Audit Committee Internal Audit Progress Report

APPENDIX A

Isle of Wight Council

FINAL

December 2018

Contents

Introduction and Internal Audit Overview

Introduction

This report presents a summary of the activities of Internal Audit for the period July to December 2018. It provides the executive summary for the final 2017/18 report, on Environmental Health.

Two reports have been finalised to date from our 2018/19 programme of work, Parking and IT General Controls. As these reports are both rated high risk in line with usual practice these are presented separately to this meeting of the Audit Committee, under the same agenda item.

2018/19 Update

Our quarter one, two and three programmes of work are now substantively complete, with reports either at the draft stage or pending finalisation. Scoping is underway for our quarter four programme of work.

Summary of performance against key performance indicators

We have met the key performance indicators which were within internal audit's control in relation to providing a high quality internal audit service to the Council. We have received two completed customer survey to date, awarding an average satisfaction score of 9.2/10.

Full details of performance against key performance indicators for 2017/18 and 2018/18 can be found in Appendix C and Appendix D within this report.

Executive Summaries from Internal Audit Reports

In this section we provide the executive summaries for the remaining 2017/18 report issued as final since the Audit Committee last met in July 2018.

Executive summary – Environmental Health

Classification	Trend	By type				By scope area					
Medium Risk	Last reviewed in 2015/16; rated as medium risk.		Control design	Operating effectiveness	Total		Critical	High	Medium	Low	Advisory
		Critical	0	0	0	Documentation	0	0	0	1	0
		High	0	0	0	Delivery	0	0	1	2	0
		Medium	0	3	3	Oversight	0	0	1	0	0
		Low	2	1	3	FSA Follow up	0	0	1	0	0
		Advisory	0	0	0						

Summary of findings

This review focussed on the Council's Environmental Health (EH) arrangements, covering:

- *Documentation*: Confirming that the standards that EH are using are appropriate and in line with best practice.
- *Delivery*: Validating that the activities of EH are delivered in line with the documented procedures.
- *Oversight: C*onfirming that performance is reviewed on a timely basis in line with documented requirements and formal performance review meetings are taking place on a regular basis.
- *FSA Follow up*: Covering the progress that EH has made in implementing the action plan that the Food Standards Agency recommended following their audit in 2016.

The conclusions of our review are mixed, however they need to be put into context. EH informed Internal Audit that they have had difficulties filling vacancies in all four areas that we reviewed, limiting the amount of work that can be delivered. EH has a good level of documentation covering the responsibilities of each function, although some is very out of date.

In summary, Internal Audit has raised the following findings:

<u>Communicable diseases</u>

EH follows the Hampshire and Isle of Wight (HIOW) case plan guidelines to inform their response times and actions following notification from a GP of a communicable disease. Internal Audit sample tested five response times to notifications from GPs of a reportable disease. EH responded to the notification of the disease in two of the sample instances tested. Both responses exceeded the recommended response time for that disease by at least one month. We also reviewed the actions taken in response to a serious outbreak of E.coli in the year. This involved a multi-agency response, led by Public Health England (PHE) to which the EH team contributed. PHE involves itself in disease outbreaks either in terms of size or the seriousness of the disease, while the EH team's response to this outbreak was in line with documented policy. This demonstrates that although EH are not consistently responding to communicable diseases in accordance with policy, serious incidents are addressed, reducing the risk to the public.

This is raised as **Medium risk** finding.

Food Standards Agency (FSA) Follow up

EH has completed 10 out of the 12 actions in the action plan agreed with the FSA. The two outstanding actions were to increase the number of FTEs to carry out the work set out in its service plan and to update the sampling procedures in order to increase the number of inspections carried out by the EH team. These findings are linked, with an increased number of staff able to undertake a greater number of inspections. The EH team have undertaken one successful recruitment drive with one officer recruited. However, the officer left in April 2016, while subsequent recruitment drives have failed due to the lack of quality applicants available. Discussions are ongoing both with the FSA and the Council's HR department as to how to best address this issue. This has an associated reputational, financial and service delivery risk on the service risk register and more widely could pose a public health risk. However the EH team do focus inspections on highest risk food establishments. This is raised as a **Medium risk** finding.

Performance Reporting

In early 2017, the EH IT system changed from Flare to IDOX. This caused EH significant problems producing performance reports to inform performance review meetings. Therefore, while these meetings have been taking place over the past 12 months, formal reports have not been produced from IDOX. This is caused by a combination of 'built in' reports not being available in the system, delays in training being provided to staff and reports requiring more technical knowledge than envisaged when the system was initially implemented. This is raised as **Medium risk** finding.

Temporary Event Notice Applications (TENS)

We planned to sample test a number of TENS based on the documented process, however, the design of the process includes deleting the documentation, so this was not available for us to review to inform sample testing. When a Licensing application is made EH are informed via a dedicated email inbox. An EH officer reviews the application to identify if there are any likely issues from an EH perspective, for example health and safety, food safety or nuisance. If they are satisfied that it does not, which according to EH happens in the majority of cases, they then delete the email from the inbox. There is no record of the original decision made by the EH officer who looked at the application. This means that applications could be processed in error and EH would have no record or detail of this. This is raised as a **Low risk** finding.

Noise Complaints Testing

We tested a sample of 25 reported noise complaints. EH aims to respond within three working days. In three instances EH had not complied with the required response time exceeding this by 1, 3 and 9 days respectively. In all three cases, no further action was required past the stage where the first letters are sent to both the perpetrator and the complainant, the normal outcome of most noise complaints, indicating that the delay in responding to these complaints would not have had a disproportionate impact on residents. This is raised as a **Low risk** finding.

Age and content of documented policies and procedures

The existing guidelines issued by the HSE do not set definitive targets or actions for Health and Safety inspections by Local Authorities. Instead, they allow for EH to respond on a risk-based approach based on "intelligence". EH have undertaken five inspections this year. In addition, the noise complaints procedures are 10 years old and should be reviewed and updated if necessary, to ensure that they continue to be in line with the Council's needs. This is raised as a **Low risk** finding.

Appendix A: Basis of our classifications

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Critical	A finding that could result in a: • Major loss of service, including several important areas of service and /or protracted period. Service Disruption 5+ Days	A finding that could result in: • Adverse and persistent national media coverage • Adverse central government response, involving (threat of) removal of delegated powers • Officer(s) and/or Members forced to resign	A finding that could results in: • Death of an individual or several people	A finding that could result in: All personal details compromised/ revealed	A finding that could result in: • Litigation/claims/ fines from Department £250k + • Corporate £500k +	A finding that could result in: • Costs over £500,000	A finding that could result in: • Complete failure of project/ extreme delay – 3 months or more
High	A finding that could result in a: • Complete loss of an important service area for a short period • Major effect to services in one or more areas for a period of weeks Service Disruption 3-5 Days	A finding that could result in: • Adverse publicity in professional/municipal press, affecting perception/standing in professional/local government community • Adverse local publicity of a major and persistent nature	A finding that could result in: • Major injury to an individual or several people	A finding that could result in: Many individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from • Department£50k to £125k • Corporate £100k to £250k	A finding that could result in: • Costs between £50,000 and £500,000	A finding that could result in: • Significant impact on project or most of expected benefits fail/ major delay – 2-3 months

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Medium	A finding that could result in a: • Major effect to an important service area for a short period • Adverse effect to services in one or more areas for a period of weeks Service Disruption 2-3 Days	A finding that could result in: • Adverse local publicity /local public opinion aware • Statutory prosecution of a non-serious nature	A finding that could result in: • Severe injury to an individual or several people	A finding that could result in: • Some individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £25k to £50k • Corporate £50k to £100k	A finding that could result in: • Costs between £5,000 and £50,000	A finding that could result in: • Adverse effect on project/ significant slippage – 3 weeks–2 months
Low	A finding that could result in a: • Brief disruption of important service area • Significant effect to non-crucial service area Service Disruption 1 Day	A finding that could result in: • Contained within section/Unit or Directorate • Complaint from individual/small group, of arguable merit	A finding that could result in: • Minor injury or discomfort to an individual or several people	A finding that could result in: • Isolated individual personal detail compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £12k to £25k • Corporate £25k to £50k	A finding that could result in: • Costs less than £5,000	A finding that could result in: • Minimal impact to project/ slight delay less than 2 weeks
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.						

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	*Points*
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification	*Points*
Low	6 points or less
Medium	7– 15 points
High	16– 39 points
Critical	40 points and over

Appendix B: Progress on the 2017/18 internal audit plan

Audit name	Fee	Current Status	Report classification for those audits completed
Adult Social Care Contracts	£7,550	Final Report	Medium Risk
Application System: SAP	£5,450	Final Report	Medium Risk
Beaulieu House	£5,450	Final Report	High Risk
Benefit Payments	£5,450	Final Report	Low Risk
Contracts/Grant Sourced Spend	£7,550	Final Report	Medium Risk
Corporate Governance/Service Planning	£7,550	Final Report	Low Risk
Cowes Floating Bridge *	£5,450	Suspended	-
Development Control	£5,450	Final Report	Low Risk
Emergency Management: Business Continuity	£7,550	Final Report	Medium Risk
Environmental Health	£5,450	Final Report	Medium Risk
Fraud and Corruption **	£7,550	Final Report	n/a
Housing / Safe & Secure Homes	£5,450	Final Report	Medium Risk

Audit name	Fee	Current Status	Report classification for those audits completed
Information Management/IG Toolkit	£7,550	Final Report	High Risk
IT Governance and Asset Management	£7,550	Final Report	Medium Risk
IT: Alignment with Business Need	£7,550	Final Report	Medium Risk
Key Financial Systems	£12,800	Final Report	n/a
Local Taxation (Council Tax and NDR)	£5,450	Final Report	Medium Risk
Public Health	£7,550	Final Report	High Risk
PFI and Pan Follow-up *	£5,450	Final Report	N/A
Recruitment	£5,450	Final Report	Low Risk
Regeneration/Strategic Support	£7,550	Final Report	Medium Risk
Schools' Audits	£5,450	Final Report	N/A
Trading Standards	£5,450	Final Report	Medium Risk
Treasury Management	£5,450	Final Report	Low Risk
Vanguard	£10,522	Final Report	Medium Risk

Audit name	Fee	Current Status	Report classification for those audits completed

* Our scheduled review of the Cowes Floating Bridge has been directly substituted with a follow-up review, to assess progress implementing the actions stemming from our 2016/17 reviews of the Highways PFI and Pan reviews.

** The results of our fraud work have been communicated directly to the Chief Internal Audit, a summary of our findings was included in the progress report presented to the last meeting of the Audit Committee.

Appendix C: Progress on the 2018/19 internal audit plan

Audit name	Fee	Current Status	Report classification for those audits completed
Asset Management	£7,800	Fieldwork	-
Commercial Strategy/Income Generation	£7,800	Scoping	-
Contract Monitoring	£7,800	Scoping	-
Cross Services Outcomes	£7,800	Scoping	-
Domiciliary Care	£7,800	Scoping	-
GDPR/Data Sharing	£7,800	Fieldwork	-
Home to School Transport	£7,800	Draft Report	-
Houses with Multiple Occupation	£7,800	Draft Report	-
Income Collection (Cowes Bridge, Shanklin Lift, Crematorium)	£7,800	Scoping	-
IT General Controls (ITGC)	£7,800	Final Report	High Risk
Key Financial Systems (KFS)	£11,600	Scoping	-
Local Care Plan	£7,800	Scoping	-

Audit name	Fee	Current Status	Report classification for those audits completed
Looked After Children	£7,800	Draft Report	-
Parking	£7,800	Final Report	High Risk
Project Management	£7,800	Scoping	-
Regulatory Compliance	£7,800	Fieldwork	-
Schools	£7,800	Fieldwork	-
Social Media/CCTV	£7,800	Draft Report	-
Special Educational Needs and Disability (SEND)	£7,800	Draft Report	-
Third Party Relationship Governance	£7,800	Scoping	-

Appendix D: Internal audit performance against key performance indicators 2017/18

	Adult Social Care Contracts	Application System: SAP	Beaulieu House and Riboleau House	Benefit Payments	Contracts/Grant Sourced Spend	Corporate Governance/Service Planning	PFI and Pan Follow-up	Development Control	Emergency Management: Business Continuity	Environmental Health	Fraud and Corruption	Housing / Safe & Secure Homes	Information Management/IG Toolkit	IT Governance and Asset Management	IT: Alignment with Business Need	Key Financial Systems	Local Taxation (Council Tax and NDR)	Public Health	Recruitment	Regeneration/Strategic Support	Schools' Audits	Trading Standards	Treasury Management	Vanguard
Scope agreed prior to fieldwork commencing?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Exit meeting held?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Draft report issued within 10 working days of completion of exit meeting?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Draft report issued within 10 working days of receiving documentation from auditee?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Management response received?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Final report issued within five working days of agreement of management response?	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	n/a	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Client satisfaction survey score (if received)?	10	9.8	-	6.5	-	9.2	-	9	7.5	-	-	8.6	-	9.6	10	7.6	8	-	9.2	10	5	-	-	-

Appendix E: Internal audit performance against key performance indicators 2018/19

	Asset Management	Commercial Strategy/Income Generation	Contract Monitoring	Cross Services Outcomes	Domiciliary Care	GDPR/Data Sharing	Home to School Transport	Houses with Multiple Occupation	Income Collection	IT General Controls (ITGC)	Key Financial Systems (KFS)	Local Care Plan	Looked After Children	Parking	Project Management	Regulatory Compliance	Schools	Social Media/CCTV	Special Educational Needs and Disability (SEND)	Third Party Relationship Governance
Scope agreed prior to fieldwork commencing?	Y	-	-	-	Y	Y	Y	Y	-	Y	-	-	Y	Y	-	Y	Y	Y	Y	-
Exit meeting held?	-	-	-	-	-	-	Y	Y	-	Y	-	-	-	Y	-		-	Y	Y	-
Draft report issued within 10 working days of completion of exit meeting?	-	-	-	-	-	-	Y	Y	-	Y	-	-	-	Y	-	-	-	Y	Y	-
Draft report issued within 10 working days of receiving documentation from auditee?	-	-	-	-	-	-	Y	Y	-	Y	-	-	-	Y	-	-	-	y	Y	-
Management response received?	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	-		-	-	-	-
Final report issued within five working days of agreement of management response?	-	-	-	-	-	-	-	-	-	Y	-	-	-	Y	-	-	-	-	-	-
Client satisfaction survey score (if received)?	-	-	-	-	-	-	-	-	-	10	-	-	-	8.4	-	-	-	-	-	-

Internal Audit Report 2018/19

IT General Controls **18-19-03**

C - 19

Isle of Wight Council

FINAL
October 2018

Contents

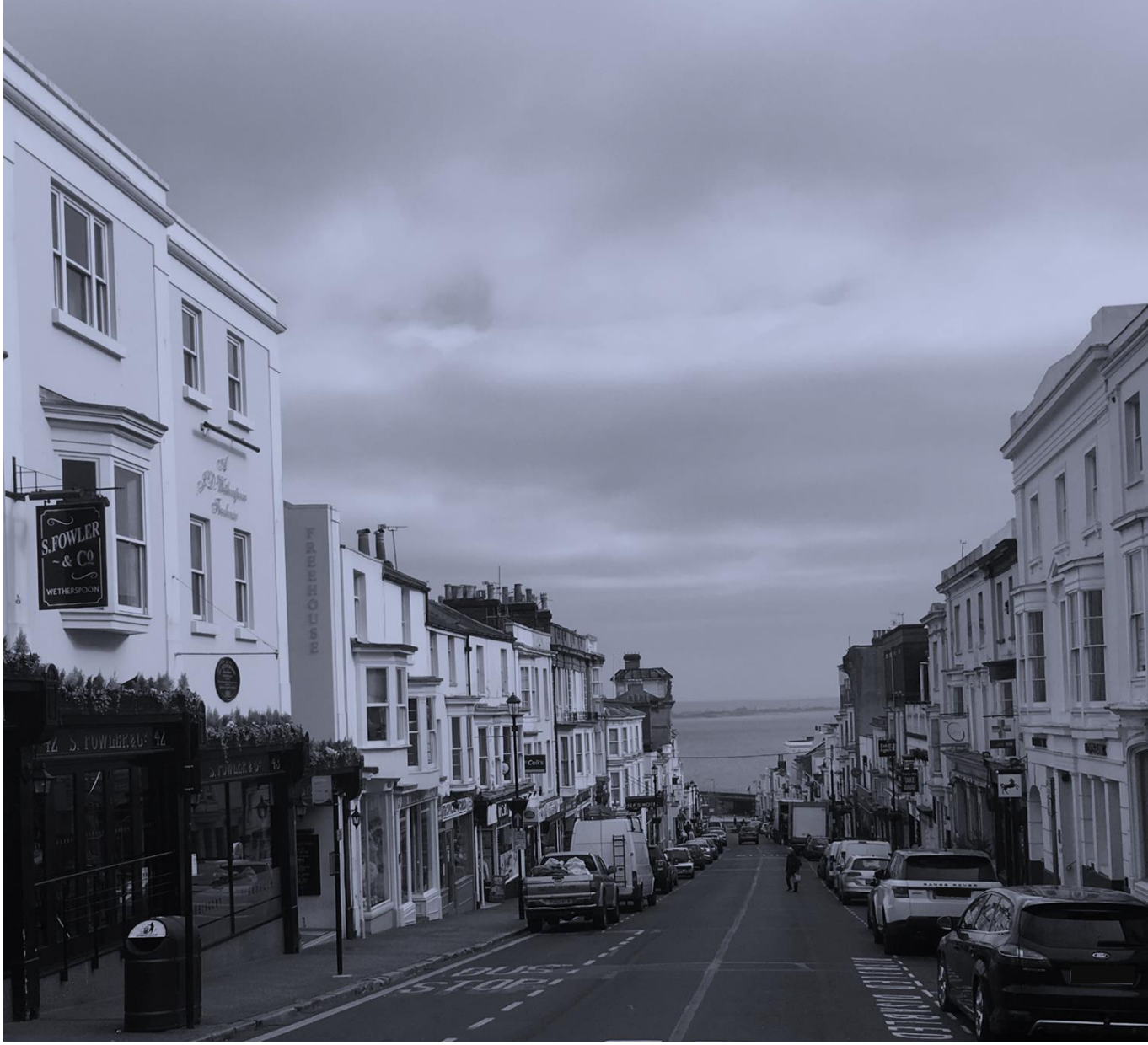
Distribution List

For action

Claire Shand, Head of Resources
Gavin Muncaster, Head of IT

For information

Elizabeth Goodwin, Chief Internal Auditor



Executive summary (1 of 2)

Classification	Trend	By type	By scope area

High Risk

We have not previously carried out a review with an equivalent scope

	Control design	Operating effectiveness	Total
Critical	0	0	**0**
High	1	1	**2**
Medium	1	0	**1**
Low	1	0	**1**
Advisory	0	0	**0**

Total findings: 4

	Critical	High	Medium	Low	Advisory
Framework	0	1	0	1	0
Automated Controls	0	0	1	0	0
IT Disaster Recovery	0	1	0	0	0

Summary of findings

IT General Controls are the IT controls which are applicable across an organisation, to ensure that the IT environment is stable, available and secure; effectively to ensure that it can be relied on to support service delivery. Many of these controls are covered as part of more specific reviews, for example focussed on how an individual corporate application such as SAP is managed. This review therefore focussed on a subset of the overarching IT General Controls, as below:

- *Framework*: confirming that an appropriate policy set, covering areas such as expectation of staff regarding security and acceptable use are in place, that these are suitably available and are supported, for example through appropriate training.
- *Automated Controls*: confirming that, wherever possible, automated technology is used to support good practice, for example sufficiently complex passwords, with reports run and acted upon to detect actions in contravention of policy.
- *IT Disaster Recovery*: confirming that there is an up to date IT Disaster Recovery Plan in place, signed off by senior management, with appropriate supporting mechanisms to ensure that it will work if needed, for example regular backups, testing and contracts with third parties.

The conclusion of our review is largely positive from a control design perspective. While there are enhancements which could be implemented, for example greater formality as to when excessive staff personal use is flagged to line management, the core content of policies, the IT Disaster Recovery Plan and automated controls is in line with good practice. In particular Internal Audit notes that the automated controls the Council has implemented on its network, for example encrypting laptop hard drives and blocking access to local removable storage, are in line with good practice expectations and we did not identify any significant gaps.

Our conclusion regarding the effectiveness of arrangements is less positive. The completion rates for mandatory IT security training is extremely poor, following on from a similar issue being identified in our 2017/18 review of Information Security, while a formal IT Disaster Recovery exercise has not taken place for a number of years. We have documented our work in four detailed findings, summarised below:

IT Security Training: (**high risk**) completion rates for mandatory IT Security Training are extremely poor, with only 8% of staff having recorded completion (either initial or 12 month renewal) as of the 23rd May 2018. Poor completion rates for IT/Information security training was also identified in Internal Audit's 2017/18 Information Management report and, while not directly comparable, completion rates do appear to have deteriorated since the time of the fieldwork for this prior review; the prior report identified that 30% of staff had certified completion of training at the end of September 2017.

Clearly this is a significant issue. Having mandatory training which is not enforced invalidates the value of the control and may make staff less likely to comply with wider mandatory Council requirements. Specific to IT Security, it will lead to staff being less likely to comply with expectations and will increase the likelihood that the Council's systems and the data they contain being compromised. This issue needs to be escalated to the Corporate Management Team (CMT), with sanctions agreed, for example withdrawal of access to IT systems, cascaded to line management if training is not completed in a reasonable timeframe.

IT Disaster Recovery: (**high risk**) while Internal Audit did not identify any significant issues with the content of the IT Disaster Recovery Plan, we did note that it is a number of years since a formal process has been undertaken to agree Recovery Time Objectives (RTO, maximum downtime), Recovery Point Objectives, (RPO, maximum data loss) and the prioritisation order of systems restoration with service areas. This exercise should be carried out, to confirm that the content of the IT Disaster Recovery Plan is in line with organisational need, with the key elements presented to the CMT for approval.

More seriously, we note that it is at least three years since a formal IT Disaster Recovery rehearsal has taken place. Carrying these out periodically is important, to confirm that they will work effectively in the event of an actual continuity incident and to enable any issues to be identified and addressed. The Council is in the process of implementing reciprocal fail over arrangements with the local NHS Trust. This is at an advanced stage (scheduled to be completed by October 2018) and will provide the Council with much quicker and less error prone fail over than would be possible with more traditional continuity arrangements. Subject to an appropriate SLA with the Trust being in place and testing during the commissioning process, this is likely to mitigate the risk, however while the arrangement is not in place the issue remains high risk.

Detective Controls/Reporting: (**medium risk**) while excessive personal use and attempts to access blocked content are clearly prohibited in IT policies and there are automated controls in place to prevent most access of inappropriate content, only ad hoc reports are run and forwarded to line management to detect this activity. Furthermore, no evidence was provided to show appropriate follow-up actions being taken. While it is unlikely that the Council has a significant issue with activity of this type, for example due to the automated preventative controls in place, a formal process, with activity banded by severity and appropriate follow-up actions agreed, should be designed and approved by senior management.

The policy also identifies that local hard drives should only be used for temporary file storage. To support this, particularly with the increased consequences for data loss, retention, consent and other expectations introduced by the General Data Protection Regulation (GDPR), hard drive data storage requirements should be added to the agenda for a future meeting of the Information Governance Group (IGG) for discussion, to identify if detective controls, for example to identify large volumes of data, or data which potentially contains personal identifiers, are warranted.

Policies: (**low risk**) the content of the IT policies we reviewed is in line with good practice, for example highlighting the importance of shutting down laptops, to ensure that drive encryption is effective; Internal Audit also notes that IT policies are easily available in the key documents section of the intranet. We identified one policy, the ICT Electronic Communication Policy, which is overdue review from February 2017. This should be reviewed and updated at the earliest opportunity. We also note that section 16.1.7 of the IT Security Policy is not explicit regarding requiring the involvement of IT in approving and configuring SaaS (Software as a Service) or cloud based systems. To remove any ambiguity this clause of the Policy should be updated to make this requirement explicit.

Management Response

While the Council recognises the issues highlighted in this report we are disappointed that IT Disaster Recovery has been rated 'high risk'. Specifically during 2017/18 there have been two occasions on which IT Disaster Recovery arrangements have been invoked and have functioned effectively. On the 21st December 2017, due to a generator failure and on the 12th December 2017, due to incorrect telephony porting; no incidents during this date have warranted invoking IT Disaster Recovery arrangements.

The report also references plans the Council has to implement reciprocal arrangements with the NHS Trust. We are pleased to report that the Trust's failover site at County Hall is now fully operational, with the Council's failover site at the Trust due to be commissioned shortly.

We would like to take this opportunity to thank Isle of Wight Council staff for their help and assistance with this review.

Current year findings (1 of 4)

IT Security Training

Operating Effectiveness

1

High

Finding and root cause

There are mandatory e-learning modules covering Information Security, Protective Marking and ICT policies. Current compliance rates for 2017/18 are summarised below:

	Information Security	Protective Marking	ICT Policies
Completed	165	141	135
Expired	363	392	341
In progress	34	15	6
Not started	1119	1142	1209
Report run on the 23rd May 2018			

From an IT security perspective the training regarding ICT Policies is the most important, although Information Security and Protective Marking training are also relevant to ensuring that the Council's systems and the data they contain are 'secure'.

For context Internal Audit also reviewed training completion rates as part of our 2017/18 review of Information Security. The fieldwork for this prior review was carried out in September 2017. Due to the time elapsed since the time of this fieldwork it is not possible to directly compare completion rates. However the position has worsened since the time of our last review, with the current position being that only 8% of staff having recorded completion of mandatory ICT Policy training. This compares to 30% at the time of our last review.

While Internal Audit was informed that there is a new set of training in the process of being provided to support GDPR (General Data Protection Regulation) compliance, this is separate to the training summarised above. Specifically, regarding the scope of this review, it is focussed on 'information', rather than more general 'IT' security practice.

Clearly having training identified as mandatory, which is then not completed by the majority of staff with no consequences, will impact on both the IT security practice of staff and their perception of how important completing training actually is. This issue needs to be escalated to the Corporate Management Team. If the training is confirmed as genuinely mandatory then this requirement needs to be cascaded to line management, with completion rates closely monitored until the completion rates improve. Further action to address non-completion also needs to be considered, for example withdrawing access to IT systems until training is completed or potentially disciplinary action. We also note that the requirement for staff to recomplete IT Security training annually may be unrealistic and/or unnecessary. Increasing this interval to triennially should be considered.

Implications

At a high level having mandatory training which is not enforced negates the purpose of mandatory training, leaves the underlying risk unaddressed and will impact on staff perception of what the Council's expectation of them is.

Specific to IT Security Training, staff will be less likely to understand requirements and comply with them, putting the Council's systems and the data they contain at increased risk.

Action plan

The Head of IT in collaboration with the Head of Resources will:

- Revisit both the need for IT Security training to be mandatory and the interval at which it needs to be re-completed, to confirm these are in line with organisational need.
- Highlight the current position to CMT, with the expectation that the requirement will be re-cascaded to line management, with clear sanctions agreed if training is not completed within a reasonable timeframe, for example three months, such as withdrawal of access to IT systems.

Responsible person/title
Gavin Muncaster, Head of IT Claire Shand, Head of Resources
Target date
November 2018
Reference number
18-19-03-01

Current year findings (2 of 4)

IT Disaster Recovery

Control design

2

High

Finding and root cause

The overarching IT Disaster Recovery Plan is maintained in MS OneNote, of which Internal Audit was provided with an extract. This is stored on a server, with all IT management having a local cached copy on their laptops, with changes synched via the server. The content of the Plan appears sensible and, from a design perspective, the only issue we identified with the overarching Plan is regarding the prioritisation list for applications. The key requirement is that the Recovery Time Objective (RTO, maximum downtime), Recovery Point Objective, (RPO, maximum data loss) and the prioritisation order of systems is in line with organisational priorities. This is accomplished by periodically confirming these with senior management, which we were informed has not taken place for a number of years, potentially leading to not all applications being captured and/or the prioritisation order being incorrect. To confirm the information in the IT Disaster Recovery Plan is correct this should be added to the agenda for a future meeting of the Corporate Management Team (CMT).

More specifically we identified that the Service Level Agreement (SLA) with the NHS Trust is not explicit regarding backup and recovery arrangements for Paris, the core system used by Adult Services. We first identified this issue in our 2017/18 review of wider business continuity arrangements and the position remains unchanged from the time of this prior review; the SLA is still not explicit regarding backup and recovery arrangements. Simplistically arrangements need to be clarified, specifically to ensure that they are in-line with the needs of Adult Services. Potentially this is a serious issue and has contributed to this finding being rated as high risk.

However the most serious issue is that there has not been a scheduled disaster recovery exercise for at least three years. While each year there are instances where elements of 'recovery' are invoked, for example during 2017/18 we were informed that continuity arrangements were invoked regarding a generator failure and telephony, both during December 2017 and worked correctly, this does not cover a 'full' recovery scenario. *

The Council has been investigating reciprocal IT continuity arrangements with the local NHS Trust for a number of years. This approach has now been agreed, with implementation at an advanced stage, scheduled to be completed by October 2018 – once in place this will provide the Council with rapid failover, far in advance of anything which would be achievable with a more traditional approach to sourcing replacement hardware. However until failover is fully tested, as part of commissioning the new arrangements, the Council is exposed, as such this finding has been rated as high risk.

** The recent survey on economic crime produced by our co-sourced partner highlighted the increased level of attacks on organisations of all types in the UK – the survey identifies that Cybercrime is now the number one fraud risk faced by UK organisations for the first time, experienced by nearly half (49%) of our survey, compared to 31% globally. Having robust, testing IT Disaster Recovery arrangements in place is vital to ensuring that an organisation can quickly recover from any penetration of its IT network.*

Implications

If the Recovery Time Objective (RTO, maximum downtime), Recovery Point Objective, (RPO, maximum data loss) and the prioritisation order of systems is not validated periodically with senior management IT effort may be incorrectly focussed and restoration of systems may not be in line with organisational need/expectations.
Without a recently reviewed and updated prioritisation list for applications there could be new applications which have been missed and are not included in IT's recovery plans.
If regular IT Disaster Recovery rehearsals are not carried out and learned from then plans/expectation may prove not to be realistic/effective in the event of an actual continuity incident. Ultimately this could lead to an unacceptable level of data loss and/or an extended interruption to the delivery of key services.

Action plan

The Head of IT will:

- Consult with service areas as necessary, to agree appropriate RTOs/RPOs for their key systems.
- Reprioritise the relative criticality of systems as necessary, in line with agreed organisational need.
- Present the revised IT Continuity Plan/key elements to CMT for formal approval.
- Schedule an IT Disaster Recovery exercise, specifically to include testing of new fail over arrangement with the local NHS Trust to ensure that key systems are both tested and any learning is acted on.

Responsible person/title
Gavin Muncaster, Head of IT
Target date
November 2018
Reference number
18-19-03-02

Current year findings (3 of 4)

Detective Controls/Reporting

Control design

3

Medium

Finding and root cause

Overarching IT policies (covered later in this report) align with good practice, however, there are gaps in the complementary detective controls, to support line managers in ensuring their staff comply with the Council's requirements in two areas.

The most important of these is regarding excessive personal use/web browsing or repeated attempts to access blocked content. While we were informed that ad hoc emails are sent to line managers where activity of this type is identified, no evidence was supplied to support this assertion, nor were we provided with any evidence of any resulting follow-up action being taken by line management.

While it is unlikely that the Council has a significant issue with excessive personal use, due to the automated preventative controls in place, for example web filtering, greater formality should be introduced, to complement the existing prohibitions in policies. A procedure note should be agreed, between IT and senior management, quantifying and banding by severity, inappropriate use, with a set of actions and consequences agreed as a result. For example attempts to access pornography or terrorism related content could lead to immediate notification to line management and likely disciplinary actions, while excessive personal web browsing could be included in a report sent periodically to line managers and result in an informal warning.

The second potential gap is regarding the prohibition of local file storage (i.e. use of local hard drives) – the policy is clear, this should only be used for temporary storage. This is less serious as approximately 50% of staff use thin clients, which do not have local file storage. However, particularly with the increased consequences introduced by the General Data Protection Regulation (GDPR), a complementary detective control may be justified. For example laptops could be remotely queried to identify where there is an excessive volume of local storage in use, with line management requested to investigate where this is identified. This should be put on the agenda for a future meeting of the Information Governance Group (IGG) for discussion, to identify if a detective control is warranted.

Implications

At a high level, if policy prohibitions are not complemented by detective controls then it is less likely they will be complied with, reducing the value of prohibitions and leaving the underlying risks unmitigated.
If there are repeated attempts to access blocked content, with no action taken as a consequence, then there is a risk that eventually perpetrators will identify a way to circumnavigate the Council's automated controls, potentially placing the entire network at risk.
If excessive personal use is not reported to line management, with appropriate follow-up action taken, then staff who are not focussed on their job responsibilities will be able to continue their inappropriate conduct unchallenged.
If there is excessive use of local storage then there will be an elevated risk of potentially sensitive information be 'lost', introducing the risk that the Council will suffer fines and/or reputational damage.

Action plan	
The Council will: • Design, document and gain approval for a process to detect and notify line management regarding inappropriate use and attempts to access blocked content. This should band/quantify activity by severity and include actions taken as a result. • Add local file storage to a future meeting of the Information Governance Group (IGG).	***Responsible person/title*** Gavin Muncaster, Head of IT ***Target date*** November 2018 ***Reference number*** 18-19-03-03

Current year findings (4 of 4)

Policies

Control design

4

Low

Finding and root cause

Internal Audit reviewed the core policies covering the Council's expectations regarding IT Security. All of these are available in the key documents section of the intranet and set out expectations in line with good practice, for example shutting down laptops fully, to ensure that drive encryption is effective. One policy, the ICT Electronic Communication Policy, is overdue review from February 2017. While we identified no issues with its content it should be sense checked and the review date updated at the earliest opportunity.

Requirements regarding acceptable software use could also be enhanced. While section 16.1.7 of the IT Security Policy makes it clear that all software must be approved and installed by IT, it does not explicitly reference SaasS (Software as a Service) or cloud based systems. Online systems of this type are often low cost, falling under procurement thresholds and do not require any involvement from IT before they can be used. Section 16.1.7 should be updated, to make it clear that this requirement also applies to SaasS/Cloud systems, to remove any ambiguity.

Implications

If policies are not reviewed at least annually they can become out of date and may not reflect organisational need, or be in line with good practice. Potentially this could lead to the Council's IT infrastructure being less secure than desirable.
If expectations are not sufficiently explicit then they may be misinterpreted by service areas, leading to the Council's IT infrastructure being less secure than desirable.

Action plan

The Council will:

- Review the ICT Electronic Communication Policy, make any changes necessary and update the next review date to 12 months' time.
- Revise the wording of section 16.1.7 of the IT Security Policy to make it clear that SaaS/Cloud software should be approved and configured by IT.

Responsible person/title
Gavin Muncaster, Head of IT
Target date
November 2018
Reference number
18-19-03-04

Appendix A: Basis of our classifications

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Critical	A finding that could result in a: • Major loss of service, including several important areas of service and /or protracted period. Service Disruption 5+ Days	A finding that could result in: • Adverse and persistent national media coverage • Adverse central government response, involving (threat of) removal of delegated powers • Officer(s) and/or Members forced to resign	A finding that could results in: • Death of an individual or several people	A finding that could result in: All personal details compromised/ revealed	A finding that could result in: • Litigation/claims/ fines from Department £250k + • Corporate £500k +	A finding that could result in: • Costs over £500,000	A finding that could result in: • Complete failure of project/ extreme delay – 3 months or more
High	A finding that could result in a: • Complete loss of an important service area for a short period • Major effect to services in one or more areas for a period of weeks Service Disruption 3-5 Days	A finding that could result in: • Adverse publicity in professional/municipal press, affecting perception/standing in professional/local government community • Adverse local publicity of a major and persistent nature	A finding that could result in: • Major injury to an individual or several people	A finding that could result in: Many individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from • Department£50k to £125k • Corporate £100k to £250k	A finding that could result in: • Costs between £50,000 and £500,000	A finding that could result in: • Significant impact on project or most of expected benefits fail/ major delay – 2-3 months

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Medium	A finding that could result in a: • Major effect to an important service area for a short period • Adverse effect to services in one or more areas for a period of weeks Service Disruption 2-3 Days	A finding that could result in: • Adverse local publicity /local public opinion aware • Statutory prosecution of a non-serious nature	A finding that could result in: • Severe injury to an individual or several people	A finding that could result in: • Some individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £25k to £50k • Corporate £50k to £100k	A finding that could result in: • Costs between £5,000 and £50,000	A finding that could result in: • Adverse effect on project/ significant slippage – 3 weeks–2 months
Low	A finding that could result in a: • Brief disruption of important service area • Significant effect to non-crucial service area Service Disruption 1 Day	A finding that could result in: • Contained within section/Unit or Directorate • Complaint from individual/small group, of arguable merit	A finding that could result in: • Minor injury or discomfort to an individual or several people	A finding that could result in: • Isolated individual personal detail compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £12k to £25k • Corporate £25k to £50k	A finding that could result in: • Costs less than £5,000	A finding that could result in: • Minimal impact to project/ slight delay less than 2 weeks
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.						

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	*Points*
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification		*Points*
	Low	6 points or less
	Medium	7– 15 points
	High	16– 39 points
	Critical	40 points and over

Appendix B: Terms of reference

Background and Scope

IT General Controls cover the key controls which operate over an organisation's IT environment, to ensure that it secure, available and reliable. This review will focus on a subset of IT General Controls, as below:

- *Policies setting out key expectations of staff*: these should make it clear to staff how they should use IT, to ensure that the Council's gets best use from IT assets and that staff usage is both secure and appropriate.
- *Automated Controls*: wherever possible technology should be deployed to enforce good practice and to further minimise risks to the Council's network, for example through use of a centrally managed Anti-Virus system.
- *IT Disaster Recovery*: service areas each have their own specific needs and varying priorities for the Council. Ultimately how limited IT resource is deployed is a decision for the Council's senior management. To varying degrees arrangements should be in place, in line with agreed/approved 'need' to back data up and ensure that systems can be restored, in line with service need.

The sub-processes, control objectives and potential related risks included in this review are:

#	Control objective	Potential risks	Summary of Fieldwork
1	**Framework** Appropriate IT policies/supporting documentation covering staff IT use are in place; these: • Have cover sheets, identifying key metrics such as ownership, applicability, approval, last and next review dates and revision history. • Are approved by an appropriate source of authority. • Are available to staff, for example through publication on the intranet and highlighted, for example via email. • Require good security practices, for example 'strong' passwords and the importance of shutting down/hibernating encrypted laptops, and prohibit local file storage, the connection of non-organisational storage devices and the use of public cloud storage. • Acceptable use, for example covering personal use, email, web browsing and social media. • Approved/corporate software, including SaaS/cloud systems allowed. Policies are supported by:	If an appropriate framework of documented, current and approved expectations of staff are not in place and sufficiently available then: • Staff may not be clear on acceptable IT use and security requirements. • Staff may not understand what is expected of them, their approach may be inconsistent and potentially poor, putting the Council, its systems and data at elevated risk.	Internal Audit will review key IT policies to confirm: • They have cover sheets, identifying key metrics such as ownership, applicability, approval, last and next review dates and revision history. • They have been approved by an appropriate source of authority. • They highlight good security practice, for example 'strong' passwords and the importance of shutting down/hibernating encrypted laptops, and prohibit local file storage, the connection of non-organisational storage devices and the use of public cloud storage. • They identify acceptable use, for example covering personal use, email, web browsing and social media. • They identify approved/corporate software, including SaaS/cloud systems allowed. We will review the Council's intranet to confirm that policies are listed in the key documents section, available to all staff.

	• Training. • Reports to line management, regarding attempts to access blocked content and excessive personal use.		We will review evidence provided, for example emails, copies of Managers' Brief and the Vine, to confirm that IT expectation have been highlighted to staff. We will review training completion/pass rates for IT Security related training for 2017/18. We will confirm that reports are provided to line management, regarding attempts to access blocked content and excessive personal use; we will sample test reports, to confirm that appropriate follow-up action has been taken by line management.
2	**Automated Controls** Automated controls are used to support/enforce good practice; specifically: • Screens auto-lock after a period of inactivity. • Strong passwords (length, complexity and expiry) are enforced at the network level. • 'Standard' users do not have local admin access and cannot install software. • Passwords are stored securely, at the network level. • Centrally managed anti-virus and DLP (Data Loss Prevention) solutions are used. • USB ports are blocked; only organisational issued devices are allowed. • Laptop hard drives are encrypted. • A blacklist of prohibited websites is enforced (e.g. public file sharing/backup), ideally web access is via a proxy, with activity logs maintained. • Two factor authentication is used for remote access. • Publicly accessible network points are either disabled at the switch, or fitted with locking devices.	If automated controls are not deployed, to support IT security then there is a greater risk that staff will compromise the security of the Council's network and data inadvertently or deliberately. The Council will be at greater risk of data loss, system loss, fraud and interruption to frontline service delivery.	Internal Audit will review configuration screens for the Council's network, key servers and a sample of individual computers to confirm: • Screens auto-lock after a period of inactivity. • Strong passwords (length, complexity and expiry) are enforced at the network level. • 'Standard' users do not have local admin access and cannot install software. • Passwords are stored securely, at the network level. • Centrally managed anti-virus and DLP (Data Loss Prevention) solutions are used. • USB ports are blocked; only organisational issued devices are allowed. • Laptop hard drives are encrypted. • A blacklist of prohibited websites is enforced (e.g. public file sharing/backup), ideally web access is via a proxy, with activity logs maintained. • Two factor authentication is used for remote access. We will inspect public areas of County Hall and a sample of meeting rooms, to confirm that network points are either disabled at the switch, or fitted with locking devices.
3	**IT Disaster Recovery** An overarching IT Disaster Recovery Plan is in place; this:	If appropriate IT Disaster Recovery arrangements are not in place then:	Internal Audit will review the Council's IT Disaster Recovery Policy and supporting documentation to confirm it:

	• Has a cover sheet, identifying key metrics such as ownership, applicability, approval, last and next review dates and revision history. • Has been approved by the Council's senior management. • Is informed by consultation with key services, to ensure it aligns with their priority recovery needs. • Categorises systems by priority, with identified Recovery Point and Recovery Time objectives (RPOs and RTOs); these have been agreed with the Council's senior management. Appropriate supporting arrangements are in place; specifically: • Separate backup cycles (at least two), with backups stored at a suitable distance from the data centre. • Arrangements to source replacement hardware, sufficient to support agreed RTOs. • A regime of testing, including annual desktop reviews and bare metal restores of key systems, on a cyclical basis.	• The Council may suffer unacceptable and potentially unrecoverable data loss. • There may be an extended delay in recovering systems/data, impacting to an unacceptable degree on front line service delivery.	• Has a cover sheet, identifying key metrics such as ownership, applicability, approval, last and next review dates and revision history. • Has been approved by the Council's senior management. • Is informed by consultation with key services, to ensure it aligns with their needs. • Categorises systems by priority, with identified Recovery Point and Recovery Time objectives (RPOs and RTOs); these have been agreed with the Council's senior management. We will inspect configuration screens for the file and database backup systems (for key systems: SAP and Northgate Revenues and Benefits), to confirm two separate backup cycles are configured. We will review Service Level Agreements (SLAs) for Paris and ICS, to confirm that backup arrangements are both documented and sufficient. We will review a sample of backup logs for in-house hosted systems, to confirm backups are completing successfully. We will confirm the Council has a Server Recovery Contract in place with a suitable provider, with terms aligned with agreed RPOs and RTOs. We will review the results of the last IT Disaster Recovery Rehearsal.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulation or other changes; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.

Internal Audit Report 2018/19

Parking **18-19-19**

Isle of Wight Council

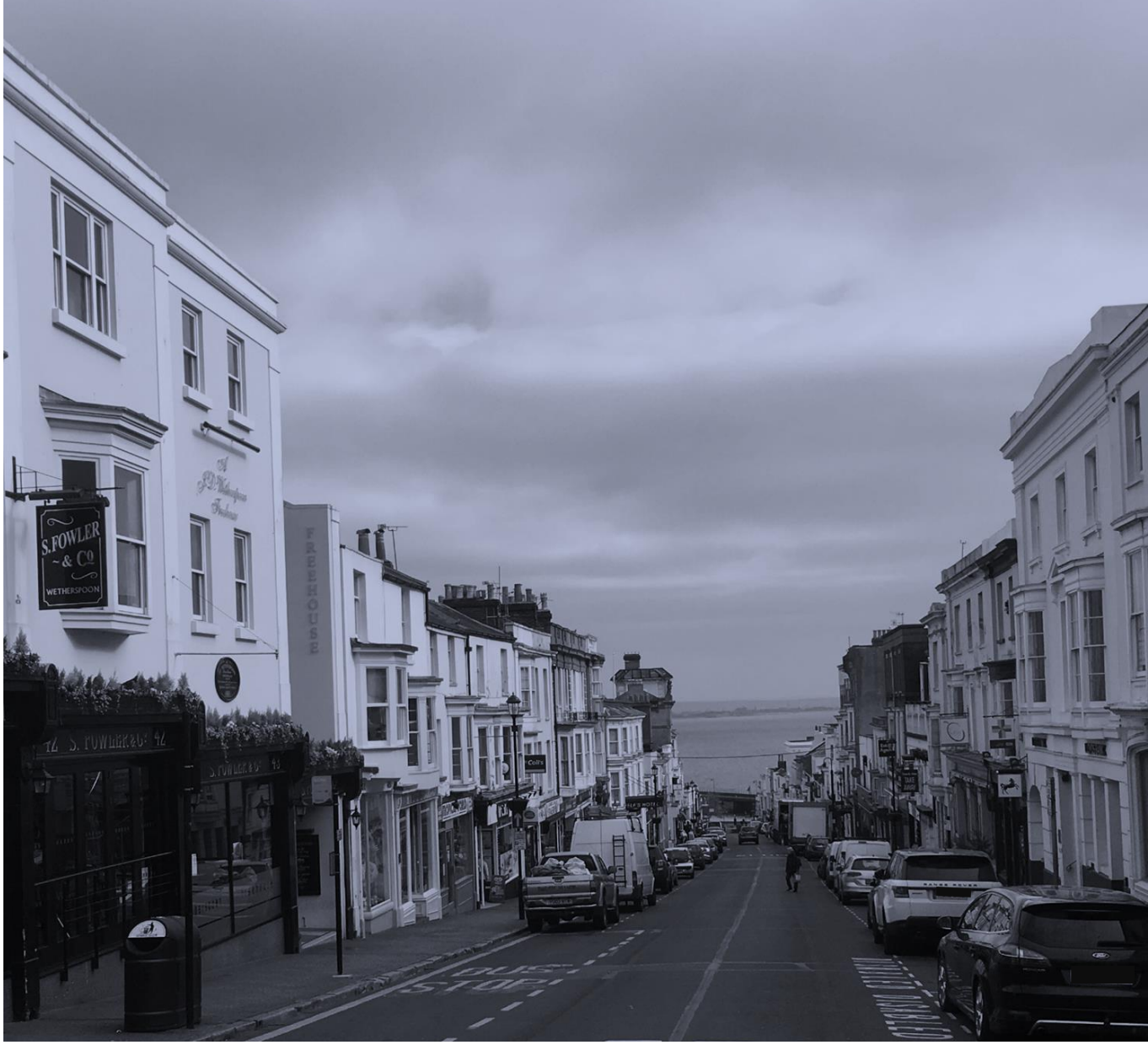
FINAL
October 2018

Contents

Distribution List

For action

Trevor Pugh, Interim Director of Neighbourhoods
Claire Shand, Director of Corporate Services
Sharon Betts, Strategic Manager for the Business Centre
Vicki Guildford, Revenues Manager
Mark Downer, Parking Operations Manager
Michele Porter, Team Leader for Business Rates and Parking Services
Jason Barrett, Contract Management Officer



Executive summary (1 of 2)

Classification	Trend	By type			By scope area					
			Control design	Operating effectiveness	Total		Critical	High	Medium	Low	Advisory
High Risk	We have not previously carried out a review with an equivalent scope	Critical	0	0	**0**	Operation	0	0	3	3	0
		High	0	0	**0**	SIM Cards	0	0	1	0	0
		Medium	5	0	**5**	Oversight	0	0	1	0	0
		Low	3	0	**3**						
		Advisory	0	0	**0**						

Total findings: 8

Summary of findings

This review focussed on the Council's management of parking covering:

- *Operation*: confirming that appropriate measures are in place to ensure that parking meters are available, levying the correct fees and that mechanisms are in place to ensure the correct level of income, including for fines, is being collected and reconciled.
- *SIM Cards*: confirming that these are known and that appropriate mechanisms are in place to ensure they are working and configured correctly, specifically to minimise the opportunity for and potential impact of any misuse.
- *Oversight*: confirming that the Service has appropriate risk, performance and oversight arrangements in place and that these are operating effectively.

For context during 2017/18 the Council generated £1,941,143 of income from off street, £1,017,484 from on street parking charges and £584,247 from permits (residential, long stay, tourist and staff).

While Internal Audit's review has identified a large number of issues we are pleased to report that management has taken immediate actions, implementing a number of enhancements to address many of the issues identified in the report. Most importantly we were informed that a range of additional management checks have been implemented to reconcile income received back to permits and Penalty Charge Notices (PCNs). Internal Audit also notes that the Service has a robust plan in place to address the issue of persistent evaders, where there are currently 15 individuals who between them have 1159 unpaid Penalty Charge Notices (PCNs), a total unpaid debt to the Council of £65,370.

The most significant weaknesses identified through this review relate to the Council's parking machine portfolio, specifically issues regarding remote reporting; reconciling cash recorded as received by machines with cash collected and banked; and ensuring that the Council has the correct number of SIM cards and that these can be tied to the machines in which they are located.

We also identified areas where greater formality is needed, for example regarding consistent management review and making sure documentation is up to date and reflective of practice. Internal Audit has raised eight detailed findings, summarised below:

Parking Machine Income: (**medium risk**) printouts of income received from parking machines are checked against cash collected, with anomalies investigated. However remote reporting/reconciliation is either not working correctly or not being used for all parking machines on the Island. For the 36 Metric machines where electronic reporting is working cash collected and banked is reconciled against the figures reported by the machines. No equivalent control is in place for the 83 Parkeon machines, while the control cannot be exercised for the 34 Metric machines where electronic reporting is not working. The immediate need is to implement a process to check the cash collected and banked from Parkeon machines against the income reported electronically. Until a more permanent solution can be implemented for the Metric machines which are not reporting electronically the cash collected should be monitored closely against historic trends, to ensure that any anomalies are identified at the earliest opportunity.

SIM Cards: (**medium risk**) there are 101 SIM cards listed on the SIM Card Register, for the corporate mobile phone contract, present in parking machines where the Council is responsible for the SIMs. However, there are only 70 parking machines where Council managed SIMs are necessary. The position is further muddied by the fact that different names/locations are used to refer to the parking machines on the SIM register and the register of parking machines provided for our review by the parking services. It has not been possible for us to definitely tie SIMs to the machines in which they are located. There are also a number of secondary issues linked to parking SIM cards, for example the inability to implement additional logical controls (i.e. to limit how they can be used if stolen, beyond the existing £50 per month, per SIM usage charge cap); the need to explicitly confirm that there would be no additional cost to the Council should SIMs be stolen from the 83 Parkeon machines; and potential efficiencies which could be realised by rationalising the service's use of mobile telephones. The immediate need is to reconcile SIM cards to actual parking machines, both to ensure that the Council is not paying for an excessive number of SIMs (these cost £6 per month each) and more importantly to ensure that if SIMs are stolen this is identified as soon as possible with the correct SIM card cancelled – Internal Audit is aware of a fraud of £55,000 at a neighbouring authority stemming from the the misuse of one SIM card

Permits: (**medium risk**) due to delays in appropriate functionality being made available in the Sidem car parking software, the Council is currently using a spreadsheet based system to manage parking permits on the Island. While permits are only issued once the separate team processing payments has confirmed that payments have been received, the process is undocumented. Furthermore, the spreadsheets contains potentially sensitive personal details while there is a lack of management oversight, for example reviewing/checking permits to payments. Longer term the system vendor should continue to be engaged with to progress a more robust mechanism for managing parking permits. In the short term the temporary spreadsheet based system needs to be documented and an appropriate level of management review agreed and implemented. The risk of personal details being held in the spreadsheets also needs to be discussed with the Corporate Information Unit (CIU).

Penalty Charge Notices (PCNs): (**medium risk**) the process of issuing and escalating PCNs is driven by legislation, with the majority of actions automated by the Sidem system. Our sample checking of 25 PCNs issued since the 1st January 2018 did not identify any issues. However we were provided with a report identifying 60 persistent evaders, the top 15 of these having 50 or more outstanding PCNs each, and the worst offender having 149 outstanding PCNs. For context this represents £65,370 of unpaid debt to the Council, of which £47,285 has been written off (debts are written off after three unsuccessful attempts to serve a debt recovery warrant). The Council is in the process of progressing a more robust approach to persistent evaders, to include seizure of vehicles; this is sensible and should continue as planned. Oversight also needs to be improved, by regularly reviewing reports from Sidem, to reconcile PCNs issued to payments received.

Risk Register: (**medium risk**) there are two risks on the Service's current Risk Register, with four live mitigations. However none of the mitigations have been updated for some time and Internal Audit notes that one of these, creating a Parking Technician post, was subsequently TUPEd to Island Roads, who made the post redundant. We also identified that there is limited content in the minutes for oversight meetings, considering risks. This report identifies a number of risks currently facing the Service; in the first instance the Risk Register should be reviewed, to ensure it fully captures the risks facing the Service and existing mitigations. Following on from this new controls/mechanisms should be implemented, documented and monitored, to address any gaps which exist and risks should be considered more fully at oversight meetings.

Parking Machine Status: (**medium risk**) 34 of the 70 Metric parking machines in use, including 12 of the 21 directly managed by the Council, are not communicating their status (i.e. if they are working or not) electronically. Additionally there is no maintenance contract in place, to ensure Metric machines are fixed in a timely manner. Together these issues could lead to a loss of

income for the Council. Costs associated with longer term measures to fully address the issue by accelerating the replacement of Metric machines with newer Parkeon machines should be investigated. In the short term, the form to enable members of the public to report faulty machines should be made more accessible, the planned Parking Technician post should be progressed as planned to facilitate timely repair of Metric machines and Civil Enforcement Officers (CEOs) should be reminded of the importance of always highlighting when parking machines are not working.

Cancellation: (**low risk**) out of our sample of 25 PCNs issued since the 1st January 2018 eight had been challenged, with five challenges being accepted, for example subsequent to proof of a valid permit being provided. While the Council's 'Guidance policies for the enforcement and cancellation of Penalty Change Notices' document is likely to be substantively correct it has not been reviewed since 2012; this document should be reviewed and updated at the earliest opportunity. We also identified that while a sample of cancelled PCNs is reviewed to confirm the reasons for cancellation are correct the process is informal. A consistent sampling rate should be agreed, with the process documented and future review evidenced.

Cash Collection Handbook: (**low risk**) while largely reflective of current practice Internal Audit identified a number of minor errors in the current document. For example references to collecting cash from schools, which is no longer carried out by the Service and a reference to the Civic Centre in Sandown, where the Service was located prior to moving to County Hall. The Cash Collection Handbook should be reviewed and updated, to ensure that it is reflective of current practice.

We would like to take this opportunity to thank Isle of Wight Council staff for their help and assistance with this review.

Current year findings (1 of 8)

Parking Machine Income

Control design

1

Medium

Finding and root cause

Printouts of income received from parking machines are checked against cash collected, with anomalies investigated. However remote reporting/reconciliation is either not working correctly or not being used for all parking machines on the Island. Parking machines on the Metric and Parkeon systems both include functionality to remotely report on cash entered into parking machines. Cash collected is reconciled electronically against that remotely reported for the 36 Metric machines, by the back office administration team, where remote reporting is working but not for the 83 Parkeon machines. This is due to a directly equivalent report not being available on the Parkeon back office system.

As covered elsewhere in this report the Council has a capital bid to replace Metric machines is high usage locations, for which the Council is responsible and Island Roads is in the process of replacing its Metric machines. Internal Audit was also informed that Island Roads have notified the Council that all of the Metric machines which Island Roads are responsible for will be replaced by January 2019.

While there is clearly a gap in current arrangements the risk is potentially reduced by the fact that the Council has informed Internal Audit that all machines impacted are considered low usage. Income reports provided for Internal Audit's review also do not identify any significant income anomalies against historic trends*.

The cash banked from Parkeon machines should be reconciled with the cash recorded as collected by the machines, as is already the cash for the Metric machines where electronic reporting is working. For the remaining Metric based machines where remote reporting is not working, the cash collected needs to be monitored closely, to identify any deviation from historic trends/anomalies at the earliest opportunity. For context the Council reported £1,941,143 of income from off street and £1,017,484 from on street parking charges (these figures include payments by phone); due the level of income involved this finding has attracted a high risk finding.

** For context off street income was £1,954,729 in 2016/17, £1,929,793 in 2017/18; on street income was £1,048,487 in 2016/17, £1,017,484 in 2017/18*

Implications

Without a regime of reconciling cash collected to that received by parking machines there is an increased opportunity for fraud, with cash potentially going missing between being collected from machines and counted at the cash collection centre.

Action plan

The Council will:

Responsible person/title

- Implement the process to reconcile the cash collected and banked from all machines with the cash reported electronically as received by each machine.
- Progress the capital project to replace as many of the Metric machines for which the Council is responsible as soon as possible.
- Monitor income reports closely, to identify any anomalies against historic trends for cash collected from all machines, with a particular focus on Metric machines where remote reporting is not working. Document anomalies on a spreadsheet or equivalent.

Mark Downer, Parking Operations Manager
Vicki Guildford, Revenues Manager

Target date

October 2018

Reference number

18-19-19-01

Current year findings (2 of 8)

SIM Cards

Control design

2

Medium

Finding and root cause

There is a service contract in place for the 83 parking machines on the Parkeon system. Internal Audit was provided with an email exchange between the Council and Parkeon which states that SIM card usage is covered as part of service charges. While it is unlikely that a misuse of SIM cards from parking machines, following theft, would not result in additional costs to the Council, this should be formally confirmed.

SIM cards in the 70 older Metric machines are managed by the Council under a corporate contract, also covering wider mobile telephones and the hand held machines used by CEOs (see further below). The overarching issue is that different names are used to refer to parking meters on the lists provided to us by the core parking team and the team responsible for the corporate mobile telephony contracts. Simplistically this means that should a SIM card be stolen it would be difficult to quickly identify the SIM which needed to be cancelled.

There are further issues with the lists provided for our review, summarised in the table below:

	Total	**Flagged 'removed'**	**Not communicating**	**Match to SIM register**
Parkeon (Island Roads)	83	0	2	15 ***
Metric (Island Roads)	57 (49*)	8	22	28 ***
Metric (Council)	21	0	12	19
Listed on SIM register	101	n/a	n/a	n/a
Discrepancy	**31****	n/a	n/a	n/a

* Less the eight machines known to have been removed.
** 153 machines (excluding those known to have been removed). This is the minimum discrepancy, as a number on the SIM register appear to refer to locations which no longer have parking machines.
*** A number of SIM card locations appear to refer to Parkeon machine locations where Metric machines which have been removed.

As noted further above the two lists provided to us use different names to refer to parking meters. Due to this is likely that the table above will not be 100% accurate.

The discrepancies above are further muddied by the Island Roads website suggesting that they are responsible for 130 parking machines rather than 132. Discrepancies above are contextualised below:

- A minimum of 31 unneeded SIM cards for which the Council is paying £186 per month (£6 per SIM card).
- 15 SIM cards where the closest name/location matches are Parkeon machines, which do not have corporate SIM cards; potential cost of £90 per month (£6 per SIM card).

In addition to the discrepancies in the table above:

- There 23 parking machines which cannot be matched to the SIM register. If the Council was notified that the SIMs from these machines had been stolen there would at best be a delay until the correct SIM could be cancelled.
- There are 31 SIM cards listed on the SIM Card Register which cannot be matched to their parking machines/locations. These could be incurring unnecessary costs to the Council (£6 per month each), or if located in parking machines at best there would be a delay in cancelling them if a SIM card was known to have been removed from a specific parking machine.

The Council needs to schedule an exercise to reconcile its SIM cards to its actual parking machines, including ensuring that in future a naming convention is used to ensure SIMs can easily be reconciled to the machines they are located in.

The overarching mobile telephony contract limits usage charges to £50 per SIM. Bills are issued monthly and any excessive usage would be identified at this point. Once SIMs can be tied to their relative parking machines, as above, if SIMs were to be stolen this would enable them to be identified within 24 hours, as the remote status of machines is checked at least once per day. To further limit the risk to the Council SIM cards should be removed from machines which are not reporting remotely if possible.

Regarding the £50 usage exposure, if SIMs were stolen, we were informed that implementing enhanced logical controls, for example restricting the numbers that SIMs can be used to call, has been discussed historically with the provider. However they are unwilling to do this under the current contract. The contract is being reviewed (a replacement contract is expected to be in place by December 2018); the potential for restricting the usage of the SIM cards in parking machines should be re-raised with the provider as part of the procurement exercise.

More widely we note that parking services are responsible for 14 SIM cards in the handheld devices used by CEOs (£171 per month, £9 per device), 15 SIM cards in blackberries (£120 per month, £8 per device) and two SIMs in mobile phones (£4 per month, £2 per phone). While not in scope for this review we were informed that the handheld devices used by CEOs are capable of being used as mobile phones. If utilised this does represent a potential saving of £124 per month, which should be investigated.

Implications

Unless the Council can validate that it has the correct number of SIM cards and the parking meters in which they are installed then:

- It may be incurring unnecessary costs for unneeded SIM cards.
- There may be a delay in cancelling SIM cards if stolen, leading to higher costs for the Council.
- SIM cards may be incorrectly cancelled, potentially leading to a loss of car parking income.

Action plan

The Council will:

- Request binding confirmation from Parkeon that there would be no additional costs to the Council should SIM cards be stolen from parking machines.
- Reconcile SIM cards to actual parking machines, to confirm that the Council is paying for the correct number of SIMs; as part of this exercise ensure that SIM cards can be definitively tied to parking machines.
- Investigate implementing logical controls on SIM cards in parking meters, as part of

Responsible person/title
Mark Downer, Parking Operations Manager
Target date
October 2018

the procurement exercise for the new mobile phone contract.

- Investigate removing SIMs from parking meters which are not communicating electronically.
- Investigate if costs associated with blackberries/mobile phones held by the service can be reduced.

Reference number
18-19-19-02

Current year findings (3 of 8)

Permits

Control design

3

Medium

Finding and root cause

Resident parking permits are applied for via a downloadable form from iwight.com, All Island/commuter permits (for use in wider Council car parks, i.e. not linked to residency requirements) via an online form, integrated into the Council's online payment system.

Forms are checked by the Business Centre Team responsible for back office parking administration and, once payment has been received, permits are issued. This process is largely manual and undocumented, with a large spreadsheet used to manage permits. Using spreadsheets to manage permits is far from ideal, with key controls such as controlling access and workflow substantively missing. We also note that these spreadsheets contain personal details such as names and addresses, which may be an issue from a GDPR (General Data Protection Regulation) perspective.

In the short term the immediate need is for the process to be documented, ensuring that it incorporates appropriate controls, for example segregation of duties and management review. Longer term a better way of managing permits needs to be identified, either approaching the Sidem vendor (the provider of the core car parking system) or potentially investigating commissioning a bespoke system from the Council's in-house development team.

As part of this process, how reconciliations are managed need to be revisited – this is a key check to confirm that income received ties back to permits issued. Bank reconciliations are carried out centrally, by another team in the Business Centre but this is high level and does not include reconciling individual payments to permits issued. We have also confirmed with the corporate finance team that they do not reconcile income received back to individual permits.

Implications

If personal details are contained in spreadsheets they may not be secure and there will be an increased opportunity for them to be compromised, making it more difficult for the Council to comply with the GDPR.
If processes are not documented then there could be an overreliance on key members of staff and processing will be more likely to be inconsistent.
If appropriate management checks are not in place then discrepancies within income collection, potentially fraudulent, may not be detected and addressed at the earliest opportunity.

Action plan

The Council will:

- Document the processes of managing resident parking permits.

Responsible person/title
Michele Porter, Team Leader for Business Rates and Parking Services

- Continue to progress/investigate alternative arrangements, to implement a more robust approach.
- Identify and implement management oversight. For example checking the total number of permits issued to income received.

Target date
October 2018
Reference number
18-19-19-03

Current year findings (4 of 8)

Penalty Charge Notices (PCNs)

Control design

4

Medium

Finding and root cause

The process of escalation associated with non-payment of PCNs is driven by legislation, with the majority of actions automated by the Sidem system. We checked a sample of 25 PCNs issued since the 1st January 2018, with no issues being identified.

Following a number of escalations, from withdrawing the initial discounted rate, through to charge certificates being authorised (required prior to debt recovery, 56 days from the PCN being issued, if unpaid) ultimately unpaid PCNs are passed to contracted bailiffs for debt recovery. We were informed that, while bailiffs have the right to cease goods to cover the debt, the warrant must be physically served on the non-payer. In practice bailiffs make three attempts to serve the warrant, after which the debt is written off.

While the majority of PCNs are paid before they reach this stage (only three of our sample had progressed to the 'order to recovery' stage, which initiates debts being passed to bailiffs) we were provided with a report on persistent evaders. This details 60 individuals who have 12 or more outstanding PCNs. Of these 15 individuals have 50 or more outstanding PCNs, the highest being number being 149, which represents £65,370 of unpaid debt to the Council for the 15 most prolific persistent evaders, of which £47,285 has been written off.

While there will be instances where there are reasons for repeated failure to pay PCNs, for example mental health issues, this is unlikely to be the case for all of the individuals on the persistent evader list. Clearly this is a significant loss of income to the Council, in addition to the cost of staff time managing these persistent evaders. The Council are actively investigating revising policy, based on sector good practice, to seize persistent evaders' vehicles. This will not only contribute to the Council recouping its costs but will also act as a deterrent against future repeated non-payment of PCNs; this initiative should continue as planned.

PCN income is replicated to Sidem (the car parking system) on an overnight extract from cash receipting. PCNs are only cancelled once it has been confirmed that payment has been received, unless PCNs progress to debt recovery, as covered above.

While there is some oversight/reporting, both from the corporate finance teams and other teams within the Business Centre, appropriate reports should be prepared and considered directly within the Business Centre team responsible for car parking. This would help to identify and address any issues at the earliest opportunity.

Implications

Failing to vigorously pursue debts using all means possible will lead to a loss of income for the Council, extra costs in terms of staff time, poorer parking on the Island and less confidence from the public in the robustness of the Council's enforcement of parking policy.

Action plan	
The Council will: • Progress the planned initiative to revise policy, to seize persistent evaders' vehicles and recoup outstanding debts wherever possible. • Ensure reports from Sidem are reviewed, to confirm payments received, against tickets issued.	***Responsible person/title*** Michele Porter, Team Leader for Business Rates and Parking Services ***Target date*** October 2018 ***Reference number*** 18-19-19-04

Current year findings (5 of 8)

Risk Register

Control design

5

Medium

Finding and root cause

Internal Audit reviewed the current Risk Register for Parking Services. While at a high level this is compliant with corporate expectations, in that a Risk Register exists and there are no overdue actions, there are a number of issues with the content of the Risk Register and its oversight.

Most importantly the Risk Register is not currently a complete and accurate record of the risks facing the Service and how these are mitigated; currently the Risk Register has two risks:

1. Parking operations - failure of pay and display machines
2. Parking operations - failure to adequately maintain parking lines and signage

There are eight mitigations identified for the risks above, four of which have been withdrawn and four are live. However none of the mitigations have been recently updated. We also note that one of the mitigations, creating a post of Parking Technician (to mitigate one above) was TUPEd to Island Roads, who then made the post redundant.

Regarding oversight of the Risk Register, while team meetings and Mini Service Board (MSB) meetings are taking place there is no content regarding risks at the team meetings and limited content regarding risks in the MSB minutes.

A number of risks are identified relevant to Parking throughout this report. In the first instance the Risk Register should be reviewed, both to fully capture relevant risks and existing mitigations and, where there are gaps in current mitigations, to identify appropriate additional controls and activities to control risks.

A specific example not covered elsewhere in this report relates to the safety of Civil Enforcement Officers (CEOs). Team meeting minutes provided for out review identify a number of concerns from CEOs regarding their safety. While we were provided with evidence as to how the Council has responded to these concerns, specifically training which is being provided and a wider 'staff wellbeing' initiative, this is not captured and monitored as a risk/mitigation on the Service's Risk Register.

For context it is important to note that 84% of the pay and display stock is maintained by Island Roads, who are subject to a financial penalty if a machine is not repaired within 24 hours when the machine is a single machine in a parking area. Fortnightly meetings are held between the Council and Island Roads, to discuss any ticket machine issues.

Implications

If appropriate risk management arrangements are not in place risks may materialise, leading to a reactive and potentially poor response.

Action plan

The Council will: • Review and update Parking Service's Risk Register, to ensure this fully captures the risks to the Service and how these are or will be mitigated.	***Responsible person/title*** Mark Downer, Parking Operations Manager ***Target date*** October 2018 ***Reference number*** 18-19-19-05

Current year findings (6 of 8)

Parking Machine Status

Control Design

6

Low

Finding and root cause

The Council receives income from a total of 153 parking machines, with 21 directly maintained by the Council and the remainder managed by Island Roads. Maintenance for all machines within the agreed project network (the sum of all the agreed constituents of the highway network on the Island for the purposes of the Highways PFI) became the responsibility of Island Roads in 2013, under the Highways PFI. Of these, 49 machines are on the older Metric system, 83 are on the newer Parkeon system; currently all of the machines which are the responsibility of the Council are on the older Metric system. Our review identified two issues with status of the parking machines:

- *Machines not communicating remotely*: this issue is mainly applicable to the Metric machines, 34 of these are not currently communicating electronically, although they are taking payments and issuing tickets, including 12 of the 21 machines where maintenance is the responsibility of the Council. This means that identifying machines not working is reliant on notification from the public or CEOs (Civil Enforcement Officers), while income received cannot be remotely monitored.
- *Not all machines are covered by maintenance contracts*: although the Council is responsible for maintaining 21 parking machines these are not covered by a maintenance contract, rather repairs being sourced as and when needed.

All of the parking machine portfolio should be moved to the Parkeon system and be accrued to the project network. However, pursuing this would incur additional costs and is unlikely to be immediately affordable. For clarity the Council is progressing a capital bid (£63,700) which will enable all bar six low usage Metric machines to be replaced. Island Roads also have their own replacement programme althoughit is unclear how long it will be until Island Roads have replaced all of their Matric machines and, under the terms of the PFI, the Council has no leverage to require the programme to be accelerated.

In the short term, costs for accelerating the move away from Metric and accruing machines to the project network should be investigated. There are less costly steps which could be taken now, to partially address the issues above; for example:

- The form for members of the public to report faulty ticket machines needs to be more accessible. This is on Island Roads' website. A link should be added from iwight.com and displayed in car parks.
- As planned a Parking Techncian post should be created by the Council, with a stock of spares held for Metric machines CEOs need to be reminded to ensure that they always flag where machines are identified as not working, with repairs triggered as a result.

Implications

Delays in identifying when Metric machines are not working, leading to delays in them being fixed and potential loss of income.
Inability to get Metric machines fixed in a sufficiently timely manner, leading to a potential loss of income.

Action plan	
The Council will: • Place a link on iwight.com to facilitate the process of reporting faulty parking machines. • Implement the Parking Technician post and stock of spares for Metric machines as planned. • Remind CEOs of the importance of identifying when parking machines are not working.	***Responsible person/title*** Mark Downer, Parking Operations Manager ***Target date*** October 2018 ***Reference number*** 18-19-19-06

Current year findings (7 of 8)

PCN Cancellation

Control design

7

Low

Finding and root cause

The process of issuing and escalating PCN is driven by legislation and largely automatically enforced by the Sidem system. At any point in the process PCNs can be challenged. The Council's approach to cancellation, for example identifying criteria which could lead to a PCN being cancelled, is documented in the 'Guidance policies for the enforcement and cancellation of Penalty Change Notices' document, provided for our review. While this document is likely to be substantively correct its document properties identify that it has not been modified since 2012. We also note that it does not contain a cover sheet setting out elements such as authorship and review schedule and that the introductory page identifies that it is a Havant Borough Council document. This document should be reviewed and updated, addressing these issues, at the earliest opportunity.

Regarding cancelled tickets eight out of our sample of 25 PCNs issued since the 1st January 2018 were challenged, five of these were successful, for example due to permits being held but not displayed (for context permits identify the registration of the vehicle) and two were unsuccessful. One PCN was also cancelled, as the car departed before ticket could be fixed to the vehicle. For the last instance this was signed off by the CEO's supervisor.

While we confirmed the reasons for cancellation/rejection were valid against the Council's Policy, current practice is that cancellations after challenge do not require management approval. We were informed that, while it is not felt to be realistic to review all cancelled tickets, a sample of cancelled tickets are reviewed to confirm the reasons for cancellation are valid. This should be formalised and documented, with a realistic sample size identified and, where cancellation is reviewed, evidence retained, either directly in Sidem or on a separate spreadsheet.

Implications

If documentation is not up to date it may not meet the Council's requirements, is less likely to lead to consistent practice and may introduce an over reliance on the skills/experience of individual members of staff.
If the work of frontline members of staff is not subject to sufficient oversight/review issues with inconsistent practice may not be identified and addressed at the earliest opportunity.

Action plan

The Council will:

- Review and update the 'Guidance policies for the enforcement and cancellation of Penalty Change Notices' document, scheduling future periodic review.
- Formalise, document and evidence the process of sample checking PCN cancellations, subsequent to challenges being accepted.

Responsible person/title
Michele Porter, Team Leader for Business Rates and Parking Services
Target date
October 2018
Reference number

18-19-19-07

Current year findings (8 of 8)

Cash Collection Handbook

Control design

8

Low

Finding and root cause

While Internal Audit notes that staff are well trained and not unfamiliar with the correct process the Cash Collection Handbook (documenting the process of collecting and counting coinage from parking machines) has not been reviewed for a number of years. While it is substantively reflective of practice it does contain a number of elements which are no longer correct, for example collecting cash from schools and referring to the Civic Centre in Sandown, the previous location for Parking Services, now located in County Hall. This should be reviewed and updated at the earliest opportunity.

Implications

If documentation is not up to date and reflective of practice, cash collection processing will be less likely to be consistently exercised. In the absence of up to date procedures new staff may be unfamiliar with the correct process.

Action plan

The Council will update the Cash Collection Handbook, to ensure this is reflective of required current practice and controls. This will circulated to all relevant staff and old Handbooks destroyed.

Responsible person/title
Mark Downer, Parking Operations Manager
Target date
October 2018
Reference number
18-19-19-08

Appendix A: Basis of our classifications

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Critical	A finding that could result in a: • Major loss of service, including several important areas of service and /or protracted period. Service Disruption 5+ Days	A finding that could result in: • Adverse and persistent national media coverage • Adverse central government response, involving (threat of) removal of delegated powers • Officer(s) and/or Members forced to resign	A finding that could results in: • Death of an individual or several people	A finding that could result in: All personal details compromised/ revealed	A finding that could result in: • Litigation/claims/ fines from Department £250k + • Corporate £500k +	A finding that could result in: • Costs over £500,000	A finding that could result in: • Complete failure of project/ extreme delay – 3 months or more
High	A finding that could result in a: • Complete loss of an important service area for a short period • Major effect to services in one or more areas for a period of weeks Service Disruption 3-5 Days	A finding that could result in: • Adverse publicity in professional/municipal press, affecting perception/standing in professional/local government community • Adverse local publicity of a major and persistent nature	A finding that could result in: • Major injury to an individual or several people	A finding that could result in: Many individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from • Department£50k to £125k • Corporate £100k to £250k	A finding that could result in: • Costs between £50,000 and £500,000	A finding that could result in: • Significant impact on project or most of expected benefits fail/ major delay – 2-3 months

	Effect on Service	*Embarrassment/ reputation*	*Personal Safety*	*Personal privacy infringement*	*Failure to provide statutory duties/meet legal obligations*	*Financial*	*Effect on Project Objectives/ Schedule Deadlines*
Medium	A finding that could result in a: • Major effect to an important service area for a short period • Adverse effect to services in one or more areas for a period of weeks Service Disruption 2-3 Days	A finding that could result in: • Adverse local publicity /local public opinion aware • Statutory prosecution of a non-serious nature	A finding that could result in: • Severe injury to an individual or several people	A finding that could result in: • Some individual personal details compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £25k to £50k • Corporate £50k to £100k	A finding that could result in: • Costs between £5,000 and £50,000	A finding that could result in: • Adverse effect on project/ significant slippage – 3 weeks–2 months
Low	A finding that could result in a: • Brief disruption of important service area • Significant effect to non-crucial service area Service Disruption 1 Day	A finding that could result in: • Contained within section/Unit or Directorate • Complaint from individual/small group, of arguable merit	A finding that could result in: • Minor injury or discomfort to an individual or several people	A finding that could result in: • Isolated individual personal detail compromised/ revealed	A finding that could result in: • Litigation/claims/fines from Department £12k to £25k • Corporate £25k to £50k	A finding that could result in: • Costs less than £5,000	A finding that could result in: • Minimal impact to project/ slight delay less than 2 weeks
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.						

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	*Points*
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification		*Points*
	Low	6 points or less
	Medium	7– 15 points
	High	16– 39 points
	Critical	40 points and over

Appendix B: Terms of reference

Background and Scope

Parking fees and charges is a significant source of revenue for the Council generating £ 4,229,855 of income during 2017/18. Operationally administration of 'transactional' services, for example permits, fines and debt recovery, sits within the Business Centre. Parking wardens and strategic management of the service sit within Place. This review will cover elements of both areas, as below:

- *Operation*: confirming that appropriate measures are in place to ensure that parking meters are available, levying the correct fees and that mechanisms are in place to ensure the correct level of income, including for fines, is being collected and reconciled.
- *SIM Cards*: confirming that these are known and that appropriate mechanisms are in place to ensure they are working and configured correctly, specifically to minimise the opportunity for and potential impact of any misuse.
- *Oversight*: confirming that the Service has appropriate risk, performance and oversight arrangements in place and that these are operating effectively.

The sub-processes, control objectives and potential related risks included in this review are:

#	Control objective	Potential risks	Summary of Fieldwork
1	**Operation** • Parking machines are either checked or remotely monitored, emptied when they reach an agreed level. • Appropriate maintenance is carried out on parking meetings, to maximise their availability. • Coinage from ticket machines is collected regularly, with appropriate physical security, counting and banking arrangements in place. • Money collected from ticket machines and tickets issued are reconciled at regular intervals. • Income received by phone is reconciled against expected income at regular intervals. • Income received from residents' permits is reconciled against permits issued at regular intervals. • Issue of controlled stationery to hotels and other authorised resellers of tourist permits is appropriate. • Payment received from resellers is collected in a timely manner, reconciled against tourist permits issued at regular intervals.	• If parking machines are not checked regularly they may cease to work, without the Council knowing, potentially leading to a loss of income and/or an excessive amount of coinage may accumulate. • If income is not reconciled regularly then discrepancies may not be identified and addressed at the earliest opportunity. • If blank permits held by resellers is not controlled then the opportunity for fraud/financial loss to the Council will be increased. • If debts are not pursued adequately then they will be less likely to be recovered, increasing the potential for financial loss to the Council.	Internal Audit will: • Review arrangements to check/remotely monitor ticket machines. Specifically system configuration screens and a sample of logs, if remote monitoring is in place; a sample of rotas/check sheets if machines are checked manually. • We will confirm that there is an appropriate maintenance/service contract in place for parking meters. • Review documentation regarding collecting, counting and banking cash from ticket machines, to ensure that the processes incorporate appropriate management oversight and segregation of duties. • Review a sample of rotas/logs regarding collecting, counting and banking cash from ticket machines. • Confirm that a sample of reconciliations have taken place in a timely manner and that any discrepancies have been investigated and resolved, or otherwise addressed.

	• Income received from fines is reconciled against fines issued at regular intervals. • Appropriate debt recovery actions are taken in relation to unpaid parking fines. • Cancelled parking tickets are appropriately authorised. • Regular reports are run to analyse income, both against historical levels for individual sites and across the wider portfolio, to identify potential anomalies; anomalies are investigated with appropriate action taken. • Charges levied are in line with published/advertised fees.		• Review a sample of debts, to confirm that appropriate debt recovery action has taken place, with any unrecoverable debts written off. • We will review a sample of cancelled parking tickets, to confirm they have been authorised. • Review a sample of income reports, to confirm that anomalies are identified and investigated. • Review fees levied in a sample of car parks, to confirm they are in line with advertised rates.
2	**SIM Cards** • A register is in place of all SIM cards present in parking machines and their location. • SIM cards are used to communicate the 'status' of parking meters and confirm they are functioning correctly. • Appropriate physical security is in place to minimise the opportunity for SIM card theft. • Appropriate logical security is in place, to minimise the opportunity for misuse and ensure that it is detected and addressed at the earliest opportunity.	• If all SIM cards are not 'known' then any they may be excluded from regular 'checks', introducing the potential for issues/thefts to take place without the Council's knowledge. • If SIM cared are not 'checked' regularly then issues/thefts/inappropriate use may not be identified and addressed at the earliest opportunity. • If appropriate physical security is not in place then the opportunity for theft will be increased. • If logical security is not sufficient then if the physical security is compromised then fraudulent will be facilitated.	Internal Audit will: • Confirm that the Council maintains a register of SIM cards present in parking machines and that there are processes in place to validate its accuracy. • Confirm that there is a system in place to monitor SIM cards and that any anomalies are investigated in a timely manner. • Confirm that there is appropriate physical security in place for a sample of ticket machines. • Review logical security in place, for example SIM locking, to confirm that it is appropriate to minimise the opportunity for fraud.
3	**Oversight** • The Service has a Risk Register and an appropriate set of performance indicators, including an income target, profiled over the year. • A regime of regular management meetings take place, with a suitable mechanism in place to capture matters arising, actions and decisions. • Reports covering risk and performance, including actual income against projections are considered at management meetings.	• If a Risk Register is not managed then unforeseen/unplanned for risks may materialise, with a poor/reactive response. • If an appropriate set of performance indicators is not measured and reported then underperformance may not be identified and addressed at the earliest opportunity and performance is less likely to be maximised. • If a regime of correctly managed team meetings, considering both risk and performance, with any	Internal Audit will: • Review the service Risk Register, to confirm that appropriate mitigations are identified to manage risks. • Confirm that a sample of mitigations have been implemented as scheduled. • Review performance indicators, to confirm that they give sufficient coverage of the work of the service. • Review a sample of meeting minutes/records, to confirm that risk and performance are discussed and

	• Risk and performance information is reported upwards to mini and full service board, in summary/by exception.	issues escalated, is not in place then managers may not be sufficiently informed to enable them to manage risks and performance appropriately.	that any issues with risks or performance have been appropriately escalated.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulation or other changes; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.