Internal Audit Progress Report

Guildford Borough Council

KPMG Governance, Risk and Compliance Services

—

November 2022

Content

Key contacts

Neil Hewitson
Director
neil.hewitson@kpmg.co.uk

Jack Crouch
Manager
jack.crouch@kpmg.co.uk

01

Executive Summary

The purpose of this document is to provide the Corporate Governance and Standards Committee with an update on the Internal Audit plan for 2022-23. We have summarised below the key points to draw your attention to in the period since we last reported to you:

Activity	Comments
Progress against the plan	— We have finalised our Corporate Risk Management and IT Infrastructure for Remote Working reviews. — Fieldwork is ongoing for our review of Corporate Programmes: Redevelopment Projects and Core Financial Controls: Budgetary Controls, which are due to be finalised in November and reported to CMB and CGSC in January 2023. — We are due to commence fieldwork for our General Ledger review in November.
Reports completed	— We have finalised our reports on Corporate Risk Management and IT Infrastructure for Remote Working.
Significant findings to highlight	— We have no significant findings to highlight at this time.

For information

- November 2022 internal audit progress report

02

Progress of plan

Below is the status of the 2022-23 Internal Audit plan as approved by the Corporate Governance and Standards Committee.

Internal audit	Status						Results	Recommendations			
	Planning	Fieldwork	Draft Report	Final Report	Reporting to CMB	Reporting to CGSC	Overall Rating	High	Medium	Low	Total
01/22: IT Infrastructure for Remote Working	✓	✓	✓	✓	✓	✓	**Significant assurance with minor improvement opportunities**	-	1	2	3
02/22: Performance Monitoring – KPI Review One	✓	✓	✓	✓	✓	✓	**Significant assurance with minor improvement opportunities**	-	1	2	3
03/22: Performance monitoring – KPI Review Two	✓	✓	✓	✓	✓	✓					
04/22: Performance monitoring – KPI Review Three	✓	✓	✓	✓	✓	✓					
05/22: Customer Services: Complaints Handling	✓	✓	✓	✓	✓	✓	**Partial assurance with improvements required**	1	2	2	5
06/22: Corporate Programmes: Redevelopment Projects	✓	In progress	w/c 21 November	w/c 05 December	20 December	19 January	Not due	-	-	-	-
07/22: Corporate Risk management	✓	✓	✓	✓	✓	✓	**Significant assurance with minor improvement opportunities**	-	1	2	3

KPMG

02

Progress of plan (cont.)

Internal audit	Status						Results	Recommendations			
	Planning	Fieldwork	Draft Report	Final Report	Reporting to CMB	Reporting to CGSC	Overall Rating	High	Medium	Low	Total
08/22: Financial controls: budgetary control	In progress	In progress	w/c 05 December	w/c 19 December	20 December	19 January	Not due	-	-	-	-
09/22; Financial controls: General Ledger	In progress	w/c 28 November	w/c 12 December	w/c 02 January	10 March	15 March	Not due	-	-	-	-
10/22: Financial controls: Payroll	✓	✓	✓	✓	✓	✓	**Significant assurance with minor improvement opportunities**	-	1	1	2
11/22: s.106 Contributions	In progress	w/c 05 December	w/c 19 December	w/c 02 January	10 March	15 March	Not due	-	-	-	-
12/22: Follow up reviews from 2021-22	November / December	w/c 09 January	w/c 30 January	w/c 13 February	10 March	15 March	Not due	-	-	-	-
13/22: Regeneration	November / December	w/c 09 January	w/c 30 January	w/c 13 February	10 March	15 March	Not due	-	-	-	-
14/22: Financial controls: Journals	November / December	w/c 09 January	w/c 30 January	w/c 13 February	10 March	15 March	Not due	-	-	-	-
							Total	**1**	**6**	**9**	**16**

KPMG

Appendix A - Corporate Risk Management

Conclusion

We reviewed the design and effectiveness of the corporate risk management processes and controls at Guildford Borough Council ('the Council') and provide 'significant assurance with minor improvement opportunities' **(amber-green)**, in line with management's forecast. This is driven by the well-designed risk management framework, clear governance structure for reporting and guidance in place to provide clarity over risk scoring and identification. We found there is the need to update the Corporate risk register to include additional fields to strengthen monitoring of risks and provide clearer reporting. We also raise a finding around the mandatory attendance of the relevant Service Leads with red rated risks to the Risk Management Group (RMG) meetings.

The Council's newly implemented 'Risk Management Strategy and Policy 2022-25' clearly sets out the approach to risk management and provides detailed guidance to all relevant staff on how to identify, categorise and record risks. The policy has been reviewed and approved by the RMG and Corporate Governance and Standards Committee (CGSC) and will be reviewed annually.

Individual corporate risks are discussed at quarterly RMG meetings. There is additional reporting twice a year to CGSC. Areas of concern are reported through to Corporate Management Board..

The corporate risk register is well designed with clear fields for assigning net & gross risk scores, RAG rating and mitigating controls/actions with target deadlines. We identified additional fields to be included in order to strengthen the risk register and bring it in line with best practice. This includes the date risks are added, links to Council Strategy , the name of responsible individuals and target risk scores.

The policy provides definitions of various risk tolerance such as accept, reduce, transfer etc. However, the individual corporate risks do not have assigned target scores to bring them in line with a centrally defined risk appetite.

Summary

Overall rating:	Significant assurance with minor improvement opportunities

Priority rating:	Control design	Operating effectiveness
High	0	0
Medium	1	0
Low	2	0

Appendix A - Corporate Risk Management

Areas of good practice

- ✓ The Risk Management Policy has been approved by CGSC.
- ✓ Guidance documents are split into strategic and operational levels to ensure clarity and consistency in the Council's risk management approach.
- ✓ Risk scoring criteria and matrix used for both service and corporate level risks registers are the same, ensuring a consistent approach to risk Council-wide.
- ✓ There are clear escalation routes for risks communicated to all service leads to ensure completeness of the corporate risk register.
- ✓ Clear definitions for potential mitigating controls (avoid, accept, transfer, reduce and/or exploit) identified in policy to ensure all potentialities are fully considered.
- ✓ The roles and responsibilities of the Risk Management Group are clearly identified and defined in the appendix of the Risk Management Strategy and Policy.

Summary of key findings

Additional risk register fields	**2.1**	The Corporate Risk Register template should be updated to include the date the risk was added to the corporate risk, links to Council Strategy, the name of responsible individuals and target risk scores.
Updates to ToR and Policy	**2.2**	The RMG ToR and policy should be updated to provide greater clarity over the requirements for service leads owning red rated risks attending RMG for escalation to CMB.
Council-wide risk appetite threshold	**2.3**	The Council has not formally defined risk appetite at a strategic level. Individual corporate risks do not have target risk scores aligning to risk tolerance thresholds.

Appendix B - IT Infrastructure for Remote Working

Conclusion

We reviewed processes relating to IT infrastructure for remote working and provide 'significant assurance with minor improvement opportunities' (**amber-green**), which is in line with management's forecast. This is driven by robust and appropriate policies and procedures and governance in place for remote working. There are opportunities for improvement in relation to policies, network infrastructure and risk management.

The Council started to introduce remote working prior to the pandemic with employees still expected in a fixed office location. Due to Covid-19 rules and regulations in 2020-21, almost all staff were required to work remotely. The Council's network infrastructure, governance, policies, and risks may have required updates at this point to reduce exposure to IT risks which remote working contributes to, such as exposure to cyber-attacks, data privacy, and the network's ability to support a large threshold of users on the infrastructure at once.

The Council has policies widely published; new joiners are required to review and sign to confirm they have acknowledged the policies. We reviewed the Acceptable Use Policy, Remote Access Policy and Agile Working Policy, which provide guidance on how Access Rights and Privileges, Anti-Virus and Firewall Protection, Information Management, Connection Requirements, System Support and Maintenance are carried out whilst working remotely. There is a Business Continuity Plan which is updated regularly by the Lead IT Specialist and a checklist for new joiners, including mandatory training and a review of the Acceptable Use of IT Equipment Policy, IT Security Policy, Information Security Framework and Reporting Personal Information Risk Incidents. The policies state the support the Council provides for their employees when working remotely, and what is expected of staff when working remotely.

We reviewed risks at Service and Corporate level, although we did not receive any specific evidence on remote working. We raise a finding for the policies which have not been reviewed at the required date; where there could be potential exposure to working remotely if the procedures are not updated when expected, keeping employees updated with current expectations of working remotely; such as the training requirements (e.g. GDPR training), the use of IT equipment and the rights and access for the use of the Councils data. Without having risk assessments documented, with the main focus based on the network infrastructure, there is a risk the Council may not fully understand the capacity of its infrastructure, will not be prepared or respond in the event of a disaster, and face exposure to cyber-attacks with users working remotely.

Summary

Overall rating:	**Significant assurance with minor improvement opportunities**

Priority rating:	Control design	Operating effectiveness
High	-	-
Medium	-	1
Low	-	2

Appendix B - IT Infrastructure for Remote Working

Areas of good practice

- ✓ The Remote Access Policy outlines the requirements for remote working and defines the Access Rights and Privileges, Anti-Virus and Firewall Protection, Information Management, Connection Requirements, and System Support and Maintenance. The policy states procedural information and that ICT Security training must be completed by all employees, showing Board and Senior Leadership understand and support the importance of Data Protection with a defined vision and unified approach to managing their systems whilst working remotely.
- ✓ The Acceptable Use Policy details the appropriate use of access information, applications and systems and rights withheld by employees of the Council, showing effective controls for the handling and storage of information and to protect information from unauthorised disclosure or misuse.
- ✓ The Agile Working Policy defines fixed and agile workers, support provided for those working remotely, and refers to the requirement of all mobile workstations to be connected to the Council Network monthly to receive updates and patches.
- ✓ The Business Continuity Plan has critical systems classified according to severity and addressed accordingly, is reviewed by the third party, Applied Resilience, and is updated periodically by the Lead IT Specialist.
- ✓ A checklist is in place for new joiners, with mandatory induction training including Data Protection training, and a review of policies: Acceptable Use of ICT Equipment Policy, IT Security Policy, Information Security Framework and Reporting Personal Information Risk Incidents.
- ✓ The Data Protection Officer (DPO) provides GDPR training for all new joiners and employees, where we note discussion of the Data Protection Act, conditions of processing personal data, use of emails and accessing Council information, and demonstrating analyses of how often data breaches can occur due to human error.

Summary of key findings

Remote Working Risk Assessments	2.1	Lack of formally documented, regular risk assessments specific to remote working performed, in light of much-increased remotely working due to Covid-19 regulations.
Corporate-level BCP	2.2	The Corporate-level Business Continuity Plan (BCP) is to be drafted and then reviewed and approved by Corporate Management Board (CMB).
Regular review of key policies	2.3	The policies have not been reviewed by the Council at the scheduled date of October 2021.

KPMG

kpmg.com/uk

This report is provided pursuant to the terms of our engagement letter dated 12 April 2018. Nothing in this report constitutes a valuation or legal advice. We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in our engagement letter. This report is for the sole benefit of Guildford Borough Council. In preparing this report we have not taken into account the interests, needs or circumstances of anyone apart from the Council, even though we may have been aware that others might read this report. This report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than Guildford Borough Council) for any purpose or in any context. Any party other than the Council that obtains access to this report or a copy (under the Freedom of Information Act 2000, the Freedom of Information (Scotland) Act 2002, through the Council's Publication Scheme or otherwise) and chooses to rely on this report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this report to any party other than the Council. Any disclosure of this report beyond what is permitted under our engagement letter may prejudice substantially our commercial interests. A request for our consent to any such wider disclosure may result in our agreement to these disclosure restrictions being lifted in part. If Guildford Borough Council receives a request for disclosure of the product of our work or this report under the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002, having regard to these actionable disclosure restrictions the Council should let us know and should not make a disclosure in response to any such request without first consulting KPMG LLP and taking into account any representations that KPMG LLP might make.

This report has been prepared solely for Guildford Borough Council in accordance with the terms and conditions set out in our engagement letter dated 12 April 2018. We do not accept or assume any liability or duty of care for any other purpose or to any other party. This terms of reference should not be disclosed to any third party, quoted or referred to without our prior written consent.