Southern Internal Audit Partnership

Assurance through excellence and innovation

Sussex Police

Internal Audit Report

IT Audit Needs Assessment 2018/19

6th December 2018

Prepared by: James Short

FINAL REPORT

Restricted

1. Introduction

1.1 As part of the Internal Audit Plan for 2018/19, we have undertaken a review of the IT audit needs for Sussex Police.

1.2 Sussex Police have entered into a range of collaborative arrangements (including IT) for which Surrey Police are the 'lead partner'. The existing IT infrastructure and proposed future developments across Sussex and Surrey Forces are contingent components to the effective delivery of the respective policing bodies objectives. Consequently, assurance over governance, risk management and internal control of the IT environment should be of prominence as part of the auditors' risk-based planning.

1.3 We are grateful to Amaraghosha Carter, Head of IT Surrey and Sussex Police for their assistance during the course of the audit.

2. Objectives

2.1 This review will inform the strategic internal audit plan for IT in 2018/2019 and the wider three-year strategic plan. Ensuring a focus on those areas which are most significance to the Office of the Sussex Police & Crime Commissioner and Sussex Police Force.

3. Circulation List

3.1 This document has been circulated to the following:

- Joseph Langford – Chief Information Officer
- Amaraghosha Carter – Head of IT Surrey and Sussex Police

Chartered Institute of Internal Auditors	The Southern Internal Audit Partnership conforms to the IIA's professional standards and its work is performed in accordance with the International Professional Practices Framework *(endorsed by the IIA).*

4. Approach

4.1 The Institute of Internal Auditors recommends that to provide IT assurance, some work should be done in each of the following headings each year:

- IT Governance
- Data Management
- Information Security
- Systems development and implementation
- Business continuity
- Networking and communications

4.2 As a starting point we developed a list of auditable areas under the ISACA headings, to ensure that all areas where assurance may be required were given consideration. This was then refined and amended to produce a list of auditable areas, considering the information gathered as part of the audit needs assessment through:

- Discussion with Amaraghosha Carter (Head of IT Surrey and Sussex Police) to gain an understanding of the IT and collaboration environment and to understand management concerns;
- Identification of the previous audit work undertaken;
- Review of the Sussex and Surrey Police risk registers with reference to IT risks;
- Other sources of assurance for example PSNP, ISO27001.

4.3 Items included in the audit universe have been risk assessed in terms of inherent risk, corporate importance (effect on service provision) and corporate sensitivity (legal and regulatory compliance, reputational risk).

4.4 The audit needs assessment shown at Appendix A is considered to cover the key aspects of the IT environment. We have included an indicative 3-year audit plan for management consideration; this will need to be reviewed periodically to take account of changes in the IT environment, emerging risks, and management concerns.

Appendix A: Audit needs assessment 2018/19 to 2020/21

Auditable area	Scope	Risk Register Reference (# HoIT Priorities)	Risk	18/19	19/20	20/21	21/22
IT GOVERNANCE							
IT Strategy and Direction	The IT Strategy is aligned to the business articulating the vision, strategic roadmap, technical architecture, planning and investment for IT. Effective governance arrangements are in place to approve, monitor and scrutinise the production, approval and delivery of the strategy.	STR1473 (A) #1	H	●	●		●
IT Policies, Standards and Procedures	Policies, Standards and Procedures are clear, up to date and aligned to relevant legislation / guidance (ITIL as appropriate). Effective governance arrangements are in place to approve and monitor compliance.		M			●	
Monitoring, Assurance and Compliance	Monitoring of compliance with internal policies and external compliance programmes. Analysis of sources which provide assurance that IT is being governed effectively.	#6	M		●		
IT Resource Management	There is a clear understanding and management of resources and competencies required to meet existing and future business needs including corporate projects, BAU and IT Service developments (local & national).	STR1489 (R) STR1984 (R) STR2026 (R) STR1882 (A) STR1825 (A) STR1578 (G) #5	H		●		●

Auditable area	Scope	Risk Register Reference (# HoIT Priorities)	Risk	18/19	19/20	20/21	21/22
IT Asset Management	Practices in place to join financial, contractual and inventory functions to support life cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware within the organisation.		M			●	
Change Management	Assurance that standardised methods and procedures are used for the efficient and effective handling of all changes, to minimise the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organisation.		M				●
Software Licensing	To ensure the adequacy, effectiveness and completeness of monitoring of software licenses across the organisation.		M		●		
Problem and Incident Management	Reported incident are effectively managed, prioritised and responded to within a timely manner. Analysis of reported incidents provides proactive action in identified areas of commonality or criticality.		M			●	
DATA MANAGEMENT							
Data Centre Facilities and Security	Maintained in an appropriate location with suitable physical and environmental controls in place.		H			●	
Data Storage and Data Backup	Data in appropriately retained in accordance with legislative and organisational requirements. Data is backed up at appropriate intervals and retrievable within known timeframes.	STR845 (R) STR1982 (R) STR2062 (A)	H		●		●

Auditable area	Scope	Risk Register Reference (# HoIT Priorities)	Risk	18/19	19/20	20/21	21/22
Capacity and Performance Monitoring	Ensure that the current system is running within safe engineering limits within the organisations network. Regular monitoring provide assurances on capacity health and stability avoiding capacity and performance exposures from occurring.	#7	H		●		
Database Management	To review areas of general security, access, database availability, backup and recovery, development and integrity of a sample of key databases.		M				●
INFORMATION SECURITY							
Security Controls	Design, implementation and monitoring of system and logical security to verify confidentiality, integrity, availability	STR845 (R) #8	H		●		
Data Classification	Data is appropriately classified and relevant procedures and processes/ controls in place to enable and monitor compliance.	#10	M			●	
Remote Access	Safeguarding access to information by mobile workers or remote staff via the internet from remote locations.		M			●	
Public Facing Internet Security	Controls to prevent loss of website access / availability which could inhibit key communication channel.		M				●
Cyber Security	Safeguards in place to protecting systems, networks, and programs from digital attacks. Such attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.	STR943 (G)	H		●		

Auditable area	Scope	Risk Register Reference (# HoIT Priorities)	Risk	18/19	19/20	20/21	21/22
Cloud	Controls in place to protect the organisation against the use of remote servers to store, manage, and process data.		M			●	
SYSTEMS DEVELOPMENT AND IMPLEMENTATION							
Systems Life Cycle Support and Planning	Management of systems which are out of support and identification of those coming to the end of support.		M			●	
Project Management Practices, Reviews and Project Controls	Effectiveness of processes and procedures in place for the planning, executing, controlling, and closing of workstreams / projects to achieve specific goals and meet identified success criteria.	STR1489 (R) STR1984 (R) STR1882 (A) STR1441 (A) #2, #3, #4	H	●			●
Application Management	Processes in place for managing the operation, maintenance, versioning and upgrading of an application throughout its lifecycle (incl. patching).	STR18996 (R) STR2033 (R) STR1934 (A)	H		●		
BUSINESS CONTINUITY							
IT Business Continuity / Disaster Recovery Planning	Effectiveness of planning to protect the organisation from the effects of significant negative events, allowing the organisation to maintain or quickly resume mission-critical functions following a disaster.	STR845 (R) STR1817 (A) STR1970 (A) #9	H		●		●
System Resilience	Processes in place to understand a systems ability to withstand a major disruption (including identification of ingle points of failure) within acceptable degradation parameters and to recover within an acceptable time.		M			●	

Auditable area	Scope	Risk Register Reference (# HoIT Priorities)	Risk	18/19	19/20	20/21	21/22
NETWORKING AND COMMUNICATIONS							
Network Security and Access Control	Effectiveness of controls to safeguard network security and access to include considerations of antivirus, host intrusion prevention, and vulnerability assessment, user or system authentication and network security enforcement.		H		●		
Network Infrastructure Management & Monitoring	Assurance with regard hardware and software resources of the network including connectivity, communication, operations and management.	STR1984 (R) STR2033 (R) STR1647 (A) STR1825 (A) STR1952 (G)	H	●			
Virtualisation	Effective management and control of virtual computer hardware platforms, storage devices, and computer network resources.		M			●	
Operating System Management	Controls and procedures in place to protect the integrity, operation, access, maintenance etc. of key operating systems		M		●		

Assignment – Progress Control Sheet

Assignment stage	Assignment Progress				Comments
Audit Outline	Issued	06/08/2018	Agreed	03/09/2018	
Fieldwork commenced	Target	17/09/2018	Actual	17/09/2018	
Fieldwork completed	Target	12/10/2018	Actual	02/11/2018	Sussex IT staff availability
Close of audit meeting	Target	N/A	Actual	N/A	
Draft Report Issued	Target[1]	19/10/2018	Actual	19/11/2018	Due to delay in fieldwork
Factual accuracy agreed and management response provided	Requested[2]	19/11/2018	Provided	22/11/2018	
Draft final report issued	Target[3]	19/10/2018	Actual	19/11/2018	Due to delay in fieldwork
Senior management sign-off	Requested[4]	04/12/2018	Provided	04/12/2018	
Final report issued	Target[5]	06/12/2018	Actual	06/12/2018	

[1] Within 10 working days of close of audit meeting

[2] Within 10 working days of draft report issued

[3] Within 5 working days of receipt of management response

[4] Within 5 working days of draft final report issued

[5] Within 2 working days of senior management sign-off