POLICE AND CRIME COMMISSIONER FOR CAMBRIDGESHIRE AND CAMBRIDGESHIRE POLICE

Internal Audit Progress Report

29 October 2020

RSM

Contents

1 Introduction

The internal audit plan for 2020/21 was approved by the Joint Audit Committee at the April 2020 meeting. This report provides an update on progress against that plans and summarises the results of our work to date. The Executive Summary and Key Findings of the assignments below are attached to this progress report.

We have finialised one Cambridgeshire only report and one Collaborative report since the last meeting.

2 Reports

2.1 Progress against the internal audit plan 2020/21 Cambridgeshire only

Assignment	Status / Opinion issued	Actions agreed			Target timing as per plan
		Low	Medium	High	
Cash, Banking, and Treasury Management (1.20.21)	**Final Report Reasonable Assurance**	**4**	**2**	**0**	**Q2**
General Ledger	Planned 6 November 2020				Q3
Payments & Creditors	Planned 6 November 2020				Q3
Payroll	Planned 16 November 2020				Q3
Business Planning	Planned 1 February 2021				Q4
Ethics & Culture **	Planned 18 Feburary 2021				TBC
Follow Up	Planned 1 March 2021				Q4

** Please see appendix B

2.2 Progress against the internal audit plan 2020/21 Bedfordshire, Cambridgeshire and Hertfordshire Collaborative

Assignment and Organisation Lead		Status / Opinion issued	Actions agreed			Target timing as per plan
			Low	Medium	High	
Cloud Security Management	**Hertfordshire**	**Final Report Advisory**	**2**	**5**	**0**	**Q1**
Occupational Health	Cambridgeshire	In Progress				Q2
Procurement – 7Force	Essex	In Progress				Q2
Risk Management	Bedfordshire	In Progress				Q2
Health & Safety	Bedfordshire	In Progress				Q2/3
Procurement - BCH	Cambridgeshire	Planned 9 November 2020				Q3
Remote Working**	Hertfordshire	Additional review added to the plan Timing – TBC but likely Q4				n/a

** Please see appendix B

Appendix A – Other matters

Changes to the 2020/21 audit plan

Please see below changes since the last JAC meeting:

Note	Auditable area	Reason for change
1	BCH - Remote Working	Due to the increased risks surrounding remote working, management have requested RSM to complete an additional review in the area of Remote Working including Cyber Security links.
2	Ethics & Culture	This was moved from quarter 3 to quarter 4 at the request of management as the Chief Officer Team are launching a new organisation-wide cultural reform piece of work on the 15th October 2020. Therefore, most of the areas within the scope of the audit will be part of this reform work.

The JAC will note that many of the audits for both the Bedfordshire, Cambridgeshire and Hertfordshire Collaborative plan are currently scheduled to be completed during Q2 and Q3. Historically we have found that the Collaborative audits have taken longer to complete to final report stage and as a consequence we have scheduled them to be conducted before the end of Q3 to allow them to be completed and reported before the end of the financial year.

We would recommend that any proposed delay to the agreed schedule is reported to and approved by the lead JAC before the audit is rescheduled to avoid any impact on our ability to provide the required assurances in a timely manner.

Other Assurances

Regional Distribution Centre - We were requested by the Director of Essex and Kent Support Services to undertake a review of the controls in place at the Regional Distribution Centre (supporting the procurement and distribution of all PPE as a result of the pandemic for the 7 Forces in the East of England) which has been set up in Essex. The report has been issued in final and we understand that the Director of Essex and Kent Support Services has shared the findings with all Forces and OPCCs.

Annual Opinion 2020/21

The JAC should note that the assurances given in our audit assignments are included within our Annual Assurance report. In particular the JAC should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion. None of the findings from the final reports to date will negatively impact the year end opinions. We will provide further updates throughout the year.

Added value work

We have issued the following client briefings since the last Joint Audit Committee:

- Audit & Risk Committee – Navigating COVID-19
- Emergency Services New Briefing – September 2020

Quality assurance and continual improvement

To ensure that RSM remains compliant with the IIA standards and the financial services recommendations for Internal Audit we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews being used to inform the training needs of our audit teams.

The Quality Assurance Team is made up of; the Head of the Quality Assurance Department (FCA qualified) and an Associate Director (FCCA qualified), with support from other team members across the department.

This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

Appendix B – Executive summaries and action plans from finalised reports

EXECUTIVE SUMMARY- CASH, BANKING AND TREASURY MANAGEMENT

With the use of emails for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to undertake our sample testing.

Why we completed this audit

The objective of this audit was to assess the design and effectiveness of the control framework in place to accurately record and account for cash income managed by the Constabulary. This also included a review of the management of cashflow within the treasury management function.

The Treasury Management Team consists of four members of staff who report to the Principal Financial Accountant, all of whom are overseen by the Head of Finance. Daily activities performed by the Treasury Management Team include the production of daily cashflow forecasts and key reconciliations are completed through the use of eFinancials. As at August 2020, we noted the Constabulary's reported cash balance was £27.2m.

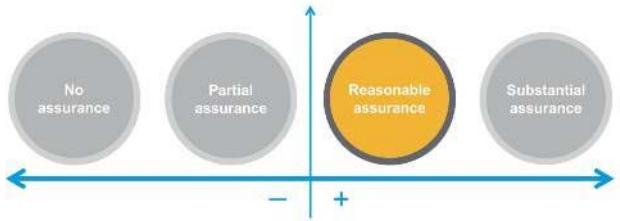
Due to the impacts presented by COVID-19, a remote working approach had been adopted from March 2020. However, a rotated working schedule was introduced in June 2020 whereby one member of staff is present in the office on Mondays, Wednesdays, and Fridays to ensure core treasury management tasks, that cannot be completed remotely, are addressed.

Conclusion

Our review found the Constabulary had in place Financial Regulations, Force Financial Instructions (FFIs) and procedures to support the activities undertaken by the Treasury Management Team pertaining to the management of cash and banking. We found this was supported by both daily and monthly cashflow forecasts which we confirmed detailed the Constabulary's position with the aid of graphics and narratives. Whilst we noted cash received via the post is to be opened by staff under dual control mechanism, we found this could not be evidenced by the Constabulary at the time of the audit. Furthermore, we selected a sample of ten instances when cash was received by the Treasury Management Team and found in five cases, receipts were not issued.

Internal audit opinion:

Taking account of the issues identified, the Constabulary can take reasonable assurance that the controls in place to manage this area are suitably designed and consistently applied. However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified area(s).



Key findings

We identified the following weakness:

Cash Income Received

We selected a sample of 10 instances when cash was received via the post between April to September 2020. We confirmed in eight instances, emails were issued by departments which stated the value to be received via internal post. Furthermore, we confirmed the values stated within emails reconciled to the values captured within the receipt spreadsheet. In the remaining two instances, we were advised by the Accountant that the Thorpe Wood Enquiry Office had not issued emails informing the Treasury Management Team that cash had been sent via the internal post. Without informing the Treasury Management Team that cash is to be received, there is a risk that misappropriation of cash may occur. **(Low)**.

Through discussion with the Accountant, we were advised that cash bags were opened with at least two members of staff present. However, this could not be corroborated through review of the samples selected as we were informed records were not maintained to capture the individuals responsible for opening cash bags. Due to the issues presented by COVID-19, we were advised by the Accountant that the number of staff present onsite had reduced significantly to only one representative from the Treasury Management Team. Due to this in relation to cash received, dual opening of cash could not be performed. The Constabulary had not considered the use of video calls to enhance the control and therefore reinstate dual controls (remotely and efficiently). Without maintain records to ensure dual controls are functioning, there is a risk of insufficient audit trails which may hinder investigations in the event that misappropriation were to occur. Furthermore, individuals may not be held accountable in the event that discrepancies occur due as audit trails are not in place. **(Medium)**

Receipts Issued

From a sample of ten cash entries captured in the receipt spreadsheet, we confirmed in only five instances receipts were issued. In the remaining five instances where receipts were not issued, we were informed that the challenges presented by COVID-19, including revised working arrangements, may have been a contributing factor. Without issuing receipts, there is a risk of insufficient audit trails as departments may not be able to take assurance that cash has been received. **(Medium).**

We have also agreed an additional three low priority actions which are outlined further in the 'Detailed Findings and Actions' section of the report

We noted the following controls to be adequately designed and operating effectively:

Financial Regulations and Force Financial Instructions (FFIs)

We confirmed the Constabulary had in place guidance in the form of the BCH Financial Regulations which we noted were last reviewed in May 2020. This was further corroborated through review of the July 2020 Business Coordination Board minutes as we noted the Board had reviewed and noted its contents. We confirmed the Regulations were accessible by staff through the Constabulary's intranet facility.

Similarly, we found FFIs were in place which we noted were last reviewed in April 2020. Through discussion with the Head of Finance, we were advised the FFIs were not subject to approval by a formalised board. However, we were informed the FFIs were to be signed off by the Chief Constable and the Constabulary Chief Finance Officer which we confirmed through review of the document. We confirmed the FFIs contained adequate guidance on the cash and banking processes.

Department Cash Exchanges

Through discussion with the Head of Finance, we were advised that departments such as the Enquiry Office and Overseas Visitors Registration Department (OVRD) may receive cash income for services provided. We confirmed the Enquiry Office had in place spreadsheets to capture money received. We were advised by the Enquiry Officer that receipts were issued to individuals. As cash is not banked by the Enquiry Office, we were advised that cash was stored within cash bags and was sent via internal post to the Treasury Management Team for banking. This was further corroborated through review of the April, May, and August 2020 spreadsheets issued to the Treasury Management Team.

Similarly, we found spreadsheets and cash sheet records were maintained by the OVRD Officer which captured money received for services provided. This was corroborated through review of an October 2020 cash sheet document and we found entries were clearly dated which were supported by descriptions of transactions and the total amounts received. We were informed by the OVRD Officer that in the event cash was received it was placed within cash bags and issued to the Treasury Management Team for banking. Additionally, we were advised emails were issued by the OVRD to confirm the value of the cash via the internal post. We confirmed this mechanism was in place through review of the previous three emails issued across March and August 2020.

To assess the accuracy of income captured within receipts spreadsheet once the exchange of money between departments had occurred, we selected a sample of ten transactions across March – August 20 from the Enquiry Office and Overseas Registration departments. We confirmed in all instances, cash exchanged from the departments were accurately recorded within the receipt spreadsheet.

Insurance coverage

We confirmed that the Constabulary has continued with its existing policy, renewable at the 1st of October each year which covers cash held within the safes and cash in transit. The policy had just renewed so the Constabulary will be with Travelers until at least until 30 September 2021. Through discussion with the Insurance Manager, we were advised a limit of £25k in any safe on the premises was covered under its existing policy. As at October 20, we noted £5.7k in cash and £8.4k was held within the safe which we noted was in line with insurance coverage.

Cash Banked

As per the Constabulary's FFIs, cash is to be banked on a weekly basis. Where cash held is considered to be of very low value, cash is to be banked on a fortnightly basis. However, through discussion with the Head of Finance, we were advised that due to a reduction in the number of staff on site due to the impacts of COVID-19, banking was performed less frequently. This was further corroborated through review of the receipts spreadsheet as we noted cash banked between two to four times per month across April to September 2020.

We selected a sample of five instances in which cash was banked between June to September 2020. Through review of the corresponding bank statements, we confirmed in all instances cash was deposited, the amounts of which reconciled to the figures captured within the receipt spreadsheet. All of our sample was within the insured level.

Reconciliations

We obtained the salaries account, payment account, and income account reconciliations performed across June, July, and August 2020. Through review of the reconciliations completed, we confirmed in all instances, balances reconciled to the Constabulary's bank statements. Whilst we noted variances were reported between expected balances and actual bank balances, we found justifications for differences were provided. We noted these were due to errors in uploading balances to the general ledger twice by mistake which we noted were identified by the Finance Officers responsible for completing the reconciliations at the time. We confirmed segregation of duties was demonstrated between the individual performing reconciliations and the individual responsible for review and approval. Furthermore, we found in all instances, reconciliations were supported by approval emails.

Loan approvals

Through discussion with the Head of Finance, we were advised that the Constabulary had taken out six loans between 2004 and 2018. However, during the October 2016 Cash, Banking, and Treasury Management audit we found testing was performed against five of six loans currently in place, therefore we have not repeated this testing.

In the remaining instance, we noted a loan amounting to £10m was taken over a 30-year period. We confirmed approval for the loan taken was approved by the Deputy Chief Executive and former Chief Financial Officer for the Constabulary. Whilst we noted the approval provided was for the £10m loan of a 40-year period, we were advised by the Accountant that there was an oversight error made by the previous Chief Financial Officer and a 30-year period was agreed instead. As we noted the initial loan value of £10m was agreed by both the Deputy Chief Executive and former Chief Financial Officer as per the Financial Regulations, and found no issues regarding repayment periods being reported through both Treasury Management and Revenue and Capital Budget Monitoring reports, we have not considered this to be an exception.

Cashflow forecasts

We confirmed the Constabulary produced both daily and monthly cashflow forecasts. We obtained a sample of 20 cashflow forecasts produced from May to September 2020 and confirmed in all instances, the Constabulary's cashflow forecast was clearly presented.

We noted these were supported by graphics which detailed the Constabulary's current investment holding balances in addition to proposed investment movements. As at the 24 September 20, we noted the Constabulary had forecasted to have between £20m to £35m available in funds between October 2020 to March 2021.

We obtained the May, June and July 2020 Budget Monitoring Reports which we noted included cashflow forecasts produced by the Treasury Management Team. Through review of the reports, we found key information such as overtime, capital funding, and cashflow forecasts were detailed. Furthermore, we confirmed cashflow forecasts were presented to the Business Coordination Board via Revenue and Capital Budget Monitoring Reports through review of the corresponding minutes. We noted no issues pertaining to treasury management were reported.

Surplus funds

Through discussion with the Accountant, we were advised that surplus funds were identified as part of the production of daily cashflow forecasts. Where investment proposals are made, we were advised that this is an indication of surplus funds available for investment in line with the Constabulary's Treasury Management Policy. We obtained a sample of ten daily cashflow forecasts produced between May to September 2020. Through review of the cashflow forecasts, we found in seven instances investment or transfer proposals (partial temporary transfer of funds from an approved institution to the Constabulary's income bank account) were made regarding the Constabulary's funds. In the remaining three instances we found investments were not proposed which we noted were accepted by the Principal Accountants.

In the seven instances where investments or transfers were proposed, we confirmed in all seven instances investments were in line with the approved list of institutions and approvals were provided by either the Principal Accountants or Head of Finance. We found investment proposal documents and corresponding approvals were retained by the Treasury Management Team. Furthermore, we confirmed in all instances agreed investments and call-backs reconciled to transactions captured within the Constabulary's bank account statements.

Investments

Through review of the 24 September 2020 daily cashflow, we found the Constabulary had invested a total of £30.085m across various institutions which included Barclays FIBCA, Money Market Funds (MMF), and a Lloyds Call Account. We confirmed the Constabulary had in place an approved list of institutions where funds may be allocated. Through review of the listing, we confirmed the Constabulary's current investments were in line with the approved list of institutions. Furthermore, we found this was in line with the Constabulary's Force Financial Instructions.

Treasury Management Updates

We found Treasury Management updates were provided to the Business Coordination Board in the form of a mid-year report, treasury management strategy review report, and an annual treasury management strategy review report.

2019/20 Mid-year Review

We obtained the 2019/20 mid-year Strategy Statement and Annual Investment Strategy Report. Through review of the report, we found it detailed key information such as economics and interest rates, strategy updates, and capital position. Through review of the corresponding December 2019 Business Coordination Board minutes, we confirmed the mid-year review report was discussed. Whilst we noted no concerns were reported regarding the report, we found prudential borrowing requirements are to be reviewed in line with the southern police station building works.

2020/21 Treasury Management Strategy Statement (TMSS) Review

We noted the 2020/21 Treasury Management Strategy formed the base for the annual strategy report presented to the Business Coordination Board. Through review of the Treasury Management Strategy, we confirmed updates regarding the Constabulary's treasury and capital position was provided. We noted the report forecasted the Constabulary to have made £52.4m in capital investments from 2020/21 to 2023/24. Through review of the February 2020 Business Coordination Board minutes, we noted the 2020/21 TMSS was presented for review. We found it was reported that the Head of Finance provided an overview of the strategy and its approach to balancing the demands of the Capital Programme with holding sufficient cash to support daily activities.

Annual Review

We confirmed an annual review of the 2019/20 TMSS took place within the July 2020 Business Coordination Board meeting. As per the annual treasury management review report, we noted the Constabulary reported £10.9m was held in investments which were managed in house. We found this was an increase of £1m of funds invested compared to holdings in March 2019. We obtained the corresponding July 2020 BCB minutes and confirmed the annual treasury management report was reviewed by the Board. We noted the Chief Finance Officer and Director of Resources reported that current borrowing rates acted as a disincentive to borrow for commercial purposes. We noted no further concerns were raised.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Income Receives via the Post				
Control	When cash income is sent via the internal post it is received within secure sealed bags containing unique serial numbers to enhance security control mechanisms. This is also supported by emails issued by receiving departments which capture the value of cash to be received by the Treasury Management Team. To reduce the risk of embezzlement and ensure cash is accurately accounted for, at least two members of staff are to be present when opening cash bags received. Once cash has been counted and logged within the Income Spreadsheet, another check is performed by the second person present to ensure cash has been accurately counted and captured within the spreadsheet. The cash received is stored within a safe located within one of the Constabulary's offices which is only accessibly by secure card passes. Email responses are provided to initial emails received, confirm cash has been successfully receipted.	**Assessment:** **Design** ✓ **Compliance** ×		
Findings / Implications 2	Through discussion with the Accountant, we were advised that cash bags were opened with at least two members of staff present. However, this could not be corroborated through review of the samples selected as we found records were not maintained to capture the individuals responsible for opening cash bags. Due to the impacts presented by COVID-19, we were advised by the Accountant that the number of staff present onsite had reduced significantly to only one representative from the Treasury Management Team. Due to this, we were informed that should cash be received, dual opening of cash could not be performed. Without maintaining records to ensure dual controls are functioning, there is a risk of insufficient audit trails which may hinder investigations in the event that misappropriation was to occur. Furthermore, individuals may not be held accountable if discrepancies occur as audit trails are not in place.			
Management Action 2	The Treasury Management team will consider the introduction of a spreadsheet to capture the individuals present when opening cash bags. The spreadsheets will capture key information such as: • Date cash was received; • Individual responsible for opening the cash bags; • Individual present overseeing the opening of cash bags; and • Email confirmation issued to the Accountant from both individuals declaring their presence opening cash bags.	**Responsible Owner:** Peter Coverdale – Accountant	**Date:** 31 October 2020	**Priority:** Medium

Income Receives via the Post				
	The Treasury Management team will also consider the use of available technology such as MS Teams to demonstrate dual control when opening cash bags where only one member of staff is present on site.			

Receipts Issued				
Control	When cash is received, members of staff from the Treasury Management Team are responsible for opening, counting, and entering cash amounts within the Income Spreadsheet. The Income Spreadsheet in place contains various Microsoft Excel macro formulae which automatically generate cash receipts in the form of PDF documents in addition to drafting emails. Once receipts have been automatically generated, emails are issued to debtors confirming the amount paid to the Constabulary. Where cash is received within other areas of the Constabulary, the Enquiry Office for example, paper cash receipts are issued, and receipt reference numbers are retained for records	**Assessment:**		
		Design	✓	
		Compliance	×	
Findings / Implications	Using the same sample of ten cash entries captured in the receipt spreadsheet, we confirmed in only five instances receipts were issued. We found these five have been issued in a timely manner by the Treasury Management Team. In the remaining five instances, we were advised by the Accountant that receipts were not issued. We were informed that the challenges presented by COVID-19 including revised working arrangements may have been contributing factors as to why receipts were not issued. Without issuing receipts, there is a risk of insufficient audit trails as departments may not be able to take assurance that cash has been received.			
Management Action	The Head of Finance will reiterate the importance of issuing receipts when cash is received. Additionally, the Head of Finance will introduce a 6-monthly spot check to confirm whether receipts have been issued following cash received. Where receipts have not been issued, this will be investigated, these checks will be documented.	**Responsible Owner:** Joanna Conlon – Head of Finance	**Date:** 31 Oct 2020	**Priority:** Medium

EXECUTIVE SUMMARY – CLOUD SECURITY MANAGEMENT

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely.

Why we completed this audit

Bedfordshire, Cambridgeshire and Hertfordshire Police and Crime Commissioners and Police ('BCH') requested an advisory review of the Cloud Security Management controls as part of the 2020/21 annual internal audit plan. BCH have been using cloud-based systems (since April 2020) for a number of key systems. The purpose of this review was to identify and evaluate key controls being used to ensure that data stored in the Cloud is kept secure and available to users.

Two systems were specifically focused on in this review, Office 365 and Foreign Nationals:

- Office 365 is a widely-used subscription-based service offered by Microsoft and BCH will use Office 365 as a Software as a Service 'SaaS' solution, with the infrastructure managed by risual, a third party service provider. It is not yet available to general users. This system was chosen as it will be a critical system used on a daily basis by BCH.
- BCH plans to use the Foreign Nationals system to register visiting foreign nationals from high risk countries. Foreign Nationals is directly managed by BCH and the Azure platform is leased from Microsoft Azure as an IaaS (Infrastructure-as-a-Service) solution. Foreign Nationals is a system that has been used by Bedfordshire and Hertfordshire previously, although it is now out of support. The cloud-based solution is yet to go live. This system was chosen as it is one of the two systems to be managed on Microsoft Azure entirely by BCH.

Appendix B sets out a glossary to support the report findings.

Conclusion

Overall, it was noted that whilst BCH has only recently started to adopt Cloud-based technologies, there are controls in place designed to reduce the risk that configurations and processes are inadequately set up. These include controls to benchmark against the NCSC's Cloud Security Guidelines (Appendix A) by the Information Assurance Unit and segregation of duties for access controls.

However, we did identify opportunities for controls improvement and in this regard this report sets out 5 'Medium' and 2 'Low' priority actions. Whilst it should be noted that the focus of this audit was on Office 365 and Foreign Nationals system specifically, the actions highlighted in the report should be applied to new systems hosted in the Cloud (if applicable) as well to ensure that best practices are applied across all Cloud environments.

Key findings

We identified the following key findings:

An Information Asset Register exists which lists systems and other information assets used by BCH. Despite the Information Asset Owner Procedure requiring owners to keep this up to date, we found that details regarding how each system is used, personal data stored within each system and data security controls have not been completed. This is required for BCH to be in line with the GDPR/Data Protection Act (DPA) 2018 requirements and to support cloud based systems governance. **(Medium)**

Two-Factor authentication is not currently used to access privileged accounts in the Microsoft Azure environment that hosts the Foreign Nationals system. As privileged accounts will have the ability to change how the environments operate and change controls upon which the system relies, these should be restricted by extra safeguards. If privileged accounts to Cloud-hosted systems are not protected sufficiently, it increases the risk that access could be compromised. **(Medium)**

Privileged user and system access activity is not currently logged for accessing the Azure environment that hosts the Foreign Nationals system. Lack of logging of critical activities, such as elevation of access rights or the activity of users with execute rights, increases the risk that a threat actor could gain and make use of elevated privileges without immediate awareness of BCH. **(Medium)**

There is no specific process in place for how Cloud-based changes will be managed for systems managed specifically by BCH, increasing the risk to any cloud based changes. Additionally, there is no control in place to designate a system owner to Cloud-based systems. If a process for Cloud-specific changes is not documented or implemented, it increases the risk that changes will not be managed appropriately, potentially leading to errors or delays in deployment and a potential adverse impact on cloud-based security and availability. Moreover, the absence of a process to formally designate cloud-based system(s) owners increases the risk that important or critical updates will not have resource assigned to manage them. **(Medium)**

At the time of this review, no evidence was available that penetration testing has been conducted on Office 365, or that this will be conducted shortly prior to (or shortly after) the go-live dates for new systems. Moreover, current cloud based project plans do not include this requirement. As such, no framework currently exist for when a penetration test should be conducted (specifically on new systems in this case). If the systems are not actively tested for exploits and vulnerabilities, it increases the risk that they may be compromised with a resulting loss arising. **(Medium)**

Examples of well-designed controls:

Inspection of reports confirmed that BCH has ensured that Office 365 and Foreign Nationals have been assessed by the Information Assurance Unit (IAU) for the configurations in place and have been benchmarked against the NCSC's Cloud Security Guidelines. Reports created by the IAU were inspected to verify that risks were raised against the Cloud Security Guidelines. This indicates that both systems are in line with the Government's suggested guidelines for cloud-hosted systems (once suggested corrective action is implemented), thereby reducing the risk to operational security and availability.

To support privileged access governance to Foreign Nationals and Office 365, segregation of duties controls in place, including formal approval required by the Business Services Team. Audit sample testing confirmed that this control is being adhered to. Moreover, we confirmed through inspection of the workflow and a log of reviews completed that privileged access the Azure environments that host Foreign Nationals and Office 365 is reviewed on a periodic basis (depending on level of access granted). Additionally, if a role is provided for a short period of time, approval must be provided by the Business Application Team and the permissions are granted to an individual for a pre-configured period of time (mostly 4 hours) before being relinquished. This was confirmed through inspection of the configured times provided for the roles and a sample of one role being approved.

Controls are in place to govern the financial amount that BCH is spending on the Azure subscriptions (areas where the system environments are hosted). Screenshots were obtained to confirm that automated alerts notify the Business Services Team if configured budgets for a month are exceeded and that corrective action taken to investigate why such overruns take place.

We confirmed through review that there are Service Level Agreements (SLAs) in place with the third parties that help to manage the cloud environments for Office 365 (risual) and Foreign Nationals (Microsoft Azure). This reduces the risk that services will not be performed to the required standard by BCH. Service Performance hours used are sent to the Business Service Team on a periodic basis.

DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Area: Data access policies and agreements with the cloud provider(s) in line with current data protection legislation and corresponding security controls				
Missing Control	There is no control is in place designed to ensure that the Information Asset Register is reviewed/ updated on a regular basis.			
Finding / Implication	Through our review of the *BCH14/008 Information Asset Owners (IAOs) Policy and Procedure*, we observed there is a requirement for the IAR to include new or major changes to information assets. Through online inspection of the IAR it was noted that information required for the Foreign Nationals system and the new Cloud-hosted systems is missing, including what data is stored, security controls in place, the lawful bases for processing data and the retention periods. An up to date IAR is required for GDPR/DPA 2018 requirements and to support cloud-based systems governance, the absence of which adversely impacts cloud-based systems governance.			
Management Action 1	Management will ensure that the Information Asset Register is reviewed, updated and that information is recorded describing what data is held, including the controls in place to safeguard data confidentiality, availability and integrity. The IAR should be reviewed by the IAOs on an annual basis and when significant changes are made to information assets.	**Responsible Owner:** Andy Gilks Director of Information Management	**Date:** 30/01/2021	**Priority:** Medium

Area: Access controls	
Missing Control	Two-Factor authentication is not used to authenticate privileged administrator accounts to the Microsoft Azure environment that hosts the Foreign Nationals system.
Finding / Implication	If privileged accounts to the Microsoft Azure environment that hosts Foreign Nationals are not protected sufficiently, it increases the risk that access could be compromised. It was noted that this is a suggested requirement in the NCSC's Cloud Security Guidelines, and therefore, all Cloud-based systems should have an additional safeguard on privileged access.

Area: Access controls				
Management Action 2	Management will ensure that privileged users accessing Microsoft Azure are using 2-Factor authentication.	**Responsible Owner:** Jonathan Black, Director of ICT	**Date:** 31/03/2021	**Priority:** Medium

Area: System access and activity logging and review				
Missing Control	There are no configurations in place to log privileged user activity using Azure Sentinel or other methods for Azure environment hosting the Foreign Nationals system.			
Finding / Implication	Whilst there are preventative controls in place (segregation of duties for access elevation), a lack processes to log critical activities, such as elevation of access rights or the activity of users with execute rights, increases the risk that any unauthorised access and activity of elevated privileges will not be detected and addressed on a timely basis. *Mitigation: Request for privileged access in Azure requires approval by the Business Applications Team.*			
Management Action 3	Management will log 'high-risk' activity on the Foreign Nationals back-end environment and future Cloud-based systems. This could include: • Privileged access escalation; and • Activity of users with write/execute ability.	**Responsible Owner:** Jonathan Black, Director of ICT	**Date:** 31/03/2021	**Priority:** Medium

Area: ICT change controls for making current and future changes to the technology service and systems				
Missing Control	Controls for Cloud specific changes have not been formally documented or implemented in the change management workflow and system owners have not been assigned to assess and prepare for critical system changes to Cloud-based systems.			
Finding / Implication	We confirmed through inspection of the *Process for Changes* document that there is a formal process for change management with changes categorised as Emergency, Normal and Standard. Discussion with the Change Manager indicated however, that there is no formal process for Cloud changes. We also observed that it was not possible to filter for Cloud-specific changes on the service desk system SupportWorks. If a process for Cloud-specific changes is not documented or implemented, it increases the risk that changes will not be managed appropriately, potentially leading to errors or delays in deployment and a potential adverse impact on cloud based security and availability. Moreover, the absence of a process to formally designate cloud-based systems owners increases the risk of a subsequent lack of system governance accountability and corresponding issues arising.			

Area: ICT change controls for making current and future changes to the technology service and systems				
Management Action 4	Management will consider documenting additional steps to follow in the event that a Cloud change is required. This may require additional approvals or planning depending on the criticality of the system(s) involved. Additionally, management will consider assigning system owners for particular Cloud systems to identify impactful changes.	**Responsible Owner:** Jonathan Black, Director of ICT	**Date:** 31/12/2020	**Priority:** Medium

Area: Vulnerability assessments and penetration testing arrangements (assessment of the scope, frequency and action planning of such assessments that have been undertaken during the last 12 months).				
Missing Control	Internal Vulnerability assessment controls are in place. No cloud based penetration testing framework detailing when a penetration test should be carried out and supporting governance arrangements are in place			
Findings / Implications	Inspection of the *Cloud Security Configuration Report,* written and issued by the BCH Information Assurance Unit in August 2020, confirmed that a Nessus vulnerability scan on the external IP addresses for the Foreign Nationals Service had been performed and that just 10 informational findings had been raised. We indicated by the Project Manager for Office 365 that a penetration test had been conducted by the National Monitoring Centre (NMC), although it was not possible to obtain evidence of this at the time of this review. Discussion with the Project Manager for Office 365 indicated that whilst there were no plans to run an additional penetration test prior to the system go-live date, it would be covered in the annual penetration test on all systems. During discussions with the BCH Information Assurance Manager & BCH Information Security Officer we were advised that it was not certain whether a penetration test would be conducted in the current year. As such, the above findings indicate that there is no penetration testing control framework is in place. If Cloud-based systems with externally facing interfaces are not actively tested for exploits and vulnerabilities prior to go-live and on an ongoing basis, it increases the risk that systems vulnerabilities may exist that are not detected and remediated on a timely basis. *Mitigation:* Microsoft Azure performs penetration testing against its services and infrastructure, but not the applications hosted by customers.			
Management Action 5	Anything outside the normal risk governance returns will be considered by the SRO for additional IT health checks	**Responsible Owner:** Andy Gilks Director of Information Management	**Date:** 30/01/ 2021	**Priority:** Medium

For more information contact

Dan Harris, Head of Internal Audit

daniel.harris@rsmuk.com

Tel: 07792 948767

Suzanne Rowlett, Senior Manager

Suzanne.rowlett@rsmuk.com

Tel: 07720 508148

rsmuk.com