Audit Committee

17 September 2020

Internal Audit report – IT controls

Executive Summary

As part of the 2020-21 Internal Audit Plan as approved by the Committee, BDO LLP have undertaken an audit of IT Controls, with a specific review of IT Governance and Management, Service Desk Management and Mobile Device Protection systems and processes. The objectives of the audit were to:

- Provide assurance that adequate governance of IT is in place and to identify strategies for strengthening internal controls in critical areas of IT governance where appropriate;
- Provide assurance that the appropriate processes, technology, and people are in place to ensure that delivery of IT services meet the needs of the organisation; and
- Assess whether mobile device management is adequate to protect personal and business data.

Previous consideration	None.
Decision	The Committee is invited to discuss the report.
Next steps	Recommended actions agreed with the Executive will be tracked for progress in the Committee's standing recommendation tracker report.
Strategic priority	Strategic priority 1: Continuously improve our performance across the organisation Strategic priority 3: Ensure the organisation is fit for the future
Risk	SR 4 - Failure to be an efficient regulator
Financial and resource implications	The cost of the audit is included in the Internal Audit annual fee.
Author	BDO LLP

HEALTH AND CARE PROFESSIONS COUNCIL

INTERNAL AUDIT REPORT - FINAL

IT CONTROLS

SEPTEMBER 2020

Contents

Document history			Distribution	
FINAL	0296398	09/09/2020	HEALTH AND CARE PROFESSIONS COUNCIL	

Auditors:	Christopher Culbert Goran Bonevski
Reviewed by:	Mathew Ring Bill Mitchell

1 Executive Summary

Introduction

1.1 As part of the Health & Care Professions Council (HCPC) internal audit plan for 2020/21, as approved by the Audit Committee, we completed an audit of IT Controls, with a specific review of IT Governance and Management, Service Desk Management and Mobile Device Protection systems and processes.

1.2 HCPC regulates 15 health and care professions so that those professions meet their standards for training, professional skills, behaviour and health. In the performance of its regulatory function, HCPC is highly reliant on the use of IT.

1.3 HCPC's Code of Corporate Governance incorporates a series of regulatory documents and policies which govern how the organisation operates, take decisions and the procedures followed to ensure that actions are fair, efficient, transparent and accountable to the stakeholders.

1.4 The IT function is delivered through a team of 13 IT professionals that provide on-site support and manages the outsourced services from a number of key technology providers. Primary IT services are delivered locally using traditional infrastructure and hybrid virtualised servers. The intention is to move all primary services to cloud services.

1.5 Based on the transformation plan and map developed with the assistance of external consultants, HCPC's Vision is to be the multi-professional regulator of choice.

1.6 A Systems Strategy Review was published in May 2020, with the key finding that HCPC should pause future technology systems spending commitments, until they have defined their operating model and strategy.

1.7 The role of Executive Director, Digital Transformation was recently introduced, with a first task to develop a new Digital Systems Strategy. The strategy will focus on using technology to improve business performance and will shape the new operating model.

1.8 The current IT strategy supports the organisation's strategy as detailed in the HCPC Strategic Intent Document 2016 – 2020 first published in January 2016.

1.9 HCPC have achieved both the ISO27001 and Cyber Essential Plus standards and frameworks certifications.

Review objectives and approach

1.10 The objectives of the audit were to:

- Provide assurance that adequate governance of IT is in place and to identify strategies for strengthening internal controls in critical areas of IT governance where appropriate;
- Provide assurance that the appropriate processes, technology, and people are in place to ensure that delivery of IT services meet the needs of the organisation; and
- Assess whether mobile device management is adequate to protect personal and business data.

1.11 We also considered whether the IT controls in place in the areas under review were scalable to meet future business requirements. The key risks with these areas of activity were whether:

- The IT governance framework is well defined, established, embedded and management of the framework is effectively owned by an appropriate governing body.

- IT enables and supports the achievements of enterprise objectives through the integration and alignment of IT strategic plans with HCPC strategic mission, vision and values.
- The effectiveness and added business value of IT is demonstrated to both the business and IT executives.
- The service desk is organised as the primary point of contact for monitoring and owning incidents, addressing user requests and questions, and providing a communications channel between IT service functions and the business users.
- Problem management is an established process for managing the lifecycle of all systematic issues raised through incident response management and aims to prevent incidents from reoccurring.
- Mobile device solutions and best practices are in place and allow HCPC to effectively manage and secure diverse mobile devices.
- Information assets are centrally recorded and owned by appropriate service managers. Adequate physical controls have been defined and are regularly reviewed by asset owners for all IT Assets.

1.12 The review was undertaken mainly through remote interviews of key staff, review of programme related documentation and seeking evidence to re-perform key management controls and substantiating the application of these controls.

Key conclusions

🟩🟧 (Green-Amber)

Whilst there are good practices related to the IT controls at HCPC, especially in the area of management of the information security, our overarching assessment of the IT controls is that an advancement is needed in the areas of IT governance and IT service desk operations.

1.13 We reviewed the IT control environment, not just from the perspective of the current ways of working, but whether the in scope controls are fit for purpose in light of planed HCPC's digital transformation.

1.14 Overall, it was apparent throughout our review that management responsible for IT have a good understanding of the need for strong IT controls and we identified many areas of good practice in the scope areas under review. The audit also highlighted that Information Assets Management and Mobile Device Management at HCPC are well implemented and controlled and we believe that IT controls around these two practices are appropriate to the risk profile and size of the organisation.

1.15 Nonetheless, we identified two key areas for improvement were noted during the review, which are summarised below and explained in more detail in Section 2:

- IT governance, where the current governance processes should be further developed and formalised.
- IT service delivery, where the existing operating model should be redesigned to match the core aspects of service delivery.

1.16 In addition, key service management processes should to be supported with appropriate formal procedures.

1.17 Management were also keen for this review to consider whether the governance and control arrangements are proportionate and would allow sufficient flexibility for its future transformational plans. Taking our findings and comparing to our experience in other organisations, we consider that the controls in the areas we examined are generally strong, but likely to be about right given the risks.

1.18 We note, as a key illustration, that HCPC have attained ISO 27001, Cyber Essentials and ITIL certifications. This indicates management's commitment to a well-managed and controlled IT environment. In our experience, having all three certifications is above standard practice for organisations of the size of HCPC, as there is a cost overhead in maintaining, auditing and re-certification. However, HCPC is very much a data driven organisation and keeping this often sensitive data secure is critical. Other controls we found in our review to reflect this overall theme, broadly striking the right balance between opportunity and risk.

1.19 With the ongoing digital transformation plans, we also reflected on whether the current control arrangements would unnecessarily inhibit the ability of the HCPC to transform its approaches, processes and IT systems. In our opinion, for the transformation agenda we consider that the current control arrangements to be also about right, so would support maintaining this level of assessment. What HCPC will need to do is ensure that IT controls and security controls are reviewed as the organisation develops its new processes and IT system changes. Designing in strong but proportionate controls into what is being developed will be key and should form a core part of transformation and system development.

1.20 With regard to the main areas for improvement, they fall into two main areas – governance and service delivery.

Governance

1.21 Taking into consideration that IT governance is a subset of organisational governance, IT governance was assessed based on two criteria. Firstly, the quality of IT governance processes in delivering strategic business value year on year. Secondly, whether the processes are repeatable, predictable and scalable to meet the current and future needs of the business. Based on these criteria, we identified and have suggested improvements to the current IT Governance practice that will support sustainable transformation. The improvements highlight the importance of IT-related matters and emphasise that strategic IT decisions should be formalised and owned by senior management.

Service delivery

1.22 At an operational level, a typical IT Service Desk is responsible for incident management, equipment supply, problem management, change management and can assist with technology knowledge management. These all play an important role in any organisational change and transformation. At HCPC, the planned digital transformation will result in new business models and will introduce new technology to support those models. In the implementation of these new services, HCPC's Service Desk will be one of main pillars. Based on these correlations, we believe that the current service desk model would benefit from further improvement to effectively support the planned transformation. It is to the organisations advantage that the Service Desk staff are ITIL[1] certified professionals.

1.23 The practices related to the Information Asset Management and Mobile Device Management form part of a regular improvement process within the Information Security Management System (ISMS). These improvements are made using the continuous improvement model of the Deming cycle (Plan-Do-Check-Act).

Recommendations summary table

1.24 The following table summarises the recommendations made across the key risks audited, grouped by priority ratings:

[1] ITIL, formerly an acronym for Information Technology Infrastructure Library, is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

	Key risk area	Rating	Recommendation Priority rating		
			1	2	3
1	The IT governance framework	Green Amber	-	1	-
2	IT enables and supports the achievements of enterprise objectives	Green	-	-	-
3	Effectiveness and added business value of IT	Green	-	-	2
4	The service desk	Amber	-	2	1
5	Problem management	Green	-	-	-
6	Mobile device solutions	Green	-	-	-
7	Information assets centrally recorded	Green	-	-	-
	Total recommendations made		-	3	3

1.25 The following tables in Section 2 Key Findings show the results of our analysis by each key risk area. Areas for improvement are highlighted with the key recommendations in the right-hand columns.

2 Key Findings

Key Risk Area 1: The IT governance framework

Assessment: Green Amber

Background

An IT Governance Framework is a framework that defines the ways and methods through which an organisation can implement, manage and monitor IT governance within an organisation. It provides guidelines and measures to effectively utilise IT resources and processes within an organisation.

Findings & implication

Positive findings

- There is a formal Code of Corporate Governance which incorporates a series of regulatory documents and policies governing how HCPC operate, take decisions and the procedures followed, to ensure that HCPC's actions are fair, efficient, transparent and accountable to their stakeholders. Such documents provide the 'backbone' for strong IT governance.
- There is formal Governance Unit (Team) lead by of the Head of Governance & Deputy Registrar.
- The ISMS manual provides the framework for the policies and procedures which HCPC have adopted to implement an Information Security Management System in compliance with ISO27001:2013.

Areas for improvement and implication

- We reviewed the Code of Governance with the supporting documents and noted that certain aspects of IT governance are not incorporated in this framework, such as regulatory requirements and organisational structures

Recommendation

1. HCPC should develop and introduce a formal IT Governance framework which aligns with the Code of Corporate Governance.

The aim of the framework should be:

- To ensure that appropriate roles, responsibilities and accountabilities are established for data, system ownership, reporting and communications. This will build on the information which already forms part of the ISMS.
- To report on IT Governance status and tracking of all IT Governance issues and remedial actions to closure; and
- To define responsibility for key IT controls, particularly in respect of IT systems managed by business units.

The IT governance framework should be reviewed periodically, and updated as needed.

Priority 2

👎

Management response

• We understand that current IT governance practices are mainly organised around the Senior Management Team (SMT). Depending on the issue, IT related topics are also discussed at the Council level. The evaluation and monitoring of IT projects are considered by the Project Management team. Although all these practices could be considered as set of IT governance work-streams, there is no comprehensive and consistent IT governance structure and processes which will: – Ensure alignment with organisational governance. – Control the information technology environment through the implementation of good practices. – Clearly distinguish management and governance responsibilities. • The fundamental consequences related to lack of clearly defined IT governance are: – IT and the IT controls may not be fully aligned to the business needs and – The absence of direction in IT investment decisions. • Furthermore, in HCPC's IT environment, where some IT systems are managed by business units, preserving of the current IT Governance practices will be a risk to the digital transformation, due to lack of formally defined processes to monitor, evaluate and direct IT.	Accept Action: The Digital Transformation has an ambitious agenda and roadmap, which means we already recognise that there is a need to develop a Governance model to support transformation activity and operations. Action Owner: Director of Digital Transformation Completion date: Q1 2021

Key Risk Area 2: IT's support for the achievements of enterprise objectives

Assessment: Green

Background

The premise of this key risk area is that the business strategy drives IT strategy and the lack of alignment between them is a major issue that can reduce IT value to the business. We reviewed the current IT strategy (2016-2020), the interim Corporate Plan (Feb – July 2020) and held discussions with the Head of Projects and the Executive Director of Digital Transformation to determine how the prioritisations of IT initiatives are aligned to HCPC's priorities.

Findings & implication

Positive findings

- An Executive Director responsible for Digital Transformation has been appointed, giving a clear direction and focus for digital transformation activities.
- A transformation plan and map has been produced with the assistance of external consultants.
- A Systems Strategy Review was published in March 2020.
- There is a short-term roadmap that allows the organisation to focus on key areas to move the digital agenda forwards, which we consider to be the prudent approach at this juncture.
- The Executive Director of Digital Transformation he has set down the appropriate principles for future transformation.

Areas for improvement & implication

- Given the new digital strategy anchors the planned digital transformation and that all other governance building blocks are influenced by it, in recommendation 1 we included a set of improvements that will mitigate the typical risks related to strategy development.

Recommendation

Please see Recommendation 1

Management response

N/A

Key Risk Area 3: Effectiveness and added business value of IT is demonstrated to both the business and IT executives

Assessment: Green

Background

Required capabilities (solutions and services) are delivered on time and IT services and other IT assets add value to the business.

Findings & implication

Positive findings

- Performance statistics relating to service availability, incident management, internet security and printer usage, which are part of the IT Department monthly reporting to the senior management team.
- From our experience across a wide range of organisations, we consider that level of IT controls are proportionate to the organisation's risks. We note that HCPC have three formal accreditations (ISO 27001, Cyber Essentials and ITIL certifications), which is above the typical level of control for similar sized organisations. However, we consider that there are grounds to maintain this level, given HCPC is a data-driven organisation and the sensitive nature of the data it handles. Our view also applies in respect of allowing flexibility during a period of change. However, during the transformation programme, there will be a need to ensure that IT controls are designed in with this proportionality being one of the objectives and benefits.

Areas for improvement & implication

- Whilst performance statistics are used as noted above, we identified that other operational Key Performance Indicators (KPIs) have not been developed to assist with the monitoring of IT value.

  Measuring IT is essential for good IT governance. In addition, HCPC, in the context of the digital transformation, need a pragmatic approach to monitoring the effectiveness of IT to enable them to adjust their program and assist with decisions on IT investment. Senior management would benefit from IT performance reports based on more detailed KPIs.

Recommendation

2. We recommend HCPC consider developing a more detailed set of KPIs to measure IT performance as a part of the digital agenda and in respect of best practice. Typical general examples for IT KPIs that could be used are as follows:
   - IT expense per employee
   - Support expense per user
   - IT expense as a % of total expense
   - The number of recurring problems.

   Furthermore, based on the new operation model specifics, HCPC should consider adopting ITIL Key Performance Indicators especially in the area of Service Design and Continual Service Improvement.
3. When processes and IT systems are being reviewed and updated as part of transformation, it is important to ensure that the proportionality of controls is kept as a critical success factor in the delivery of new systems.

Both Priority 3

✓

Management response

Accept

Action: Review and revise KPIs against strategic imperatives and best practice.

Action Owner: Head of IT and Projects

Completion date: Q1 20201

Key Risk Area 4: The service desk

Assessment: Amber

Background

HCPC's business environment and employees depend on complex information technology. This dependence results in a challenge: supporting the users of IT technology when they need help. The service desk - a single point of contact within a HCPC for managing users' incidents and service requests – provides this support.

Findings & implication

Positive findings

- Staff in the service desk team are ITIL certified practitioners.
- The replacement of the current IT service management tool is scheduled.
- There is regular and relevant reporting of service desk performance against agreed SLAs to the IT Service Manager.
- The need for further improvement has been identified by IT Service Manager.
- Help articles are published on the Intranet to assist employees with IT services.

Areas for improvement & implication

- We reviewed the current IT Service Catalogue and we noted attributes for IT services are not recorded completely. In addition, we were informed that there is no formal management of the IT services' lifecycle and the IT Service Catalogue has not been updated since it was introduced. We understand, however, that there is a plan to update the catalogue later in 2020.
- The Service Catalogue is at the core of IT service delivery and contains a centralised list of services from the IT service portfolio. The purpose of the Service Catalogue is to provide a single source of consistent information on all agreed services, and ensure that it is available to those who are approved to access it.
- We reviewed the IT service processes and noted that service desk procedures have not been formalised, although there is a process workflow. A procedure document being the step-by-step detailed set of instructions that describes how to perform the tasks in a process.
- The IT service desk mission, vision and values have not been formally established, although we understand this is work in progress. Without a clearly defined mission that is determined by its "customers" needs, a service desk may not meet business requirements.

Recommendation

4. HCPC should develop a Service Portfolio to manage the entire lifecycle of all services, and include three categories: Service Pipeline (proposed or in development); Service Catalogue (Live or available for deployment); and retired services.

   In the development of the Service Catalogue, business unit managers and other decision makers should work with both end users and stakeholders to determine the level of required IT services. Categorisation of the services should be undertaken together with access permissions, restricting access to specific services.

   We recommend that for each identified IT service within the Service Catalogue, the following attributes should be recorded:

   - Name of the service
   - Description of each individual service
   - Service category (i.e. Infrastructure, Software, Hardware, Video, Support, etc.)
   - Supported and related services
   - Service Level Agreement
   - Who can request the service
   - Service owner
   - Costs associated with the service
   - Delivery expectations
   - Security Requirements

Priority 2

5. For the key IT services desk processes, HCPC should develop formal procedures. Procedures streamline the internal process, but also ensure compliance, give guidelines for decision making and provide the roadmap for day-to-day operations.

Priority 2

6. The IT Service desk manager should develop the Service Desk Mission, Vision and Values. This should be approved by Senior Management and distributed to all staff.

Priority 3

⚑

Management response

Accept

Action: This is work that is already identified and will be implemented as part of the service desk improvement.

Action Owner: Head of IT and Projects

Completion date: Q1 2021

Key Risk Area 5: Problem & Incident Management

Assessment: Green Amber

Background

Problem Management is the process responsible for managing the lifecycle of all IT related problems. The primary objective of Problem Management is to minimise the impact of incidents that cannot be prevented.

Findings & implication

Positive findings

- There is a formal Incident Management and Problem Management business process. These are both included in the ISMS manual.

Areas for improvement & implication

- We noted, however, that the Problem Management business process is not supported with a formal procedure. This should be considered together with the issue set out in KRA 4.

Recommendation

Please see Recommendation 4

Management response

N/A

Key Risk Area 6: Mobile device solutions

Assessment: Green

Background

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorised users from accessing the enterprise network.

Findings & implication

Positive findings

- The Mobile System policy sets out HCPC's principles for managing information security controls relating to mobile devices, and for remote working arrangements.
- Symantec Endpoint Protection Manager has been used for blocking the access to the USB, Imaging devices, 1394 Fire wire devices, Modem and Infrared devices, on all Windows endpoints, including the laptops at HCPC.
- Microsoft Intune is implemented as Mobile Device Management platform for the mobile devices at HCPC – a standard security system.
- Two-factor authentications is implemented over access to mobile devices.
- Windows AppLocker is used to whitelist applications on the mobile devices.
- Windows BitLocker is used to encrypt the data on mobile devices drive.
- As a part of the Cyber Essential Plus certification, process systems are independently tested for access control, secure configuration, malware protection and patch management. This provides additional assurance that any security breaches on other systems at the HCPC IT estate should not impact mobile devices.
- There is a comprehensive set of Information Security related policies that provides a multi-layer security approach in protecting the IT estate including the mobile devices. This practice of multi –layer approach in security narrowing the attack surface on the mobile device with isolation of security attach between layers of security.
- The Information Security Officer is responsible for the compliance of mobile devices' technical security controls.
- Data privacy impact assessments are undertaken and approved by owners prior to transferring or sharing data through the available platforms and servers

Areas for improvement & implication

None identified.

Recommendation

None

✓

Management response

N/A

Key Risk Area 7: Information assets recording

Assessment: Green

Background

All information assets must have an identified owner and be catalogued, and the value must be determined and classified as to criticality and sensitivity throughout its life cycle. The information assets from the perspective of information security is everything that has value to the business including people, applications and databases, documentation (in paper and electronic form), ICT equipment and other equipment, infrastructure and outsourced services.

Findings & implication

Positive findings

- HCPC holds the ISO 27001:2013 certification. Appropriate management of Information Asset management is one of the standard's key areas.
- There is a formal Asset Management policy that defines roles and responsibilities related to asset management.
- HCPC maintains an inventory of information assets, which are subdivided by asset owners into separate asset groups.
- There is a formal Physical and Environmental Security procedure that defines the security parameters at HCPC.
- A 'Clear Desk' Policy sets guidelines which reduce the risk of a security breach, fraud and information theft caused by documents or information being left unattended on HCPC premises, or off site where HCPC employees or contractors may work. This also covers information left on display on computer equipment.
- There is a service asset and configuration management process as part of the IT service desk. This process is responsible for collecting and maintaining information about IT assets and showing the relationships that exist among those assets.

Areas for improvement & implication

None identified.

Recommendation

None

✓

Management response

N/A

A Additional information

None

B Audit objectives, Risks & Scope

Terms of reference	
Objectives	The objectives of the audit are to 1) provide assurance that adequate governance of IT is in place and to identify strategies for strengthening internal controls in critical areas of IT governance where appropriate; 2) provide assurance that the appropriate processes, technology, and people are put in place to make sure that delivery of IT services meet the needs of the organisation; and 3) to assess whether mobile device management is adequate to protect personal and business data.
Key risk areas	• The IT governance framework is well defined, established, embedded and management of the framework is effectively owned by an appropriate governing body. • IT enables and supports the achievements of enterprise objectives through the integration and alignment of IT strategic plans with HCPC strategic mission, vision and values. • Effectiveness and added business value of IT is demonstrated to both the business and IT executives. • The service desk is organised as the primary point of contact for monitoring and owning incidents, addressing user requests and questions, and providing a communications channel between IT service functions and the business users. • Problem management is an established process for managing the lifecycle of all systematic issues raised through incident response management and aims to prevent incidents from reoccurring. • Mobile device solutions and best practices are in place and allow HCPC to effectively manage and secure diverse mobile devices. • Information assets are centrally recorded and owned by appropriate service managers. Adequate physical controls have been defined and are regularly reviewed by asset owners for all IT Assets.
Scope	The scope of the review included the following: • Whether IT strategic planning is effectively undertaken with engagement with key business stakeholders and is aligned to HCPC goals and strategic business plan. • Whether the IT strategy is owned and effec4ively monitored by an appropriate executive body in HCPC. • Whether feasible key performance measures have been defined and agreed with management, and whether relevant and sufficient reporting is undertaken which provides owners with adequate oversight. • Whether contracts with external suppliers are commissioned and monitored on a sound basis of aligning to business needs and the IT strategy • Whether service level agreement deliverables and timeframes have been defined and agreed with service desk officers, and whether they are understood by these officers • Whether management regularly review performance of the service desk with the aim of continual service improvement to reduce timeframes for successful responses and to improve end user experience • Whether problem management is undertaken and root cause analysis is performed, with the aim of prevent reoccurring issues and incidents • Whether reporting in relation to service desk management is relevant and useful, and is owned and monitored by appropriate managers with key outcomes being documented • Whether mobile device management tools are effectively configured and implemented in line with best practice

	• Whether all IT assets including mobile devices are securely locked down and local drives are either secure or encrypted in lie with best practice • Whether data as an information asset is centrally recorded and owned by appropriate managers in HCPC, and whether physical controls are regularly reviewed by owners to ensure risks of breach, disclosure or loss are mitigated • Whether data privacy impact assessment are undertaken and approved by owners prior to transferring or sharing data through the available platforms and servers
Approach	The review was undertaken mainly through remote interviews of key staff, review of programme related documentation and seeking evidence to re-perform key management controls and substantiating the application of these controls.

C Audit definitions

Opinion/conclusion	
🟩 (Green)	Overall, there is a sound control framework in place to achieve system objectives and the controls to manage the risks audited are being consistently applied. There may be some weaknesses but these are relatively small or relate to attaining higher or best practice standards.
🟩🟧 (Green-Amber)	Generally a good control framework is in place. However, some minor weaknesses have been identified in the control framework or areas of non-compliance which may put achievement of system or business objectives at risk.
🟧 (Amber)	Weaknesses have been identified in the control framework or non-compliance which put achievement of system objectives at risk. Some remedial action will be required.
🟧🟥 (Amber-Red)	Significant weaknesses have been identified in the control framework or non-compliance with controls which put achievement of system objectives at risk. Remedial action should be taken promptly.
🟥 (Red)	Fundamental weaknesses have been identified in the control framework or non-compliance with controls leaving the systems open to error or abuse. Remedial action is required as a priority.

Any areas for improvement are highlighted with the key recommendations in the right-hand columns. The symbols summarise our conclusions and are shown in the far right column of the table:

Good or reasonable practice	✓
An issue needing improvement	⚑
A key issue needing improvement	✖

Recommendation rating	
Priority ranking 1:	There is potential for financial loss, damage to the organisation’s reputation or loss of information. This may have implications for the achievement of business objectives and the recommendation should be actioned immediately.
Priority ranking 2:	There is a need to strengthen internal control or enhance business efficiency.
Priority ranking 3:	Internal control should be strengthened, but there is little risk of material loss or recommendation is of a housekeeping nature.

D Staff consulted during review

Name	Job title
Neil Cuthbertson	Executive Director, Digital Transformation
Rory Dunn	Chief Information Security & Risk Officer
Paul Cooper	Covid-19 Programme Lead
Claire Amor	Head of Governance
Rick Welsby	IT Support Manager
Jason Roth	Infrastructure Manager

We would like to thank these staff for the assistance provided during the completion of this review.

FOR MORE INFORMATION:

SARAH HILLARY

+44 (0)20 7651 1347
Sarah.Hillary@bdo.co.uk

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

www.bdo.co.uk

Freedom of Information Disclaimer

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 (“the Act”), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.