POLICE AND CRIME COMMISSIONER FOR CAMBRIDGESHIRE AND CAMBRIDGESHIRE CONSTABULARY

Internal Audit Progress Report

9 August 2022

RSM

Contents

1 Introduction

The internal audit plan for 2021/22 was approved by the Joint Audit Committee at the April 2021 meeting and for the 2022/23 plan in April 2022. 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 in **bold** are attached to this progress report.

2021/22 IA Plan

Final Reports - Since the last JAC, we have finalised one Cambridgeshire only report and three BCH reports. This completes the 2021/22 plan:

- Commissioning (Cambridgeshire only)
- Firearms Licensing (BCH)
- Data Resilience (BC)
- Payroll including overtime (BCH)

2022/23 IA Plan

Draft Reports – We have issued one Cambridgeshire only draft report (Complaints (OPCC)) from the 2022/23 plan.

Year end Opinions - Our 2021/22 draft (positive) opinions were presented to the last meeting and we have also for completeness included a final annual report now that all 2021/22 reports are finalised. We have finalised only three reports with a negative opinion to date (BCH Procurement Follow Up - 'Little Progress', ICT Asset Distribution - 'Partial Assurance' and Firearms Licensing – 'Minimal Assurance'). The JAC should note that any negative assurance opinions will need to be noted in the annual report.

2 Reports 2021/22

2.1 Progress against the internal audit plan 2021/22 Cambridgeshire only

Assignment	Status / Opinion issued	Actions agreed			Target timing as per plan
		Low	Medium	High	
Estates – Project Management	Final Report Reasonable Assurance	2	3	0	Q1
Risk Management (OPCC & Constabulary)	Final Report Reasonable Assurance (Constabulary)	2	1	0	Q2
	Substantial Assurance (OPCC)	3	0	0	
Budgetary Control*	Final Report Reasonable Assurance	3	4	0	Q3
Capital Accounting & Fixed Assets	Final Report Reasonable Assurance	4	2	0	Q3
Covert Human Intelligence Source (CHIS) Payments and Covert Accounts	Final Report Reasonable Assurance	4	4	0	Q3
Seized/Lost Property and Controlled Drugs	Final Report Substantial Assurance	2	0	0	Q3
Follow Up	Final Report Good Progress	0	0	0	Q4
Commissioning*	**Final Report Substantial**	**0**	**0**	**0**	**Q2**

*Please see appendix A

2.2 Progress against the internal audit plan 2021/22 Bedfordshire, Cambridgeshire and Hertfordshire Collaborative

Assignment and Organisation Lead		Status / Opinion issued	Actions agreed			Target start date (As per Audit Plan)
			Low	Medium	High	
Remote Working*	Hertfordshire	Final Report Advisory	0	2	0	N/A
ICT – Distribution of Assets	Hertfordshire	Final Report Partial Assurance	0	5	1	Q2
Proceeds of Crime	Bedfordshire	Final Report Reasonable Assurance	8	2	0	Q2
Procurement Follow up	Cambridgeshire	Final Report Little Progress	1	2	1	Q3
Firearms Licensing	**Hertfordshire**	**Final Report Minimal Assurance**	**2**	**4**	**3**	**Q3**
Corporate Review – BCH Governance	Cambridgeshire	Paused – carried into next year				Q1/2
Data Resilience	**Hertfordshire**	**Final Report Reasonable Assurance**	**0**	**2**	**0**	**Q3**
Payroll including overtime*	**Cambridgeshire**	**Final Report Substantial Assurance**	**0**	**1**	**0**	**Q3**

3 Reports 2022/23

3.1 Progress against the internal audit plan 2022/23 Cambridgeshire only

Assignment	Status / Opinion issued	Actions agreed			Target timing as per plan
		Low	Medium	High	
Complaints (OPCC)	Draft Report Issued 7 July Revised Draft Issued 19 July				Q2
Fraud Risk Assessment	In Progress				Q1
GDPR (Constabulary)	Planned August 2022				Q2
Governance (OPCC & Constabulary)	Planned August 2022				Q2
Payments and Creditors	Planned October 2022				Q3
General Ledger	Planned October 2022				Q3
Follow up	Planned February 2023				Q4
Victims Code of Practice*	Planned March 2023				Q3
Agile Working (Constabulary)*	Deferred				
Value for Money (Constabulary)*	Deferred				

* see appendix A

3.2 Progress against the internal audit plan 2022/23 Bedfordshire, Cambridgeshire and Hertfordshire Collaborative

Assignment and Organisation Lead		Status / Opinion issued	Actions agreed			Target start date (As per Audit Plan)
			Low	Medium	High	
ERSOU (budgeting/financial controls)	Bedfordshire	In Progress				Q2
Cameras, Tickets and Collisions	Bedfordshire	In Progress				Q3
BCH Procurement*	Cambridgeshire	Planned September 2022				Q1
Corporate Review – BCH Governance	Cambridgeshire	Planned November 2022				Q3
Health and Safety*	Cambridgeshire	Planned November 2022				Q2
Transactional HR Systems*	Cambridgeshire	Planned November 2022				Q1
ICT (audit one TBC)	Hertfordshire	TBC				Q3
ICT (audit two TBC)	Hertfordshire	TBC				Q3
Preparedness for Emergency Service Network (ESN)	Hertfordshire	Planned January 2023				Q4
Police Education Qualifications Framework (including uplift)	Hertfordshire	Planned February 2023				Q4

* See appendix A

Appendix A – Other matters

Changes to the 2021/22 audit plan

There have been no further changes to the 2021/22 plan since the last Committee and this plan is now complete.

Changes to the 2022/23 audit plan

Since the last Committee, we have agreed the following changes to the 2022/23 audit plan.

Note	Auditable area	Reason for change
1	Agile Working and Value for Money	Management requested these two audits to be deferred to 2023/24 to meet the internal audit budget for the current year.
2	Collaboration - Health & Safety	Requested by Management to delay the start of this audit as the department have staff members on long term sick leave.
3	HR Transactions	Requested by Management to delay the start of this audit while the Team implement a new recruitment system.
4	BCH Procurement	Requested by Management to delay as Finance teams deal with year end.

Annual Opinions 2021/22 and 2022/23

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.

2021/22 – Our 2021/22 draft (positive) opinions were presented to the last meeting and we have also for completeness included a final annual report now that all 2021/22 reports are finalised. We have finalised only three reports with a negative opinion to date (BCH Procurement Follow Up - 'Little Progress', ICT Asset Distribution Partial Assurance and Firearms Licencing Minimal Assurance.

2022/23 - As our reports are finalised, we will provide further updates throughout the year.

Added value work

We have issued the following client briefings since the last Joint Audit Committee and these are on the agenda for information:

- Emergency Services News Briefing June 2022

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 – COMISSIONING AND GRANTS

Why we completed this audit

An audit of commissioning and grants was completed as part of the approved Internal Audit Plan for 2021/22, to enable the OPCC to take assurance that control processes are in place and operating effectively across the commissioning process. The Police and Crime Commissioner (PCC) awards funding to people or organisations in the county who contribute to the delivery of the objectives set out in the Police and Crime Plan 2021-24.

The PCC's commissioning approach is guided by a set of key principles, which are set out in the Commissioning, and Grants Strategy. These are underpinned by the 'Understand, Plan, Do, Review' Commissioning Model. In 2021/22, there were a total of 75 separate funding awards which the PCC has published, and these were made from the following funds:

- Supporting victims and witnesses of crime.
- Crime and Disorder Reduction.
- The Casualty Reduction and Support Reserve.
- Domestic Abuse and Sexual Violence Funding Opportunity.
- Youth Fund.
- Communities Fund.

The Director of Commissioning and the Commissioning Support Officer have responsibility for the commissioning process with the PCC responsible for commissioning decisions. The Commissioning and Grants Strategy explains how funding is awarded, which can be through a grant agreement, a contract, a contribution to a co-commissioned contract (sometimes called a collaborative commissioning agreement) or an invoice. Where there are multiple providers who could deliver a planned service, the OPCC follow the rules set within the Financial Regulations and Contract Standing Orders.

Conclusion

We found that the OPCC has a robust process in place to managing the commissioning process with adequate controls in place that were operating effectively. This included a strategy and procedure, guidance for applicants and the transparency of grants on the website.

We confirmed declaration of interests forms to act with impartiality had been completed and due diligence checks were also evidenced. We also confirmed adequate monitoring of providers through a spreadsheet and contract meetings and the approval of commissioning decisions by the PCC. We have not agreed any management actions as a result of this review.

Internal audit opinion:

Taking account of the issues identified, the OPCC can take substantial assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied and effective.

Key findings

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

Strategy and Procedures

The OPCC has a Commissioning and Grants Strategy 2021-24 approved by the PCC and presented to the Police and Crime Panel in November 2021. From our review, we confirmed that it clearly states how the strategy was developed to transparently set out the approach taken to award funding to people or organisations in the county. We noted that it included how funding is provided to enable the delivery of the objectives set out in the Police and Crime Plan 2021-24, and it explains what those objectives are, and references the joint Financial Regulations with Bedfordshire and Hertfordshire which include contract standing orders.

The strategy explains the commissioning cycle in the terms of 'understand, plan, do and review' process. This incorporates understanding of needs and desired outcomes, planning services together with partners and service measures, 'do' by engaging with providers, agreeing contracts, reviewing outcomes and the delivery of services. The Strategy further describes the process for awarding grants and contracts, the funds available together with information on the source of funding.

We confirmed that the Strategy is supported with the Commissioning and Small Grants procedures. This explains the procedure for grants of £3,500 or less that can be made to voluntary and community organisations and can be made subject to any conditions the Commissioner deems appropriate.

Information for Applicants and the Public

From a review of the PCC's website, we confirmed there was clear information supplied on each of the funds available with a short description.

Application information for each fund is published, and this currently includes applications for funding under Domestic Abuse and Sexual Violence and from the Youth Fund. In each, there is clear information covering:

- The purpose of each fund.
- Guidance on making an application.
- Copy of the application form.

Within that same section of the PCC's website, additional guidance is given with copies of the Commissioning and Grants Strategy, the Small Grants procedure and the 7 Force Procurement Supplier Charter.

Procurement Process

We confirmed in discussion with the Director of Commissioning and through review of the supporting evidence, that providers are carried forward from year to year subject to continuing need of the service and the providers performance. Although from time to time, subject to funds and service need, new procurement exercises are conducted. We also confirmed that some awards for funding are dictated the Ministry of Justice where grants are made to the PCC for funding for specific purposes and specific providers, these had been clearly documented in the OPCC spreadsheet 'Provider Information Tracker' which also records the procurement method used for each provider.

For our sample of seven providers, we found none of the providers required a tendering exercise or a number of quotes, although we noted that a tendering exercise was commencing at the time of this review for a new service.

We also confirmed from an example that the procurement method used is completed in consultation with 7Force Commercial Services, who provide advice on the option to follow to ensure compliance with procurement standing orders. Six of our sample went through the Grants process for which there were signed agreements, and one went through the Small Grants process.

Purchase Orders

We confirmed purchase orders are raised by the Strategic Accountant once a signed agreement was in place. We selected the below sample of seven providers across funds:

- The Shrievalty Trust (Bobby Scheme).
- Embrace.
- Victims of Crime and Witness Hub.
- Cambridgeshire Countryside Watch.
- Safeguarding Board.
- Road Victims Trust.
- Cambridge Sports Development Foundation.

We confirmed for four of the sample there was a purchase order in place against which payments could be made and the values agreed with the agreement. For one, as the payments had been completed, a copy of the purchase order could not be downloaded for review, however we confirmed from a ledger report that the payments were consistent with the agreement.

For the remaining two, the Victims and Witness Hub is managed by the Constabulary, payments are managed though a journal between accounts, which we confirmed agreed to the contract. The other for Cambridge Sports Development Foundation, payment is made from the Police Property Act Fund, and we confirmed the Strategic Account has requested a BACS payment in line with the agreement.

Conflict of Interest

All grants are approved by the PCC, with the commissioning and grants process being managed by the Director of Commissioning and the Commissioning Support Officer.

We confirmed that both the Director of Commissioning and the Commissioning Support Officer had signed a declaration at the start of the current procurement process in February 2022, this is a standard form issued by 7Force Commercial Services and states that if they any personal, financial or business-related interest in any of the companies who express an interest in or submit proposals in respect of this procurement exercise they agree to declare that interest immediately.

We also noted that both the PCC and CEO had completed a declaration of interests published on the OPCC website and dated September 2021.

Funding Approval

We confirmed from our sample our sample of seven providers that there was evidence that the Commissioner gave approval for each award of funding, for the Cambridge Sports Development Foundation that went through the Small Grants Process, this was through the Small Grants Authorisation meeting, for the other six, this was through the Business Coordination Meeting.

We also reviewed the Funding Decision Log noting when and where Commissioner approval was given for each award for each fund. However, we noted in a few cases this had not been clear as the decision was verbal and not formally recorded. In all but one example this dated back to the Previous Commissioner or Acting Commissioner.

We selected two funding agreements where there was no direct reference to evidence of the PCC's approval and the Director of Commissioning was able to supply evidence through correspondence that the PCC consented to the grant awards. As most of these exceptions were historic and the log was established to ensure there is documented evidence of approval prior to issuing agreements we have not agreed an action.

Due Diligence

From the sample of seven providers, we could only evidence checks for one from the small grants process, the others being not relevant as statutory grants or older on-going funding. We therefore selected another two new providers, in addition to the one in our original sample, and confirmed due diligence checks were performed. For these three, we confirmed that checks included: Safeguarding requirements, Public Liability Insurance, their website and the existence and make up of their Board or Governing Body. We noted that the checklist had been updated for 2022 and now includes: Charity Commission registration, a fraud risk assessment, and Financial Accounts.

Monitoring and Recording

We selected a sample of seven providers across funds and confirmed the process as documented was followed in each case.

With the exception of the provider that went through the Small Grants Process, we confirmed for each there was a grant agreement including a service specification, expected outcomes and a payment schedule. There were also completed records within the Provider Information Tracker with information matching the agreement, including:

- The service being provided.
- Procurement method followed.
- Data protection and vetting compliance if applicable.
- Receipt of financial and outcome monitoring reports.
- Providers contact details.
- Date of contract meeting completed and due.

For all seven of our sample, we confirmed there was a record in the Funding Decision Log, which included the value of the funding, the date of the decision, where the decision was made and the rationale for the decision to make the award.

EXECUTIVE SUMMARY – DATA RESILIENCE REVIEW

Background

An audit on Data Resilience was requested as part of the 2021/22 internal audit plan for Bedfordshire, Cambridgeshire and Hertfordshire (BCH). The objective of the review was to assess the control framework in place designed to ensure that BCH data resilience requirements are managed and controlled. The following areas were covered:

- the data backup strategy and scope;
- the data backup policy;
- the data backup procedures;
- the data backup control processes;
- the data backup management information systems;
- data backup restore testing;
- linkages between data back-up and IT Disaster Recovery controls; and
- M365 (Cloud based Microsoft solution) data resiliency, risk assessment and future planning.

To combat data loss, organisations can employ safeguards to ensure sensitive information is resilient. Often, however, these controls are inconsistent and are managed at different points in the business with different levels of diligence and effectiveness. The result is that despite efforts, organisations can lose significant amounts of sensitive information. These weaknesses in data resiliency create significant risk to the business, their customers, and partners with the potential to negatively impact reputation, compliance, finances, customer trust and business partnerships.

This audit involved the review of documentation, controls testing and interviews with key management, including the Infrastructure Manager, ICT Manager, Enterprise Architecture Manager, and ICT Network & Security Manager.

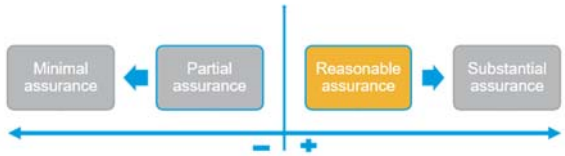
Conclusion

Overall, we found that BCH have a well-established data resilience and backup control process managed in-house by the BCH Infrastructure team. BCH Backup policies and procedures are well documented and backup teams conduct weekly restoration testing to ensure that backup jobs are completed successfully. Our review did however identify control improvements required to ensure that data backup arrangements for M365 are reviewed and failover testing is completed on a periodic basis. Two medium priority management actions have been agreed.

Internal audit opinion:

Taking account of the issues identified, the Forces can take reasonable assurance that the controls in place to manage this risk 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 risks.



Key findings

We identified the following weaknesses, leading to two medium priority management actions being agreed:

BCH have followed the national NEP data risk assessment guidance. However, in this regard BCH have not implemented M365 data backup and resiliency arrangements. M365 offers geo redundancy but not data backup. Geo redundancy protects against hardware failure so that infrastructure outages will not affect end users. However, if data is accidentally deleted, lost, or maliciously attacked via ransomware, direct access to and control over backups is key to aid in timely recovery of BCH data assets. The UK National Cyber Security Centre (NCSC) have reported several ransomware incidents that have encrypted both the original data on disk as well as compromised the connected cloud storage sites.

NCSC guidance recommends maintaining resilient backups in multiple backup locations in the event one is compromised. Unplanned and ineffective M365 data backup and recovery procedures could result in BCH being unable to meet processing or availability requirements. **(Medium)**

The BCH Backup Policy states that recovery of full systems will be completed in line with the Business Disaster Recovery Coordinator to agreed schedules, these are documented in the Disaster Recovery (DR) Test Schedule. The test schedule notes that the last failover completed was the Kempston Routers Failover DR Test on 12 November 2021 which resulted in a raised change request to resolve a failover issue. We noted thar the testing process was documented. However, we noted a lack of comprehensive documentation regarding testing results actions which resulted in difficulty in tracking related actions.

Moreover, BCH have not conducted further failover testing for business ‘mission critical’ systems and key BCH IT infrastructure. Without regular failover testing there is a risk that the failover is not fully functional in the event of the primary circuit becoming unavailable. **(Medium)**

We identified the following good practice during the audit:

Back-up policy controls including:

The Data Backups Policy (last updated in August 2020) applies to all internal system resources including all network devices (firewalls, routers, switches, load balancers, other network devices), physical and virtual servers (and the operating systems and applications and any other system resources. The backup policy includes appropriate details on the types of backups performed at BCH, the required default backup scheduling, and the requirements for backup reporting metrics.

BCH backups are held digitally between two on-site data centres in Hertfordshire and Cambridgeshire with replications stored in the opposite data centre and audit testing confirmed controls operation. Through review of the WAN schematic, we noted the data centres at Hertfordshire and Cambridgeshire have a dedicated point to point network, which is used for backup and replication. Two geographically diverse 10Gbps Virgin Media Business links are used for this replication and there is additional carrier resilience as each data centre has a Virgin Connection and BT Open Reach via the Multi-Protocol Label Switching (MPLS) WAN.

Data backup procedures including:

Microsoft System Centre Data Protection Manager (DPM) is the backup and replication system used by BCH. Nightly incremental backups are performed each weekday at agreed times to disk which was confirmed by audit testing, and the agreed Recovery Point Objective (RPO) of these backups is one business day. This is combined with a weekly full backup to enable complete recovery and these back-ups are preserved for a minimum of six weeks, again confirmed by compliance testing.

Replication is performed nightly to a replica area in the opposite datacentre, these replications can be run in real time where data is considered critical for business continuity. Additionally, high value data is backed up on every six hours in order to minimise disruption in the event of a major incident and overall audit testing confirmed the operation of the cyclical data back-up process.

Data backup process controls including:

BCH have established the following backup teams that are managed by the Infrastructure Manager:

- Server and Storage Administrator Team (North and South); and,
- Database Administrator Team

The backup teams review the status for the previous day's backup jobs every morning on weekdays using the DPM Recovery Point Status Reports to verify that all jobs have been completed successfully. We confirmed that these reports have been configured to be sent as an

automated email to the respective BCH backup team so that administrators do not need to login to the DPM server to track recovery point status.

We confirmed that the Recovery Point Status Reports provides the lists of recovery jobs and shows the total number of successes and failures for recovery points. Backup errors or unsuccessful jobs are investigated by the respective backup team to determine the root cause and action taken to remediate unsuccessful jobs.

BCH have also established the following DPM server controls:

- The DPM servers use a designated service account that allows access to the stored backup data on the Server. Administrator accounts, or domain administrator accounts do not have access to backup data, hence preventing unauthorised access or accidental deletion of backup data held on the DPM servers.

- We noted that DPM servers are patched on a monthly basis, and BCH have configured an update schedule for DPM servers to automatically reboot weekly on Wednesdays to apply any patches, hence mitigating the risk of data loss through attempts to exploit known vulnerabilities on unpatched DPM servers. Our audit testing confirmed this control is operating as intended.

- DPM servers and clients use Windows Defender as their anti-virus solution which is configured to check for Anti-Virus (AV) definition updates three times a day. Definition updates are collected by the System Centre Configuration Manager server and copied to a global share that the servers have access to. These updates are then collected and installed by the servers and AV scans then autorun.

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: M365 data resiliency		Assessment	
Control	BCH do not have M365 data backup and resiliency arrangements. However, we do acknowledge that a risk assessment and recommendations and action plans for M365 data backup and resiliency have been clearly defined and approved by management prior to completion of M365 migration.	**Design** **Compliance**	× N/A
Findings / Implications	BCH have an ongoing programme of work to migrate data to M365 with work expected to complete in October 2022. As part of this, BCH have drafted a Cloud Hosted System and Data Backup Report detailing the potential data loss threats and risks associated with a lack of a backup solution for data held in M365. We also noted the BCH has followed implementation guidance set out in a NEP risk assessment report. It was noted that Microsoft have shared responsibility during regular operations and during a service incident, with Microsoft being responsible for the infrastructure which runs M365, but responsibility of data governance is held with the customer. M365 have configured protections to mitigate against some data loss risk that occur through hardware failure and natural disasters. However, the current protections in place for M365 do not adequately reduce the risk of data loss in relation of the implementation of retention policies and the risk of data corruption. As such, the Cloud Hosted System and Data Backup Report recommend that BCH procure a third-party backup solution for M365 such as a fully SaaS hosted offering to mitigate against data loss risk. The Cloud Hosted System and Data Backup Report paper received approval via the BCH Information Management Board in November 2021, however, a business case for the intended M365 backup solution has not been developed. (we do acknowledge an outline case was submitted as part of the business planning cycle review for 21/22 but was not supported at the time due to cost). BCH do not have M365 data backup and resiliency arrangements. M365 offers geo redundancy but not data backup (Geo redundancy protects against hardware failure so that infrastructure outages will not affect end users). However, if data is accidentally deleted, lost, or maliciously attacked via ransomware, direct access to and control over backups is key to aid in timely recovery of BCH data assets. The UK National Cyber Security Centre (NCSC) have reported several ransomware incidents that have encrypted both the original data on disk as well as compromised the connected cloud storage sites. Unplanned and ineffective M365 data backup and recovery procedures could result in BCH being unable to meet processing or availability requirements.		

Management Action 1	Management should develop a business case for the intended M365 backup solution and ensure that the backup solution is implemented to protect data held on M365. This should be reviewed by chief officers as part of the business planning cycle 22/23' If additional back-up resilience is agreed, management will also ensure that the BCH Data Backup Policies and Procedures are updated to include the data backup and recovery requirements and procedures for M365.	**Responsible Owner:** *Jon Black*	**Date:** *22 November 2022*	**Priority:** Medium

Area: Restoration and Failover testing		**Assessment**	
Control	Formal failover tests are not performed across BCH systems and key IT infrastructure on a periodic basis to ensure that the failovers are fully functional in the event of the primary network circuit becoming unavailable.	**Design** **Compliance**	× N/A

Findings / Implications

BCH backup teams conduct recovery tests weekly to verify that the recovery procedures enable BCH to restore data successfully and gain assurance that backup information can be reliably retrieved. Each weekly test includes a recovery of selected files and databases and the checksum of the restored files is compared to the original, inability to restore all of the files or any difference in the checksum is noted as a failure. Through review of the Recovery Test Log, we confirmed that weekly tests are performed with details on the scope of the test, when it was performed and status of the test (success or failure).

The BCH Backup Policy states that recovery of the full system will be completed in line with the Business Disaster Recovery Coordinator to agreed schedules, these are documented in the Disaster Recovery (DR) Test Schedule. The test schedule notes that the last failover completed was the Kempston Routers Failover DR Test on 12 November 2021 which resulted in a raised change request to resolve a failover issue. However, we noted a lack of documentation for this failover test that detailed the scope of testing, start and end times, issues and actions and lessons learned.

The test schedule also documents the following planned failover tests for 2022:

- full failover DR Test for Web Servers to Huntington;
- full failover Test of CLIO system; and
- full failover test on iManage system.

However, BCH have not conducted further failover testing for business 'mission critical' systems and key BCH IT infrastructure. Without regular failover testing there is a risk that the failover is not fully functional in the event of the primary circuit becoming unavailable.

Management Action 2	A formal failover test schedule for 22/23 will be agreed and monitored through the Ops Support Delivery Board. Details on action resolution and lessons learned from failover tests will be documented in the Recovery Test Log on completion of failover test actions.	**Responsible Owner:** *Jon Black*	**Date:** *May 2022*	**Priority:** Medium

EXECUTIVE SUMMARY – COLLABORATION – PAYROLL INC. CARM

Why we completed this audit

An audit of Payroll was undertaken as part of the 2021/22 approved internal audit plan to allow management to take assurance that payroll is correctly processed in a timely manner, with adequate controls in place.

The CARM resource management system has been introduced across BCH. The system is used to manage shift patterns including claims for overtime working which requires line manager approval. Shift patterns are set by Human Resources (HR) however, a line manager can make amendments via an activity request, for annual leave and training, which requires HR approval. An interface downloads payroll data from CARM each month.

BCH also use iTrent which is an integrated HR and Payroll software system, meaning BCH can manage both HR and payroll functions through a single platform. HR can add starters, remove leavers and make amendments such as changes to hours or promotions, to which Payroll do not have access.

We have also performed an analysis of overtime recorded in CARM with a monthly breakdown by Force in appendix A.

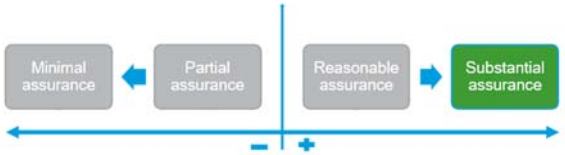
Conclusion

Our review identified a robust control framework was in place, including for key control areas such as the processing of starters, leavers and payroll amendments, overtime, exception reporting and processing of the payroll.

We identified that effective controls were in place to ensure that additional payments are approved and evidenced. We also noted from sample testing that starters and leavers were appropriately added to and removed from their respective schemes. We have agreed one medium priority action resulting from our analysis of overtime which identified very high rates for some individuals, where some additional review and reporting may be required.

Internal audit opinion:

Taking account of the issues identified, the Forces and OPCCs can take substantial assurance that the controls upon which the organisation relies to manage this area are suitably designed, consistently applied and effective.



Key findings

We identified the following weakness, resulting in a medium priority management action being agreed:

We performed an analysis of all overtime claims processed through CARM for each Force between March and December 2021 and identified the total number of overtime hours worked by each employee per month.

- For Bedfordshire, we found 1050 instances of staff working over 100 hours of overtime in a single month, and 67 instances of staff working over 200 hours of overtime in one month.
- For Cambridgeshire, we found 735 instances of staff working over 100 hours of overtime in a single month, and 38 instances of staff working over 200 hours of overtime in one month.
- For Hertfordshire, we found 840 instances of staff working over 100 hours of overtime in a single month, and 35 instances of staff working over 200 hours of overtime in one month.

We were advised that there could be a number of explanations for the high number of overtime hours above. For example, the system allows staff to store up overtime and claim it retrospectively. In addition, those working overtime could include part time staff and therefore this may not be excessive, particularly if the hours include working on a bank holiday. We also noted a number of staff attended COPS26 and these large deployments may inflate staff hours.

We were informed that outside pay costs, there is no review of overtime including where individuals perform high numbers of hours. Failure to review excessive hours may impact on the health and wellbeing of individuals. **(Medium)**

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

Authorisation

We confirmed by review that changes to personnel, staff and officers are updated in CARMs using daily HR reports of starters, leavers, skills and limited duties.

Supervisors are being updated on an ‘ad hoc’ basis as a report in a useable format is not yet available, however, comparison reports from HR to CARM are being used. Whilst there is no interface with CARM to enable automated updates. To allow for differing shift pattens and leave, an individual can select another line manager for the approval of overtime or annual leave, and therefore a delay in assigning an individual to supervisor level is not considered a significant issue.

Starters

Through review of a sample of 30 new starters, covering staff and officers from each Force, we noted that all 30 individuals had a new starter form on file with HR approval evidenced. Further review of sample of 30 new starters noted that the new starter forms were imported accurately, in a timely manner and with a segregation of duties between input and review.

In 25 instances, the new starters pension details had been correctly input and their first payment agreed with the pension scheme they were enlisted on. In five instances staff starters had opted out of the pension scheme and therefore had no pension deductions.

Leavers

From a sample of 30 leavers including staff and officers from the three forces between April 2021 and December 2021, we noted that in all instances.

- The leavers notifications had been appropriately processed by the relevant manager or department.
- The leavers had been processed in a timely manner following notification.
- Remaining annual leave had been appropriately calculated, processed and paid in line with the expected last pay date with no overpayments noted.
- The leavers had been appropriately removed from the pension schemes in line with their expected last pay date.

Amendments

We selected a sample of 30 amendments between April 2021 and December 2021 of staff and officers from the three forces, with amendments including increments, honorariums and bonus payments, tax code changes and change of hours. We noted that all had been subject to, line manager approval where required, independent review between actioning the amendment request and reviewing the changes were evidenced, and all had supporting documentation on file which reconciled to the change made.

Unsocial Hours

Where unsocial hours fall into a shift patten set up on CARM, there is no requirement for additional approval as this is automatically transferred for payment. However, through review of a sample of 30 unsocial hour payments made since April 2021, we found in all cases, the unsocial hours rate used had been calculated correctly.

Overtime

During testing of a sample of 30 overtime claims made since April 2021, in 29 cases all overtime has been appropriately approved through CARM by the individuals line manager or an officer ranking at least one rank higher, payment had been made in accordance with the approved rate, and payment had been made accurately through review of the payslip. In the remaining instance, the entry had correctly been identified by the line manager as a duplicate entry and payment had been rejected.

Expenses

We selected a sample of 30 expense claims submitted across the three forces and noted that 26 claims were appropriately completed and subject to appropriate authorisation, and that expense payments matched the claim which was made through the iTrent system.

For the remaining four, there were no receipts and as a result, these were declined, and no payment was made. We also confirmed that payroll perform ‘dip sampling’ of expenses each month. From a random sample of two months for each Force in 2021/22, we confirmed that where exceptions were found, such as missing receipts, these were requested from the claimant, or the payment was withheld.

Overpayments

Overpayments may be identified by the payroll team as part of their sample checks each month, due to review by HR or notification by the individual member of staff or officer. Payroll maintain a log of over payments for each Force and the deductions each month until the repayment is completed.

We were provided with the log for each Force and for all entries and confirmed that reasoning for why the overpayment had occurred was documented and that timely and appropriate actions had been taken to recover the money owed, e.g., emailing the member of staff in a timely manner and agreeing a repayment plan.

Payroll Reports

We noted during review of the October, November and December 2021 variance reports that they had been produced for the last three months. Through review of the corresponding months' payroll checklists, we found that the variance reports had been completed in a timely manner which included the net pay variance report, high earners etc.
We confirmed that the checklist includes each of the activities for the payroll cycle which were initialled or signed when completed. We noted that the checklist also included the issue of reports to each Force Financial Accounting & Treasury function and confirmation of balance to the general ledger.

Pensions

We reviewed the Service Level Agreement for pensions between the three individual forces and Kier Business Services Limited and noted that they are in place until 31 August 2022 to ensure that the dates of all three agreement align and can be recontacted under one agreement. Through review of the agreements, we noted that Kier Business Services undertake the day to day running of the pensions, whilst the Forces review their pension reconciliations on a monthly basis prior to the pay run.

Through undertaking the starter and leavers testing across the three Forces above, we noted that those individuals who had opted-in to the pension schemes had their pensions processed in line with the schemes and level of contributions recorded on their new starter from. In all instances where the individuals left the Force, we noted that the leavers last pension contributions had been accurately processed and no overpayments had occurred.

IT Backups

We reviewed the back-up files for the Force including CARM during January 2022 and noted that full back ups were undertaken on a daily basis at 17:30pm with an automatic rule set up across the Force to ensure that the backups are consistently run.

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.

Overtime Data Analysis				
Findings / Implications	We performed an analysis of all overtime claims processed through CARM for each Force between March and December 2021 and identified the total number of overtime hours worked by each employee per month. • For Bedfordshire, we found 1050 instances of staff working over 100 hours of overtime in a single month, and 67 instances of staff working over 200 hours of overtime in one month. • For Cambridgeshire, we found 735 instances of staff working over 100 hours of overtime in a single month, and 38 instances of staff working over 200 hours of overtime in one month. • For Hertfordshire, we found 840 instances of staff working over 100 hours of overtime in a single month, and 35 instances of staff working over 200 hours of overtime in one month. We were advised that there could be a number of explanations for the high number of overtime hours above. For example, the system allows staff to store up overtime and claim it retrospectively. In addition, those working overtime could include part time staff and therefore this may not be excessive, particularly if the hours include working on a bank holiday. We also noted a number of staff attended COPS26 and these large deployments may inflate staff hours. We were informed that outside pay costs, there is no review of overtime including where individuals perform high numbers of hours. Failure to review excessive hours may impact on the health and wellbeing of individuals. We were informed that outside pay costs there is no review of overtime including where individuals perform high numbers of hours, with the exception of Cambridgeshire where overtime reports are sent monthly to each Supt and these include a list of the top 5 officers claiming hours. Failure to review excessive hours may impact on health and wellbeing of individuals. **Please see appendix A below for the analysis of all overtime through CARM for this period.**			
Management Action	Each Force will review overtime claimed by individuals for excess hours being worked, with a monitoring process through line managers to ensure the wellbeing of individuals.	**Responsible Owner:** Heads of Finance (Bedfordshire, Cambridgeshire and Hertfordshire)	**Date:** 30 September 2022	**Priority:** Medium

For more information contact

Dan Harris, Head of Internal Audit
daniel.harris@rsmuk.com
Tel: 07792 948767

Shalini Gandhi, Manager
Shalini.gandhi@rsmuk.com
Tel: 01908 687806

Emergency Services News Briefing

June 2022

Contents

Introduction

In this edition of our news briefing, we draw attention to some of the key developments and publications in the sector, with particular focus on the latest reports from Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) and the Police, Crime, Sentencing and Courts Act.

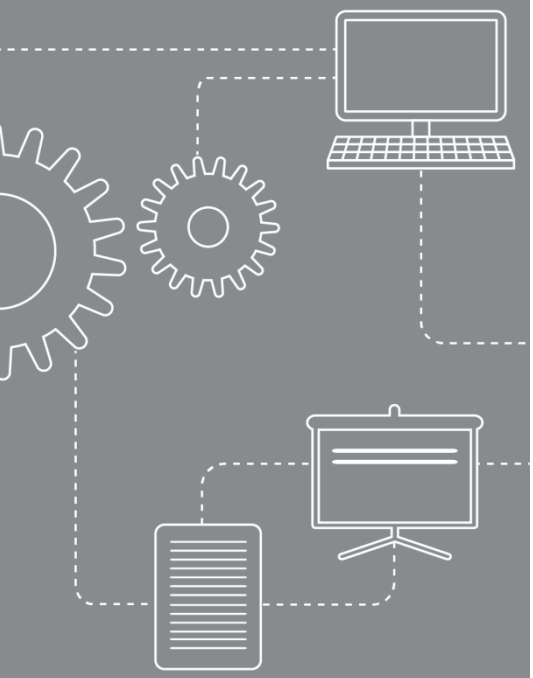
In relation to fire, we look at proposals set out by the Home Office to introduce a 'system-wide reform that will strengthen fire and rescue services in England.'

We also highlight our latest report on an analysis of secure remote working and operational resilience audits.

A few questions for audit committees to consider on the articles covered within this publication.

- Have you been briefed on these issues and whether management have considered the impacts on your organisation(s), and how it affects the risk profile(s)?
- Are you receiving (where relevant) timely, second or third line assurance on the items contained within this briefing
- Does this duplicate any other assurance you are receiving?
- Are there any assurance gaps highlighted by this briefing?

Police



State of Policing

The HMICFRS has published its annual assessment of policing in England and Wales 2021.

The annual assessment provides an overview of the findings of inspections, which were carried out between 1 April and 30 November 2021, including a summary of police effectiveness, efficiency and legitimacy (PEEL) inspections. HMICFRS also sets out the full list of its inspections and other work. The results of individual inspections enable an assessment of the performance of individual forces, or a more general assessment of performance in specific aspects of policing. In his final annual report after nearly a decade in post, Sir Thomas Winsor, the Chief Inspector of Constabulary, described how demand on the police has changed very significantly, for example:

- online crime is now the most prevalent type of crime and online fraud has increased, ‘eclipsing all other crimes in volume’;
- total demand and public expectations cannot be met without sufficient funding and the public must decide how much threat, harm and risk they are prepared to tolerate; and
- the rapid advancement of technology has provided opportunities for both criminals and the police, but the police have sometimes struggled to keep pace.

In his report, the Chief Inspector also draws attention to:

- the causes of crime and low detection rates;
- the need for proactive as well as reactive policing to protect vulnerable people;
- the state of the system of local police accountability and the sometimes ‘brittle and fragile relationships between chief constables and police and crime commissioners’, and the need for trust and confidence in a special constitutional relationship which the public needs to work;
- the successes and potential of the National Crime Agency, and its ability, with sufficient investment, to do a great deal more to disrupt or break sophisticated criminal networks; and
- the need for significant investment in police technology.

The Chief Inspector stated the ‘fragile architecture of the 43-force model, born in 1962, is not fit for purpose.’ Sir Thomas also reiterated his proposal for a network code, which would dissolve the barriers preventing policing and law enforcement from 'operating as a single system and secure fair, reliable and sustainable decisions on regional and nation-wide problems.

Read more

Boost for public safety as bill receives Royal Assent

The Police, Crime, Sentencing and Courts Bill received Royal Assent and became an Act of Parliament on 28 April 2022. The Police, Crime, Sentencing and Courts (PCSC) Act 2022 equips the police with the powers and tools they need to combat crime and create safer communities. The Act builds on the government's Beating Crime Plan to reduce crime, better protect victims and make the country safer. It has already seen the recruitment of more than 13,500 of the 20,000 extra police officers promised by March 2023.

Read more

Impact of the pandemic on the Criminal Justice System

In January 2021, HMICFRS, HM Inspectorate of Probation, HM Crown Prosecution Service Inspectorate and HM Inspectorate of Prisons conducted inspections of its respective agencies' responses to coronavirus and published 'Impact of the pandemic on the Criminal Justice System'.

The progress report provides an update to the original report and is based on combined inspection findings during 2021. The structure follows the flow of work through the Criminal Justice System (CJS) from policing to prisons. It sets out findings from inspections, 'as well as cross-cutting themes, and highlights the successes of the CJS, but also the challenges that it has faced and still faces.'

Read more

National Stop and Search learning report

The Independent Office for Police Conduct (IOPC) has published its latest report on National Stop and Search. This report brings together evidence from the IOPC work, stakeholder engagement and published research to highlight concerns about transparency, legitimacy, scrutiny, and disproportionality that must be considered and addressed by the police service and others. This report aims to support change and improvement in policing practice to help increase public confidence.

Read more

An inspection of the service provided to victims of crime

HMICFRS has published a report assessing the quality of the service provided to victims of crime by the British Transport Police (BTP). The investigation reviewed the service provided by the BTP for each of the six components of the victim service assessment:

- call handling;
- deployment of resources;
- crime recording;
- screening and allocation;
- investigation; and
- outcomes.

HMICFRS has worked collaboratively with Her Majesty's Inspectorate of Constabulary in Scotland to produce a single report that covers BTP's whole jurisdiction across England, Wales and Scotland.

Read more

The Police Uplift Programme

The National Audit Office (NAO) has published a report examining whether the Home Office is well placed to deliver value for money from the programme. It covers the:

- aims of the programme;
- management of the programme and progress against its objectives; and
- challenges in maximising the impact from the programme.

The NAO notes that it is too early to assess whether the additional officers are delivering the government's aims to improving public safety and reducing crime, as they will 'need time to become fully effective in their roles.' Furthermore, improvements in wider criminal justice outcomes depend on many more factors than the number of police officers. This paper looks at how far the recruiting process has progressed so far, as well as how the Home Office intends to show the impact of the extra officers in the future.

Read more

Police Covenant update

The Home Office has published a policy document which provides a summary of latest activity on the Police Covenant and the progress made so far. The Police Covenant Oversight Board outlined that a number of workstreams have been progressed and finished. Key activity over the past year includes:

- pre-deployment mental health care incorporated into all providers of the Police Education Qualifications Framework (PEQF)
- over 30 police forces attended a three-day workshop led by the National Police Wellbeing Service, where the clinical team provided extensive advice and support for occupational health teams; and
- 'the addition of new workstream priorities: to develop a support model for those who leave policing and to progress NHS engagement.'

Read more

Extra £150m to tackle crime and anti-social behaviour

The Home Office has launched round four of the Safer Streets Fund as part of the government's commitment to reduce crime and promote public safety. As a result, £150m is available over the next three financial years for police and crime commissioners and local authorities across England and Wales, as well as certain civil society organisations. The Safer Streets Programme provides funding to areas most affected by crime and anti-social behaviour and will allow local authorities, civil society organisations and police and crime commissioners to bid for up to £500,000 per year for each project.

Read more

Observations on the third generation of force management statements

A force management statement (FMS) is a self-assessment that chief constables (and London equivalents) prepare and submit to HMICFRS each year.

HMICFRS has published the observations of the FMS steering group on the third round of FMSs following statements that were submitted by police forces. The steering group is made up of HMICFRS, the National Police Chiefs Council, the College of Policing, the Association of Police and Crime Commissioners, the Home Office, and other parties interested in the development of FMSs.

The summary observations note:

- FMSs continue to improve and focus on national policing issues; and
- police forces understand demand better but need to improve understanding of workforce capabilities.

Read more

'Whole-system' approach to tackling violent crime is working

The Home Office has announced a further £130m to strengthen efforts in tackling serious violence. Violence Reduction Units and 'hotspot policing initiatives' have avoided 49,000 violent offences across England and Wales. The government's funding package includes:

- a further £64m for Violence Reduction Units, supporting the existing 18 and enabling two new units to be established in Cleveland and Humberside;
- an additional £30m into the 'Grip' police enforcement programme; and
- supporting the implementation of the new Serious Violence Duty and Serious Violence Reduction Orders, being brought into law as part of the Police, Crime, Sentencing and Courts Act 2022.

Read more

Police and Fire

Evaluation of remote inspection methods

HMICFRS has published its report on the evaluation of remote inspection methods required during the coronavirus pandemic. Key findings include:

- interviews, remote case file reviews, staff surveys, self-assessment, team debriefs and meeting observations were all effective remote inspection methods. Large focus groups, on the other hand, were more difficult to conduct remotely than small focus groups. HMICFRS noted that all methods of remote inspections relied on effective IT capabilities;
- working remotely had a mixed response on staff wellbeing, with some employees adjusting well and others finding it more challenging. Challenges included integrating home and work life and the intensity of working online all day without pauses; and
- the findings of the review have also prompted more permanent changes to HMICFRS' inspection process, including the use of remote inspection technologies when suitable. HMICFRS now employs a combination of on-site and remote inspection techniques.

Read more

Local Government and Emergency Services VAT Webinar

We are pleased to announce our next VAT and tax webinar for local authorities and emergency services is taking place on 16 June 2022.

Our webinars aim to help officers gain up-to-date and bite-size insights on VAT and tax issues affecting their organisations.

This webinar will be an excellent opportunity for you to hear and raise questions on sector related VAT issues within a trusted forum. As well as hearing about technical updates, our sector specialists will be on hand to provide feedback on recent developments.

In our session, topical sector updates will include mutual trading status of subsidiaries and our top tax queries from FY21/22:

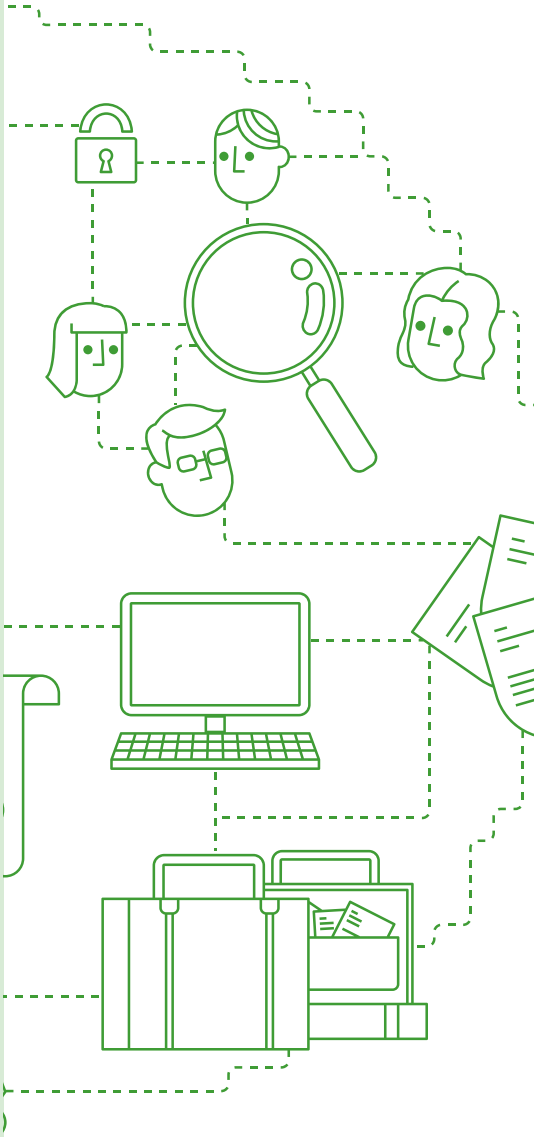
- recent case law and legislative changes affecting the sector;
- HMRC VAT policy changes including sector activity;
- sector activity;
- VAT saving opportunities; and
- questions and answers.

To register for the webinar, please click here.

If you have any questions relating to the webinar, please do not hesitate to contact us. Please also feel free to forward this invitation to your colleagues or to officers in other authorities.

Secure remote working and operational resilience in a hybrid world

As the coronavirus pandemic took hold, organisations quickly moved their workforces to their homes. The speed at which organisations had to adapt was remarkable, and we know that some were better placed than others to move successfully. With the shift to homeworking, the risk landscape changed and organisations were exposed to greater and more complex threats.



Across the diverse sectors we work in, we have undertaken secure remote working and operational resilience audits, assessing how management have implemented and managed controls to enable remote working. Through reviewing and assessing IT infrastructure and remote working processes, we have provided assurance over the design of key controls and adherence to them in respect of governance over business-critical data while working remotely, whilst also ensuring adequate capacity is available to meet the needs of the business.

From our reviews, we have seen several key outcomes emerge, highlighted from where we have agreed management actions.

Overview of key internal audit review outcomes

- Only 12 per cent of businesses could take substantial assurance that the controls in place to ensure secure remote working are operating effectively to manage risks. This illustrates there is significant room for many businesses to improve and strengthen the IT control environment to ensure data security, manage cyber-crime threats and enhance IT operational effectiveness.
- In those areas where we agreed management actions, 80 per cent of the controls in place were deemed to be ineffective in terms of design.
- Given the spike in phishing and ransomware attacks, there is perhaps now more than ever, a need to ensure a comprehensive incident response plan is in place, to guide the organisation's response, should an attack occur.

Access our report on the RSM website.

The ESG Risk Landscape

The Global Institute of Internal Auditors (IIA) has published a collection of Global Knowledge briefs providing information and analysis on changes to the dynamic environmental, social and governance (ESG) risk landscape. Collectively, they provide practical information to help internal auditors anticipate and prepare for new reporting regulations, position internal audit functions to provide high-quality services related to ESG and offer direction on identifying ESG risks within organisations.

ESG Appetite

ESG is becoming increasingly important, both for us as individuals and for organisations. We are seeing investors, employees, customers and business partners demanding that organisations act responsibly and ethically.

As internal auditors we are in a unique position to help an organisation start to understand what its approach or 'appetite' is to ESG, and how the organisation is starting on its ESG journey around developing and embedding an ESG culture.

RSM has an audit approach which is designed to look at your external commitment and communication in relation to ESG matters and compares it to the views held by senior management and an organisations largest stakeholder group — its employees.

How an ESG Appetite review can benefit you.

- Understand what actions have been undertaken to date as part of your ESG journey.
- Understand what matters to your employees and how they view the organisation's ESG related activities and programmes.
- Demonstrate commitment to corporate responsibility and continuous improvement.

Next steps

Speak to your usual internal audit contact about having an 'ESG appetite review' built into your internal audit plan, or request the review as an additional piece of work. The appetite review is delivered by your Internal Audit team, with support from an ESG subject matter expert.

Discuss with your internal audit contact as to whether an ESG maturity assessment may benefit you more. This falls outside of the internal audit plan, but may be more appropriate for where you are on your ESG journey

ESG maturity assessment

Building on ESG Appetite, a more in-depth ESG maturity assessment can be undertaken. RSM's full maturity assessment places an organisation in one of four stages in its ESG journey: Awareness; Defining and Reporting; Managing; and Maturity.

For a copy of our briefing papers, please get in touch with your usual RSM contact.

Public sector sustainability reporting consultation

The International Public Sector Accounting Standards Board (IPSAB) has launched a consultation aimed at producing a global set of standards for sustainability reporting by government bodies. 'The aims of this public consultation process are to evaluate the demand from stakeholders for such guidance, as well as the degree of support for the IPSASB's involvement in the process.' The consultation is seeking views on what topics should be prioritised and whether IPSASB is the right organisation to develop the guidance.

The consultation closes on 9 September 2022.

Read more

Audit and Risk Assurance Committee effectiveness tool

Audit and Risk Assurance Committees (ARACs) play a crucial role in supporting the effective governance of central government departments, their agencies and arm's length bodies.

The NAO's effectiveness tool is a comprehensive way for ARACs in central government to assess their effectiveness on a regular basis.

Read more

The Real Economy: Cyber Security

In The Real Economy's latest topical survey, we have revisited the topic of cyber security. Encouragingly, the middle market is acting against the accelerating threat. Since the 2021 survey, our panel of over 400 business leaders experienced a 7 per cent increase in successful cyber-attacks. It's not surprising to see such an increase with cyber criminals constantly innovating and adapting their strategies to include increasingly sophisticated attacks. In our report we note the top things to consider over the next 12 months including, governance, frameworks, threat modelling, penetration testing, phishing and whaling exercises and incident response.

Whilst the report follows on from our survey with middle market business leaders, there are areas raised in this report which provide useful insight for police and fire and rescue services.

Access our report on the RSM website

Fire

Data management fire standard consultation

The Data Management Fire Standard has been developed with expert input from the National Fire Chiefs Council (NFCC) Digital and Data Programme, NFCC Leads for Data, Apollo Gerolymbos and Andy Hopkinson, Government Digital Services and colleagues, with data expertise from a wide range of fire and rescue services. This consultation focuses on fire and rescue services delivering excellence to our communities by maximising the value of good quality and reliable data.

The consultation closed on 27 April 2022; the responses will be considered and the 'Fire Standard will undergo a quality assurance process before the final Fire Standard is proposed to the Fire Standards Board for approval.'

Read more

Fire Standard is launched

The Fire Standards Board (FSB) has announced the launch of the tenth professional Fire Standard; Fire Investigation. The Standard focuses on ensuring fire and rescue services (FRS) deliver effective, efficient and valid fire investigations into the origin, cause and development of fire. An anticipated outcome of the Standard is that services will have a competent and resilient capability to undertake fire investigations, adhering to relevant legislation, guidance and codes of practice. By identifying risk and reporting product safety issues, the Fire Standard is expected 'to improve the safety and wellbeing of members of the public (FRS communities) and FRS employees.' The Standard also contains other anticipated benefits.

Read more

Reforming fire and rescue services

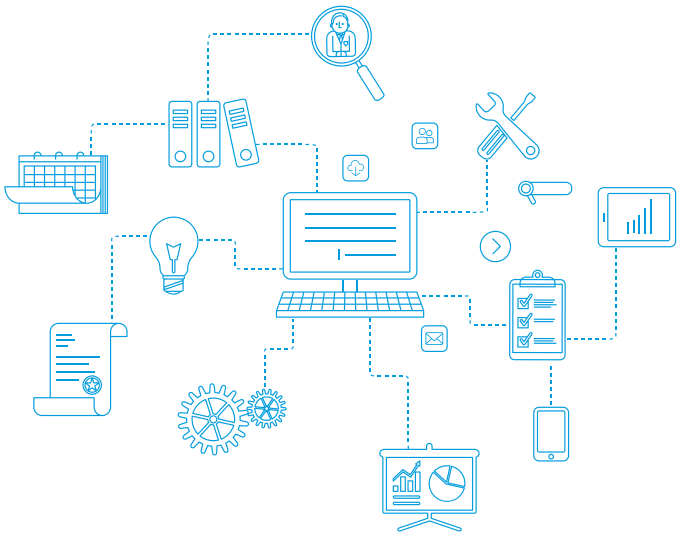
The Home Office has launched a consultation seeking views on proposals to introduce a 'system-wide reform that will strengthen fire and rescue services in England.' The changes announced include the commencement of the Fire Safety Act 2021 which will make sure all blocks of flats are properly assessed for fire safety risks. The Fire Safety (England) Regulations 2022 was also announced which implements eight recommendations from the Grenfell Tower Inquiry report and will help ensure people feel safe in their homes.

At the centre of the White Paper are plans to deliver:

- increased public safety: by improving the professionalism of the fire and rescue service through modern workforce practices and potentially establishing a College of Fire and Rescue;
- improved accountability: through the proposals to transfer fire governance to a single elected individual, overseeing delivery by operationally independent Chief Fire Officers; and
- better engagement with the public: through the 10-week consultation the government will listen to the views of the public and stakeholders, after which it will finalise its reform programme.

The consultation closes on 26 July 2022

Read more



The Fire Risk Assessment Prioritisation Tool

The government has launched its risk prioritisation tool, which has been set up to encourage building owners to review fire risk assessments (FRAs) on their most dangerous buildings. The new tool comes in after the Fire Safety Act said it will now force building owners to consider the external walls and balconies in periodic fire risk assessments. Prior to this, the focus was on the internal walls of a block and the external fell out of scope.

The Fire Risk Assessment Prioritisation Tool takes responsible persons through a series of specific questions, which are each carefully scored to assist them to determine the priority of their buildings for the purpose of reviewing their fire risk assessments. The tool does this by allocating each building to one of five priority tiers.

Read more

Authors

Daniel Harris

National Head of Emergency Services and Local Government

T +44 (0)7792 948 767

daniel.harris@rsmuk.com

Zara Raza

Risk Assurance Technical

zara.raza@rsmuk.com