Audit Committee

4 March 2020

Internal Audit report – Business Continuity Planning

Executive Summary

As part of the 2019-20 Internal Audit Plan as approved by the Committee, BDO LLP have undertaken a review to of the HCPC's Business Continuity Planning.

The objective of the audit was to provide assurance over the design and effectiveness of the key controls operating around the business continuity management process.

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 3: Ensure the organisation is fit for the future and able to anticipate and adapt to changes in the external environment
Risk	SR 2 - Failure to anticipate and respond to changes in the external environment SR 5 - Failure of leadership, governance or culture
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

BUSINESS CONTINUITY PLANNING
JANUARY 2020

Contents

Document history			Distribution
FINAL	296398	28/01/2020	

Auditor:	Louise Sadler Aayushi Karsan
Reviewed by:	Bill Mitchell Gavin Fernandes

1 Executive Summary

Introduction

1.1 As part of the Health and Care Professions Council internal audit plan for 2019/20, as approved by the Audit Committee, we completed an audit of Business Continuity Planning.

1.2 Business Continuity can be defined as "the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident." (Source: ISO 22301:2012)

1.3 Business Continuity Management (BCM) can be seen as "a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." (Source: ISO 22301:2012).

1.4 Overall responsibility for the co-ordination of business continuity plans (BCP) across HCPC was assigned to the Chief Information Security and Risk Officer. The current business continuity arrangements are with the third party Daisy who provide equipment and desk space to allow HCPC to continue their operations. A separate business continuity site is based at Wapping, London.

1.5 HCPC have contracted the use of Shadow Planner which is a smart phone application that stores the business continuity details such as invocation plan, key contacts and partners.

Review objectives and approach

1.6 The objective of the audit was to provide assurance over the design and effectiveness of the key controls operating around the business continuity management process.

1.7 The key risks with this area of activity were whether:

- A Business Continuity Strategy has been defined, which is aligned with the Corporate Business Plan.
- An effective risk assessment process is in place that ensures key systems were identified and included within the plan.
- A BCP is in place and sufficient to enable business critical elements of the plan to be backed up and running within required timeframes to prevent significant business disruption.
- Adequate third party management practices existed to ensure that the levels of controls expected by the organisation were being adhered to by the provider.
- The BCP and/ or IT DRP have been tested for robustness and are kept up-to-date.
- Preparedness of staff resulting in the BCP being implemented correctly in the event of an incident.
- Adequate backup and restore provisions are in place to ensure the availability of information required to resume processing.
- The organisation's disaster recovery plan enables the recovery of IT processing capabilities in the event of a disaster.

1.8 Our approach to the review included:

- Documentation review of the BCP and supporting documentation.
- Interviews with key staff who are responsible for business continuity.
- Analysis and review of the business continuity testing and training documentation.
- Review of third party arrangements focussing on service level agreements.

- Walkthrough of the backup and restore provisions and comparing these to the business continuity provisions.
- Review of the IT disaster recovery plan and the supporting test documentation.

Key conclusions

(Green-Amber)	Minor weaknesses have been identified in the control framework or non-compliance which may put achievement of system objectives at risk.

1.9 Overall, our review of the business continuity arrangements confirmed the business continuity plan has generally been well developed to ensure that the organisation is equipped to respond effectively and efficiently in the event of a disaster. Business continuity roles and responsibilities have been well defined and it was clear that there was an awareness of the business continuity arrangements from discussions with relevant stakeholders. The key risks in the event of a disaster have been defined with HCPC's top 10 organisational risks which also includes the risks to critical business systems that would cause significant impact to HCPC. The Shadow Planner applications serves as an effective tool to host the business continuity plan and contains key information such as invocation procedures, key contacts and suppliers and assembly points. The plan has been tested at least annually either through a live incident or desktop exercise which showed that the business continuity plan was effective in minimising the impact of the incident. In terms of the IT disaster recovery arrangements, there are daily backup schedules to ensure that data is consistently backed up and HCPC uses the third party Azure to deliver the disaster recovery solution which has also been tested on an annual basis.

1.10 HCPC has adopted Shadow Planner, which enables selected employees to access sections of the business continuity plan via a mobile app, and access key contact information in a secure, agile format which can be easily updated by the Chief Information Security Officer. The app contains key business continuity roles and responsibilities that defines their role in the event of an incident. Supplier information such as supplier contact details also exist within the app. Business continuity risks feed into the overarching risk management framework which identifies the top 10 organisational risks that would significantly impact HCPC in the event of a disaster. These risks have designated risk owners and are managed on an ongoing basis to assess the likelihood and impact.

1.11 The business continuity plan is subject to testing on at least an annual basis. The last test was performed in July 2019 testing the effectiveness of the Shadow Planner app and this test did not highlight any significant failings. The business continuity plan was last invoked in 2015 in response to a flood on the main road outside HCPC head office. This was followed up by a lessons learned report which identified areas for improvement if the incident were to occur again.

1.12 To ensure that relevant staff are aware of the business continuity arrangements and their roles and responsibilities, training is administered during the first six months of the employee probationary period.

1.13 HCPC uses the Veeam backup solution which has a pre-input backup schedule to ensure that organisational data is backed up on a regular basis. In addition to this, HCPC contracts with Azure (Microsoft recovery services) with failover capacity, and HCPC has engaged with Daisy Work Recovery site, located in Wapping.

1.14 However, our audit identified a number of areas for improvement with regards to the business continuity arrangements. These relate to aligning the business continuity plan to HCPC corporate objectives, explicitly defining the business impact analysis, maintaining an up to date list of suppliers, formalising the training that is administered to staff and aligning the IT disaster recovery arrangements such as backup frequency to the requirements of the operational processes.

1.15 As a result the business continuity arrangements need to developed in light of the following issues:

- The business continuity plan has not been explicitly aligned to HCPC corporate objectives.
- There is a requirement to maintain an up to date list of key suppliers that HCPC may rely on in the event of an incident.
- Evidence of staff business continuity training is not currently maintained.
- There is a requirement to align the backup recovery timescales to the operational requirements of the organisation.
- Finally, when gaps identified in this report have been addressed, we would recommend that HCPC performs a test of BCP arrangements to ensure that processes are operating effectively identify any further gaps or areas for improvement.

1.16 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.

Recommendations summary table

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

Key risk area		Rating	Recommendation Priority rating		
			1	2	3
1	Alignment between business continuity and corporate objectives	Amber	-	1	-
2	Risk assessments and business impact analysis	Green	-	-	1
3	The business continuity plan	Green	-	-	1
4	Third party management practices	Amber	-	2	-
5	Business continuity testing	Amber	-	1	-
6	Staff awareness	Amber	-	2	-
7	Backup and restore provisions	Green / Amber	-	1	1
8	IT disaster recovery plan	Green	-	-	-
	Total recommendations made		-	7	3

1.18 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: Alignment between business continuity and corporate objectives

Assessment: Amber

Background

A defined business continuity strategy which is aligned to corporate strategic objectives, helps to ensure that key business processes are prioritised during a time of emergency or disaster. We reviewed key business continuity documentation and held discussions with Senior Management regarding the development of business continuity strategy and continued alignment with strategic objectives.

Findings & implication

Positive findings

- The scope of the Business Continuity Management system defines the approach taken by HCPC in determining what actions and steps are required by the organisation to ensure that effective business continuity and disaster recovery controls are in place.
- There is a Roles and Responsibilities document in place, which documents key business continuity personnel and their role in the event of an incident. Specific actions outlining who does what in the event of an incident are documented in the shadow planner app.

Areas for improvement and implication

- The BCP was first developed in 2014 and we confirmed that the plan has been reviewed and re-issued at least annually. We understand that HCPC recently prioritised people as being the most important asset to the organisation and therefore the key priority in the event of an incident or disaster. Whilst we understand that people are an organisation's greatest asset, we were unable to confirm that the BCP has been formally mapped to HCPC corporate plan and strategies to fully understand how a disaster would impact the organisation's ability to achieve their strategic objectives. If the BCP is not aligned to corporate strategic objectives, there is a risk of a divergence between organisational priorities, and what Senior Management deem to be the priorities in the event of an incident. We therefore recommend that the business continuity strategy is reviewed and updated to ensure alignment with the organisational objectives.

Recommendation

1. HCPC should review the current BCP and ensure that this is aligned to strategic objectives. This should include reviewing how the current business continuity arrangements maintain HCPC's ability to achieve the strategic objectives in the event of a disaster.

Priority 2

Management response

Accept

Action: Strategic Priorities and Risks are referenced in the updated DOC A17 Business Continuity Management v1.9 of the ISMS. The BC/DR Plan aims to restore business activity as soon as possible, in light of the organisational size and budget. This will be approved by SMT.

Action Owner: Roy Dunn, CISRO

Completion date: Complete

Key Risk Area 2: Risk assessments and business impact analysis

Assessment: Green

Background

We would expect HCPC to have identified risks of disruption to the organisation's activities and assess which would require action. We reviewed BCP documents and held discussions with management to determine the process for prioritising key systems based on organisational objectives.

Findings & implication

Positive findings

- HCPC have identified the top ten organisational risks, which include unexpected change of legislation and interruption to electricity supply. Key risks (including risks to key systems) have been documented under department headings in the risk register and treatment plan.
- Existing risks are monitored and assessed by risk owners against likelihood and impact on HCPC, the effectiveness of mitigations and the levels of residual risk. This includes description, risk owner, impact before and after mitigations, risk score, mitigations and residual risk score.

Areas for improvement & implication

- We identified that the Business Continuity Management document refers to completing a Business Impact Analysis for the organisation. Our discussions with the Chief Information Security and Risk Officer indicated that the business impact assessment is not a formalised document, but a dynamic assessment which is completed at the time of the incident, by the individual invoking the plan through a combination of knowledge from recent tests, the risk information asset register and the risk register. Whilst we recognise the need for business continuity arrangements to be flexible to cater for a range of scenarios, for the avoidance of doubt during an incident guidance documents should be unambiguous. We therefore recommend that the dynamic nature of the risk assessment should be explicitly stated in the Business Management document.

Recommendation

2. For clarity and the avoidance of doubt in the event of an incident we recommend that the dynamic nature of the Business Impact Analysis is explicitly stated in the Business Continuity Management Document. This should clearly identify the risks of disruption to the organisation's activities and assess which would require action and identify activities that support the provision of products and services to assess the impact over time of not performing these activities.

Priority 3

Management response

Accept

Action: A list of aspects to consider in the dynamic impact analysis has been included in the new training material, and will be added to the ShadowPlanner app.

Action Owner: Roy Dunn CISRO

Completion date: 31/01/2020

Key Risk Area 3: A BCP is in place to enable business critical elements of the plan to be backed up and running to prevent significant business disruption

Assessment: Green

Background

We would expect business continuity arrangements to document prioritised business-critical processes to be bought back up and running, following a period of significant disruption. We reviewed business continuity arrangements, documentation and held discussions with Senior Management as part of our assessment.

Findings & implication

Positive findings

- We confirmed that HCPC has adopted the Shadow Planner app, which is held on key employee mobiles and contains the full Business BCP. We reviewed a report extracted from Shadow Planner, and performed a walkthrough of the app. Our testing highlighted that the BCP includes business critical elements including the invocation trigger, actions, responsible personnel, documents required, and additional requirements, evacuation and stay put procedures, building safety and assembly points within the app.
- The Shadow Planner report documents the requirement to contact employees via the cascade list. It was positive to note that the HR department shares updated staff lists with contact details with the Chief Information Security and Risk Officer on a monthly basis, in order for the Shadow Planner app to be updated.
- The access list for HCPC disaster recovery plan details photographs, names, job title, contact number and the authority to invoke or modify the list, authorise access for themselves or for third parties.
- The 'DOC A17 - Business Continuity Management Document' was approved by the Chief Executive and Registrar and last issued on 27 March 2019 which is in line with the annual review cycle.

Areas for improvement & implication

- We identified that although the Recovery Time Objectives (RTOs) have been formally documented, HCPC has not documented the Maximum Tolerable Period of disruption (MTPD) within the BCP arrangements. Documenting the MTPD can be a useful tool to determine recovery options, depending on the amount of time systems are down for.

Recommendation

3. HCPC should consider formalising the maximum tolerable period of disruption in business continuity arrangements.

Priority 3

Management response

Accept

Action: Business systems owners have provided MTPD, which have been recorded in the document REC 17A. Disaster recovery / business Continuity order of restoration of principle IRT system for HCPC, and maximum tolerable period of disruption v1.7

Action Owner: Roy Dunn CISRO

Completion date: 06/12/2019

Key Risk Area 4: Third party management practices

Assessment: Amber

Background

As organisations increasingly rely on a network of stakeholders and suppliers, business continuity arrangements should identify which key suppliers and third party stakeholders, are critical to continue the delivery of critical services. To determine HCPC BCP arrangements with third parties, we held discussions with Senior Management and reviewed documentation.

Findings & implication

Positive Findings

- We confirmed that HCPC has developed a list of key stakeholders, including relevant regulatory bodies, however we understand that this is still in draft.
- We confirmed that the Shadow Planner app contains some information regarding key suppliers.

Areas for improvement & implication

- We reviewed the 'DOC A17 - Business Continuity Management' document, which broadly lists the groups of key suppliers. However, discussions with the Chief Information Security and Risk Officer highlighted that there is currently ambiguity within HCPC between whether the responsibility for maintaining key supplier information as part of business continuity arrangements should sit with the wider business or within the finance department. Currently therefore, there is no direct ownership for maintaining an up to date list of key suppliers as part of BCP arrangements. In the absence of regularly updating BCP arrangements with key supplier information, there is a significant risk that BCP arrangements will not accurately reflect key supplier information required in the event of an incident.
- We understand from discussions with the Chief Information Security and Risk Officer, that a list of relevant stakeholders (to be notified when the BCP is invoked) is currently in draft, by the Communications team but this was not in place at the time of our audit. If a current list of key stakeholders is not developed and kept up to date, there is a risk that HCPC will not be able to communicate key information in the event of an incident.

Recommendation

4. HCPC should determine whether ownership for maintaining supplier data should sit with the business or the finance department. Once agreed, the responsible department should consider sending monthly updates to Chief Information Security Officer, much like the monthly HR data reports.

Priority 2

5. The list of key stakeholders, (i.e. Regulators and Government departments) is currently in development by the Communications team should be finalised and incorporated into BCP arrangements. To ensure that this remains up to date, the list should be periodically reviewed and amended, as required.

Priority 2

Management response

Accept

Action: A stakeholder list has been provided and will be uploaded to ShadowPlanner, and maintained by the Communications Dept. A list of Suppliers and their contact details will be provided by the Finance Dept for upload to ShadowPlanner

Action Owner: Roz Allison (Head of Communications); Tian Tian (Finance Director)

Completion date: 31/01/2020

Key Risk Area 5: Business continuity testing

Assessment: Amber

Background

Business continuity arrangements should be regularly tested, to ensure that plans reflect business requirements and are fit for purpose. This can also be a good opportunity to determine staff familiarity with the process, and identify and gaps which should be addressed. We reviewed key documentation and met with senior management to identify the nature and frequency of BCP testing.

Findings & implication

Positive findings

- The Business Continuity Management documents states the tests or exercises at company or departmental level will be used to evaluate the effectiveness of the plan. Discussions identified that table top tests occur on an annual basis, unless real events supersede the requirements to test the plan. This was also confirmed through discussions with Senior Management. The BCP was last tested in July 2019.
- The Business Continuity Management document states that the process and tables of content for BC and DR are evaluated at least every 12 months. Review of key documents confirmed this. The extract from the Shadow Planner business continuity app was last updated on 29-08-2019 by the Chief Information Security and Risk Officer.
- We confirmed that the BCP was fully invoked in 2015, following a flood on Kennington Park Road. It was positive to note that a follow up report to the Executive team was collated, which identified lessons learned. We also verified that lessons learned from the BCP invocations were captured via the organisation-wide incident log and actioned as completed.

Areas for improvement & implication

- Given that we have identified some gaps in current BCP arrangements at HCPC (see KRA 1-4), BCP arrangements will need to be tested to ensure that these areas are working effectively.

Recommendation

6. HCPC should address identified gaps in the current BCP and schedule another planned BCP test to ensure that updated areas are working effectively.

Priority 2

Management response

Accept

Action: A further test will be carried out in the next Financial year

Action Owner: Roy Dunn CISRO

Completion date: 31/03/2020

Key Risk Area 6: Staff awareness

Assessment: Amber

Background

Staff training at induction on-going awareness is key to ensure that BCP arrangements are successfully implemented in the event of an incident. We discussed arrangements for staff BCP training with Senior Management and consulted with individuals across the business to determine whether current arrangements are adequate and appropriate.

Findings & implication

Positive findings

- BCP training is delivered to relevant new staff, who are line managers or key stakeholder in the business identified as requiring access to Shadow Planner, following successful completion of the employee's six month probation period. The training is delivered by the Chief Information Security and Risk Officer, following installation of the Shadow Planner app on the employee's mobile device.

Areas for improvement & implication

- We confirmed that BCP training for staff of the Shadow Planner app is not formally documented or recorded, we were advised that this is only because certain individuals within HCPC are required to have access. If staff training is not formally recorded, HCPC will not be able to track employee training coverage.
- We also confirmed that Shadow Planner app training is not periodically refreshed, and is only used by staff in the business as part of BCP testing or a real life incident. If staff are not regularly appraised of BCP arrangements and use of the Shadow Planner app, there is a risk that staff will not use the system correctly in the case of a real life incident. Furthermore in view of the difficulty and business disruption associated with fully testing the BCP on a regular basis, it can be difficult to identify staff knowledge gaps, especially regarding the functionality of Shadow Planner in real time. To maintain staff knowledge and awareness HCPC could refresh BCP training, for individuals who require it, or develop refresher material for app users, to ensure a maintained knowledge of the functionality.

Recommendation

7. The Chief Information Security and Risk Officer should document staff training (in the use of the Shadow Planner App).

Priority 2

8. HCPC should refresh Shadow Planner app training at least annually for users and could consider developing training and guidance to ensure a continued knowledge and awareness of the app.

Priority 2

Management response

Accept

Action: ShadowPlanner users are already trained on its use as the app is delivered to their device. Annual testing includes a training element. Standalone generic BCM/DR training is being developed for SMT & Business system owners and Heads of department.

Action Owner: Roy Dunn CISRO

Completion date: 31/01/2020

Key Risk Area 7: Backup and restore provisions

Assessment: Green Amber

Background

Backup and recovery testing is an essential part of the disaster recovery plan to ensure that data can be reliability retrieved in the event of an incident. Testing backup and recovery arrangements is an essential part of the disaster recovery plan to ensure timely recovery plan of IT processing capabilities

Findings & implication

Positive findings

- HCPC uses the Veeam back up tool solution, which has a virtual machine schedule based on the different type of machines. The schedule is based on the criticality of the systems. For example, if the system is deemed critical then the schedule will be set to take more regular backups compared to a system that is not critical to the business.
- HCPC uses separate technology for their data backups. This is agents based where agents are installed on various servers such as SQL servers. These backups have set schedules which are daily incremental followed by full weekly backups followed by monthly backups which are taken offsite and retained and stored by a company called Recall.
- We also reviewed the Disaster Recovery/Business Continuity Order of Restoration of Principle IT systems for HCPC - this document details the applications and order in which these should be brought back per priority.

Areas for improvement & implication

- We understand that criticality for back-up and restore provisions has been defined by IT and has not been formally confirmed with the business. In the absence of confirmation with business owners, there is a risk that IT back up priorities will not be aligned to organisational strategic priorities and objectives. Whilst it may be appropriate that IT set the criticality there needs to confirmation with the business owners of the various operational processes to confirm this.
- The review highlighted that whilst the data backup frequency is likely to be appropriate there needs to be confirmation that this aligns with the recovery point objectives of the various business processes. For example, if a Recovery Point Objective is 4 hours for a given business process then a daily incremental of 24 hours is likely to be insufficient.

Recommendation

9. Senior Management should review the Veeam back up schedule and confirm that priorities are aligned to HCPC business operational processes.

Priority 3

10. Senior Management should confirm that the data back-up frequency is appropriate to meet Recovery Point Objectives in the event of an incident.

Priority 2

Management response

Accept

Action: A paper will be presented to SMT detailing the current recovery time service standards set out by data owning departments.

Action Owner: Executive Director of IT and Resources

Completion date: 27/02/2020

Key Risk Area 8: IT disaster recovery plan

Assessment: Green

Background

Disaster recovery should include IT recovery plan capabilities to ensure the continuity of key systems, in the event of an incident. Often, organisations achieve this through the transfer of system components to a secondary system. To assess IT processing capabilities in the event of a disaster, we met with staff from IT and reviewed key documentation.

Findings & implication

Positive findings

- HCPC use Azure site recovery services with failover capacity. Discussions with Management confirmed that the recovery target time is 15 minutes.
- Recovery services are tested alongside the backups and restore tests. We reviewed screenshots which confirmed that the last successful test failover was completed on 21 September 2019. No issues were identified. We also reviewed systems which confirmed that backups occur daily, over the weekend and at month end.
- Shadow copies of file server dating back to more than a month are completed twice a day.
- A review of the disaster recovery contract confirmed that HCPC have engaged with Daisy Work Recovery site, located in Wapping.

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 objective of the audit was to provide assurance over the design and effectiveness of the key controls operating around the business continuity management process.
Key risk areas	• A Business Continuity Strategy has been defined, which is aligned with the Corporate Business Plan. • An effective risk assessment process is in place that ensures key systems are identified and included within the plan. • A BCP is in place and are sufficient to enable business critical elements of the plan to be backed up and running within required timeframes to prevent significant business disruption. • Adequate third party management practices exist to ensure that the levels of controls expected by the organisation are being adhered to by the provider. • The BCP and/ or IT DRP have been tested for robustness and are kept up-to-date. • Preparedness of staff results in the BCP being implemented correctly in the event of an incident. • Adequate backup and restore provisions are in place to ensure the availability of information required to resume processing • The organisation's disaster recovery plan enables the recovery of IT processing capabilities in the event of a disaster.
Scope	The scope of the review included the following: • Review of the business continuity strategy and how HCPC have aligned this to the organisation's corporate plan • Review of the business impact analysis that HCPC has undertaken to assess the business continuity risks and the impact on how this could affect the organisation and the corresponding recovery time and recovery point objectives. • Review of the process to create the BCP and how this has been aligned to the business critical elements of the organisation. • Review of the third party business continuity arrangements in place that HCPC rely on and how these contracts are managed and tested. • Review of the business continuity testing that has been carried out and how lessons learnt have been incorporated into the feedback loop to refine the BCP. • Review of the training that has been provided to staff to ensure that relevant staff are well prepared in the event of a disaster. • Review of the backup and restore provisions that HCPC has in place and how this aligns to the business continuity arrangements. • Review of the IT disaster recovery plan and whether this has been tested to ensure HCPC can restore their operational systems.
Approach	Our approach to the review included: • Documentation review of the BCP and supporting documentation. • Interviews with key staff who are responsible for business continuity. • Analysis and review of the business continuity testing and training documentation. • Review of third party arrangements focussing on service level agreements. • Walkthrough of the backup and restore provisions and comparing these to the business continuity provisions. • Review of the IT disaster recovery plan and the supporting test documentation.

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
John Barwick	Executive Director & Interim Chief Executive Officer
Guy Gaskins	Executive Director of IT & Resources
Jacqueline Ladds	Executive Director of Policy & External Relations
Roy Dunn	Chief Information Security and Risk Officer
Ewan Shears	Governance Officer
James McMahon	Office services Manager
Richard Houghton	Head of Registration

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