Cumbria Shared Internal Audit Service

Internal Audit Report for Cumbria Constabulary

Audit of ICT Capacity

Draft Report Issued: **10th April 2018**

Final Report Issued: **26th April 2018**

Audit Resources

Title	Name	Email	Telephone
Audit Manager	Emma Toyne	emma.toyne@cumbria.gov.uk	01228 226261
Lead Auditor(s)	Sarah Fitzpatrick	sarah.fitzpatrick@cumbria.gov.uk	01228 226255

Audit Report Distribution

For Action:	Ian Hogarth (Head of ICT)
For Information:	Stephen Kirkpatrick (Director of Corporate Support)
Audit Committee	The Joint Audit & Standards Committee, which is due to be held on 24th May 2018, will receive the report.

Note: Audit reports should not be circulated wider than the above distribution without the consent of the Audit Manager.

Executive Summary

1. Background

1.1. This report summarises the findings from the audit of ICT Capacity. This was a planned audit assignment which was undertaken in accordance with the 2017/18 Audit Plan.

1.2. ICT capacity is important to the organisation because ICT resources and capability need to meet current and future business requirements efficiently. ICT capacity impacts upon the organisation's ability to modernise and support elements in the Police and Crime Plan through investment in technology to make efficiency savings, ensuring sustainability, improving visibility and maximising the efficiency and effectiveness of front line policing.

1.3. There has been a long standing corporate risk within the Constabulary's strategic risk register around a 'failure to deliver the Change programme and Corporate Support Business Plan **caused by *insufficient capacity across the organisation, in particular the reliance on IT to deliver systems* which improve officer productivity and reduce manual intervention in processes** resulting in a requirement to find further significant savings from the front line (reduce officer and staff numbers) and the significant detrimental impact this has on policing services over the longer term, damage to reputation and loss of public confidence. The risk description was amended in the strategic risk register in June 2017 to remove any reference to ICT capacity due to actions taken to mitigate this element of the risk. The revised risk register was approved by Chief Officer Group, in accordance with the organisation's Risk Management Policy.

2. Audit Approach

2.1. **Audit Objectives and Methodology**

2.2. Compliance with the mandatory Public Sector Internal Audit Standards requires that internal audit activity evaluates the exposures to risks relating to the organisation's governance, operations and information systems. A risk based audit approach has been applied which aligns to the five key audit control objectives which are outlined in section 4; detailed findings and recommendations are reported within section 5 of this report.

2.3. **Audit Scope and Limitations**

2.3.1. The Audit Scope was agreed with management prior to the commencement of this audit review. The Client Sponsor for this review was the Director of Corporate Support. The agreed scope of the audit was to provide assurance over management's arrangements for ensuring effective governance, risk management and internal control in the following area:

- Mitigating actions recorded in the strategic risk register.

2.3.2. There were no instances whereby the audit work undertaken was impaired by the availability of information.

3. Assurance Opinion

3.1. Each audit review is given an assurance opinion and these are intended to assist Members and Officers in their assessment of the overall level of control and potential impact of any identified system weaknesses. There are 4 levels of assurance opinion which may be applied. The definition for each level is explained in **Appendix A.**

3.2. From the areas examined and tested as part of this audit review, we consider the current controls to address the ICT capacity risk provide **substantial** assurance.

Note: as audit work is restricted by the areas identified in the Audit Scope and is primarily sample based, full coverage of the system and complete assurance cannot be given to an audit area.

4. Summary of Recommendations, Audit Findings and Report Distribution

4.1. There are three levels of audit recommendation; the definition for each level is explained in **Appendix B**.

4.2 There are no audit recommendations arising from this review.

4.3 **Strengths:** The following areas of good practice were identified during the course of the audit:

- Roles and responsibilities for ICT risk management are clearly defined and communicated.
- The ICT team fully and regularly consult with senior managers on strategic plans and programmes and future ICT requirements to support change and manage capacity.
- Senior management have agreed a prioritisation process for ICT projects and Force Strategic Delivery Board ensures the process is complied with.
- Arrangements are in place for ICT risks to be assessed, monitored and managed on a regular basis.

- Provision is made for regular senior management oversight and challenge of ICT strategic risks through progress reports to Chief Officer Group.
- Adequate assurances were provided to Chief Officer Group on mitigating actions to address the ICT capacity element of the strategic risk to support revisions to the risk description.
- There is regular reporting and independent scrutiny of the strategic risk register by the Joint Audit and Standards Committee.

Comment from the Director of Corporate Support :
I am very pleased that this review of ICT Capacity has provided Substantial assurance and that there are no areas for action identified. ICT capacity to support and enable strategic organisational change has been logged as an area of concern on the Constabulary Strategic Risk Register for a significant period of time. Throughout this time, the ICT department have continued to successfully balance priorities and challenges to effectively support evolving organisational needs.

The audit has confirmed that the Constabulary has an excellent approach to managing risks and demand with regards to ICT enabled change. I am particularly pleased that this audit has highlighted that ICT Programme and Project management governance takes a robust and thorough approach to risk management and that there are strong working relationships between ICT and the full range of key organisational stakeholders in terms of managing ICT demands and priorities, including challenge where necessary.

These findings are extremely positive in recognising the excellent work undertaken regarding managing ICT demand which is a credit to all involved.

Audit Assurance Opinions

There are four levels of assurance used; these are defined as follows:

	Definition:	Rating Reason
Substantial	There is a sound system of internal control designed to achieve the system objectives and this minimises risk.	The controls tested are being consistently applied and no weaknesses were identified. Recommendations, if any, are of an advisory nature in context of the systems and operating controls & management of risks.
Reasonable	There is a reasonable system of internal control in place which should ensure that system objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Recommendations are no greater than medium priority.
Partial	The system of internal control designed to achieve the system objectives is not sufficient. Some areas are satisfactory but there are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an unsatisfactory level of internal control in place as controls are not being operated effectively and consistently; this is likely to be evidenced by a significant level of error being identified. Recommendations may include high and medium priority matters for address.
Limited / None	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Control is generally weak/does not exist. Recommendations will include high priority matters for address. Some medium priority matters may also be present.

Grading of Audit Recommendations

Audit recommendations are graded in terms of their priority and risk exposure if the issue identified was to remain unaddressed. There are three levels of audit recommendations used; high, medium and advisory, the definitions of which are explained below.

		Definition:
High	●	Significant risk exposure identified arising from a fundamental weakness in the system of internal control
Medium	●	Some risk exposure identified from a weakness in the system of internal control
Advisory	●	Minor risk exposure / suggested improvement to enhance the system of control

Recommendation Follow Up Arrangements:

- High priority recommendations will be formally followed up by Internal Audit and reported within the defined follow up timescales. This follow up work may include additional audit verification and testing to ensure the agreed actions have been effectively implemented.
- Medium priority recommendations will be followed with the responsible officer within the defined timescales.
- Advisory issues are for management consideration.