONSIBILITIES	

Individual/Group	Responsibilities
Accounting Officer/Chief Executive	• Has ultimate responsibility for the CCMS system of internal control and ensures that an effective risk management process is in place and is regularly reviewed. • Provides clear direction to staff. • Establishes, promotes and embeds an organisational risk culture.
The Council	The Council will collectively agree the risks to be included in the CCMS Risk Register. The Council is responsible for agreeing the CCMS 'appetite for risk', setting the tone and influencing the culture of risk management within the organisation. This includes: • examining residual risks to determine whether they are acceptable. For those that are not, ensuring that appropriate mitigation measures are put in place; • discussing and approving issues that significantly affect CCMS risk profile or exposure; • continually monitoring the management of significant risks and ensuring that actions to remedy control weaknesses are implemented; • ensuring that effective arrangements are in place to provide assurance on risk management, governance and internal control. In this respect, the Council will be independently advised by ARAC and Internal Audit. In fulfilling this role, the Council will take account of the following aspects: <u>Control Environment:</u> • CCMS objectives and performance targets; • Commitment to competence and integrity; • Culture, approach, and resources required to manage risk; • Delegation of authority; and • Public reporting. <u>Ongoing Identification and Evaluation of Significant Risks:</u> • Timely identification and assessment of significant risks; and • Prioritisation of risks and putting in place measures to address areas of high exposure.

Individual/Group	Responsibilities
	Information and Communication: • Quality and timeliness of information on significant risks; and • Prompt recognition of control breakdowns and prompt identification of new risks. Monitoring and Corrective Action: • The ability of CCMS to learn from its experiences in managing risk; and • The commitment and speed at which corrective actions are implemented.
Audit and Risk Assurance Committee	In relation to Risk Management, the Committee will provide a forum to discuss Risk matters and advise the Council on: • The strategic processes for risk, control and governance and the Governance Statement; • The CCMS Risk Management approach as captured in the CCMS Risk Register; • The accounting policies, the accounts, and the annual report of the organisation, including the process for review of the accounts prior to submission for audit, levels of error identified, and management's letter of representation to the external auditors; • The planned activity and results of both internal and external audit; • Adequacy of management response to issues identified by audit activity, including external audit's management letter; • Assurances relating to the corporate governance requirements for the organisation; and • Fraud Prevention and Raising Concerns (whistle-blowing) processes, and arrangements for special investigations.
Senior Leadership Team	The SLT is responsible for: • Supporting the Chief Executive/Accounting Officer with the development and maintenance of a culture of risk management within CCMS; • Ensuring that the CCMS Corporate Risk Register is developed and maintained;

Individual/Group	Responsibilities
	• The strategic oversight of the process of ongoing identification of risks and their management and control across the organisation; • Establishing and maintaining a sound system of internal control within CCMS and individual directorates/localities; • active engagement of Directors and Locality Leads with their teams ensuring that risk identification and management has an appropriate focus through structured discussion of existing operational organisational risks and potential new risks at Directorate/Locality team meetings using the template at Appendix B; • Involving relevant staff at all levels in business planning and risk management activities; • Working openly and effectively with the Council and ARAC on risk management; • Monitoring and reviewing risks on a regular basis (at least quarterly)
Chief Finance Officer	The Chief Finance Officer has operational oversight of the process of Risk Management within CCMS. He ensures that formal risk management papers are presented to the SLT, Audit and Risk Management Committee and Council as required and that management decisions on Risk Management are clearly recorded. The Chief Finance Officer has an editor-in chief role in relation to Risk Management in CCMS and works with Directors, Lead Risk Owners and Directorate and Locality Risk Co-ordinators to ensure consistency in terms of risk identification, assessment and

Individual/Group	Responsibilities
	scoring and management. The Chief Finance Officer ensures that as far as possible the CCMS Risk Management approach is aligned with the Department's.
Lead Risk Owner (LRO)	The LRO is responsible for: • Management and control of all aspects of the risk allocated to them including the identification of effective risk countermeasures and business continuity and/or contingency plans. • Liaising with other parts of the business where appropriate; • Monitoring and reviewing risks for which they are the LRO on a regular basis (at least quarterly)
Directorate/Locality Risk Co-Ordinator	The Directorate/Locality Risk Co-ordinator is responsible for ensuring that the outputs from Team discussions on risk (as described at Appendix B) are considered with the relevant Director and the Chief Finance Officer and issues escalated where required. This role is an important part of the CCMS bottom-up approach to Risk Management. They will ensure a nominated team member updates the Operational Risk Register following team risk discussions.
All Staff	Staff responsibilities include: • Reporting new or emerging risks to management and highlighting areas where risks are not being effectively managed. • Actively contributing to the continuous improvement of risk management within CCMS
Internal Audit	Internal Audit will carry out independent reviews of the effectiveness of risk management and control and report these results to the Accounting Officer and ARAC. Internal Audit will use the information in the Risk Register to help develop its audit strategy and periodic plans. The Internal Audit programme may cover: • reviews of the extent to which CCMS has maintained and embedded the risk management process and implemented actions identified by the process; and • specific internal audits of key business processes. Internal Audit also has a role to play with regard to: • providing advice on the management of risk, especially those issues surrounding the design, implementation and operation of systems of internal control; and • promoting risk and control concepts within CCMS.

Individual/Group	Responsibilities
External Audit	External Audit will be kept informed of the status of the risk management process. Any findings in the area of risk management identified during the annual external audit process will be factored into the annual review of the CCMS internal control process carried out by the Council Departmental and the ARAC.

Appendix B

CCMS Risk Management: Template for Team Discussion of Risk

The CCMS Corporate Risk Register [CRR] is underpinned by an Operational Risk Register [ORR] which outlines risks at Directorate or Locality level as appropriate to the work of the organisation. The ORR enables Directorate or Locality teams to monitor risks in the relevant area of work and escalate risks to the CRR when needed.

The ORR will be reviewed regularly at Directorate or Locality teams as appropriate. A nominated team member will update the ORR spreadsheet on behalf of the respective team.

1. Consider the current version of the CCMS Operational Risk Register.

2. Identify/update risks which apply to your Directorate/Locality.

3. Review the CCMS Risk Management Framework paying particular attention to steps 1-5 in the Risk Management Process as set out at paragraphs 17-34.

4. For risks relevant to your Directorate/Locality consider the risk description, risk scores, current actions to manage the risk and actions for improvement. Are these still appropriate? Do they need updated? If so, discuss and agree the required updates. Where updates are required ensure that a clear rationale exists for the changes being proposed.

5. Consider whether there are any potential new risks presenting in your Directorate/Locality. If there are update the spreadsheet and

    - Describe the risk;
    - Assess the likely impact and likelihood;
    - Consider the necessary actions to manage the new risk.

6. The outputs of your team discussion will be updated by your Directorate/Locality Risk Co-ordinator for further consideration. Any matters requiring escalation will be discussed further with the relevant Director and/or the Chief Finance Officer and if appropriate a recommendation will be made to the SLT to escalate to the CCMS CRR.

Appendix C

Risk Categories and Risk Appetite

The risk categories listed below provide a framework for identifying and categorising a broad range of risks. This is because the RMF is the organisation's agreed policy on risk management, so there should not be any scope to deviate from the categories contained in it.

Where a risk falls under more than one category, consider selecting the one which requires the greater level of control. For example, an Infrastructure risk could be categorised as amber (modest/cautious), but if it includes reference to the safety of buildings, a categorisation of Health and Wellbeing' (green: averse) might be more appropriate.

Risk Category	Description	Risk Appetite	Acceptable Range (Up to and including)
Health and well-being	Physical injury; stress; emotional / psychological harm; major incidents; child protection concerns; death.	**'Averse',** meaning the avoidance of risk and uncertainty in relation to the physical and psychological well-being of children, young people, staff and members of the public is of fundamental importance.	**Green**
Financial / VFM / Governance	Availability and allocation of resources; inappropriate investment decisions; monetary loss; theft; fraud; impropriety; over/under-spending; poor value for money; waste; poor use of assets; lack of financial	**Modest / Cautious** ***'Modest'***, meaning CCMS is only	**Amber**

	expertise; inaccuracy; lack of integrity; unreliability of financial information; inadequate control systems.	prepared to accept the possibility of very limited financial loss if essential. Value for money is the primary concern. This reflects the fact that: public money can only be used for the purposes intended and authorised; and there are higher public expectations on public sector organisations to safeguard and make good use of public funds than there would be on a private organisation. ***'Cautious'***, meaning CCMS has limited tolerance for risks in this area and would wish to be	
Compliance	Failure to meet standards, laws and regulations; damages or compensation claims; judicial review; drafting of legislation allows or gives rise to unintended outcomes; inadequate response to new legislation		
Security	Physical assets compromised; IT obsolescence; ineffective storage arrangements; inappropriate use of information by CCMS or others; inappropriate disclosure; hacking; corruption of data		
Major stakeholder relationships and reliance on 3rd parties	Provider failure; quality; wrong balance between autonomy and control; lack of knowledge-sharing about performance and risks; emphasis on targets distorts outcomes.		
Information	Failure to properly use, protect and manage information; the integrity, availability and confidentiality of information assets; staff unaware of or not applying correct procedures or processes; third party organisations / suppliers / key partners unclear and/or not held to account for shared information; no culture of valuing information as an asset within the organisation.		
Human Resources	Knowledge expertise; effectiveness; availability; retention; staff turnaround; capacity issues; over-reliance on key officers; employee motivation; failure to comply with employment law; succession planning; training; risk of error; industrial action.		
Infrastructure	Premises, facilities, equipment; transport for staff; power supply; business relationships with partners; dependency on internet and e-mail.		

Major Systems / Projects (change)	Resource constraints (funding / time / personnel); overall delays; delays to stages on the critical path; changes to output requirements; being overtaken by events; difficulties in obtaining necessary information; facilities or equipment; personnel changes; lack of suitably qualified or experienced staff means incurring costs of consultants; quality control; differing priorities of different stakeholders.	reasonably sure that breaches would be unlikely to occur or that it would not incur significant censure or would win any challenge.	
Operational	Failure to meet objectives; failure to deliver services to users within agreed/set terms; insufficient capacity to deliver; customer dissatisfaction.	**Open / Hungry** ***'Open'***, meaning that CCMS is prepared to support innovation which demonstrates commensurate management controls. ***'Open'***, meaning that CCMS is prepared to take decisions with the potential to expose it to additional scrutiny – but only where appropriate steps have been taken to minimise exposure.	**Orange**
Opportunity	**Missing opportunities to improve on delivery of the organisation's objectives; resources which might have been allocated elsewhere.**		
Policy Development	Conflicts / inconsistencies with Departmental or other public sector bodies; being overtaken by events; lack of appropriate consultation; failure to address issues relating to equality, diversity / human rights / rural needs.		
Policy Implementation / delivery	Delays in implementation; inadequate resource to deliver effectively (funding / time / personnel); loss of experienced staff before completion; ineffective or unintended outcomes; failure to evaluate and learn lessons.		
Political	Cross-cutting and/or controversial measures.		
Reputation, Ethics and Responsibility	Minister's / Department's reputation and credibility suffer through adverse media attention; policies misunderstood or misinterpreted; negative implications identified by others which have not previously been considered; failure to keep partners on side; breach of confidentiality; excessive caution can be as damaging as unnecessary risk taking.		

		'Hungry', meaning that CCMS is eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).	

RISK IMPACT - SCORING GUIDE

This material can be illustrative only. Ultimately, the assessment of impact is a matter of management judgement. In all cases, management must be able to substantiate the reasons for the level of impact assigned.

Category	Impact				
	Minor (1)	**Moderate (2)**	**Significant (3)**	**Major (4)**	**Critical (5)**
Operational Delivery	No interruption to service.	Some disruption manageable by altered operational routine.	Disruption to a number of operational areas within a location	All operational areas of a location compromised.	Total system dysfunction. Total shutdown of operations.
Financial	Financial loss, loss of funding or inescapable unfunded pressures under £34K +/- 1% variance to budget.	Financial loss, loss of funding or inescapable unfunded pressures £35k- £67k +/- 2% variance to budget. NIAO criticism	Financial loss, loss of funding or inescapable unfunded pressures £68k-167k +/- 5% variance to budget. NIAO qualification of accounts Fraud, corruption and serious irregularity	Financial loss, loss of funding or inescapable unfunded pressures £168k-£334k +/- 10% variance to budget. NIAO qualification of accounts Fraud, corruption and serious irregularity at Senior Management level.	Financial loss, loss of funding or inescapable unfunded pressures over £335k +/- 15% variance to budget. NIAO qualification of accounts
Compliance/ Regulatory/ Legal	Breach of local procedures not requiring external	Breach of National Procedures/ Standards.	Breach of subordinate legislation.	Breach of Primary legislation.	Breach of national or international statutory duties.

	intervention/ sanction.	Potential for minor legal challenge to CCMS	Failure to comply with relevant guidance results in expenditure being deemed irregular. Potential for moderate legal challenge to CCMS Likelihood that CCMS will lose challenge and a policy change will be required.	Potential for significant legal challenge to CCMS Likelihood that damages will be awarded against CCMS or changes will be required to subordinate legislation to ensure compliance	Legal challenge which halts delivery of policy. Major damages awarded against CCMS
Security	Non-notifiable or reportable incident.	Localised incident. No effect on operations.	Localised incident. Significant effect on operations.	Significant incident involving multiple locations.	Extreme incident seriously affecting continuity of operations.
Health & Well-being	Isolated incident – no significant health impact.	Small number of minor injuries requiring first aid treatment.	Compensatable injury/stress.	Serious injury/ stress resulting in hospitalisation Possible fatalities. Local Child Protection issue.	Fatality. Widespread Child Protection Issue
Reputational Reputational contd.	Minor adverse publicity in local media	Significant adverse publicity in local media	Significant Assembly scrutiny	Sustained adverse publicity in media.	Council/Chief Executive or SLT resignation/removal

	Event that will lead to public criticism by external stakeholders as anticipated.	Increased Assembly scrutiny. Event that may lead to widespread public criticism.	Formal communication required with public. Significant adverse publicity in national media Incompetence/ maladministration or other event that will undermine public trust or a key relationship for a short period.	Incompetence/ maladministration or other event that will undermine public trust or a key relationship for a sustained period or at a critical moment.	Incompetence/ maladministration or other event that will destroy public trust or a key relationship.

Risk Likelihood – Scoring Guide

Descriptor	Detailed Description
1. Unlikely	<11% chance of occurrence. May occur only in exceptional circumstances. Has never occurred before within the remit of CCMS Unlikely to occur during the lifespan of the policy/programme/project/ operation.
2. Remote	11-30% chance of occurrence. Might conceivably occur at some time. More likely not to occur than to occur. Has not occurred recently within the remit of CCMS There is a small chance that this may occur at some stage during the lifespan of the policy/programme/project/ operation.
3. Possible	31-60% chance of occurrence. Could occur at some time. Has occurred recently within the remit of another public body Might occur at some stage during the lifespan of the policy/programme/project/operation.
4. Probable	61-85% chance of occurrence. Will probably occur in most circumstances. More likely to occur than not to occur. Has occurred recently within the remit of CCMS Likely to occur within the next 1-2 years or during the lifespan of the policy/programme/project/operation.
5. Almost Certain	>85% chance of occurrence. Is expected to occur in most circumstances. This is known to occur in similar projects and programmes. Happens frequently within the remit of CCMS Highly likely to occur within the financial year or lifespan of the policy/programme/project/operation – probably early on and possibly more than once.

Risk Assessment Matrix

Impact	Critical	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Significant	3	3	6	9	12	15
	Moderate	2	2	4	6	8	10
	Minor	1	1	2	3	4	5
			Unlikely (<11%)	Remote (11-30%)	Possible (31-60%)	Probable (61-85%)	Almost Certain (>85%)
			1	2	3	4	5
			Likelihood				

RISK REGISTER TEMPLATE

Risk x			
Objective			
The achievement of x Corporate Goals in the CCMS 2021-22 Business Plan This risk is aligned to Risk x in the Department's Corporate Risk Register			
Risk Description		**Consequences**	
Risk Appetite:		•	
Lead Risk Owner	**Risk Category**	**Risk Dashboard** A = Appetite I = Inherent Status R= Residual Status	
Inherent Risk Rating (before any actions being to manage the risk are considered)			
Impact	**Likelihood**	**Risk Score**	
x	x	x	
Primary Root Causes	**Current Actions to Manage Risk**	**Responsible Officer**	
Residual Risk Rating (in light of current actions to manage risk)			
Impact	**Likelihood**	**Risk Score**	
x	x		
Action Plan for Improvement (if required)		**Responsible Officer**	**Target Date**
Contingency Plan (if required)			
Review			
Date	**Outcome**	**Risk Movement: ▲▼►**	

Further Information

The following documents provide advice and information on various aspects of risk management in Government.

- The Orange Book: Management of Risk - Principles and Concepts (HM Treasury February 2020) – Issued under cover of DAO (DoF) 04/20
- Managing Public Money Northern Ireland - MPMNI – Chapter 4 – Internal Management (DOF)
- Managing Public Money – Annex 4.3 – Risk (HM Treasury: rev August 2015)
- Supporting Innovation: Managing Risk in Government Departments (National Audit Office: August 2000)
- Managing Risks to Improve Public Services (National Audit Office: October 2004)
- Thinking About Risk - Managing your Risk Appetite: A Practitioner's Guide (HM Treasury: November 2006)
- Thinking About Risk - Managing your Risk Appetite: Good Practice Examples (HM Treasury: November 2006)
- Thinking About Your Risk - Setting and Communicating Your Risk Appetite (HM Treasury: November 2006)
- Good Governance - Effective Relationships between Departments and their Arms length Bodies (Northern Ireland Audit Office: May 2007)
- Managing Risks with Delivery Partners (HM Treasury, Office of Government Commerce)
- Good Practice in Risk Management: (NIAO: 8 June 2011)
- Framework for Management of Risk in Government (A Non-Executive's Review) (Cabinet Office: January 2017)
- Anti-Fraud Guidance (A range of documents available on the DOF website)
- Managing the Risk of Bribery and Corruption - a Good Practice Guide (NIAO: November 2017)
- Assurance Frameworks Guide (HM Treasury: December 2012)