Deloitte.

Future Generations Commissioner for Wales

Internal Audit Report 2018/19

Cyber Security and Data Protection Act Follow Up

Distribution List:

Final Report

- Future Generations Commissioner for Wales
- Director of Finance and Corporate Governance
- Audit and Risk Assurance Committee
- Responsible Officer(s)

Date of fieldwork: May 2018
Date of draft report: May 2018
Date of final report: May 2018

Contents

1. Executive Summary

1.1 Background

The internal audit assessed the adequacy and effectiveness of the Future Generation's Commissioner for Wales (the Commissioner's) internal controls in operation regarding Cyber Security and Data Protection Follow Up.

The internal audit work was carried out through discussion with relevant staff (a list of staff interviewed can be found at Appendix B), examination of documentation and sample testing, as necessary, to confirm the effectiveness of the controls in place.

1.2 Audit Objectives and Scope

The internal audit assessed the adequacy and effectiveness of internal controls in operation. Weaknesses were brought to the attention of management and advice issued on how particular problems may be resolved and controlled.

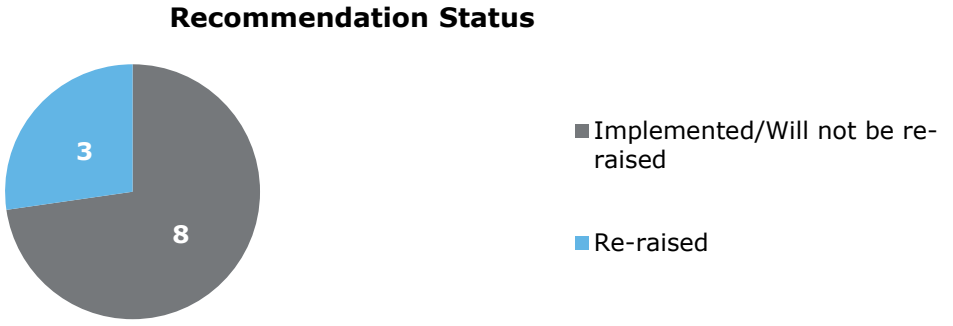
The internal audit sought to assess progress made in implementing the following recommendations raised by internal audit:

- The six recommendations raised in the High Level Cyber Security Review Internal Audit Report issued by Deloitte in 2017/18; and
- The five recommendations raised in the Data Protection Act Internal Audit Report issued by Deloitte in 2017/18.

1.3 Key Findings

Follow up

We followed up progress made in implementing the 11 recommendations identified in the High Level Cyber Security and Data Protection Act Internal Audit Reports issued by Deloitte in 2017/18. We are pleased to report that eight of the 11 prior year recommendations have been implemented. Three recommendations have been re-raised. The findings are detailed in the "Follow Up of Prior Year Recommendations" section.



1.4 Conclusion

We are pleased to report that eight of the 11 prior year recommendations have been implemented. Three recommendations have been re-raised.

Management should be aware that our internal audit work was performed according to Public Sector Internal Audit Standards (PSIAS) which are different from internal audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance classifications provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Our internal audit testing was performed on a judgemental sample basis and focussed on the key controls mitigating risks. Internal audit testing is designed to assess the adequacy and effectiveness of key controls in operation at the time of an audit. Definitions of the assurance classifications and recommendation classifications used in this internal audit report are provided in Appendix A.

1.5 Restriction of Use

We wish to draw to your attention that this report may only be used in accordance with our contract and may not be made available to third parties, except as may be required by law.

1.6 Acknowledgement

We would like to thank the staff who participated in this internal audit for their assistance and co-operation.

2. Follow Up of Prior Year Recommendations

Recommendations that have been implemented or will not be re-raised are shaded in grey.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
High Level Cyber Security Review 2017/18			
2.1 Policies and Procedures It is recommended that the Commissioner compiles and implements an IT Security Policy, covering IT usage, cyber security, and processes and procedures for responding to and dealing with a cyber-incident. It is recommended that the policy should also set out roles and responsibilities in relation to cyber security. This policy should be communicated to all staff as it would be relevant to all IT users. It is further recommended that a Data Classification Policy is established and implemented to ensure data is classified in accordance with legal requirements, criticality, value and sensitivity to unauthorised disclosure or modification. Within this policy, individuals within the organisation should be identified as data owners to ensure accountability for this data.	An IT Security Policy will be prepared as part of our wider information governance review. Phase 1 of this review was completed and reported on in January 2018. Policy revisions will be completed in Stage 2 as set out in the project plan. (Completion date March 2018) IT Security policy is a key element of a good Information Governance approach and the policy will include explicit mention of the requirement for all those working for the Commissioner to follow the policy and the consequences if they don't. There will also be a Data Breach Policy/Guidance Policy alongside it. In the meantime, this report recognises that responsibility for IT is clearly set out in the Director of Finance Corporate Governance's job description and the Office Manager role, created under our recent restructure, explicitly includes responsibility for IT including cyber security. We have assessed our risk of being a target for cyber-attack as	During our testing, we found that the IT Security Policy has been rolled out as part of a full Information Governance update throughout Future Generations Commissioner for Wales' Office. We identified that the policy is on SharePoint, and as a result of this we are confident that all staff have access to the policy. The policy includes IT usage (setting out the acceptable use policy and guidance) cyber security (with guidelines for setting passwords, noting that staff should not deliberately introduce viruses etc.) and processes and procedures for responding to and dealing with a cyber-incident (referring staff to the Data Breach Policy), as well as the relevant roles and responsibilities. We were informed that there is the intention to follow up on the implementation of this policy where it will be confirmed that staff have familiarised themselves with the policy by collecting Declaration Forms. In relation to a Data Classification Policy, given the size of the organization we are satisfied by the reasons given in the original management response for not introducing such a policy. **Recommendation implemented.**	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
Priority: High	low because of the nature of our work and in our judgment the relatively low value of the information we hold to a potential hacker. We have a range of measures in place to safeguard against cyber-attacks – a firewall, anti-virus software, password protected access to our network. We have made the team aware of what to do in the event of a cyber-attack - In May 2017 the Commissioner emailed all staff to remind them to be vigilant and report any suspicious IT activity to the Director of Finance and Corporate Governance and all new entrants are made aware of their IT security responsibilities and what to do if there is a cyber-attack. Our IT services are managed by an external contractor, Orbits IT and whilst responsibility for dealing with a cyber-incident is not specifically listed as a service provided they have confirmed that it would be assumed to feature as part of the general IT support package they provide. Data Classification Policy We are aware that many public bodies use this kind of		

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
	classification system to mark documents but are not convinced that introducing a data classification policy is the right approach for our organisation. We hold relatively small amounts of personal data and safeguard against unauthorised disclosure or modification by restricting access to it in our system either by limiting access to the files and folders where the personal information is held and/or password protecting files that include personal data. In our view this satisfactorily discharges our legal responsibility and introducing a classification system and the resources needed to maintain and monitor the associated processes are not necessary. **Responsible Officer:** Helen Verity **Implementation Date:** 31 March 2018		
2.2 Service Level Agreement It is recommended that an SLA is produced, which comprehensively covers all the tasks and responsibilities undertaken by the external IT contractor, Orbits IT. This process should include confirming with Orbits IT the level of service provided	A formal SLA for general IT support was provided as part of the initial tender process with Welsh Government and an updated version was sent over to FGC on 11th August 2016. This is being reviewed and revised to include services added as a result of the Cyber Essentials accreditation process.	We confirmed, as per discussion with the Finance and Governance Officer that the Commissioner prompted and liaised with Orbits IT, the service provider, in order to obtain an up to date and accurate Service Level Agreement. The resulting contract contains details of the services provided, as well as pricing, and was signed 20 May 2018 by the provider and by the Finance and	Accepted whilst we have no evidence of control weaknesses in our External IT provider's management of our IT systems, we will consider options for gaining formal assurance of this in 2018 when the SLA comes up for renewal. Sang-Jin Park August 2018

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
over network security and access controls as well as a target response to cyber incidents experienced. It is further recommended that the Commissioner should identify any ways in which assurance can be gained from the provider over the services provided and the controls that are in place. **Priority: Medium**	**Responsible Officer:** Sang-Jin Park **Implementation Date:** 31 March 2018	Corporate Governance Officer on 25 May 2018. Within our report for Cyber Security for 1718, we identified a number of areas within which the IT contractors had responsibilities. These included responsibilities for network security and access controls. We note that the SLA sets out the activities that will be covered by Orbits IT, and whilst these are not explicitly in line with the responsibilities identified in our previous report, these cover areas such as system maintenance, managing networks and maintaining security which is deemed satisfactory. In order to monitor the service provided, the Commissioner is sent monthly reports regarding action items, such as updates which need to take place. The Commissioner may wish to consider further options to gain assurance over the IT provider and that the controls they are responsible for are operating effectively. For example, the Commissioner may wish to consider including some time in the next three year internal audit cycle for the internal auditors to visit the IT provider and carry out testing. **Recommendation partially implemented.** **Revised recommendation raised:** It is recommended that the Commissioner considers options available to gain assurance over the external IT provider and the controls that they are responsible for in relation to the Commissioner's IT systems.	

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
2.3 Risk Register It is recommended that the risk register is updated to consider cyber security risks separate from business continuity IT risks. Cyber security risks should be considered in the same format as all other risks. **Priority: Medium**	The Risk register (Risk 7) has been updated to reflect our assessment of risks regarding cyber security. We consider that having gone through the cyber essentials certification process and the mitigating actions we took i.e. removing the video conferencing kit from our network and introducing regular penetrative testing that both the residual likelihood and impact risks are low. We know that if we were to repeat the Cyber Essentials certification process that we would pass the Cyber Security penetration testing without incident but repeating the process comes at a cost and we do not consider this to be a good use of public money. We will continue to monitor our approach to cyber security and will consider our risk assessment rating as a sub set of risk 7 in our monthly SMT risk register reviews. No action.	We identified on inspection of the Risk Register ("Wall of Woe"), that this includes Cyber Security within risk 7. However, this risk has not been separated from business continuity. As a result this recommendation has been re-raised on the grounds that we recommend the Commissioner considers Cyber Security as an entirely separate, new risk within the register. For instance, rather than including this along with lack of funding and staff shortages, Cyber Security should have a consideration of its own, particularly as the level and type of risk regularly changes. **Recommendation to be re-raised.**	Not accepted. Risk 7 was discussed in ARAC March 18 and SMT considered a revised approach to monitoring and reporting on all elements of Strategic Risk 7 in April 2018. Agreed to remove Risk 7 from Strategic risk register and replace by a quarterly risk management report that will include an update on data, physical and cyber system security. Propose to share with ARAC in June meeting and if acceptable the first quarterly report will be prepared for July 2018. Helen Verity
2.4 Asset Risk Action Plan It is recommended that the information assets audit is completed as planned. It is further recommended that in conjunction with the update of the risk register to include cyber	The information assets audit has been completed and will be reviewed with the consultant 21 February. Depending on the outcome of this review a cyber security action plan will be developed and implemented.	We were informed that the information assets audit was completed and we were provided with a copy of the Information Assets Audit spreadsheet. A Cyber Security Action Plan has been produced which includes responsible officers and implementation dates. **Recommendation implemented.**	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
security risks and the results of the information assets audit and implementation of a data classification policy, a specific cyber security action plan is developed to respond to those risks, which includes the actions, implementation dates and responsible officers. **Priority: Medium**	**Responsible Officer:** Sang-Jin Park **Implementation Date:** March 2018		
2.5 Staff Training It is recommended that all staff complete the information security training covering online security and acknowledge completion by signing the declaration sheet. It is also recommended that the induction checklist is updated to include the training for all new starters. **Priority: Medium**	We accept and agree that an efficient organisation needs to set consistent standards, influence behaviour and hold individuals to account. To do this we need to have policy/procedures, give information, advice and training. So our information governance project plan includes a training element as part of new policy roll out. **Responsible Officer:** Sang-Jin Park **Implementation Date:** July 2018	We identified that Information Governance training was provided as part of the monthly staff meeting in May 2018. We evidenced the PowerPoint used to deliver the training and note that this did include online security, along with other sections as part of the full GDPR/Information Governance roll out. Part of the training was for staff to follow up by familiarising themselves with new Information Governance Policies and following this sign to confirm the training has been completed and policies read. With regards to the declaration signing, these be completed once staff have familiarized themselves with all relevant policies. As these are yet to be completed, we were unable to complete testing on this to confirm whether all staff had attended the training. New joiners receive general HR training, as well as an IT training course, we evidenced the list of induction training via email;	Recommendation has already been partially implemented (implementation date: 23 May 2018) An email has been circulated to ask staff to confirm: a. I know where the information Governance Structure is saved. b. I understand the nature and scope of the IG structure c. I have familiarised myself with the contents of the IG structure d. I will abide by the policies and procedures set out in the IG structure and will be in compliance with the GDPR and the FOI Act, and other regulations mentioned in the IG structure With all staff's responses, a declaration sheet will

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
		and in addition to this evidenced that the latest new joiner had signed a form to confirm she had completed the Information Governance/Data Protection course. **Recommendation partially implemented.** **Revised recommendation raised:** It is recommended that the Information Governance training is followed up by all staff members by familiarising themselves with the updated policies and signing declarations to confirm they have done so. It is further recommended that these declarations are logged in order to track who has and has not completed the necessary training.	be created to record which staff members have declared completion of the tasks listed above. Also training will be provided for any new staff members as part of their induction. Review of staff declaration will be completed by July 2018. Sang-Jin Park
2.6 User Access Reviews It is recommended that a user access review is undertaken on a regular basis, at least annually. It is further recommended that the Commissioner considers suspending the network accounts relating to external auditors when usage is not required. **Priority: Medium**	Orbits grant access to data only upon request from authorised FGC staff. FGC request deletion or disablement as part of the wider leaver procedure. In future we will ask Orbits to generate a monthly user audit report to identify users on the Office 365/NAS systems, from which FGC can then review that requests for deletion/disablement have been actioned by Orbits. **Responsible Officer:** Susan Crutcher **Implementation Date:** March 2018	It is noted within the Cyber Security Action plan that User Access Reviews are to be conducted on a regular basis. We were informed on discussion with the Finance and Governance Officer, that Orbits IT now send monthly reports of user accessibility which the Office Manager checks to the internal ICT database in order to confirm that no updates need to be made. We evidenced the latest report from Orbits IT, and also confirmed this to the ICT Database with no issues noted. We note that the network accounts relating to the external auditors have been deleted. **Recommendation implemented.**	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
Data Protection Act 2017/18			
2.7 Data Request and Response Procedure It is recommended that the Commissioner creates and implements subject access and data access request and response procedure in order to help ensure that a response is given within 30 days to be compliant with GDPR. It is further recommended that the Commissioner creates a centralised mailbox for subject access and data access requests and retains request and responses to show evidence of compliance. **Priority: Medium**	We are currently undertaking an information governance project designed to ensure preparedness for the requirements of GDPR and FOIA. We are looking at dealing with data requests over the coming weeks and we will test our process to ensure that time scales and responses can be managed efficiently and evidence of this retained in the best way for our business. We could create a separate mail box to direct requests to (if we do, we will need to determine who will monitor this inbox, and also how the front end of the process will be managed and incorporate this into our policy and procedures). However, as we do not consider email as the appropriate place to keep requests and responses, we will create a centralised point within our system where requests and responses are kept more securely as evidence of compliance. **Responsible Officer:** Sang-Jin Park **Implementation Date:** March 2018	The following process for managing a request for personal information is documented within the Data Protection Policy: • Record request received • Pass to DPO • Open file and apply unique reference number • Identify respond by date – 20 days from receipt • Clarify request - scope • Identity check • All staff email with response date • Collate information • Check 3rd party content • Prepare response to data subject • Content check • Response to data subject within 20 days We note that email requests and responses are kept as PDF files within a centralised site on SharePoint, as the Commissioner feels this is more effective and secure than a mailbox, particularly as mailboxes expire after 12 months. **Recommendation implemented.**	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
2.8 Data Breach Procedure (Staff) It is recommended that the Commissioner creates a procedure document for all staff in relation to data breaches, highlighting the importance of notifying breaches to regulatory bodies within 72 hours, and obtains confirmation from all staff that they are aware of what to do in the event of a data breach. **Priority: Medium**	Data breach is a key component of our information governance structure (as detailed in our project plan). Once the data breach policy is in place the roll out will include training for all staff. Confirmation from all staff that they are aware of what to do in the event of a data breach will be obtained during the stage of staff training. **Responsible Officer:** Sang-Jin Park **Implementation Date:** May 2018	We identified that a Personal Data Breach Policy has been established. The policy was created in May 2018, and is due for review in May 2019. The following is included in relation to notifying breaches: *"In certain circumstances we are required to report a breach/loss Information Commissioners Office within 72 hours and to inform the data subject without undue delay (should the breach potentially impact on the rights and freedoms of the data subject). This must be assessed on a case by case basis and any decision not to notify must be recorded."* At the time of the audit we were unable to gain assurance that staff have taken the training due to the lack of signed declarations or evidence of training. This, as a result, links to a revised recommendation raised within recommendation 2.5. As a result this recommendation will not be re-raised. **Recommendation will not be re-raised.**	Not applicable – recommendation implemented.
2.9 Data Breach Procedure (Management) It is recommended that the Commissioner creates a procedure document for the Finance and Corporate Governance Officer and Line Managers to include the process in which they report to the regulatory bodies and retain	Data breach will be structured around a policy statement highlighting the issue from senior management perspective, followed by definitions of what a data breach is, then a standalone set of procedures and 'to do' checklist. **Responsible Officer:** Sang-Jin Park **Implementation Date:** April 2018	See above for details on the policy. With regard to retaining documentation, the policy states that any breaches "must be assessed on a case by case basis and any decision not to notify must be recorded." Whilst the policy does not specifically set out that documentation in relation to all breaches must be retained, it does note that "Actual or near miss data/loss incidents will be regularly reported through	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
documentation in relation to all breaches regardless if they need to be reported. **Priority: Medium**		the Commissioners senior staff team to the Commissioner and her Audit Committee" and the Policy also includes a Data Breach/Loss Report template to record the details of any incidents. This is deemed satisfactory. **Recommendation implemented.**	
2.10 Privacy Policy It is recommended that the Commissioner publishes a privacy policy document on the website to ensure the public has adequate guidance in relation to the Data Protection Act and the forthcoming General Data Protection Regulation specifically explaining the rights of individuals. **Priority: Medium**	The current terms and conditions agreement on the website has components of a privacy policy. A separate privacy policy will be developed and made publicly available on the website. **Responsible Officer:** Sang-Jin Park **Implementation Date:** April 2018	The privacy policy update to the website includes information on cookies and how personal data is used. The website includes a section titled 'Your Rights' which includes what the individual has a right to request and other rights such as the right for personal data to be erased. **Recommendation implemented.**	Not applicable – recommendation implemented.
2.11 Data Protection Act Policy It is recommended that Data Protection Act (DPA) policies and procedures are updated in line with GDPR. It is further recommended that this policy is updated to reflect the importance of minimising personal data saved on laptops and personal devices.	Part of the current information governance project is to update the DPA policy and procedures (as detailed in the project plan) in line with GDPR. Once the policy and procedures are in place the roll out will include training for all staff. **Responsible Officer:** Sang-Jin Park **Implementation Date:** May 2018	We identified that the Data Protection Policy was created in May 2018 and is next due for review in May 2019. The policy includes sections relating to GDPR such as the GDPR principles and notes the designated Data Protection Officer. In addition to this, we note that the policy states, in relation to the minimisation of personal data kept, that it must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the	Not applicable – recommendation implemented.

Original Recommendation	Original Agreed Management Action	Current Finding	Updated Agreed Management Action, Responsibility and Timetable
Priority: Low		personal data are processed". No issues noted. **Recommendation implemented.**	

Appendix A – Reporting Definitions

Audit Assurance
We have four categories by which we classify internal audit assurance over the systems we examine: Substantial, Moderate, Limited or Unsatisfactory which are defined as follows:

Assurance level	Definitions for Annual and Engagement assurance level	Factors influencing choice of assurance level
	There is a reasonable framework of governance, risk management and control which should ensure that objectives are achieved.	• Adequacy and effectiveness of the governance, risk management and control framework; • Impact of any weakness on delivery of objectives; • Extent of risk exposure; • Materiality: by value to the entity, by value in the engagement context and by nature (eg irregularity and reputational risk); and • We may also take account of management responses to recommendations.
	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.	
	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.	
	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.	

The assurance gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Grading of Recommendations
In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Priority Level	Definition
	Recommendations which are fundamental to the system and upon which the organisation should take immediate action;
	Recommendations which, although not fundamental to the system, provide scope for improvements to be made; and
	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.

Appendix B – Staff Interviewed

Susan Crutcher	Office Manager
Sang-Jin Park	Finance and Governance Officer

Appendix C – Terms of Reference

Internal Audit:	**Cyber Security and Data Protection Act Follow Up**
Commencement:	21 May 2018
Budget:	3 days
Auditor:	Meghan Sugrue
Key contact(s):	Helen Verity Sang-Jin Park
Agreed with:	Helen Verity

Report distribution:

- Future Generations Commissioner for Wales
- Director of Finance and Corporate Governance
- Audit and Risk Assurance Committee
- Responsible Officer(s)

Introduction

This internal audit forms part of the delivery of the approved internal audit plan for 2018/19.

Objectives

The internal audit will seek to assess progress made in implementing the following recommendations raised by internal audit:

- The six recommendations raised in the High Level Cyber Security Review Internal Audit Report issued by Deloitte in 2017/18; and
- The five recommendations raised in the Data Protection Act Internal Audit Report issued by Deloitte in 2017/18.

Methodology

The internal audit work will be carried out by discussion with relevant staff, reading of documents and testing, as necessary, to confirm the effectiveness of the controls in place. The internal audit shall be carried out with due awareness of the risks of fraud and corruption in the processes under examination however it cannot be relied on to identify all fraud and corruption risks. When the internal audit work has been completed, the findings and any recommendations made will be discussed at a pre-arranged exit meeting.

Reporting

A draft report will be issued within 15 working days from the exit meeting to which the auditee will be asked to formally respond. A final report will be issued when all responses have been received and any outstanding issues addressed.

Appendix D – 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

Cardiff

May 2018