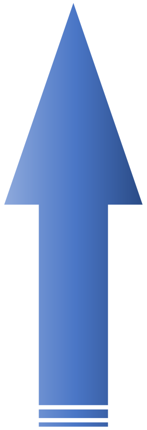
MIAA
2023/2024 Checklist Series –
Risk Management (Local Authorities)

September 2023

Risk management encompasses the identification, analysis, and response to risk factors that an organisation is exposed to in preventing its objectives being achieved and in delivering planned services. The effective management of risks will reduce both the possibility of a risk occurring and its potential impact whilst providing the basis for making sound business decisions and supporting the effective use of resources.

Risk management and internal controls should be fully embedded at all levels of the organisation and the effectiveness of arrangements will determine the risk maturity of an organisation, or put another way - how does an organisation view risks and how well does it utilise its understanding of risks to make key decisions?

The Institute of Internal Auditors (IIA) risk maturity assessment model (*2019*) includes five levels of an organisations risk maturity, the key characteristics at each level are described as follows:



Level 5: Risk enabled	*Risk Management and internal controls fully embedded into the operations.*
Level 4: Risk managed	*Enterprise approach to risk management developed and communicated.*
Level 3: Risk defined	*Strategy and policies are in place and communicated. Risk appetite defined.*
Level 2: Risk aware	*Scattered silo based approach to risk management.*
Level 1: Risk naïve	*No formal approach developed for risk management*

Internal audit reviews of risk management have identified the following key areas for development:

- Risk management strategy/procedures – roles and responsibilities of key officers not clearly defined.
- Training arrangements – training needs analysis and monitoring arrangements not fully developed.
- Risk appetite – not clearly defined and communicated.
- Risk register - format/quality of content not in line with best practice.

- Risk reporting and scrutiny arrangements - are not robust and risk escalation procedures are not clearly defined.

This checklist has been developed to assist in the assessment of your organisation’s risk maturity broadly based on the IIA’s characteristic at each level and the core controls that would be reviewed as part of a typical internal audit of risk management arrangements, referencing best practice where applicable.

We referred to the following when developing the checklist:

- Institute of Internal Auditors (IIA) Risk Maturity Assessment Guidance
- CIPFA/SOLACE Delivering Good Governance in Local Government Framework 2016 edition
- CIPFA Audit Committees Practice Guidance for Local Authorities and Police 2022 edition
- CIPFA International Framework: Good Governance in the Public Sector 2014

Risk Management Checklist – Local Authority

Areas for Local Authorities to consider		Organisation’s Response
Strategy and Policy	**A comprehensive risk management strategy/policy is in place and is made available to staff**	
	Does the organisation have an up-to-date risk management strategy and/or policy in place that covers the following: ○ Clearly defined roles and responsibilities of key groups/ committees and staff with risk management responsibility at all levels ○ Statement of risk appetite and review frequency ○ Risk identification, assessment and management process (terminate, transfer, tolerate, treat) with guidance on describing and scoring risks. ○ Risks rating and scoring methodology (likelihood and impact) ○ Risk assessment template and risk register template ○ Risk reporting and escalation arrangements ○ Risk management training matrix ○ Reference to related policies/procedures ○ Reference to relevant guidance	

Areas for Local Authorities to consider		Organisation’s Response
	Has the strategy/policy been published and made available to all staff?	

Areas for Local Authorities to consider		Organisation’s Response
Training	**Staff Awareness and Training**	
	Have the risk management training needs for all staff been identified and are timescales for training (including refresher) defined and communicated to staff?	
	Are arrangements in place to monitor and periodically report compliance with training requirements?	
	Do job descriptions relating to risk management roles refer to the key responsibilities?	
	Are managing risk responsibilities set out in role objectives for senior managers, departmental leads and those with oversight responsibility?	
	Are managers assessed on their risk management performance i.e. through the appraisal process?	

Areas for Local Authorities to consider		Organisation’s Response
Risk Management	**Risk identification, recording and monitoring is included in business as usual activities**	
	Are staff encouraged to identify risks within their remit and to report these if outside of their personal accountabilities, is this covered in local induction processes for new starters?	
	Is appropriate risk taking encouraged, particularly to respond to opportunities arising? Is this consistent with the overall risk management culture?	
	Is there a standardised documented risk assessment process in place (e.g. template to score risks and rationale) as set out in the Risk Management Strategy/Policy? Is the same risk scoring model adopted across the organisation? Is there a process to review risk assessments to check risk scores for consistency of similar or related risks?	
	Is the same risk scoring model adopted across the organisation?	
	Is there a process to review risk assessments to check risk scores for consistency of similar or related risks?	

Areas for Local Authorities to consider		Organisation's Response
	Do current decision-making processes support the identification of related risks e.g. project initiation documents and business cases include a risk assessment, decision making papers presented to committees include reference to related risks, before partnership/collaboration arrangements are agreed risks are identified, authority planning processes include consideration of risks	
	Are risks considered as part of new policy/change in policy review and scrutiny arrangements?	
	Are all departmental/service level risks recorded in a standardised format and included in a risk register?	
	Are risks linked to departmental/service level objectives?	
	Are departmental/service risk registers periodically reviewed to ensure risks remain current and are up to date?	
	Is there a process for escalating risks for inclusion on the corporate/strategic risk register and has the criteria been clearly defined i.e. risk above a certain score, risks which would have a significant impact on public/staff safety, finances etc?	

Areas for Local Authorities to consider		Organisation’s Response
	Is it clear how such risks would be managed in terms of responsibility and the same where risks are de-escalated?	

Areas for Local Authorities to consider		Organisation’s Response
Strategic Risks	**Strategic risks are clearly linked to organisational objectives**	
	• Have the organisation’s objectives been clearly defined and communicated to all staff? • Are all other objectives and targets consistent with the strategic objectives?	
	• Have the risks to the achievement of the organisation’s objectives been identified and are these periodically reviewed?	
	• Is there a process for identifying and considering emerging risks?	
	• Has an assurance mapping exercise been undertaken using the three lines of assurance model (IIA)?	
	• Has the organisation defined its’ risk appetite and is this periodically reviewed by the governing body?	

Areas for Local Authorities to consider		Organisation's Response
Risk Register	**Risk Register Format and Quality of Content – Good Practice**	
	Is there a standard risk register template in place for recording risks? and does this include the following: ○ Risk reference ○ Date risk added to register ○ Clearly described risk statements using the event-cause-consequence format ○ Risk owner and Senior Responsible Officer ○ Key controls in place to reduce risk ○ Assurances ○ Gaps in controls and assurances ○ Actions to address gaps in controls and assurances ○ Are actions specific, measurable, attainable, relevant, time bound (SMART) ○ Officers responsible for actions ○ Risk movement ○ Date risk last reviewed	
	Does the risk register/s cover all areas within the organisation and incorporate key strategic, operational, financial, health and safety, reputational, environmental/social corporate responsibility and fraud risks?	

Areas for Local Authorities to consider		Organisation’s Response
	Where risks are managed using an electronic system, is access sufficiently controlled? Have users been provided with the appropriate training? Where alternative arrangements are in place, is access to make changes the master documents restricted?	
	Are reminders sent to responsible officers in a timely manner when actions to mitigate risks become due (via the risk management system or otherwise)? Is the effectiveness of the action in controlling the risk assessed?	
	Is there a process in place to identify actions that have passed their due date and no update has been provided?	
	Are regular review meetings held with risk managers to discuss issues, progress with actions etc?	
	Where officers with risk management responsibilities leave a post or the organisation what mechanisms are in place to ensure risk responsibility is transferred in a timely manner?	
	Is the organisation’s risk profile regularly reviewed and are all appropriate officers involved in the process?	

Areas for Local Authorities to consider		Organisation’s Response
	Where risks have been included on a risk register for a substantial amount of time is there a process in place to review these to ensure they remain active and are current?	
	Is there a process for ensuring high rated risks are more frequently reviewed and concerns escalated to the appropriate groups/committees?	
	Is there a process in place for any risks to be escalated to the responsible group/committee where risk score is above the risk appetite/target score and actions have not been taken in a timely manner or have been delayed?	

Areas for Local Authorities to consider		Organisation’s Response
Risk Reporting and Oversight	**Risk Reporting and Oversight Arrangements are effective and support the development of the Annual Governance Statement**	
	Are risk reporting/oversight arrangements in place at department/service level?	
	If a risk management group/committee is in place:	

Areas for Local Authorities to consider		Organisation’s Response
	○ Does the terms of reference clearly set out roles and responsibilities including escalation arrangements? ○ Is the membership representative and is member knowledge and skill set considered in ensuring appropriate scrutiny/challenge of risks and decisions made regarding escalation and de-escalation of risks to and from corporate/strategic to service/department risk registers? ○ Are reporting arrangements into other groups/committees defined? ○ Is the risk register reviewed at least quarterly?	
	For groups/committees with risk oversight responsibilities: ○ Do the terms of reference set out the roles and responsibilities and reporting arrangement to and from other groups/committees? ○ Is reporting exception based or high risks only – if so does the group/committee have access to the risk register or is this periodically provided? ○ Is the frequency at which the risk registers will be reviewed defined?	
	Are risks grouped into categories for reporting/oversight to provide an additional level of	

Areas for Local Authorities to consider		Organisation’s Response
	input on controls/assurances for example, finance risks and resource and staffing risks are regularly reported at Senior Leadership meetings?	
	Does the Audit Committee or equivalent group/function independent of the executive and accountable to the governing body regularly review/monitor the risks management framework and seek assurance in relation to the governance of risk and the effectiveness for risk management and do they have sight of risks at different points in a year?	
	Does the governing body have sight of all high rated risks?	