Deloitte.

ofgem

OFGEM Internal Audit

FY17-06: Fraud Protection and Whistleblowing

FINAL REPORT

Draft to Management:	3 March 2017
Revised Draft to Management:	10 April 2017
Management Response:	19 April 2017
Final:	05 May 2017
Distribution:	Sarah Cox, Chief Operating Officer Chris Poulton, Acting Managing Director, E-Serve Karen Boyle, Head of Counter Fraud, E-Serve Counter Fraud Team Paul Heseltine, Associate Director, Finance and Risk Management Morna Welsh, Enforcement Manager, Enforcement and Compliance Chris Chapman, Senior HR Whistleblowing Manager
Date of Fieldwork:	13 – 17 February 2017

This audit forms part of the FY17 risk based internal audit plan agreed with the Audit and Risk Assurance Committee in February 2016. The objective of this internal audit was to provide an independent assessment of the adequacy and effectiveness of key controls related to fraud risk management, prevention and detection, and the internal and external whistleblowing processes.

This report is prepared on the basis of the limitations in Appendix B.

Contents

1. Executive summary

Background

This audit forms part of the FY17 risk based internal audit plan agreed with the Audit and Risk Assurance Committee in February 2016.

Fraud risk at Ofgem is managed by the Corporate Functions (for Ofgem Regulatory) and E-Serve Counter Fraud teams, responsible for fraud risk management, prevention and detection.

The E-Serve Counter Fraud Team are responsible for recording, investigating and reporting allegations of suspected fraud on E-Serve environmental schemes and social programmes. A key part of this work is the investigation of concerns raised through internal and external whistle-blowers. Each E-Serve scheme is supported by a Counter Fraud Manager, and a dedicated Counter Fraud email address and phone number has been set up for reports of suspected abuse, misuse or fraud.

The E-Serve Risk and Fraud Management Group meets periodically to provide scrutiny of, and challenge to, the activities undertaken by E-Serve to minimise, amongst other things, the risks of fraud. The Associate Director, Finance and Risk Management, attends as the Corporate representative.

Internal and external whistleblowing concerns not related to E-Serve schemes are managed by the HR and Enforcement & Compliance Teams respectively.

In January 2016, the Government Internal Audit Agency reported on a review titled 'Counter-Fraud Agreements for the DECC Schemes'. The audit objective was to provide assurance on how effectively DECC manages the counter fraud arrangements in place with E-Serve for each of the energy-related environmental schemes and social programmes it delivers on behalf of DECC. The internal audit also included the follow-up of recommendations requiring action by E-Serve, if any.

Objective

The objective of this internal audit was to provide an independent assessment of the adequacy and effectiveness of key controls related to fraud risk management, prevention and detection, and the internal and external whistleblowing processes.

Key findings

As a result of our work, we have raised four medium priority findings as follows:

Completeness and contents of E-Serve scheme risk registers (medium)

Examination of the Domestic RHI Fraud Risk Register and E-Serve Schemes Highest Risk Register suggested gaps in the risks included and incomplete/misleading reporting to senior management, Senior Leadership Team, GEMA and the E-Serve Board. In particular there are separately managed risk register and fraud risk register for Domestic RHI.

Corporate Functions fraud risk assessment and reporting (medium)

We reviewed the process for assessing Corporate Functions fraud risk at the strategic, divisional and sub-divisional levels and identified an overall absence of evidence to demonstrate appropriate and sufficient consideration of fraud risks and fraud risk ratings.

Internal whistleblowing monitoring and training (medium)

A central process and database for tracking all internal whistleblowing cases reported, or complaints about Ofgem and their status is currently not in place.

In addition, the Ofgem Internal Whistleblowing Policy states that managers and other staff who may deal with concerns or investigations under this Policy are required to receive regular whistleblower training, however, there is no evidence that such training has been delivered.

Review of E-**Serve's s**chemes highest risk summary report (medium)

As current risk registers are continuously updated with live information and previous versions of the individual scheme risk registers are not saved at a point in time, we were unable to validate the data reported to the RFMG to the underlying risk registers and supporting evidence. Additionally, there were changes in what was reported in the E-Serve Schemes Highest Risk Report between November and January 2017 (in respect of the DRHI Scheme) without appropriate explanation.

Our detailed findings are set out in Section 3.

Summary of evaluation of controls

Area	Evaluation of controls	Number of findings identified as:		
		High	Medium	Low
There is a robust process to identify, assess and manage fraud risks in a timely, continuous and consistent manner		-	1	1
Ownership for each fraud risk is clearly assigned to individuals within Ofgem and E-Serve		-	-	-
Fraud risks are prioritised in an appropriate and timely manner		-	-	-
Fraud risks are added to the relevant fraud risk registers on a timely basis		-	-	-
Fraud risk mitigation plans are clear and proportionate and include specific actions, resources required, responsibilities and timeframes		-	-	-
Fraud risk information is reported in an accurate, consistent and timely manner to Ofgem and E-Serve governing bodies in accordance with Ofgem's governance arrangements, and is subject to detailed review and scrutiny on a periodic basis			2	1
There are formal policies, procedures and guidance documentation related to fraud prevention and this is appropriately communicated to, and accessible by all staff		-	-	2
There is an established process and formal guidance for staff / consumers on internal and external whistle-blower concerns		-	1	1
Appropriate and sufficient training is provided to Ofgem and E-Serve staff related to fraud prevention and whistleblowing concerns		-	-	1
		-	4	6

Responsibility for implementing the recommendations of the GIAA 'Counter-Fraud Agreements for The DECC Schemes' internal audit report was with the GIAA; no action was required by E-Serve.

Overall assessment

We have concluded that SATISFACTORY ASSURANCE can be given on activities in this area based on the level of work and detailed testing performed. While there is a basically sound system, there are weaknesses which put some of the system objectives at risk, and / or prevent achievement of the potential value to the organisation of the resources invested in and expended.

The definitions of the evaluation ratings and categorisation of recommendations are presented in Appendix A.

Delivery of scope

We considered all scope areas indicated in Section 2 and can confirm that weaknesses have been identified against the objectives referenced above. A summary of the issues raised in this audit is set out above in the Executive Summary and full details are provided in Section 3.

Acknowledgement

We should like to take this opportunity to thank all staff involved for their co-operation during this internal audit.

2. Scope of internal audit

Objective

The objective of this internal audit is to provide an independent assessment of the adequacy and effectiveness of key controls related to fraud risk management, prevention and detection, and the internal and external whistleblowing processes.

Scope

This internal audit will consider the processes and controls related to:

Fraud Risk Identification & Management

- There is a robust process to identify, assess and manage fraud risks in a timely, continuous and consistent manner;
- Ownership for each fraud risk is clearly assigned to individuals within Ofgem and E-Serve;
- Fraud risks are prioritised in an appropriate and timely manner;
- Fraud risks are added to the relevant fraud risk registers on a timely basis; and
- Fraud risk mitigation plans are clear and proportionate and include specific actions, resources required, responsibilities and timeframes.

Fraud Risk Reporting

- Fraud risk information is reported in an accurate, consistent and timely manner to Ofgem and E-Serve governing bodies in accordance with Ofgem's governance arrangements, and is subject to detailed review and scrutiny on a periodic basis.

Policies, procedures and training

- There are formal policies, procedures and guidance documentation related to fraud prevention and this is appropriately communicated to, and accessible by all staff;
- There is an established process and formal guidance for staff / consumers on internal and external whistle-blower concerns; and
- Appropriate and sufficient training is provided to Ofgem and E-Serve staff related to fraud prevention and whistleblowing concerns.

GIAA 'Counter-Fraud Agreements for the DECC Schemes' follow up

- Follow up of recommendations requiring action by E-Serve, if any.

Scope Limitations

This internal audit did not extend to providing an assessment on the effectiveness of the fraud prevention strategies, mitigating controls or an opinion on the completeness and prioritisation of fraud risk registers in place across Ofgem and E-Serve.

Approach

We applied the following approach:

- Made contact prior to commencement of the audit to identify key staff, arrange initial meetings and provide details of documentation to which we required access;
- Conducted process discussions with key staff to understand the processes and controls in place for each of the above scope areas;
- Assessed the design appropriateness of key controls;
- Conducted sample testing to assess the operating effectiveness of key controls. Our sample testing covered the period commencing 1 April 2016;
- Met with responsible management to discuss any findings and our proposed recommendations; and
- Produced and issued a draft report, incorporating any actions and recommendations which we agreed prior to issuing the final report.

3. Detailed Findings

3.1 Completeness and contents of E-Serve scheme risk registers

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
Our examination of fraud risk registers identified apparent omissions and raised concerns as to their effectiveness. Specifically: • The Domestic RHI Risk Register only contains one summary fraud risk. Management advised this is due to a legacy business decision to limit the Domestic RHI Risk Register to 20 risks, such that the granular detail of fraud risks to which this scheme is exposed is not well defined. Fraud risks are tracked by the Counter Fraud Team on a separate spreadsheet. • The E-Serve Schemes Highest Risk Register (we inspected this register as at November 2016 and January 2017) contains only one risk for Domestic RHI, being failure to meet publically reported performance measures in 2016/17, which does not appear to reflect the risks actually being faced within the Scheme.	Medium	If risk registers are not operated effectively, an incomplete and misleading view of risks and issues will be presented to the Senior Leadership Team, GEMA and the E-Serve Board.	A refresh of E-Serve risk register content should be undertaken at each level of the risk register hierarchy, including combining the Domestic RHI Risk Register and Fraud Risk Register to present a shared, single view of risks relevant for the Scheme.	Management Response: Agree to refresh DRHI register to include all identified fraud risks. Responsible Party: Gareth John Due Date: 31 May 2017

3.2 Ofgem corporate fraud risk assessment and reporting

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
Ofgem corporate fraud risk (excluding E-Serve) is assessed and recorded via a number of risk registers. The following risk register hierarchy is in operation: (a) Strategic risk register; (b) Divisional risk registers; and (c) Sub-divisional risk registers. We reviewed the contents of, and process for updating the above registers where fraud risks are relevant, and identified an overall absence of evidence to demonstrate appropriate and sufficient consideration of fraud risks and fraud risk ratings, as outlined below: • For the period April 2016 to January 2017, informal meetings were held between the Ofgem Risk Manager and COO (as fraud risk owner) to review the strategic risk register prior to being presented to GEMA. Evidence of the discussions, decisions and actions from these meetings have not been recorded. We note that the Executive Risk Board responsible for reviewing strategic risks was replaced by a Strategy and Risk Board in March 2016. During fieldwork we did not see evidence of any formal meetings having been held since March 2016 and the future existence of this board under the new governance arrangements is in question;	Medium	Fraud risks are not assessed and prioritised appropriately, or are not adequately reported to GEMA, leading to insufficient mitigating controls in place.	1. Management should maintain evidence that the status of fraud risks is periodically considered and discussed with the appropriate staff, including documented records of decisions and actions from these meetings (whether that be at the strategic, divisional or sub-divisional level) to provide transparency over the risk identification and assessment process; and 2. The Corporate Services divisional risk register should be assessed at least quarterly in accordance with the	Management Response: Agree the proposed actions. Corporate Services divisional risk register will be reviewed quarterly as per the Risk Management Strategy. This will be forward-scheduled in the Corporate Services Heads meeting schedule. Responsible Party: Mike Allibone, Head of COO Business Management Services Shaun Scullion, Governance Manager Due Date: Implemented from 2017

OFG-133580

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
• The Ofgem (excluding E-Serve) Corporate Services divisional risk register does not contain any fraud risks, nor is there any documentation to show that fraud risks have been considered. Additionally, the register has not been updated since Q1 2016, whereas page 10 of the Risk Management Handbook recommends quarterly updates; and • The Finance & Risk Management and Procurement sub-divisional risk register contains an overview of the fraud risks identified for the area, however documentation evidencing regular meetings to consider and update this register is not maintained.			Risk Management Strategy.	

3.3 Internal whistleblowing monitoring and training

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
<u>Recording and monitoring of incidents</u> A central process and database for tracking all internal whistleblowing cases reported or complaints about Ofgem and their status is currently not in place. <u>Training</u> In accordance with page 5 of the Ofgem Internal Whistleblowing Policy under "Responsibility for the success of the policy", all managers and other staff who may deal with concerns or investigations under this Policy are required to receive regular training. These staff members include: (a) All line managers; (b) Senior HR Whistleblowing Manager; (c) Senior Partners; (d) Managing Directors; and (e) Audit Committee Chair. However, there is no evidence of the above mentioned roles receiving internal whistleblowing training.	Medium	Tracking and recording of internal whistleblowing concerns is not in place, resulting in cases not being followed through and resolved. Training on handling internal whistleblowing concerns raised is not in place and responsible individuals are not equipped to handle cases in an adequate manner.	Management should: 1. Formally log and monitor all internal whistleblowing incidents or complaints about Ofgem. This should be reviewed periodically by the Senior HR Whistleblowing Manager; and 2. Conduct whistleblowing training for all relevant employees on a periodic basis. Evidence of this (e.g. attendance registers) should be formally maintained.	Management Response: 1. Agreed 2. We will undertake a review to determine who 'relevant' employees should encompass and, following that, ensure appropriate guidance and/or training is available to those staff. Responsible Party: Chris Chapman Due Date: 30 September 2017

3.4 Review of E-Serve's schemes highest risk summary report

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
On a bi-monthly basis the Risk Fraud Management Group (RFMG) Secretariat produces a summary report of the highest risks recorded on the individual E-Serve scheme risk registers, for review and discussion by the RFMG. We requested evidence of review of the RFMG report for November 2016 and January 2017 respectively. There is no formalised evidence of review to validate the accuracy and completeness of the information reported within the RFMG papers. We could only obtain evidence of calendar entries for the review of the RFMG papers, however, Management advised that feedback and suggested amendments are usually communicated verbally. In addition, for two months (November 2016 and January 2017) we attempted to validate the number of high risks reported within the RFMG Summary report by comparing this information to the individual Scheme Risk registers for two schemes i.e. FITs and ECO. Although this information has been validated retrospectively through the assistance of IT, we were unable to do so during fieldwork as the risk registers are continuously updated with live information and previous versions of the individual scheme risk registers at a particular point in time are not saved. Finally, the high risk recorded for the Domestic RHI Scheme (as per the E-Serve Schemes Highest Risk	Medium	Reports produced and issued to the RFMG are not a complete and accurate representation of all the highest risks across the various Schemes. An incomplete and/or misleading view of Scheme risks is presented to the Senior Leadership Team, GEMA and E-Serve Board.	Management should: 1. Implement a checklist to incorporate the steps required to produce the Highest Scheme Risk Register Summary Report (including evidence of review); 2. The checklist should be signed off by both the RFMG Secretariat and Head of Counter Fraud as evidence that the data contained within the report is accurate and complete (with appropriate supporting documentation maintained, such as a copy of the relevant fraud risk registers at a point in time); and 3. Re-examine the current structure and governance of scheme	Management Response: 1. Agreed. Checklist implemented for March 2017 RFMG meeting. 2. Agreed. 3. Re-examination agreed of structure and relationship between RFMG and Scheme Boards, in relation to risk management. Responsible Party: 1. Karen Boyle, Head of Counter Fraud 2. Karen Boyle, Head of Counter Fraud 3. Trish Dreghorn Due Date: 1. Completed. 2. Completed

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
Register) had a severity rating of 20 (almost certain, major) in November 2016, having been increased from 12 (likely, moderate) on 31 October 2016 in recognition of current performance on the auto-accreditation KPI and its inclusion within the E-Serve reporting framework. However, in the January 2017 version the severity rating had been reduced to 15 (almost certain, moderate) with no explanation or justification for the change. While we were subsequently provided with other documentation to support the change, recording the rationale on the risk register would be helpful for a reader's understanding and consistent with the approach taken when the risk is increased.			risks so there is a more 'joined-up' approach to reviewing, assessing and tracking scheme risks between E-Serve's Risk and Fraud Management Group and individual Scheme Boards.	3. 31 May 2017

3.5 Corporate Fraud awareness training

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
Ofgem regulatory staff are not required to undertake mandatory fraud awareness training at even a basic level, and the Ofgem corporate fraud policy does not incorporate fraud training requirements. Management advised a Fraud Awareness training day took place on 9 February 2017, however, this was voluntary. In addition, the fraud awareness eLearning module is not mandatory.	Low	Members of staff have not undergone fraud prevention training and are therefore unable to detect fraud and/or report it adequately.	Management should implement compulsory Fraud Prevention training for Ofgem Orange employees who have a direct and relevant role in fraud prevention or where there is an increased fraud risk (relevant staff include those within Finance, Procurement, etc.). Management should also consider basic fraud awareness training for all staff, for example by including in the new staff induction process and providing periodic refreshers.	Management Response: Agreed We will undertake a review to determine who 'relevant' employees should encompass and, following that, ensure appropriate guidance and/or training is available to those staff. Responsible Party: Paul Heseltine Due Date: 30 July 2017

3.6 E-Serve Counter Fraud Standard Operating Procedures

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
We identified two instances whereby the Counter Fraud Team Manual and E-Serve Risk Management Framework, which includes the Standard Operating Procedures, guidance and templates utilised by the team are not reflective of the actual processes followed by business: • Monthly reporting of suspected fraud cases: in accordance with paragraph 11.1 (page 13) of the Counter Fraud Team Manual, the Counter Fraud team reports monthly to the key stakeholders the status of all suspected fraud cases logged on the Counter Fraud database. However, the reports are only produced every two months; • Extraction of highest Risks: In accordance with paragraph 4.11 of the E-Serve Risk Management Framework, risks captured at scheme level which have a current risk severity of 15 or more (i.e. "red risks") are automatically extracted onto the E-Serve Schemes Highest Risk Register using a data analytics tool, Qlikview. However, these risks are actually extracted using a protected vlookup formula instead of Qlikview.	Low	Processes are not followed consistently or correctly, resulting in an increased risk of knowledge loss if key personnel leave the organisation.	Management should: 1. Updated the Counter Fraud Team Manual and E-Serve Risk Management Framework to address the identified discrepancies; and 2. Continue to perform periodic reviews of all SOPs for accuracy, currency and completeness (e.g. annually).	Management Response: Agreed. Responsible Party: Karen Boyle, Head of Counter Fraud Due Date: 31 May 2017

3.7 Transparency of E-Serve risk register reviews

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
An E-Serve risk register hierarchy is in place, and high priority risks can be escalated through the various levels of the hierarchy to ensure they are appropriately mitigated and managed. The hierarchy of risk registers are as follows: (a) Individual Scheme Risk Registers (b) E-Serve Schemes Highest Risk Register (c) E-Serve Risk Register <u>Monthly reviews of Individual Scheme Risk Registers</u> On a monthly basis, individual Scheme risk registers are reviewed by appropriate Management. We requested the minutes to the meetings for the months of June and November 2016. Whilst we were able to inspect the meeting invites within the respective risk owner's diaries, documented records of what is discussed during these meetings are currently not produced and retained to evidence that fraud risks are being reviewed in accordance with the E-Serve Risk Management Framework. Management also advised that improvements could be made to standardise individual schemes' risk register review process, including evidence to demonstrate that this is consistently performed across all of E-Serve.	Low	Risks are not being reviewed for relevance, and proposed changes following risk review meetings have not been actioned appropriately. As a result, the Scheme Risk Registers are not accurate reflection of the current risk environment.	Management should: 1. Standardise the monthly individual scheme risk register review process through formally documented guidelines; 2. Produce a record of decisions and actions from risk register review meetings (e.g. meeting minutes) for transparency; and 3. Save copies of the above documentation on SharePoint, in the relevant drive, to evidence the review of these registers are consistent with the E-Serve Risk Management Framework.	Management Response: Agreed. Responsible Party: 1. Karen Boyle, Head of Counter Fraud 2. Scheme Risk Managers 3. Scheme Risk Managers Due Date: 31 May 2017

3.8 Periodic user access reviews

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
<u>Counter Fraud</u> Suspected frauds are logged in a restricted access Counter Fraud database. We obtained a copy of the user access list for our period of review and confirmed that all staff have appropriate access. However, periodic user access reviews are not performed. Furthermore, IT send Stealth Audit Reports to the Counter Fraud team each month, which shows a list of users with access to the restricted Counter Fraud and RFMG libraries on SharePoint. However, we could not obtain evidence of review of these reports. <u>External Whistleblowing</u> All whistleblowing incidents referred to the Enforcement Team are logged on an Excel spreadsheet and monitored by the Enforcement Manager. This spreadsheet is restricted to authorised personnel only, however, periodic user access reviews are not performed. Through inspection of the user access listing obtained from IT, we confirmed that two users contained within the listing are not appropriate. One Band D has left the organisation, and the other is no longer involved in performing whistleblowing responsibilities within the team.	Low	Access to sensitive information pertaining to counter fraud or whistleblowing incidents are not restricted to current and appropriate users.	Management should perform periodic user access reviews of the above noted systems / databases. Evidence of this should be formally maintained.	Management Response: Counter Fraud: Agreed. We have requested a stealth audit report for the restricted folder where the counter fraud database is saved so that we can conduct a monthly review of user permissions. External Whistleblowing: A review has now been completed and the two users flagged removed. A quarterly review process has been put in place to monitor access. Responsible Party: Counter Fraud: Karen Boyle, Head of Counter Fraud

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
				External Whistleblowing: Morna Welsh Due Date: Counter Fraud: 31 May 2017 External Whistleblowing: Completed.

3.9 Quality review of Counter Fraud and External Whistleblowing incidents

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
<u>Counter Fraud</u> The Counter Fraud database consists of multiple directories (referrals; open and closed cases) within Microsoft Access; all suspected fraud cases are logged within this database. The Counter Fraud Manager / Assistant Manager will manually update the status of a case based on approval obtained by the Head of Counter Fraud and the relevant Head of Scheme. Closed cases are copied into a different tab for closed cases and manually removed from the list of current cases within Microsoft Access. Currently, there is no evidence of a completeness review performed to ensure that the list of closed cases has been moved accurately and completely within Microsoft Access. <u>External Whistleblowing</u> External whistleblowing incidents referred to the Enforcement Team are logged on an Excel spreadsheet by members of the team. The Enforcement Manager reconciles the total number of incidents received via the central inbox to the Excel spreadsheet, however, evidence of this is not maintained.	Low	All cases reported to the Counter Fraud / Enforcement team is not actioned.	Management should perform a periodic reconciliation of closed counter fraud / external whistleblowing cases for accuracy and completeness. Evidence of this should be formally retained.	Management Response: Counter Fraud: Agreed. Log of closed case completeness review to be introduced. External Whistleblowing: We accept the proposed recommendation and will retain evidence of the validation checks in the existing enforcement whistleblower log. Responsible Party: Counter Fraud: Karen Boyle, Head of Counter Fraud External Whistleblowing: Morna Welsh

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
				Due Date: Counter Fraud: 31 May 2017 External Whistleblowing: 31 May 2017

3.10 Complaints signposting

Rationale	Priority	Risk / Opportunity	Proposed Management Action	Management Response and Timeframe
The signposting for complaints about Ofgem is inadequate and the processes are cumbersome, in stark contrast to the requirements imposed on suppliers and businesses under the Complaint Handling Standards. On the website, complaints about Ofgem is located not under Complaints but instead under Freedom of Information with an office address for written complaints only; there is no email address, telephone number or web-based complaint facility.	Low	Complaints are misdirected internally and response times missed. Ofgem is open to challenge when it fails to practise what it preaches.	Management should update the Ofgem website so that signposting for Complaints about Ofgem is easier to find. Management should also consider introducing a dedicated email address or phone number for complaints.	Management Response: Complaints about Ofgem is now a main heading under Transparency (along with Freedom of Information and Whistleblowing) and describes the response timeline and escalation to the Parliamentary Ombudsman. The webpage is now the first item returned on searching for "complaints about Ofgem". Responsible Party: Already actioned. Due Date: Already actioned.

Appendix A: Definitions of audit opinion

Definitions of assurance levels

Level of Assurance	Description
	Control is generally weak leaving the system open to significant error or abuse.
	Weaknesses in the system are such to put the system objectives at risk.
	While there is a basically sound system, there are weaknesses which put some of the system objectives at risk, and/or prevent achievement of the potential value to the organisation of the resources invested in and expended.
	There is a sound system of control designed to achieve the system objectives.

Prioritisation of findings

Priority	Description
High	Significant and urgent improvement(s) required to address a serious weakness which exposes the organisation to a material extent in terms of achievement of corporate objectives, financial results or otherwise impairs its reputation.
Medium	Essential improvement(s) required to address control weaknesses that may result in the failure of the process under review or improvement required to achieve efficiencies.
Low	Process improvement advised to address minor control weaknesses or align processes with good practice or to achieve efficiencies.

Management should be aware that our internal audit work was performed according to Public Sector Internal Audit Standards which came into effect on 1 April 2013 which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board.

Similarly, the assurance levels provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the level "Substantial Assurance" does not imply that there are no risks to the stated control objective.

Appendix B: Statement of responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Deloitte LLP
London

May 2017