



GEDLING BOROUGH COUNCIL

Internal Audit Progress Report

Audit Committee

19 March 2019

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.

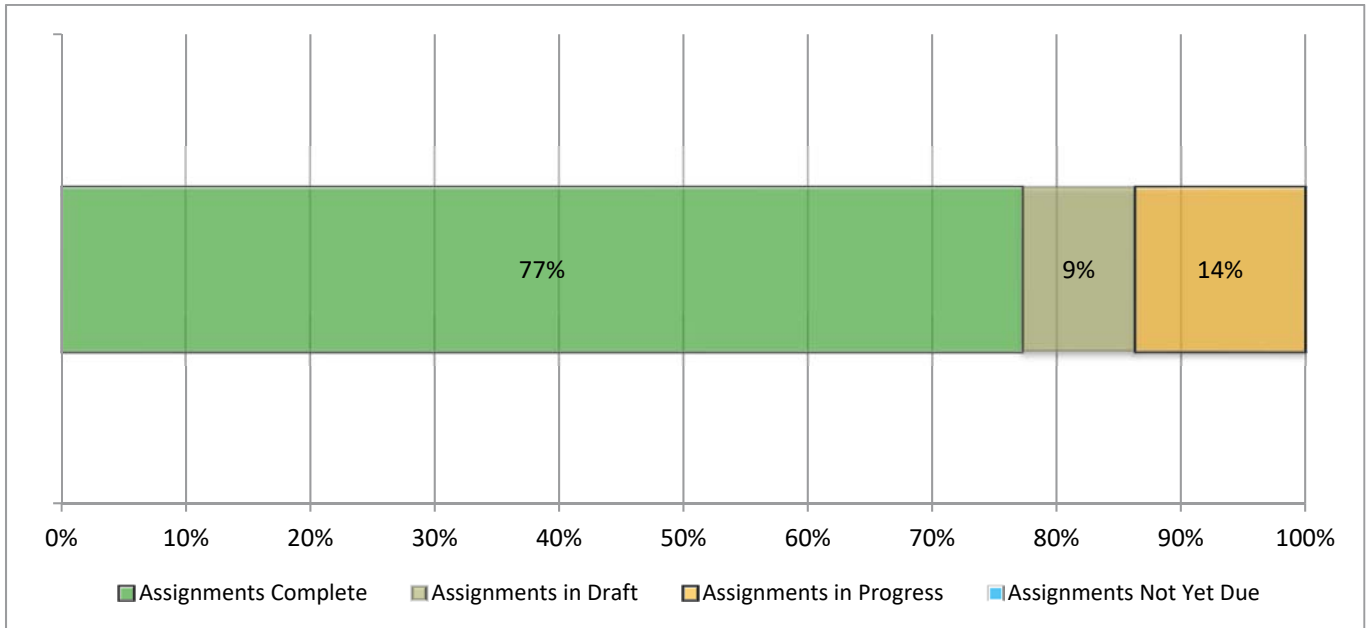


CONTENTS

1	Introduction.....	2
2	Reports considered at this Audit Committee.....	3
3	Looking ahead.....	6
4	Other matters	7
	Appendix A: Internal audit assignments completed to date	8
	For further information contact	9

1 INTRODUCTION

The internal audit plan for 2018/19 was approved by the Audit Committee on 20 March 2018. Below provides a summary update on progress against that plan and summarises the results of our work to date. Please see chart below for current progress with the plan.



2 REPORTS CONSIDERED AT THIS AUDIT COMMITTEE

This table informs of the audit assignments that have been completed and the impacts of those findings since the last Audit Committee held. The Executive Summary and Key Findings of the assignments below are attached to this progress report.

Assignments	Status	Opinion issued	Actions agreed		
			H	M	L
NNDR (10.18/19)	Final		0	1	1
Health and Safety (11.18/19)	Final		0	3	1
Grounds Maintenance, Parks and Open Spaces (12.18/19)	Final		0	2	3
Landlord Licensing (13.18/19)	Final		0	1	1
Development Management (14.18/19)	Final		0	0	4
Risk Management (16.18/19)	Final		0	0	0
General Data Protection Regulation (GDPR) Governance (17.18/19)	Final	Advisory	Seven management actions to consider.		
IT Review – Ethical Phishing Campaign	Final	Advisory	Three management actions to consider		

2.1 Impact of findings to date



NNDR (10.18/19)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing, one medium and one low priority actions were identified, and management actions were agreed in respect of these findings.

The medium management action is in relation to:

- For a sample of 20 refund payments, five instances were authorised outside of delegated authority limit.
-



Health and Safety (11.18/19)

Conclusion: Reasonable Assurance

Impact on Annual Opinion: Positive

As a result of testing, three medium and one low priority actions were identified, and management actions were agreed in respect of these findings.

The medium management actions are in relation to:

- Testing a sample of 10 risk assessments confirmed one was incomplete, one was missing and only two had been uploaded to AssessNET.
 - The contractor list was not a complete record of all contractors used and therefore could not confirm all had been subject to health and safety checks.
 - Eight out of 10 new starters sampled had not undertaken the health and safety awareness mandatory training.
-



Grounds Maintenance, Parks and Open Spaces (12.18/19)

Conclusion: Reasonable Assurance

Impact on Annual Opinion: Positive

As a result of testing, two medium and three low priority actions were identified, and management actions were agreed in respect of these findings.

The medium management actions are in relation to:

- The Green Space Strategy 2012-2017 was revised in April 2017 but was deemed out of date at the time of the audit.
 - There were no policies or procedures in place for regular inspections and risk assessments of the tree assets.
-



Landlord Licensing (13.18/19)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing, one medium and one low priority actions were identified, and management actions were agreed in respect of these findings.

The medium management action is in relation to:

- A gap of 198 properties in the Council are yet to apply for licensing.



Development Management (14.18/19)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing, four low priority actions were identified, and management actions were agreed in respect of these findings.



Risk Management (16.18/19)

Conclusion: Substantial Assurance

Impact on Annual Opinion: Positive

As a result of testing, no management actions were identified.



General Data Protection Regulations (GDPR) Governance – Post Implementation Review (17.18/19)

Conclusion: Advisory Review

Impact on Annual Opinion: n/a

The key findings and observations from this advisory review are detailed in the Executive Summary and Action Plan attached to this report.



IT Review – Ethical Phishing Campaign

Conclusion: Advisory Review

Impact on Annual Opinion: n/a

The key findings and observations from this advisory review are detailed in the Executive Summary and Action Plan attached to this report.

3 LOOKING AHEAD

Assignment area	Timing per approved IA Plan 2018/19	Status	Target Audit Committee
Follow Up 2	Quarter 3	Draft report issued	28 May 2019
Cash and Banking	Quarter 3	Draft report issued	28 May 2019
Contract and Procurement	Quarter 3	In progress	28 May 2019
Anti-Fraud Review	Quarter 4	In progress	28 May 2019
Property – Investment, Miscellaneous Properties and Facilities Management	Quarter 4	In progress	28 May 2019

4 OTHER MATTERS

4.1 Changes to the audit plan

There have been no changes made to the audit plan since the previous Audit Committee.

4.2 Quality Assurance and Continual Improvement

To ensure that RSM remains compliant with the PSIAS framework we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews being used to inform the training needs of our audit teams.

The Quality Assurance Team is made up of: Ross Wood (Manager, Quality Assurance Department) with support from other team members across the Department. All reports are reviewed by James Farnbrough as the Head of the Quality Assurance Department.

This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

4.3 Post Assignment Surveys


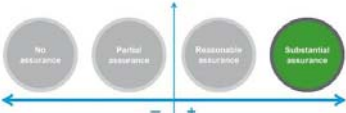
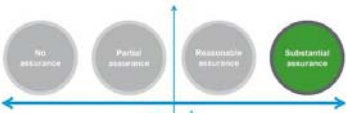



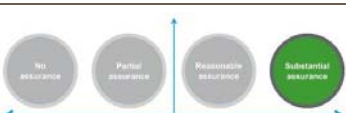

We are committed to delivering an excellent client experience every time we work with you. Your feedback helps us to improve the quality of the service we deliver to you. Currently, following the completion of each product we deliver we attached a brief survey for the client lead to complete.

We would like to give you the opportunity to consider how frequently you receive these feedback requests; and whether the current format works. Options available are:

- After each product (current option);
- Monthly / quarterly / annual feedback request; and
- Executive lead only, or executive lead and key team members.

APPENDIX A: INTERNAL AUDIT ASSIGNMENTS COMPLETED TO DATE

Report previously seen by the Audit Committee and included for information purposes only:

Assignment	Status	Opinion issued	Actions agreed		
			H	M	L
Mail Room (1.18/19)	Final		0	0	3
Customer Services and One Stop Shop Areas (2.18/19)	Final		0	0	1
Gedling Country Park Visitor Centre (3.18/19)	Final		0	0	1
Community Centres (4.18/19)	Final		0	4	1
Reconciliations (5.18/19)	Final		0	2	6
Follow Up 1 (6.18/19)	Final	Reasonable Progress	0	1	4
Main Accounting System (7.18/19)	Final		0	0	2
Corporate Governance (8.18/19)	Final		0	1	2
Payroll and Expenses (9.18/19)	Final		0	0	1

FOR FURTHER INFORMATION CONTACT

Chris Williams, Head of Internal Audit

chris.williams@rsmuk.com

Address:

RSM Risk Assurance Services LLP
Suite A, 7th Floor
City Gate East
Tollhouse Hill
Nottingham NG1 5FS

Phone: 01159 644450

Mobile: 07753 584993

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of Gedling Borough Council, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

NNDR - EXECUTIVE SUMMARY

1.1 Background

An audit of National Non-Domestic Rates (NNDR) was undertaken as part of the approved internal audit periodic plan for 2018/19.

The Local Government Finance Act 1988 provided an administrative framework for assessing and billing NNDR.

The Valuation Office Agency (VOA) is an executive agency of HM Revenue and Customs (HMRC) and provides the Government with valuations and property advice required for taxation and benefits. The VOA compiles and maintains lists of Council tax bands and details the rateable value of non-domestic properties for business rates. Changes to these bands and values are notified by collecting authorities such as the Council on an ongoing basis for them to action.

Of the £22m of NNDR collected by the Council during 2017/18, £4m was retained for its own services, with the balance apportioned to Central Government, Nottinghamshire County Council and the Combined Fire Authority. The Council successfully collected 99 per cent of business rates due for the period.

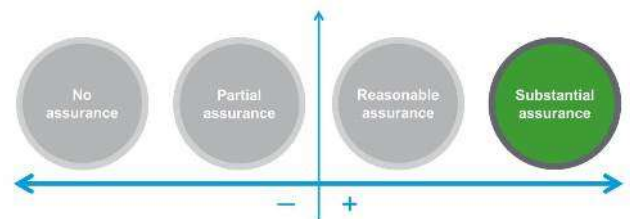
Non-domestic rating multipliers for the year issued by the VOA had been applied to the Council's revenues system. £34,807.35 was written off for NNDR during the year to audit (November 2018).

1.2 Conclusion

The review of NNDR identified that overall the control framework is well designed and operating effectively. However, two weaknesses in compliance with the established control framework have been identified which has resulted in one medium and one low priority management actions being raised. The reported exceptions relate to the inspection of void properties and the authorisation of refund payment batches.

Internal audit opinion:

Taking account of the issues identified, the Council can take substantial assurance that the controls upon which the Council relies to manage the identified area(s) are suitably designed, consistently applied and operating effectively.



1.3 Key findings

Our audit review identified that the following controls are suitably designed, consistently applied and are operating effectively:

- A Fair Collection and Debt Recovery Policy is in place which was last updated in May 2017 and is next due for review on 1 June 2019.
- Changes in circumstances are evidenced in the revenues system and processed in a timely manner following notification.
- Exemptions are granted on receipt of adequate supporting documentation and are reviewed on an annual basis.
- Mandatory and discretionary reliefs are assessed for non-domestic accounts. Applications and decisions are uploaded to the revenues system. Demand notices were issued to liable parties following decisions.
- The debt recovery timetable was followed for business rates, with demand notices, reminders and court summonses issued to liable parties documented in Civica.
- Authorisation limits are adhered to for write offs. Evidence is retained for all write offs, including for justification and approval.
- NNDR outturns were submitted to the Department for Communities and Local Government. All submitted returns were signed by the Deputy Chief Executive and Finance Director.
- Each month the Revenues Team Leader compiles the latest Key Performance Indicator (KPI) figures. These figures are e-mailed to the Service Manager - Revenues and Welfare Support, who will input the data within the Covalent system.
- Each month, Commencement and Completion reports are collated by the Planning and Building Control Team and emailed to the NNDR Department. This allows the NNDR Department to identify any new properties/businesses within the area which are currently or will be liable for NNDR.
- Testing identified delays in the timeliness of reconciliations between VOA schedules of changes and the Council's revenues system but there were just within the allowable time limits and so no action has been raised.
- Where circumstances have changed regarding an existing write-off, causing the original liability to become recoverable, a write-off reversal is actioned within the Civica system.

However, the following areas of non-compliance with the established control framework were identified which primarily related to the follow up of agreed management actions from the 2017/18 internal audit report on this area:

- One instance was noted where a void property had not been inspected despite having an original void date of April 2018.
- Sample testing of 20 refund payments within the current financial year, noted five instances where batch payments had been authorised outside of delegated authority limits.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Area	Control design not effective*		Non Compliance with controls*		Agreed management actions		
	Low	Medium	High	Low	Medium	High	
NNDR	0	(16)	2	(16)	1	1	0
Total					1	1	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

1.5 Progress made with previous audit findings

Date of previous audit	Low	Medium	High
Number of actions agreed during previous audit	3	2	0
Number of actions implemented	2	0	0
Number of actions not implemented	1	2	0

As part of this review, Gedling Borough Council has demonstrated **poor progress** in implementing agreed NNDR actions made within the **18.17/18 Council Tax and NNDR** audit report. Of the three low and two medium priority agreed management actions raised previously, we confirmed that two have been implemented in full and two have not been implemented and are the basis of the management actions agreed within this report. The final action related to NNDR reconciliations which was followed up separately as part of a specific internal audit on reconciliations. This action was again deemed to be not implemented and a further action raised in the 2018/19 report (5.18/19).

2 DETAILED FINDINGS AND ACTION PLAN

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/ reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

Our internal audit findings and the resulting actions are shown below.

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Area: NNDR								
2	Refunds arising from overpayments or adjustments to circumstances and rateable values are properly authorised. All supporting documentation is added to Civica. For any identified refunds, liable parties are issued with an updated demand notice stating the refund to be made.	Yes	No	A sample of 20 refunds issued during the current financial year were selected to confirm suitable evidence and authorisation. In all cases, refund reasons were clear, and documentation had been recorded within the Civica system. Updated demand notices were issued in a timely manner following receipt of evidence and a decision being made, clearly stating the refund amount. In 13 cases, refunds were approved by the Service Manager - Revenues	Medium	Refund batch payments will be appropriately approved prior to payment in line with delegated limits. Consideration will be given to the most suitable member of staff to deputise in instances of absence.	30 November 2018	Revenues Manager

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>and Welfare Support as part of refund batches.</p> <p>All batches documented the same value of refund as that evidenced in the Civica system and recorded on demand notices to liable parties.</p> <p>In seven cases three refunds were approved as part of five separate payments batches by the Client Officer.</p> <p>The Client Officer has no budget holder authority and therefore should not deputise in the absence of the Service Manager - Revenues and Welfare and refunds should only be authorised in line with delegated limits.</p> <p>One of the payment batches tested was found to have a significant value of £51,882.73, and therefore delegated authority should be documented.</p> <p>By failing to adhere to delegated limits, there is a risk that unsuitable refunds will be paid and not identified, or that budget will be committed where it is not available.</p>				

HEALTH & SAFETY - EXECUTIVE SUMMARY

1.1 Background

An audit of Health and Safety was undertaken as part of the approved internal audit periodic plan for 2018/19.

The Council has overall responsibility for health and safety within the Council and this is advised upon by the Chief Executive. Day to day health and safety responsibilities are managed by the role of the Health, Safety and Emergency Planning Officer. The Council uses AssessNET where incidents, accidents and hazards can all be logged by staff and managed through the system. Risk assessments can also be stored and monitored on the system with monitoring of review dates possible. The system was acquired in January 2018 and has been used for incident logging since. The Council are in the process of uploading all the risk assessments onto the system of which 628 currently exist.

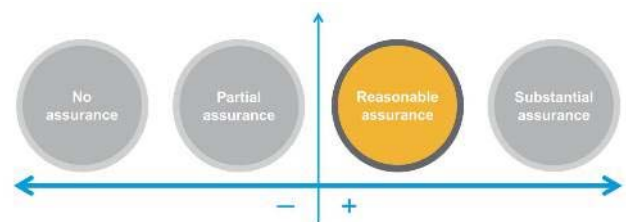
At the time of the audit, a total of 222 incidents had been logged on AssessNET and risk assessment additions had commenced. Health and safety is monitored quarterly by the Corporate Health and Safety Group (CHAS) and reported annually to the Senior Leadership Team (SLT). Various health and safety courses are offered which are conducted both internally and by external providers with a total of 200 attendances by the end of September 2018.

1.2 Conclusion

Our overall opinion was formed by undertaking interviews with key staff and sample testing on the processes in place to ensure that the controls upon which the Council relies on to manage health and safety are being. Our review has confirmed that there is an adequate control framework in place, however, examples of non-adherence and control improvements have resulted in three "medium" and one "low" management actions being raised.

Internal audit opinion:

Taking account of the issues identified, the Council can take reasonable assurance that the controls in place to manage this risk are suitably designed and consistently applied. However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).



1.3 Key findings

The key findings from this review are as follows:

- A Health and Safety Policy is in place and up to date with the last review in August 2018. This Policy is supported by procedure notes for the management and day to day processing of health and safety within the Council.
- Testing a sample of 10 incidents logged on AssessNET confirmed in all instances detailed notes on the incidents and any investigations required were documented. Furthermore, where follow up actions were required, these were completed, and the incidents formally closed off.
- Health and safety is reported quarterly to the CHAS Group with updates on incident statistics and training matters and this was confirmed through review of minutes. An overall annual health and safety report was produced and presented to SLT in May 2018 and the Joint Consultative Safety Committee in August 2018.

- There is a Health and Safety Audit Planner Document in place which outlines which areas of the Council are to undergo an audit each year with the target for six to take place annually. For the current year, it was confirmed six have taken place with five being conducted by an external source.
- Guidance notes and standard documents are in place to be completed for all contractors working on Council premises or on behalf of the Council. These are completed prior to commencing the service.
- Health and safety files are held in a securely locked cupboard in the office of the Health, Safety and Emergency Planning Officer and AssessNET access is limited to current staff only via password and security question.
- A suite of training is offered by both the Health, Safety and Emergency Planning Officer and external sources and a plan of training has been developed for the current year and next year. Attendance is reported through the CHAS Group and monitored by its members.

However, the following control improvements or non-adherence to controls were identified:

- Testing a sample of 10 risk assessments identified that one could not be located, and one was incomplete. Furthermore, it was identified that only two had been uploaded currently onto AssessNET.
- It was confirmed an annual report was presented to SLT and the Joint Consultative Safety Committee, however, it was identified that it would be good practice to report annually to Cabinet as well.
- It was confirmed that the contractor list in place is not a complete record of all contractors used by the Council and therefore cannot confirm all have been subject to health and safety checks.
- Testing a sample of 10 new starters identified eight instances where the health and safety awareness mandatory training had not been undertaken.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non-Compliance with controls*		Agreed Management Actions		
	Low	Medium	High	Low	Medium	High	
Failure to protect staff, including health and safety issues (Risk Register: 3)	0	(7)	2	(7)	1	1	0
Failure to protect and utilise physical assets (Risk Register: 6)	0	(5)	1	(5)	0	1	0
Failure to react to changes in legislation (Risk Register: 7)	0	(2)	1	(2)	0	1	0
Total	1	3	0	0	1	3	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Risk: Failure to protect staff, including health and safety issues								
1	Risk assessments are completed by Managers and Supervisors in their relevant areas and these are to be updated at least every two years. A process has begun to upload all risk assessments to the AssessNET system and these are required to be signed off by the relevant Manager.	Yes	No	<p>Testing a sample of 10 risk assessments provided on a manual list, it was confirmed that in eight instances they had been completed within the last two years.</p> <p>In the remaining two instances, one could not be located to confirm it had been updated in the last two years and one risk assessment was incomplete.</p> <p>It was further confirmed that only two of the risk assessments had been uploaded onto AssessNet, however, these did still require management sign off.</p> <p>There is a risk that there is not a single central record for all risk</p>	Medium	All risk assessments will be fully completed, uploaded to AssessNET and signed off by managers.	31 July 2019	Health, Safety and Emergency Planning Officer

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				assessments to be held for ease of access when required. Furthermore, there is a risk that where not completed or unable to be found, if an incident occurs relating to the specific area, the Council maybe further liable.				
Risk: Failure to protect and utilise physical assets								
3	A contractor list is in place with all contractors used by the Council, when they were last health and safety checked and the date this is due to expire.	Yes	No	<p>Testing a sample of 10 contractors confirmed in all instances the health and safety competence was checked prior to use and evidence was maintained on file of the questionnaire, rules and induction.</p> <p>However, it was identified through review of the contractor list and discussion with the Health, Safety and Emergency Planning Officer that this list is not a full list of all contractors.</p> <p>Therefore, there is a risk that some contractors used may not have been health and safety checked or these have expired and continued to be used leading to an increased risk of accidents or claims against the Council.</p>	Medium	A comprehensive list of all contractors will be formed with all Managers notifying of all their used contractors. Furthermore, all of these contractors will be subject to health and safety checks prior to use.	31 December 2019	Health, Safety and Emergency Planning Officer / Deputy Chief Executive and Director of Finance
Risk: Failure to react to changes in legislation								
4	Health and safety awareness courses are run every quarter and all new starters are required to attend this course at the earliest opportunity.	Yes	No	Testing a sample of 10 new starters confirmed in eight instances no health and safety awareness training had been provided or no evidence could be obtained to confirm this had taken place.	Medium	All staff will be reminded of the process to ensure health and safety awareness training is attended by new starters and the forms to be returned to the Health,	31 March 2019	Health, Safety and Emergency Planning Officer / Deputy Chief Executive and Director of Finance

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>There is an increased risk of incidents occurring due to a lack of health and safety awareness of employees due to a lack of training.</p> <p>Training sessions have been put on, it is the employees and the employee's managers responsibility to ensure they are booked onto the course.</p>		Safety and Emergency Planning Officer.		

GROUNDS MAINTENANCE, PARKS AND OPEN SPACES - EXECUTIVE SUMMARY

1.1 Background

We carried out an audit of Grounds Maintenance, Parks and Open Spaces; as at of the agreed internal audit plan for 2018/19. Our objective was to ensure the Council provides an effective grounds maintenance service within the Borough contributing to the better health and well-being of the residents and wildlife of Gedling.

The Council owns and manages a total of 35 parks and 32 play areas, spread throughout the Council's boundaries. These range from the large, rural 'country parks, which includes Bestwood, Burnt Stump and Gedling Country Parks: to the smaller, urban parks and open spaces which provide a range of play, sports and recreational facilities, making them very much, a part of community life. The 'Gedling Conversation' survey of all residents identified in 2017/18, that 77 per cent of households that responded, were satisfied with the quality of the parks and open spaces provided in the Borough. In addition, three of the Council's parks have been recognised nationally and have been awarded 'Green Flag' quality status. These include Arnott Hill Park, which has been awarded 'Green Flag' status for 12 consecutive years. The Green Flag Award recognises and rewards well managed parks and green spaces, and sets the benchmark for the management of recreational outdoor spaces across the UK and the world.

The Council's parks and open spaces are regularly used as venues for community events and organised play schemes. The Council ensures that all parks and open spaces are maintained in order to ensure that they are always clean and safe places for members of the public to use. The Council's public website includes full information on the location and facilities available, at each of the Council's parks and open spaces. Weekly play area inspections are carried out to identify any defects or damage to play equipment which could cause potential harm to user's and appropriate remedial action is taken.

The Parks Development Officer is responsible for identifying and developing new opportunities within parks and to organise events and activities that promote the parks and raise awareness of the facilities that are available in the Borough's parks and open spaces. The Development Officer is also responsible for identifying new sources of funding to fund or co-fund new development projects. Grants totalling over £200k have been obtained in the last three years, from WREN (recycling credits) to fund new play areas and multi-use activity centres. Other sources of funding for enhancement projects include Section 106 community benefits funds and the Community Infrastructure Levy, both of which are funded by developers. The Parks Development Officer is also responsible for developing and supporting 'Friends' groups, for many of the Borough's parks and for coordinating the activities of volunteers who work in parks and open spaces, carrying out a range of skilled and unskilled tasks. During 2017/18; volunteers contributed a total of 1,272.2 equivalent man-days of labour maintaining parks and open spaces.

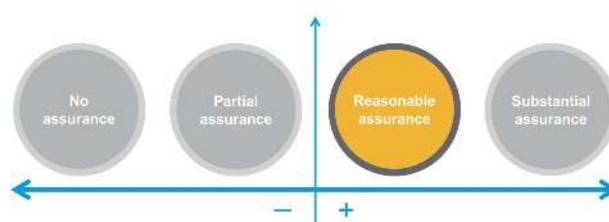
1.2 Conclusion

Our audit testing identified a total of five control weaknesses and as a result: we have raised two 'medium' and three 'low' priority management actions. All five management actions are agreed by management.

Internal audit opinion:

Taking account of the issues identified, the Council can take reasonable assurance that the controls in place to manage this risk are suitably designed and consistently applied.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.



1.3 Key findings

The key findings from this review are as follows:

- The Service Manager, Parks and Street Care produces a detailed Service Plan 2018/19. This identifies the key strengths, weaknesses, opportunities and threats; affecting service delivery, performance levels and customer satisfaction and sets out how and when, key service delivery objectives will be achieved.
- Risk Assessments are carried out for all tasks undertaken by Grounds Maintenance, Parks and Open Spaces staff. All risk assessments are reviewed and updated annually by the Service Manager and clearly identify the hazard and associated risks. Current control and mitigation arrangements are identified for each risk; enabling both inherent and residual risk scores to be evaluated.
- Work programmes / schedules of work are in place which detail the frequency in which work is required for each relevant operational activity. They identify the tools required and any specific training required to operate the tools necessary to complete each task. A summary of the methods to be employed e.g. a safe way of working; are detailed on each work programme. This ensures that each employee knows what to do; what tools are required and what levels of training and competency are needed to complete each task.
- All Grounds Maintenance, Parks and Open Spaces operatives are allocated work on a daily basis. At start of each shift, all staff meet in the Deployment Room and the Supervisors issue all daily work sheets. A Daily Deployment Sheet is maintained up to date and includes details of all work allocated, machinery required, radio call signs and all other contact details, in case of emergency.
- The Council's Fees and Charges are reviewed annually, as part of the budget setting process and are approved by Cabinet. When determining the fees to be charged for hire of sports pitches and facilities, the Head of Services takes into account the current rate of inflation, as advised by Finance and they are bench-marked, to compare charges, with those charged by neighbouring authorities.
- Weekly internal playground inspections are completed to ensure management are made aware of any defects or damage to play equipment. Reported damage or defects are recorded for action and rectified in a timely manner.
- The quality of the Council's Parks has been recognised by the Green Flag awarding body and for eleven successive years, the Council's parks at Arnott Hill Park, Burton Road Jubilee Park and Gedling Country Park, have achieved Green Flag status. There is a strict criteria that must be met before a park can be awarded Green Flag status.
- The 'Gedling Conversation' survey of all residents identified in 2017, that 77 per cent of households that responded, were satisfied with the quality of the Parks and Open Spaces provided in the Borough.
- Key Performance Indicators are established for the Parks and Street Cleansing Service Area. These are monitored regularly and the results are reported.
- All hazardous materials used by the Parks and Street Cleansing Team are recorded on a control register. Risk Assessments and COSHH data sheets are available for all hazardous materials used. Stock control sheets are used for all hazardous materials and all issues are recorded. A weekly stock check is carried out to ensure that all stocks are accounted for.
- All items of plant and equipment are securely stored in Site Safes. these are solid steel reinforced containers with no external indication of what they might contain. Two keys are required to open each site safe and these are stored in a locked key-safe held in the Deployment Supervisors Office. The keys are only issued when an operative is issued with a daily deployment sheet that requires the use of equipment that is contained in a Site Safe.

However, we have identified the following control weaknesses and as a result, we have raised two 'medium' and three 'low' priority management actions. These relate to: -

- The Council has produced a Green Space Strategy covering the period 2012 to 2017. Some amendments and revisions were made in April 2017; however, as a strategic planning document, covering future, medium term strategic planning for the development and management of Parks and Open Spaces, this document is effectively out of date.
- There are no policies or procedures in place to ensure that the Council carries out regular inspections and risk assessments of the tree assets present in its parks and open spaces. A Tree Asset Register should be introduced which identifies each tree; its species; its approximate age; its current condition and any maintenance actions necessary to ensure that it is maintained in a safe condition.
- We found that not all the weekly play area health and safety checks were completed in full.
- Due to staff sickness, delays in raising invoices have occurred. If additional staff were trained in the invoicing process, cover could be provided at times of staff sickness or leave.
- The spreadsheet used to control the raising of sales invoices is old and is no longer fully functional, with links and formula no longer responsive. It requires overhaul and updating to meet current business needs.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non-Compliance with controls*		Agreed management actions		
	Count	Total	Count	Total	Low	Medium	High
Failure to protect and utilise physical assets (Risk Register: 6)	1	(10)	1	(10)	0	2	0
Failure to maintain service standards, customer satisfaction, and/or meet customer expectations (Risk Register: 10)	0	(11)	3	(11)	3	0	0
Total					3	2	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Risk: Failure to protect and utilise physical assets (Risk Register: 6)								
1	The Council has a Green Space Strategy in place. This sets out the Council's vision and objectives for the planning and management of green spaces, throughout the Borough. It has been reviewed and approved by the Council and is available to relevant staff and the public. The Green Space Strategy is linked to the Council's Corporate Plan and reflects the corporate policies of	Yes	No	The Council has produced a Green Space Strategy covering the period 2012 to 2017. Some amendments and revisions were made in April 2017; however, as a strategic planning document, covering future, medium term strategic planning for the development and management of Parks and Open Spaces, this document is effectively out of date. A Green Space Strategy should identify opportunities for the development and improvement of its parks and open spaces, reflecting their importance to the community and to the environment; taking full account of relevant national planning guidelines and local priorities and	Medium	We will ensure that the Council's Green Space Strategy is reviewed and updated, to provide a medium term strategy for the development and improvement of parks and open spaces for the benefit of the whole of the Borough.	30 June 2019	Service Manager - Parks and Street Care

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	"People; Homes; Jobs; Place; Performance and Recreation. It is also linked to Policy 16 and 17 of the Council's Core Strategy.			<p>strategies in terms of bio-diversity and providing recreational opportunities for the community.</p> <p>Without a Green Space Strategy, there is a risk that the Council could be seen as not taking sufficiently seriously; its role in developing and enhancing local facilities for recreation, participation in sports and for making use of parks and open spaces an integral part of life in the Borough.</p>				
2	<p>Missing Control</p> <p>The Council has a procedure in place to ensure that the trees contained within its Parks and Open Spaces are subject to regular inspection and risk assessment; to ensure that no staff or members of the public are put at risk of harm, should any branches or complete trees, fall on unsuspecting park users.</p>	No	-	<p>We confirmed that there are no policies or procedures in place to ensure that the Council carries out regular inspections and risk assessments of the tree assets present in its parks and open spaces.</p> <p>A Tree Asset Register should be introduced which identifies each tree; its species; its approximate age; its current condition and any maintenance actions necessary to ensure that it is maintained in a safe condition.</p> <p>There is a risk that unmanaged and as a result, unsafe trees or branches could fall onto staff working in the parks or members of the public visiting the parks, for recreational purposes. In recent years, a number of injuries have been caused to members of the public, by falling branches and Councils have been</p>	Medium	We will commence a park by park survey of all trees to identify their value in bio-diversity terms, their current condition and create an action plan for their ongoing maintenance.	30 June 2019	Service Manager - Parks and Street Care

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				found liable, due to a lack of a proper tree assessment and management procedure.				

LANDLORD LICENSING - EXECUTIVE SUMMARY

1.1 Background

A review of Landlord Licensing was undertaken as part of the approved internal audit periodic plan for 2018/19.

From 1 October 2018 all privately rented homes in the Netherfield ward required a licence from Gedling Borough Council under a scheme known as 'Selective Licensing'. Under the Housing Act 2004, local authorities currently have powers to introduce selective licensing of privately rented homes to address problems in their area, or any part of them, caused by low housing demand and/or significant anti-social behaviour.

Netherfield is a railway town situated five kilometres east of Nottingham, making up one of the 19 wards served by Gedling Borough Council. It comprises around 2,780 properties, and according to the 2011 census data; 22.5 per cent of the ward is privately rented.

The main characteristics of architecture in Netherfield are rows of terraced Victorian houses. These were built towards the end of the 1800's in order to accommodate the workforce of Colwick sidings; a large railway marshalling yard that was built in stages from 1872, designed for the concentration of coal traffic from Nottinghamshire and Derbyshire Coalfield for transfer to other marshalling yards.

Since the introduction of the Selective Licensing Scheme, a dedicated Licencing Team has been introduced to deal with licence applications and the day-to-day management of Selective Licensing. The Team is currently made up of a Senior Environmental Health Officer, two temporary-contract support staff members and an admin apprentice. Additionally, the Council has a Contact Centre Team who also assist Landlords with the Selective Licence application process.

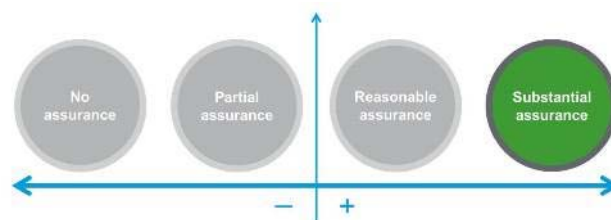
At the time of audit, the Selective Licensing Scheme had received 427 applications since its introduction in October 2018.

1.2 Conclusion

There is an appropriate control framework in place for governing the Selective Licensing Scheme. Our work confirmed that there are adequate controls in place, however testing identified that the controls are not always consistently applied. Areas of improvements have been noted which has resulted in the agreement of one 'low' and one 'medium' priority management actions.

Internal audit opinion:

Taking account of the issues identified, the Council can take substantial assurance that the controls upon which the organisation relies to manage the identified risk(s) are suitably designed, consistently applied and operating effectively.



1.3 Key findings

The key findings from this review are as follows:

Our audit review identified that the following controls are suitably designed, consistently applied and are operating effectively:

- Introduction of the Selective Licensing Scheme across the Netherfield ward was found to be compliant with the requirements documented within the Part 3 of the Housing Act 2004. Through review of documentation it was confirmed that Netherfield is an area with a high concentration of privately rented accommodation and that there is evidence to suggest the following conditions are satisfied;
 - High levels of deprivation;
 - A significant and persistent problem caused by anti-social behaviour;
 - High levels of crime; and
 - Poor property conditions.
- The Council conducted a 12-week public consultation in accordance with the requirements set out in Housing Act 2004. The consultation on Selective Licensing in the Netherfield ward was held between 16 October 2017 and 5 January 2018.
- A proposal report to approve the designation of the Netherfield ward as being subject to Selective Licensing with effect from 1 October 2018 was presented to and subsequently approved by Cabinet on 8 March 2018.
- The introduction of Selective Licensing in Netherfield is key to Gedling Borough Council's Housing Strategy and Corporate Priorities to tackle and improve the quality of homes within the Borough and create a balanced housing market to support social and economic improvements.
- The Council adopted the following methods of informing local landlords within the Netherfield ward regarding the introduction of the Selective Licensing Scheme:
 - Issuance of a Public Notice;
 - Landlord Forum Presentation;
 - Updates on the Council Website; and
 - Gedling Contacts Magazine.
- Landlords can apply for property licences via the Council's website. An online application form is available which allows landlords to pay their part one application fees via online payment. All fees and charges in relation to Selective Licensing are clearly stated on the Council's website.
- Once the correct fees and essential paperwork has been received, acknowledgement is sent to applicant by the Council confirming the received application.
- Upon receipt of a Selective Licence application, the following checks are completed on the landlord and property to determine whether licensing criteria is met:
 - Assessment of management arrangements;
 - Property inspection is arranged and carried out; and
 - Fit and proper assessment (in line with the Fit and Proper Policy).
- If the Council deem the application satisfactory, a draft licence will be prepared and at this point the applicant will be invoiced to pay the second portion of the licensing fee.

- Any breaches of Selective Licensing conditions by landlords are processed in line with the Council's Private Sector Housing Enforcement Policy. Any continual breaches of conditions will result in the Council obtaining a management order for the property in question.
- Any complaints in relation to the Selective Licensing process will be dealt with in line with the Council's Complaints Policy.
- The Council attends the annual South Nottinghamshire Private Landlord Forum with local landlords to provide them with any updates or changes which affect their position as private landlords within the Gedling Borough.
- Quarterly updates are provided to Cabinet in respect of the Selective Licensing Scheme. Additionally, Informal monthly meetings also take place between the Service Manager, Public Protection and the Portfolio Holder for Public Protection to discuss the progress of the scheme.
- The number of Category One and Two Hazards are recorded within the Council's performance management system (Pentana) and are reported with all the Council's Key Performance Indicators (KPI's) to Cabinet on a quarterly basis.
- Procedure notes are in place for the Selective Licensing Team and Call Centre Team to provide guidance in the processing of Selective Licensing.

However, we identified the following exceptions with the Council's established control framework:

- Through testing it was noted that supporting documentation for licence applications was not always transferred/scanned on to the UNIFORM system. As a result, information was having to be sourced from various locations to establish a full audit trail of the application process.
- According to the 2011 census, there are 2,780 dwellings within the Netherfield ward, of which approximately 625 properties (22.5 per cent) are subject to private rental. Based on initial observations, the Council believes around 68 per cent of privately rented properties within the ward have applied for licensing. Therefore, a gap remains of approximately 198 properties who have yet to apply for licensing.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non Compliance with controls*		Agreed management actions		
					Low	Medium	High
Failure to react to changes in legislation.	0	(4)	0	(4)	0	0	0
Failure to maintain service standards, customer satisfaction, and/or meet customer expectations.	1	(10)	1	(10)	1	1	0
Total					1	1	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

2 DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
Risk: Failure to maintain service standards, customer satisfaction, and/or meet customer expectations.								
2	<p>Missing Control</p> <p>Any 'non-registrations' within the Netherfield ward are contacted to instruct them that they will require a license to continue acting as a private landlord.</p> <p>Further failure to apply for licensing will result in the Council taking enforcement action against the Landlord.</p>	No	-	<p>At the time of audit, the Selective Licensing Scheme had received 427 applications since its implementation in October 2018 across the Netherfield ward.</p> <p>According to the 2011 census, there are 2,780 dwellings within the Netherfield ward, of which approximately 625 properties (22.5 per cent) are subject to private rental.</p> <p>Based on initial observations, the Council believes around 68 per cent of privately rented properties within the ward have applied for licensing. Therefore, a gap remains of</p>	Medium	Once the initial applications to the Selective Licensing Scheme have been processed and issued, a process will be developed and implemented to identify any 'non-registrations' within the Netherfield Ward.	31 October 2019	Service Manager, Public Protection

Ref	Control	Adequate control design	Controls complied with	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
				<p>approximately 198 properties who have yet to apply for licensing.</p> <p>Discussion with the Service Manager - Public Protection confirmed that the Council is currently working through the large influx of initial applications to the scheme, with a view of having all licenses processed and issued within 12 months of the initial application date.</p> <p>Once this has been completed, the Council will determine the best method to identify all 'non-registrations' and potentially close the gap of landlords within the ward who have not signed up for a licence.</p> <p>If all 'non-registrations' within the Netherfield ward are not identified and actioned, there is a risk of non-licensed landlords providing private rental accommodation which is not compliant with the Council's requirements.</p>				

DEVELOPMENT MANAGEMENT - EXECUTIVE SUMMARY

1.1 Background

A review of Development Management was undertaken at Gedling Borough Council (the Council) as part of the approved internal audit periodic plan for 2018/19.

Planning and Building Control at the Council is undertaken by the Development Services Department. The Department is led by the Service Manager - Development Services and is assisted by two Principal Development Management Officers, five Planning Officers, a Service Support Team Leader and a team of administrative staff. IDOX Uniform software system is used to manage planning and building control and is linked to an electronic document management system and interfaces.

Planning applications can be received in paper form or through the Planning Portal (external website which provides a hub of tools, services and guidance on planning and building). On receipt of the paper applications the service support staff log the applications onto Uniform. Applications received through the Planning Portal are upload onto Uniform via an interface. Planning appeals are administered and undertaken by the Planning Inspectorate (an executive agency, sponsored by the Ministry of Housing, Communities and Local Government and the Welsh Government) which is independent of the Council.

For the period April 2018 to December 2018 the Council received 624 planning applications.

For major planning applications determined within 13 weeks the national target is set at 60 per cent. The Council's target is set at 90 per cent and performance for Quarter two was reported at 100 per cent and for quarter three at 94.4 per cent. Current year performance exceeds the Council's target.

For minor planning applications determined within eight weeks the national target is set at 65 per cent. The Council's target is set at 70 per cent and performance for quarter two was reported at 94.6 per cent and for quarter three at 97 per cent. This comfortably exceeds the Council's target.

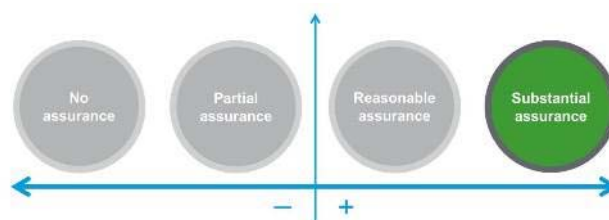
For other planning applications determined within eight weeks the national target is set at 80 per cent. The Council's target is set at 80 per cent and performance for Quarter two was reported at 99.1 per cent and for quarter three at 93.3 per cent. This again exceeds the Council's target.

1.2 Conclusion

This review has confirmed that Gedling Borough Council has in place adequate controls surrounding Development Management and that these controls are sufficiently complied with. However, we identified some weaknesses in the controls and have agreed four 'low' category management actions. Further details on the four 'low' category management actions agreed are provided in section 2 of this report.

Internal audit opinion:

Taking account of the issues identified, the Council can take substantial assurance that the controls upon which the organisation relies to manage the identified risk(s) are suitably designed, consistently applied and operating effectively.



1.3 Key findings

The key findings from this review are as follows:

- On review of the Council's website it was established that planning and building control information is published on it for public viewing.
- The Council has adopted the Aligned Core Strategy (Part one Local Plan) (ACS). The document provides a broad guide to development and growth in the Borough, setting out locations for major sites (over 500 houses); key issues faced by the Borough to 2028; and co-ordinates policies, priorities and programmes together with the public resources to deliver them. The ACS is published on the Council's website.
- The Local Planning Document works with the ACS to shape future development in Gedling Borough by planning for new homes, jobs and infrastructure. These documents are used to help decide planning applications and guide the location and design of development in Gedling Borough. The Local Planning Document was adopted on 18 July 2018. There are also Supplementary Planning documents (SPDs) and these add further detail to the policies in the Local Plan.
- The Council has also published a number of informal planning guidance documents and these have a similar function to SPDs, although they have less weight in determining planning applications as they have not been formally consulted on or their contents may not be appropriate for an SPD for example: Air Quality and Emissions Mitigation (2018).
- For a sample of 20 planning applications, testing confirmed where appropriate the fees were received prior to the planning application being validated and process commencing.
- All planning decisions are reviewed by the Service Manager – Development Services or a Principal Planning Officer before being issued to the applicant. For a sample of 20 planning applications testing confirmed that the decision was communicated to the applicant and a copy of the letter was maintained on Uniform. For the sample of 10 Appeals, testing established that in all cases the decision was reported to the Planning Committee.
- Testing confirmed that the fees charged by the Council for planning application are as set out in the Town and Country Planning (Fees for Applications, Deemed Applications, Requests and Site Visits) (England) (Amendment) Regulations 2017.
- Key Performance Indicators (KPI's) on Major planning applications determined at 13 weeks, Minor planning applications determined within eight weeks and other planning applications determined within eight weeks are produced and monitored for development management each month. A review of the Planning Committee minutes of meetings and papers for 2018 confirmed that the KPI's are reported each quarter.
- Staff attend Continuous Professional Development (CPD) events throughout the year including events hosted by East Midlands Council's as appropriate. Changes to legislation are discussed at monthly team meetings and key members of staff prepare email briefing notes which are circulated to the wider team.
- Testing confirmed for the last year to date the performance returns were submitted quarterly to the Department for Communities and Local Government (DCLG) as required.

However, testing identified the following weaknesses and as a result we have agreed four 'low' priority management actions:

- Procedural guidance is not in place for the tasks undertaken by the staff assisting the Planners.

- For a sample of 20 planning applications testing confirmed that in one case the application was made for 69 properties and the correct fee had been received. This was subsequently changed to 71 properties and planning permission was granted for 71 properties, however, no additional fee was requested from the applicant. In another case the fee was charged for a domestic dwelling instead of a commercial dwelling. In six cases it was noted that the method used to make the payment was not recorded on Uniform.
- For a sample of 20 applications, testing identified that in two cases the target times set for determining the planning applications were not met, and an extension had not been agreed with the applicant.
- For a sample of 10 appeals, testing identified that all the information relating to the appeal was not always recorded onto Uniform; in three cases the appeals file could not be located at the time of the audit; and in three cases the decision was not maintained on the appeals file.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non-Compliance with controls*		Agreed management actions		
	Low	Medium	High	Low	Medium	High	
Failure to maintain financial integrity (Risk Register: 2)	0	(13)	4	(13)	4	0	0
Failure to protect and utilise physical assets (Risk Register: 6)							
Total					4	0	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

RISK MANAGEMENT - EXECUTIVE SUMMARY

1.1 Background

A review of Risk Management was undertaken as part of the approved internal audit periodic plan for 2018/19. Our review was undertaken to ensure processes are in place to identify, assess and manage the risks facing the Council.

Effective risk management assists in achieving the Council's vision and strategic objectives and helps to optimise the quality and efficiency of its service delivery. Therefore, it is imperative that there is an effective risk management system and assurance framework in place. The achievement of the Council's strategic objectives is underpinned by the effectiveness of the controls identified to mitigate the principal risks which could impact on the objectives being achieved.

The Council has an established Risk Management Strategy and Framework in place, which is designed to reflect current best practice in Local Authority Risk Management. The Risk Management Strategy and Framework were last reviewed in July 2017 and are next due for review in July 2020.

The risks identified are recorded at either the corporate level, in a Corporate Risk Register or at an operational level, in Service Risk Registers. This two-tier approach ensures that the highest level strategic risks, those which present the greatest challenge to the Council, are identified, evaluated and closely monitored. All risks, both strategic and operational, are monitored by the Senior Leadership Team, which discusses the risk registers quarterly and then report to the Audit Committee. This enables risk scores to be challenged and re-evaluated and facilitates discussion regarding emerging and changing risks.

A formal Corporate Risk Management Scorecard is presented by the Financial Services Manager on a quarterly basis to the Audit Committee. The purpose of the scorecard is to update the Committee on the current level of assurance that can be provided against each corporate risk.

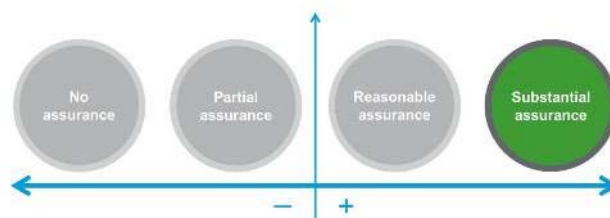
Risks are plotted on a matrix and categorised as 'red', 'amber' or 'green', depending upon where they have been ranked in terms on likelihood and impact. At the time of audit, the Council had 13 'live' risks recorded on its Corporate Risk Register. Of the 13 risks documented, there were two risks within the 'red' category and five risks within the 'amber' category. The remaining six risks were classified as a 'green' current risk level.

1.2 Conclusion

There is an appropriate control framework in place for governing Risk Management. Our review concluded that key controls are being applied adequately and effectively. We identified no issues that required us to comment upon or to raise management actions that would require improvement actions to be taken.

Internal audit opinion:

Taking account of the issues identified, the Council can take substantial assurance that the controls upon which the organisation relies to manage the identified risk are suitably designed, consistently applied and operating effectively.



1.3 Key findings

The key findings from this review are as follows:

- The Council's Constitution contains high level key controls and defines the ownership arrangements for the management of all levels of risk within the Council.
- The Council has a Risk Management Strategy in place and is approved by the Audit Committee and by full Council.
- The latest Risk Management Strategy includes guidance on the identification, scoring and assessment, evaluation, treatment and reporting of risks.
- The Council has determined its risk appetite and this to set out on a risk by risk basis in the Corporate and Service Risk Registers.
- A Senior Leadership Team is in place which meets each quarter to discuss the risks faced by the Council.
- The Audit Committee receive quarterly reports with reference to the effectiveness of risk management procedures and notification of Internal Audit management actions in respect of these.
- A Corporate Risk Register is maintained which contains key strategic risks and is subject to review at each quarterly Senior Leadership Team meeting.
- A risk register is maintained for each service area and which is updated and reviewed each quarter by the Service Manager before being reported to the Senior Leadership Team.
- All risks have been assigned a risk owner who is responsible for assessing and monitoring that risk.
- Risks are documented and assessed in terms of likelihood and impact.
- Risks are scored consistently using pre-determined definitions and plotted on the risk registers correctly.
- Any significant service area risks are raised at Senior Leadership Team meetings and if necessary, are evaluated and are escalated into the Corporate Risk Register.
- Controls are put in place to mitigate each risk and these are documented on the risk register.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Risk	Control design not effective*		Non Compliance with controls*		Agreed management actions		
	Low	Medium	High	Low	Medium	High	
Inadequate and/or inappropriate Risk Management Strategy in place at the Council.	0	(10)	0	(10)	0	0	0
Total	0	0	0	0	0	0	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

GENERAL DATA PROTECTION REGULATION (GDPR) GOVERNANCE - EXECUTIVE SUMMARY

1.1 Background

From 25 May 2018 the General Data Protection Regulations (GDPR) replaced the EU Directive 95/46/EC.

Whilst many of the GDPR's main concepts and principles remain largely the same as those in the former Data Protection Act 1998, there are significant new elements and enhancements which will require Councils to perform some specific compliance activities for the first time. In particular, GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability.

We have been commissioned to perform an agreed upon procedures assignment of the current data governance processes, procedures and controls. Our report is a factual report and we do not provide a level of assurance, or internal audit opinion, and should not be taken to provide such.

1.2 Headline findings

The key findings from this review are as follows:

Business Processes and Data Discovery

- The Council has designed an Information Asset Register (IAR) template and these were issued to departments for completion. All departments have completed and returned their IAR's, however, the returns require review by the Council as these have identified some queries which require resolution before the process is fully completed.

Third Parties

- Third parties have been identified through the IAR's and contracts register where in scope data is transferred, and the third parties have been contacted to update their contract terms and conditions to reflect the changes of GDPR. However, there are still third parties that do not have up to date sharing agreements and require follow up by the Council.

Data Ownership

- Data owners have been identified as part of the IAR process.

Data Security System Level Controls

- An Information Security Policy is in place and staff and visitors are required to read and sign the Personal Data Security Commitment. However, it has been identified that a control weakness exists where not all contractors or third parties are ID checked prior to being provided access to the Council offices.

Data Storage and Retention

- A Data Retention Policy is in place but still requires updating to reflect GDPR. Storage locations have been identified as part of the IARs and retention periods have been assigned in line with the retention schedule posted on the Council website. However, not all retention periods have been documented on the IAR's.

Awareness

- GDPR training has been undertaken by staff members and a GDPR Plan is in place and is updated by the Data Protection Officer and Deputy Data Protection Officers.

Data Policy, Roles and Responsibilities

- The Council's Data Protection Policy has been reviewed and updated due to the implementation of GDPR. However, it was identified that the job description of the Data Protection Officer has not been updated to explicitly document the associated roles and responsibilities required.

Individuals' Rights

- The Council has published a privacy statement for each department on its website which has been updated due to the iGDPR requirements. It was identified that the subject access request procedure is yet to be updated to reflect that no fee can be charged.

Consent

- It was noted that consent gained through application forms includes unticked boxes (to facilitate explicit consent). Consent is also documented for each data item on the IAR's, however, it was identified that this is not always completed, and areas may have been documented as consent which actually have a different legal basis as opposed to consent.

Data Breaches

- The current Information Security Policy has been updated to reflect GDPR and the 72-hour reporting requirements of a data breach. A data breach log and forms have also been created.

2 DETAILED FINDINGS

The results of our testing are set out below.

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
1	Business Processes and Data Discovery	<p>Information asset registers (IAR) are in place for all departments at the Council and these were carried out by the departments individually with assistance from the Deputy Data Protection Officers.</p> <p>At the time of the audit there was a total of 17 IAR's covering all Council departments.</p> <p>Information captured in these registers includes:</p> <ul style="list-style-type: none"> • Purpose of processing the data; • Type of data; • Legal grounds for processing; • Retention periods; • Approximate users and data subjects; • Recipients and transfers; and • Data owners. <p>Through review of the IAR's it was identified that notable omissions existed for some departments for retention periods, basis for processing and volumes of data.</p> <p>The asset registers were completed and reviewed in early 2018 or late 2017 and therefore prior to GDPR being live. As a result, these registers require updating/reviewing to ensure they are current, and no omissions are present.</p> <p>Furthermore, a lack of consistency was identified between departments with how the registers had been completed. Although the table headings were identical on all registers, some departments have left boxes empty whereas some have documented the cell to be</p>	<p>A review of all IAR's will be completed ensuring all cells are completed in full.</p> <p>Furthermore, a periodic review will be implemented to ensure registers remain up to date.</p>	Data Protection Officer/Deputy Data Protection Officer	30 April 2019

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		<p>“n/a” which could cause an issue when merging registers.</p> <p>This action is already planned and included on the Council’s GDPR action plan.</p> <p>Without a comprehensive and accurate record of the location and origin of all personal data held in house and shared with third parties, there is an increased risk of non-compliance with the requirements of the new Act relating to information held.</p> <p>Examples of potential non-compliance include:</p> <ul style="list-style-type: none"> • The inability to notify third parties of any inaccuracies in data shared with them, due to lack of awareness of the information sharing arrangements in question; and • Non-compliance with the GDPR accountability principle by demonstrating that the Council has effective policies and procedures in place for the management of personal data. 			
2	Third Parties	<p>As part of the IAR’s, it is identified for each data processing activity of the data is received from third parties, if data is shared with third parties and if a data sharing agreement is in place.</p> <p>Following the completion of the IAR’s, review of the contract’s registers, and a list of all contracts being passed to the Legal Department, a letter was issued to all third parties. This was to ensure an up to date sharing agreement is in place.</p> <p>At the time of the audit, a number of third parties had not responded and thus up to date sharing agreements were not in place. It was identified however, that new contracts and tenders entered have a new sharing agreement in place. A Legal Intern is due to start with the Council and their task will be to follow up third party responses.</p>	<p>A review of all IAR’s will be conducted with any third parties identified being reconciled to the list of third parties to whom data is shared with to ensure the list is complete.</p> <p>Third parties will be contacted to agree to the amended terms and conditions.</p>	Data Protection Officer/Deputy Data Protection Officer	31 December 2019

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		<p>Instances on the IAR's were also identified where the department did not document who the information was shared with and noted question marks or left the cell blank. This action is already planned and included on the Council's GDPR action plan.</p> <p>There is an increased risk of non-compliance with the requirements of the new Act relating to information held.</p>			
3	Data Ownership	For the 17 IAR's completed by the Council, it was identified that data owners have been explicitly documented.	No Action	No Action	No Action
4	Data Storage and Retention	<p>Data storage and retention locations have been identified as part of the IAR's. However, it was noted on some IAR's that departments are unsure of the specific retention periods for data and have left this cell blank or with a question mark.</p> <p>A Records Retention and Disposal Policy is in place and was last updated in July 2011. This Policy has no referral to GDPR and requires updating to ensure it is current.</p> <p>The Deputy Data Protection Officer is in the process of completing the review of this document and will be presenting this to the Director of Organisation Development and Democratic Services for review.</p> <p>There is a risk that where retention periods are unknown, not documented and not recorded in a schedule/policy, data may be kept for longer than necessary and thus conflicts with data protection regulations.</p>	<p>a) A review of all IAR's will be conducted to ensure all retention periods are documented and this will be matched to the updated Records Retention and Disposal Policy.</p> <p>b) The Records Retention and Disposal Policy will be updated, setting out standard retention periods for specific categories of data, based on purpose and business need. Data should then be deleted on a cyclical basis in line with retention requirements.</p>	Deputy Data Protection Officer	31 May 2019
5	Data Storage and Retention	A privacy impact assessment (PIA) is a process which helps an organisation to identify and reduce the privacy risks of a project i.e. to ensure that the project considers 'privacy by design'.	No Action	No Action	No Action

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		<p>An effective PIA should be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.</p> <p>A DPIA process form is in place documenting the process for identifying when a PIA is required and how it should be conducted. Within the document is the template for staff to follow when conducting a PIA to understand the extent of the processing of data with reference to its scope, context and purpose.</p> <p>It was informed by the Data Protection Officer that departments are currently completing DPIA's for existing systems of high risk and these are to be completed by the end of March 2019. Any new projects require a DPIA and this process is embedded for this.</p>			
6	Data Security System Level Controls	<p>Physical access to the building is via the main entrance for anyone or side entrances for staff only. To access the areas off limits to the general public, a Council issued swipe card is required.</p> <p>General access to computers is via username and password with specific systems also having username and password login access.</p> <p>Confidential waste is collected in marked bins and are either shredded internally or externally collected and shredded.</p> <p>An Information Security Policy is in place and was last reviewed in August 2018 which contains in depth guidance on IT security such as:</p> <ul style="list-style-type: none"> • Backups; • Patching; 	A process document will be created outlining the responsibilities of reception staff to ensure all contractors are ID checked prior to being issued with a building swipe card.	Service Manager Customer Services and Communications	31 May 2019

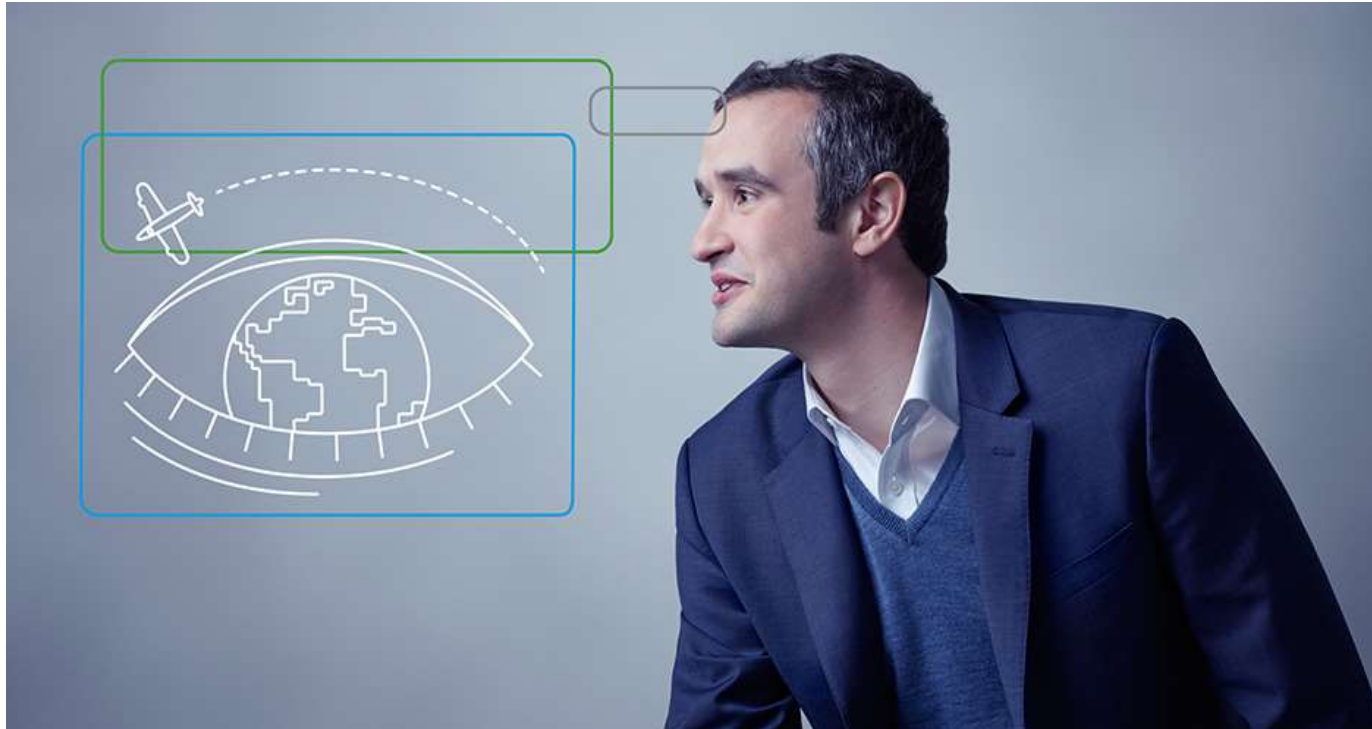
Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		<ul style="list-style-type: none"> • Password requirements; • Remote access; and • Access controls. <p>In addition to the Information Security Policy, staff and visitors requiring IT access are required to read and sign the Personal Data Security Commitment.</p> <p>However, a control weakness has been identified with regards to access to the Council building where contractors are not checked for identification prior to receiving a swipe card. As a result, there is an increased risk of a data breach occurring with the possibility for unauthorised personnel to receive access to unauthorised areas.</p>			
7	Awareness – Management	<p>It was informed by the Data Protection Officer that a cross-county working group was established (Nottingham Information Officers Group) to work towards GDPR compliance. These meetings are attended by the Data Protection Officer or the Deputy Data Protection Officer. The Group work together to create core documents or processes which can then be adapted by each Council to tailor to their specific needs.</p> <p>This Group has continued to exist even after GDPR has gone live. In addition, the Council has in place a GDPR action plan with high level actions, notes on the action to be completed and a deadline date. The key areas for GDPR compliance are listed with remaining actions to be completed. This is updated by the Data Protection Officer.</p> <p>Cabinet were presented with a report on 3 May 2018 to advise the Members in relation to the implications of GDPR and to update Members on the steps the Council were taking to ensure compliance. GDPR training has also been presented to Members.</p>	No Action	No Action	No Action

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
8	Awareness – All Staff	<p>Training has been provided to members of staff via the medium of presentations conducted by the Data Protection Officer. These were obtained during the audit and confirmed to detail the key principles and processes of GDPR. Additional briefings have been issued to all staff or departments via email or the intranet and a GDPR employee guide has been created and issued to all staff.</p> <p>Training has also been provided to Service Managers of departments on more specific tasks such as DPIA's. Two training sessions on DPIA's have taken place with one more to be completed in January 2018.</p> <p>The Council are currently looking into the introduction of E-Learning to deliver GDPR training.</p>	No Action	No Action	No Action
9	Data Policy, Roles and Responsibilities	<p>It was confirmed a Data Protection Policy was in place for the Council and this was updated in 2018 to reflect the changes as a result of GDPR.</p> <p>Through review of the policy, it was identified the key areas of GDPR were covered including:</p> <ul style="list-style-type: none"> • Overview of the Data Protection Legislation; • Data Protection Principles; • Gathering Data; • Disclosure of Data to Third Parties; • Security of Data and Access to Data; and • Retention of Data. <p>The policy is available to staff via the shared drive and documents key contacts of the Data Protection Officer and supporting policies to provide guidance and advice on data protection matters.</p>	No Action	No Action	No Action

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
10	Data Policy, Roles and Responsibilities	<p>The allocation and responsibilities pertaining to data protection within the Council had been defined or explicitly documented.</p> <p>Through review of the Data Protection Policy, it was confirmed readers are signposted to the Legal Department for any queries relating to data protection or using the specific Data Protection Officer email address.</p> <p>Through review of the Council website it was also confirmed that the Data Protection Officer is detailed and how to contact them with any queries or requests.</p> <p>In May 2018 a report was presented to Cabinet detailing the changes of GDPR and the requirement for a DPO to be in place. The report explains the reasons for the DPO and who the Data Protection Officer is. The documented also informed of two Deputy Data Protection Officers to assist in the role.</p> <p>These were all approved by Cabinet at the meeting in May 2018.</p> <p>However, it was informed by the Data Protection Officer that their job description from their current role had not been updated and therefore not explicitly defined and this could lead to an increased risk of lack of accountability and leadership with regard to ensuring compliance with the GDPR arrangements. This in turn could lead to financial penalties and reputational damage.</p>	<p>Upon reviewing the success of the roles of the Data Protection Officer in the current Council structure in May 2019, the job description of the Data Protection Officer will be updated.</p>	Data Protection Officer	30 June 2019
11	Individuals' Rights	<p>The following work was being undertaken to address the new rights for individuals:</p> <p>Privacy statements for all departments have been created and are included on the Council website for information. The details included on the privacy statements are:</p> <ul style="list-style-type: none"> • What personal data is collected; 	<p>The subject access request procedure will be updated to reflect the current requirements of GDPR.</p>	Data Protection Officer/Deputy Data Protection Officer	31 May 2019

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		<ul style="list-style-type: none"> • What the data is used for; • How long data is kept for; • Lawful basis for processing the data (and the GDPR Article it relates to); and • Who the data is shared with and a list of the rights available to the individual. <p>The rights of individuals on the privacy notice are up to date and clearly defined. A subject access request procedure has been created outlining the process to be followed when subject access requests are received, however, the document requires updating to disclose that the fee of £10.00 is no longer to be charged.</p> <p>There is a risk staff are unaware of the process and may attempt to charge a fee for a subject access request which is not compliant with GDPR.</p>			
12	Consent	<p>Through review of a sample of application forms and consent methods in place for the Council, it was apparent consent gained was explicit with unticked boxes. Furthermore, the consent gained also has options to “opt in” as opposed to “opt out” in line with GDPR expectations.</p> <p>Consent is documented within the Data Protection Policy and provides detailed guidance to staff on the processes and legislation to be followed with regards to consent. As part of the IAR’s, how consent is gained and the lawful basis for processing is required to be documented. However, through review it was identified for some of the IAR’s the consent information has not been detailed. Furthermore, through discussion with the Data Protection Officer, the Council do not use consent as the legal basis for processing where possible and the IAR’s require review to confirm this.</p> <p>Without undertaking a review and updating consent processes in relation to personal data processing, there</p>	The IAR’s will be reviewed and all consent processes and legal basis for processing will be documented.	Data Protection Officer/Deputy Data Protection Officer	31 May 2019

Ref	Area	Findings summary	Actions for management	Responsible owner	Implementation date
		is an increased risk of a breach of the new GDPR rules regarding consent, with associated increased risks of litigation and loss of reputation.			
13	Data Breaches	<p>Through review of the Information Security Policy it was confirmed that the data breach process is documented with the requirements to report within 72 hours of becoming aware.</p> <p>Furthermore, the internal reporting process is also documented. This process is also documented within the Data Protection Policy.</p> <p>A standardised Data Protection Breach Incident Report is in place to be completed by any member of staff immediately after detecting a breach. Information obtained through this form is:</p> <ul style="list-style-type: none"> • When the breach occurred; • How it was detected; • What happened; • What information has been compromised; and • Any action taken to mitigate the effect. <p>At the time of the audit a total of 26 breaches had been reported internally with two escalated to the ICO. These are recorded on a breach log.</p>	No Action	No Action	No Action



ETHICAL PHISHING CAMPAIGN – REVISED DRAFT REPORT

Gedling Borough Council
27 February 2019

Contents

- Executive summary
- Introduction
- Scope and approach
- Phishing event 1
- Phishing event 2
- Phishing benchmarking
- Conclusion
- Next steps

Executive Summary

- We conducted two phishing exercises against a sample population list of 413 members of staff in November and December 2018. The pre-texts were agreed in advance.
- The first (spear phishing) appeared to come from inside the organisation, notifying staff of an IT issue.



- The second (generic phishing attack) was confirmation of a large purchase order from Amazon.



- IT controls initially prevented some emails from being sent, only once they were white-listed at the firewall were they received. However, others went through by-passing controls.



‘It’s the emails you **don’t** identify as
“phishing” that are the problem.’

Introduction

- Phishing is the practice of targeting many individuals with enticing e-mails in order to trick at least some of the recipients into opening an attachment or going to a specific web site. The aim is to steal confidential details or download malicious content.
- Spear phishing is a more advanced type of phishing where the content of the scam is based on research specific to the target. The target could be an individual, organisation or business.
- A simulated phishing campaign provides tangible benefits to a security conscious organisation:
 - The results will benchmark the organisation's vulnerability to a phishing attack by providing metrics on what percentage of their employee population is likely to fall victim to a genuine phishing e-mail.
- Attackers only need to attract one phishing click to be successful, whilst staff have to get it right 100% of the time. Every successful click on a phishing e-mail can be seen as an 'opportunity' for the hacker.

Scope and Approach

- Following the completion of a cyber security review performed as part of the internal audit plan, we were engaged by the Head of ICT at Gedling Borough Council to carry out a simulated phishing and spear phishing campaign to assess the level of user awareness in respect of current cyber risks.
- The timing, scope and content of the exercise was agreed with the Head of ICT and his staff.
- We performed two distinct exercises over a period of **three weeks** (27/11/18 – 17/12/18) to ensure that the recipients had ample time to click the links before the campaign was closed.
- The exercise recorded what the individuals who received the e-mails did (Ignore, Open, Delete, Click, Notify).

Scope and Approach

PHISHING EVENT 1

- The number of users in the sample population was **413** and the following email domain was used : @boroughofgedling.co.uk.
- The text of the e-mail was agreed between RSM and agreed with the Research and Development Manager, IT Support.
- The user sample was supplied to RSM by Gedling Borough Council.

PHISHING EVENT 2

- The number of users in the sample population was **413** and the following email domain was used: @amazon-orders.net
- The text of the e-mail was agreed between RSM and agreed with the Research and Development Manager, IT Support.
- The user sample was supplied to RSM by Gedling Borough Council.

Firewall defences deployed to protect Gedling Borough Council from email threats

- Cloud based filtering service: Email Laundry.
- On premises Sophos email appliance.
- Exchange based checks: Sophos PureMessage.

Phishing event 1

- The 'From Address' used by RSM was admin@it-helpdesk.systems.
- The link pointed to the following when hovered over: <https://boroughofgedling.co.uk>

Email pre-text

Your Shared Drive G:\ is full.

24GB 25GB

Dear {{FirstName}}

Files stored on your shared G drive have now significantly exceeded the limit assigned to you. No further files will can be saved to your drive and any attempts to add additional files to this volume will not be saved and IT will not be able to recover those documents. Please take action now to ensure that work is not lost.

What should you do?

Please login to your network account via the Citrix web-app portal [here](#). Once logged in you will either need to delete documents no longer need or archive documents to alternative media.

Do you need more information?

We have some helpful information on the intranet regarding storage settings. Follow this link: <http://intranet.gedling.gov.uk.com>

--
Gedling Borough Council Information Technology Services

This message is generated automatically by the server when you exceed the assigned capacity of your allocated space on drive G:\. Please follow the instructions in the email to resolve this issue or contact your network administrator.

Landing page

CITRIX Sign In

Username

Password [Reset password](#)

Keep me signed in

Sign in

[Create Citrix Account](#)
[Can't access your account? Let us know!](#)

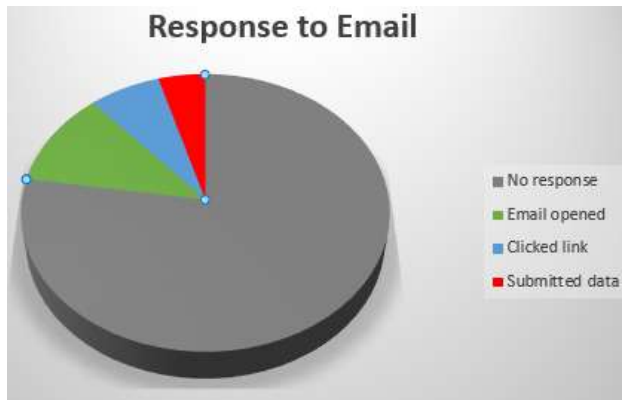


Phishing event 1 - Launch

- We sent initial e-mail from admin@it-helpdesk.systems.
- The simulated phishing campaign upon Gedling Borough Council was launched on 26/11/2018 in the morning (6:32am) and continued until 10:47am on 27/11/2018 for all supplied email addresses. One recipient accidentally received two identical emails.
- The phishing campaign remained open until 4:00pm on Friday 14 December 2018.

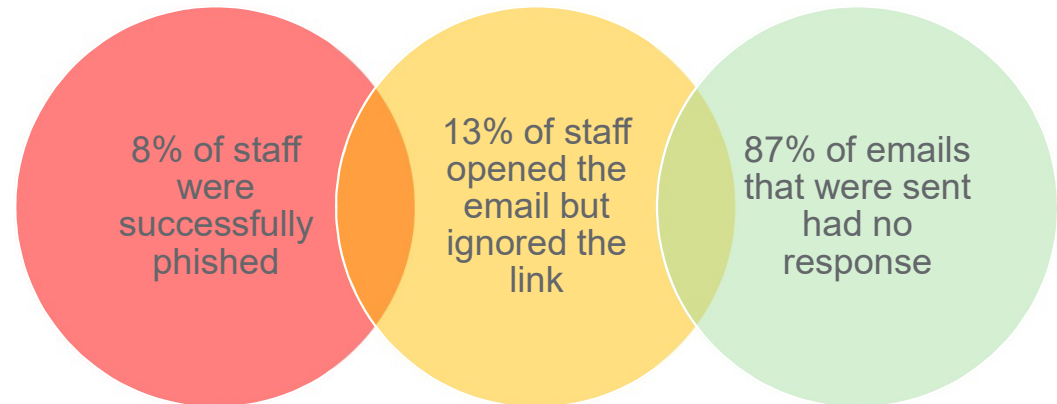
Phishing event 1: Final results

21 of 413 user gave away their username and password



Emails sent	No response	Email opened	Clicked link	Submitted data
413	360	52	32	21

Phishing test results



It should be noted that these e-mails by-passed the firewall controls.

Phishing event 2

Your Recommendations Your Orders Amazon

Shipping Confirmation

Order # [1001 December 2018](#), Delivery slot: 8am - 12pm


Hello {{ FirstName }} {{ LastName }}

Thank you for shopping with us. We thought you'd like to know that we shipped your item, and that this completes your order. Your order is on its way, and can no longer be changed. If you need to return an item from this shipment or manage other orders, please visit [Your Orders on Amazon](#).

Your estimated delivery date is:	Your order was sent to:
16th December 2018, delivery slot: 8am - 12pm	{{ FirstName }} {{ LastName }} 209 South Street Dudley West Midlands, DY32 0BS United Kingdom

Depending on the ship speed you choose, it may take 24 hours for tracking information to be available in your account.

Shipment Details

	Apple MacBook Pro (13 Inch Retina, 2.3 GHz Quad-Core Intel Core i5, 8 GB RAM, 256 GB SSD)	£2399.99
---	---	----------

Item Subtotal:	£2399.99
Shipping & handling:	£102.00
Free shipping discount:	-.00
Total Before Tax:	£2501.99
Shipment Total:	£2702.99
Paid by Visa:	£2702.99

You have only been charged for the items sent in this shipment. Per our policy, you only pay for items when we ship them to you.

Other Items That Have Shipped

For order # [8am - 12pm 16th December 2018](#)
Placed on 11/14pm 09th December 2018

Delivery Estimate: 8am - 12pm 16th December 2018
[Apple MacBook Pro \(13 Inch, 2.3 GHz Quad-Core Intel Core i5, 8 GB RAM, 256 GB SSD\)](#)

Returns are easy. Visit our [Online Return Center](#).
If you need further assistance with your order, please visit [Customer Service](#).

- The 'From Address' used was no.reply@amazon-orders.net.
- The link pointed to the following when hovered over: <https://amazon-orders.net>.
- Users clicking the link were taken to the following landing page.

<https://amazon-orders.net/?rid=76GH591>

Sign in

E-mail (phone for mobile accounts)

Password [Forgot Password](#)

[Sign in](#)

Keep me signed in. [Details](#)

[New to Amazon?](#)

[Create your Amazon account](#)



Phishing event 2 - Launch

- We attempted an initial e-mail from @amazon-orders.net. This was successfully blocked by the spam filtration systems.
- In order to allow the test to proceed, emails from @amazon-orders.net were explicitly white listed by ICT to enable the phishing campaign to deliver emails to the users.
- The initial blocking of the attempted e-mail shows that the firewall systems were operating effectively.
- This simulated phishing campaign upon Gedling Borough Council was launched on 11/12/2018 in the afternoon (9:56am) for all the supplied email addresses on the list provided by the Head of ICT.
- The phishing campaign ended and was closed on 17 December 2018 at 5:00pm.

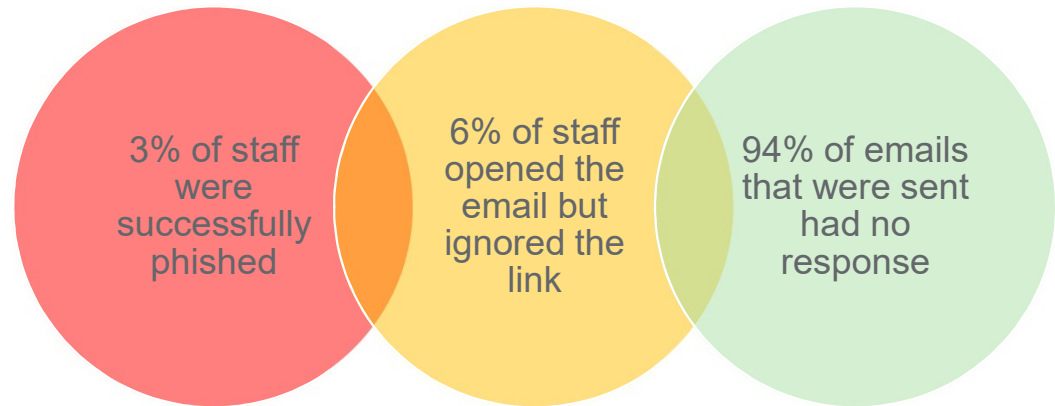
Phishing event 2: Final results

11 users of 413 clicked the link.
1 user supplied their password.



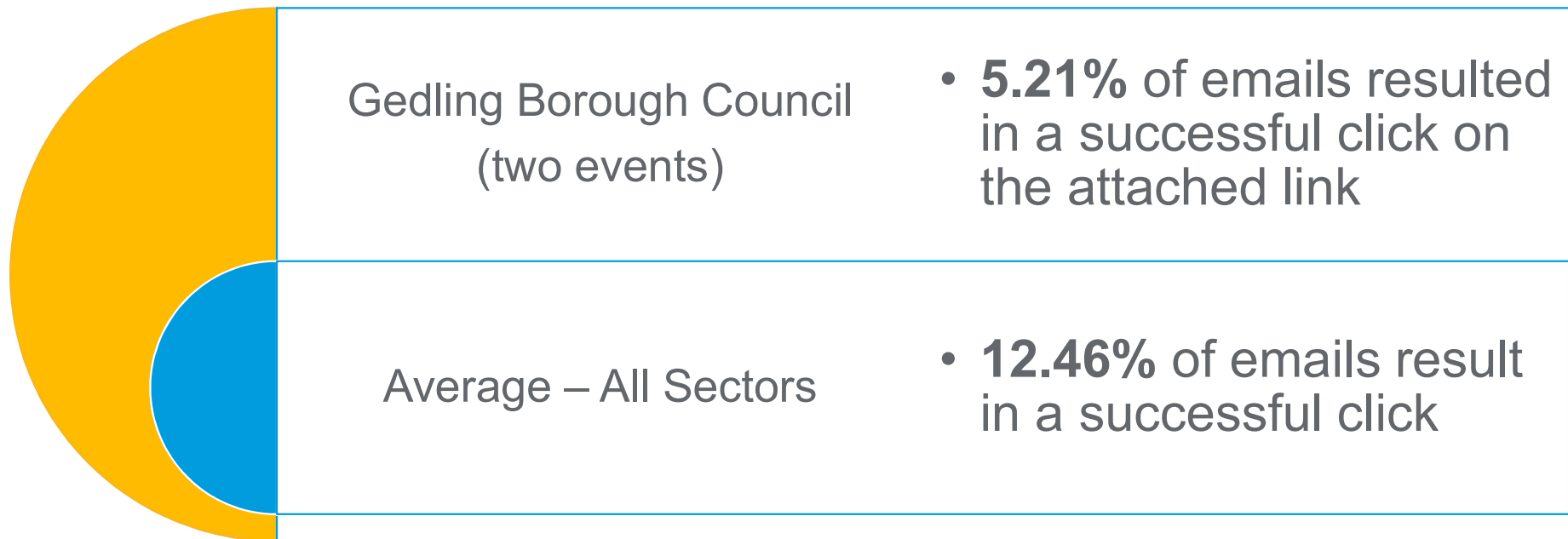
Emails sent	No response	Email opened	Clicked link	Submitted data
413	388	25	11	1

Phishing test results



It should be noted that these e-mails had to be allowed through the firewall by ICT in order for the test to proceed.

Non-spear phishing benchmarking



- The highest response we have recorded is **51.5%**.
- The lowest response we have recorded is **1%**.

Conclusion

We would draw attention to the following **positive** aspects of the exercise:

- The spam filters did their job and prevented the initial e-mails when sent from our own SMTP (email sending) server.
- Very low password submission rates for amazon based pre-text.
- Some staff reported the e-mails to either the ICT Department of the Director of Finance and voiced their concerns.
- The results of this exercise are an improvement from the previous review performed in August 2017. This is due to improved staff awareness through the delivery of training to all staff detailing email phishing and scams. The previous review resulted in an overall success rate of 26.69% compared to this years result of 5.21%. This is a significant improvement.

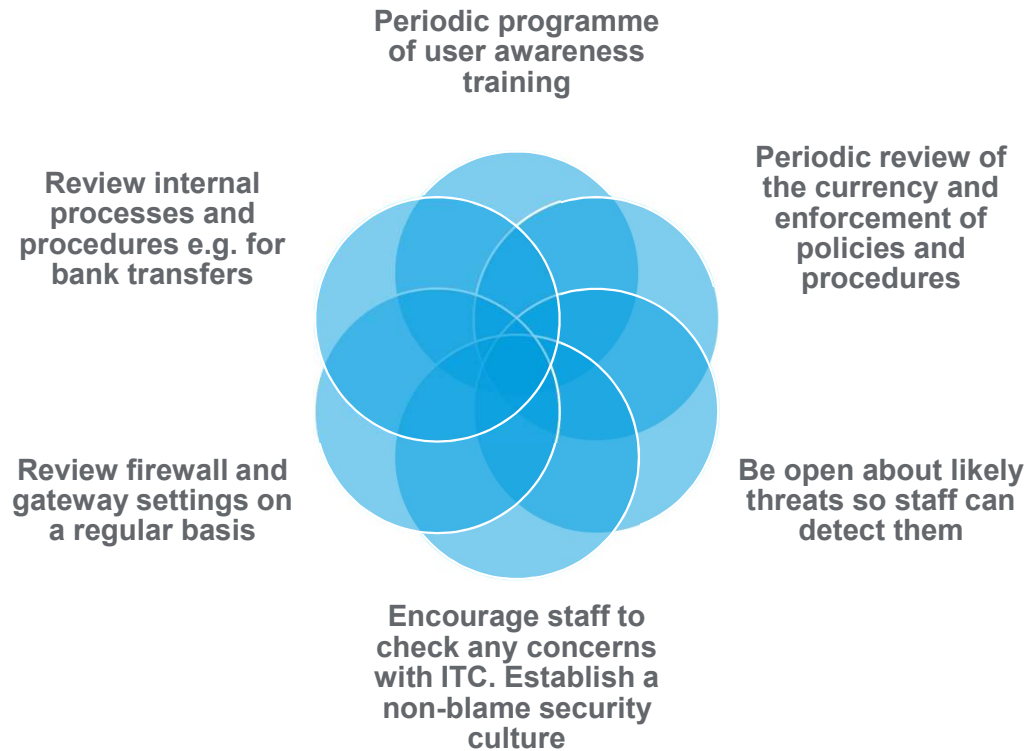
However, the following **issues** should also be noted:

- When the attackers had knowledge of the systems and processes of the organisation, and that information was used to create a more targeted attack, significantly more users were successfully phished.
- Whilst the percentage of staff who clicked on the phishing links was lower than the sector average, it still represents a significant risk to the organisation.

Actions for Management to consider

- User Education - The Council should consider continuing to deliver training for all staff to ensure that they remain up to date with the latest threats.
- Spam Filter Controls - The Council should consider reviewing the current configuration of the spam filter as emails from the “admin@it-helpdesk.systems” domain were permitted delivery without being blocked.
- Continuous Improvement - The Council should consider reviewing the areas of best practice from the next slide and identify areas for improvement as required.

Best Practice and areas to ensure adequate focus

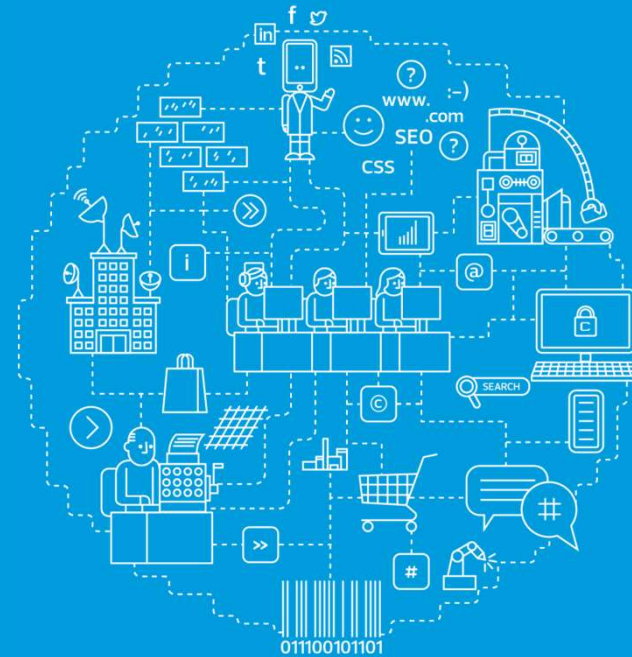


For further information contact:

David Morris (Director)
Mobile: +44 7800 617128
Email: david.morris@rsmuk.com

Joe Web (Manager)
Mobile: +44 7528 970350
Email: joe.webb@rsmuk.com

Whilst every care has been taken to ensure that the information provided in this report is as accurate, complete and timely as possible, no complete guarantee, assurance or warranty can be given with regard to the advice and information contained herein.



Collaboration. Understanding. Ideas and insight.