



Norfolk and Suffolk Police and Crime Commissioners and Chief Constables

3 Year Strategic Internal Audit Plan 2016/17 to 2018/19 and Annual Internal Audit Plan 2016/17

March 2016

Three Year Strategic Internal Audit Plan 2016/17 to 2018/19 and Annual Internal Audit Plan 2016/17

INTRODUCTION

This Three Year Strategic Internal Audit Plan is drawn up in accordance with the Terms of Reference of TIAA and the requirements of the Public Sector Internal Audit Standards (PSIAS).

AUDIT STRATEGY

The internal audit programme of work, outlined in the Three Year Strategic Internal Audit Plan, is designed to determine the extent to which Norfolk and Suffolk Police's network of risk management, control and governance processes are adequate and operating in the designed manner.

Assessing the audit risk attached to each system

In order to obtain the best use of the internal audit resource it is necessary to assess the risk to Norfolk and Suffolk Police of a failure of the internal controls or absence of appropriate internal controls in each system. This is achieved by a risk analysis model, drawn up by TIAA, which has been used to determine the risk category for each system. The model considers the:

Norfolk and Suffolk Police identified major risks - The Norfolk and Suffolk Police's risk registers lists the business significant risks. Many of these risks relate to external factors where internal audit could have very limited impact. Major risks, which relate to internal factors, have been considered as part of the production of the Three Year Strategic Internal Audit Plan.

Audit risks - This element considers the control risks associated with the operation of an activity. The risk assessments make allowance for previous internal audit reviews carried out, though the extent of the allowance reduces as the elapsed time increases. The risk analysis model also makes allowance for assurances from other external reports e.g. financial

statements auditor. The highest risk areas identified are included in the Three Year Strategic Internal Audit Plan.

Public relations risks - The risk is not just the immediate financial loss that may arise but also the impact of the adverse publicity that may occur from a control failure. In the medium to longer term it is likely that the latter will have the greater adverse impact for Norfolk and Suffolk Police.

Determining the period over which all systems will be audited

The internal audit work to be planned over a three year cycle. A cyclical approach to audit work can be used if a system has been subject to an internal audit review, which has indicated that there are effective controls, as it is then not necessary to undertake detailed assurance reviews on that system in each year.

THREE YEAR STRATEGIC INTERNAL AUDIT PLAN 2016/17 TO 2018/19 AND ANNUAL INTERNAL AUDIT PLAN 2016/17

Annex A sets out the overall template for the rolling review of Norfolk and Suffolk Police's systems of internal control over a three-year cycle. This Three Year Strategic Internal Audit Plan assumes that there is no significant change in the risk assessments or in the operations of Norfolk and Suffolk Police. It also assumes that no significant control weaknesses will be identified by the internal audit reviews. As a consequence TIAA will prepare an Annual Internal Audit Plan in each of the financial years which will modify the Three Year Strategic Internal Audit Plan to take into consideration all known changes.

An Annual Internal Audit Plan will be prepared prior to the start of each financial year (Annex B). The programme of work within the Annual Internal Audit Plan will be in accordance with the Three Year Strategic Internal Audit

Plan and any variations will be agreed with the senior staff at Norfolk and Suffolk Police and will be reported to the Audit Committees.

LIAISON WITH THE EXTERNAL AUDITOR

We will liaise with the External Auditor for Norfolk and Suffolk Police. Any matters in the areas included in an Annual Internal Audit Plan that are identified by the External Auditor in their audit management letters will be included in the scope of the appropriate review.

LIMITATIONS AND RESPONSIBILITY

Internal controls can only provide reasonable and not absolute assurance against misstatement or loss. The limitations on assurance include the possibility of one or more of the following situations, control activities being circumvented by the collusion of two or more persons, human error, or the overriding of controls by management. Additionally, no assurance can be provided that the internal controls will continue to operate effectively in future periods or that the controls will be adequate to mitigate all significant risks that may arise in future.

The responsibility for a sound system of internal controls rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses that may exist. Neither should internal audit work be relied upon to identify all circumstances of fraud or irregularity, should there be any, although the audit procedures have been designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control may not be proof against collusive fraud.

Reliance will be placed on management to provide internal audit with full access to staff and to accounting records and transactions and to ensure the authenticity of these documents.

The matters raised in the audit reports will be only those that come to the attention of the auditor during the course of the internal audit reviews and are not necessarily a comprehensive statement of all the weaknesses that

exist or all the improvements that might be made. The audit reports are prepared solely for management's use and are not prepared for any other purpose.

REPORTING

Assignment Reports: A separate report will be prepared for each review carried out. Each report will be prepared in accordance with the arrangements contained in the Terms of Reference agreed with TIAA and which accord with the requirements of the Public Sector Internal Audit Standards (PSIAS).

Progress Reports: Progress reports will be prepared for each Audit Committee meeting. Each report will detail progress achieved to date against the agreed annual plan.

Annual Report: An Annual Report will be prepared for each year in accordance with the requirements set out in the PSIAS. The Annual Report will include our opinion of the overall adequacy and effectiveness of Norfolk and Suffolk Police's risk management, control and governance processes.

ASSESSMENT OF THE KEY RISK CONTROL OBJECTIVES

For each assurance review an assessment of the combined effectiveness of the controls in mitigating the key control risks will be provided. The assurance mapping process is set out in Annex C.

AUDIT REMIT

The Audit Remit (Annex D) formally defines internal audit's purpose, authority and responsibility. It establishes internal audit's position within Norfolk and Suffolk Police and defines the scope of internal audit activities.

COUNTER FRAUD

Due consideration is given to the risk of fraud and a number of audits include pro-active counter fraud work. E.g. proceeds of crime, reviewing changes to bank accounts as part of the accounts payable audit, expenses audit. Therefore a specific allocation of time has not been included within the plan.

RELEASE OF REPORT

The table below sets out the history of this plan.

Date plan issued:	January and March 2016
-------------------	------------------------

Annex A

Internal Audit Strategic Plan – 2016/17 – 2018/19

System	Type of review	Notes	2015/16	2016/17	2017/18	2018/19
Strategic						
Governance – Strategic Control and Corporate Governance	Assurance			12		12
Governance – Strategic Planning	Assurance				12	
Governance – Performance Management	Assurance	Days from 15/16 to 16/17		15		15
Governance – Transformation and Change Management	Assurance				12	
Governance – Ethical Standards	Assurance		12		12	
Governance – Assurance Framework	Assurance			10		
Risk						
Risk Management – Strategy / Policy OPCCs	Assurance		12	10		12
Risk Management – Mitigating Controls	Assurance			15		
Risk Management – Business Continuity	Assurance				12	
Risk Management – RAID log	Assurance		15			
ICT						
ICT – Cyber Security	Assurance		10			
ICT – Network Security	Assurance	Days from 15/16 to 16/17		12		
ICT – t-Police	Assurance		12			
ICT - ITIL Framework Gap Analysis	Assurance		10			
ICT – Exchange 2010/email Archiving	Assurance			12		
ICT – Data Assurance	Assurance				12	12
ICT –Social Networking/Website Content Management	Assurance				12	
ICT – Firewall	Assurance			12		

System	Type of review	Notes	2015/16	2016/17	2017/18	2018/19
ICT – IT Governance	Assurance				12	
ICT – Disaster Recovery	Assurance			12		
ICT – Business Continuity	Assurance					12
ICT - ERP Second/third line support	Assurance			12		
ICT – Software Licensing	Assurance					12
Finance						
Key Financial Controls	Assurance	Financial systems combined for key control testing		30	30	30
Payroll	Assurance		10	10		10
Accounts Payable	Assurance		10		10	
Accounts Receivable	Assurance		10			10
Purchase Ordering	Assurance		12		10	
Purchase Cards	Assurance		10	12		
General Ledger	Assurance		10			10
Treasury Management	Assurance		10			10
Capital Expenditure	Assurance		10		10	
Budgetary Control	Assurance			12		12
Fixed Assets	Assurance					
Pensions Administration	Assurance				10	
Overtime, Expenses and Additional Payments	Assurance			16		18
Operational						
Estates Management - Strategy	Assurance				12	
Estates Management – Duty of Care / Cost Allocations	Assurance			12		
Estates Management – Maintenance and Repair	Assurance		8 (Norfolk)	12		15
Estates Management - Procurement	Assurance				10	
Estates Management – Facilities (Catering Suffolk only)	Assurance			10 (Suffolk)		

System	Type of review	Notes	2015/16	2016/17	2017/18	2018/19
Estates Management – Building Access	Assurance				12	
Fleet Management - Strategy	Assurance				10	
Fleet Management - Procurement	Assurance					10
Fleet Management – Maintenance, Repair and Fuel Usage	Assurance			12		
Fleet Management – Vehicle Security	Assurance				12	
HR – Absence Management	Assurance		10		10	
HR - Strategy	Assurance			10		
HR - Recruitment	Assurance	Days from 15/16 to 16/17		12		12
HR – Learning and Development	Assurance				12	
Collaborations	Assurance			10		
Duty Management System	Assurance	Days from 15/16 to 16/17		15		12
Corporate Communications	Assurance			12		
Mobile Devices	Assurance		15			
Digital Data	Assurance				12	
Data Quality	Assurance				12	12
Firearms Management	Assurance			12		
Commissioners Grants – Norfolk only	Assurance	Reduced from 18 - 9	9 (Norfolk)	10	10	10
Proceeds of Crime	Assurance		15			12
Contract Review	Assurance		12			12
Safeguarding and investigations	Assurance					10
Police Stations	Assurance		7 (Suffolk)			
Lone Working	Assurance					10
Freedom of Information / Data Protection / Document Security Management	Assurance			15		
Complaints	Assurance			10		
Specified Information Order	Assurance				10	
Records Management / Follow Up	Assurance		4		12	
Other						

	Type of	Notes	2015/16	2016/17	2017/18	2018/19
System	review					
Contingency including Local Counter Fraud Work		Days from 15/16 to 16/17	19	15	12	12
Follow Up			8	10	10	10
Audit Management (to include: audit planning, client liaison, external audit, annual report, Audit Committee)			20	20	20	20
		Total Days 15/16 to 16/17	(69)	69		
	Totals		261	399	330	330

Internal Audit Annual Plan – 2016/17

Quarter	Audit	Type	Days	Scope
Q1	Assurance Framework	Assurance	10	<p><u>Scope</u></p> <p>The review will follow up on the outcome of the previous assurance framework audit by the previous internal auditors. This will include an appraisal of the assurance framework established and streamlining of the framework.</p> <p><u>Rationale</u></p> <p>The embedding of a streamlined assurance framework would provide a basis to gain assurance on the control environment.</p> <p><u>Lead Officers</u></p> <p>PCC</p>
Q1	Risk Management – Strategy / Policy (PCCs)	Assurance	10	<p><u>Scope</u></p> <p>The review will appraise how the OPCCs have developed a risk management strategy and policy. Key staff will be interviewed to assess how they use risk management in their everyday activities.</p> <p><u>Rationale</u></p> <p>The risk management strategy and policy will determine how risk management is managed across the organisations.</p> <p><u>Lead Officers</u></p> <p>PCC</p>
Q1	ICT – Exchange 2010/email Archiving	Assurance	12	<p><u>Scope</u></p> <p>The review will consider the effectiveness of the controls in place around exchange 2010 and email archiving.</p> <p><u>Rationale</u></p> <p>Rolling programme of technical ICT reviews. Agreed with the Director of ICT</p> <p><u>Lead Officers</u></p> <p>Director of ICT</p>

Quarter	Audit	Type	Days	Scope
Q1	Overtime, Expenses and Additional Payments	Assurance	16	<p><u>Scope</u> The review considers the arrangements for overtime, expenses and additional payment transactions through CAPITA and ERP, for compliance with policy and procedures. These will include overtime, mileage, car parking, meals, train travel and accommodation.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> Chief Finance Officers</p>
Q1	Fleet Management – Maintenance, Repair and Fuel Usage	Assurance	12	<p><u>Scope</u> The review considers the processes around the maintenance and repair of vehicles and the usage of fuel.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> Head of Fleet</p>
Q1	Corporate Communications	Assurance	12	<p><u>Scope</u> The review considers the handling of data and information, use of government security marking, KPIs and compliance with policy.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> Communications</p>
Q1	Firearms Management	Assurance	12	<p><u>Scope</u> The review considers the effectiveness of managing firearms and compliance with policy.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> ACC</p>

Quarter	Audit	Type	Days	Scope
Q1	Freedom of Information / Data Protection / Document Security	Assurance	15	<p><u>Scope</u> The review considers the effectiveness of managing freedom of information requests, data protection and document security.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> Head of Information Management</p>
Q1	Complaints	Assurance	10	<p><u>Scope</u> The review considers the effectiveness and efficiency of handling complaints.</p> <p><u>Rationale</u> Key Audit risk area.</p> <p><u>Lead Officers</u> Head of Information Management</p>
Q1	ICT – Network Security (Days brought forward from 2015/16)	Assurance	12	<p><u>Scope</u> The review considers the arrangements for the physical and access security of hardware and software. To include: Domain accounts policies; Audit policy setting: User privileges; Trusted and trusting hosts; User accounts and passwords; Services and drivers; Home directories and logon scripts; Security options settings; Logical drives; Default login accounts; Discretionary access controls.</p> <p>The scope of the review does not include the types of hardware and software used, the access rights to the individual software; or the depreciation policies.</p> <p><u>Rationale</u> Rolling programme of technical ICT reviews. Agreed with the Director of ICT</p> <p><u>Lead Officers</u> Director of ICT</p>
Q1	HR – Recruitment (Days brought forward from 2015/16)	Assurance	12	<p><u>Scope</u> The review will consider the arrangements for advertising, shortlisting, interviewing and appointing staff/Officers. The review will include the business case supporting the recruitment requirements.</p> <p><u>Rationale</u> An important area for the PCC. Agreed with CFO</p>

Quarter	Audit	Type	Days	Scope
				<u>Lead Officers</u> Director of HR
Q1	Duty Management System (Days brought forward from 2015/16)	Assurance	15	<u>Scope</u> The review will appraise the effectiveness of the duty resource management system. <u>Rationale</u> An important system for the Forces <u>Lead Officers</u> Director of HR
Q2	Strategic Control and Corporate Governance	Assurance	12	<u>Scope</u> The review will consider the overall strategic governance of the organisations. Compare and contrast, such as decision notices. <u>Rationale</u> Reputationally a high risk area. <u>Lead Officers</u> Head of PSD
Q2	Governance – Performance Management (Days brought forward from 2015/16)	Assurance	15	<u>Scope</u> The review considers the arrangements for providing assurance to the PCC and Chief Officers through the use of Key Performance Indicators and the systems that are used to track and manage the attainment of these targets. The scope of the review does not include consideration of the accuracy or completeness of all reports presented to the committees/groups or the appropriateness of all decisions taken. <u>Rationale</u> Key area of Governance, reviews included every other year of the plan. <u>Lead Officer</u> Head of JPAD

Quarter	Audit	Type	Days	Scope
Q2	Risk Management – Mitigating Controls	Assurance	15	<p><u>Scope</u> The review will appraise how the documented mitigating controls within the risk register address the documented risks.</p> <p><u>Rationale</u> Providing assurance that documented actions and controls effectively mitigate the risks.</p> <p><u>Lead Officers</u> Head of Organisational Development</p>
Q2	ICT - Firewall	Assurance	12	<p><u>Scope</u> The review will consider the effectiveness of the controls in place around the firewalls.</p> <p><u>Rationale</u> Rolling programme of technical ICT reviews. Agreed with the Director of ICT</p> <p><u>Lead Officers</u> Director of ICT</p>
Q2	Estates – Duty of Care / Cost Allocations	Assurance	12	<p><u>Scope</u> The review will appraise the cost and equipment ownership assigned to each force, along with the devolved budgetary control.</p> <p><u>Rationale</u> The collaboration between the forces provides a high risk of equipment transferring between locations and forces.</p> <p><u>Lead Officers</u> Head of Estates</p>
Q2	Collaborations	Assurance	10	<p><u>Scope</u> The review will appraise the strategy for collaborations between forces.</p> <p><u>Rationale</u> The collaboration between the existing two forces and with other forces may continue to increase.</p> <p><u>Lead Officers</u> Chief Finance Officers</p>

Quarter	Audit	Type	Days	Scope
Q2	Estates – Facilities (Catering – Suffolk only)	Assurance	10	<p><u>Scope</u> The review will appraise the new contract for the catering facilities at Martlesham, to assess the processes in place for managing the service for catering across the force.</p> <p><u>Rationale</u> The new contract will continue to involve catering services across departments, with a view to streamlining processes.</p> <p><u>Lead Officers</u> Head of Estates</p>
Q3	ICT – Disaster Recovery	Assurance	12	<p><u>Scope</u> The review will consider the effectiveness of the controls in place around ICT Disaster Recovery.</p> <p><u>Rationale</u> Rolling programme of technical ICT reviews. Agreed with the Director of ICT</p> <p><u>Lead Officers</u> Director of ICT</p>
Q3	HR - Strategy	Assurance	10	<p><u>Scope</u> The review will consider the strategies in place for current and future HR needs for the forces.</p> <p><u>Rationale</u> An important area for the PCC.</p> <p><u>Lead Officers</u> Director of HR</p>
Q3	Purchase Cards	Assurance	12	<p><u>Scope</u> To examine a number of orders placed to confirm compliance with the Force's Purchasing card procedures when goods and/or services are procured.</p> <p>Ensure compliance with operating procedures for Purchasing</p> <p>Review the system and procedures for contract procurement</p> <p>To verify that internal controls are in place and working to manage the purchase ordering procedures</p>

Quarter	Audit	Type	Days	Scope
				<p><u>Rationale</u> A high risk area for the Force. Agreed with the CFOs</p> <p><u>Lead Officers</u> Chief Finance Officers</p>
Q3	ICT – ERP Second/Third Line Support	Assurance	12	<p><u>Scope</u> The review will consider the effectiveness of the controls in place around ERP second/third line support.</p> <p><u>Rationale</u> Rolling programme of technical ICT reviews. Agreed with the Director of ICT</p> <p><u>Lead Officers</u> Director of ICT</p>
Q3	Budgetary Control	Assurance		<p><u>Scope</u> The review considers the arrangements for: budget setting, budget holder involvement, budget monitoring.</p> <p><u>Rationale</u> Key Audit risk area - completed annually.</p> <p><u>Lead Officers</u> Chief Finance Officers</p>
Q4	Key Financial Controls	Assurance	30	<p><u>Scope</u> The review considers the arrangements for key controls operating within the following systems; Accounts Payable, Accounts Receivable, General Ledger, Treasury Management, Capital Expenditure and Purchase Cards.</p> <p><u>Rationale</u> Key Audit risk area – completed annually.</p> <p><u>Lead Officers</u> Chief Finance Officers</p>
Q4	Payroll	Assurance	10	<p><u>Scope</u> The review considers the arrangements for: the creation, amendment and deletion of payroll records; payment of allowances and pay awards; and payment of salaries. The scope of the review does not include determination of salary scales, appointment and</p>

Quarter	Audit	Type	Days	Scope
				removal of staff, severance payments or reimbursement of travel and subsistence expenses, or pension arrangements. <u>Rationale</u> Key Audit risk area - completed annually due to large percentage of overall budget. <u>Lead Officers</u> Chief Finance Officers
Q4	Estates – Maintenance and Repair	Assurance	12	<u>Scope</u> The review will appraise the effectiveness, efficiency and timeliness of reactive maintenance call handling to the most appropriate contractor to undertake the work. <u>Rationale</u> An important area for the PCC. <u>Lead Officers</u> Head of Estates
Q4	Commissioners Grants (Norfolk only)	Assurance	10	<u>Scope</u> The review will consider the arrangements for the assessing, awarding and compliance monitoring process for the grants issued by the Commissioners. <u>Rationale</u> An important area requiring high levels of governance and probity. <u>Lead Officers</u> Chief Executives (OPCC)
	Contingency including LCFS and days brought from 2015/16		15	Only to be used with the express permission of the Chief Finance Officers
Q2 / Q4	Follow up work		10	The review ascertains whether management action has been taken to address the Priority 1 & 2 recommendations arising from internal audit work carried out in the financial year.
1-4	Audit Management		20	This time includes planning, annual report, attendance at Audit Committee meetings, client meetings and overall contract management.
		Total days 2016/17	399	

Assurance Mapping

Corporate assurance risks

We consider four corporate assurance risks; directed; compliance; operational and reputational. The outcomes of our work on these corporate assurance risks informs both the individual assignment assurance assessment and also the annual assurance opinion statement. Detailed explanations of these assurance assessments are set out in full in each audit report.

Assurance assessment gradings

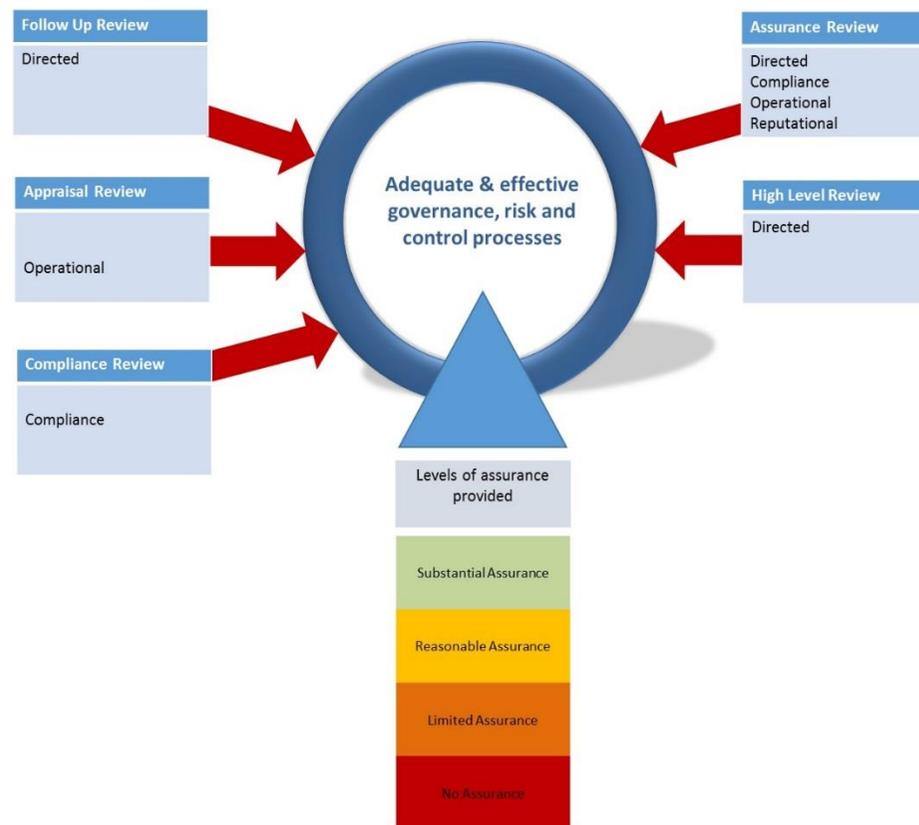
We use four levels of assurance assessment: substantial; reasonable, limited and no. Detailed explanations of these assurance assessments are set out in full in each audit report.

Types of audit review

The Annual Internal Audit Plan includes a range of types of audit review. The different types of review focus on a one or more of the corporate assurance risks. This approach enables more in-depth work to be carried out in the individual assignments than would be possible if all four assurance risks were considered in every review. The suite of audit reviews and how they individually and collectively enable us to inform our overall opinion on the adequacy and effectiveness of the governance, risk and control arrangements is set out in the assurance mapping diagram.

Directed Risk: Failure to direct the process through approved policy & procedures.

Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.



Operational Risk: Failure to identify opportunities to operate more efficiently or to be prepared for forthcoming changes.

Reputational Risk: Failure to deliver in a manner that meets the expectations of the organisation.

Audit Remit

Role

The main objective of the internal audit activity carried out by TIAA is to provide, in an economical, efficient and timely manner, an objective evaluation of, and opinion on, the overall adequacy and effectiveness of the Norfolk and Suffolk Police's framework of governance, risk management and control. TIAA is responsible for giving assurance to Norfolk and Suffolk Police's Audit Committees on the adequacy and effectiveness of Norfolk and Suffolk Police's risk management, control and governance processes.

Scope

All Norfolk and Suffolk Police's activities fall within the remit of TIAA. TIAA may consider the adequacy of controls necessary to secure propriety, economy, efficiency and effectiveness in all areas. It will seek to confirm that Norfolk and Suffolk Police's management has taken the necessary steps to achieve these objectives and manage the associated risks. It is not within the remit of TIAA to question the appropriateness of policy decisions. However, TIAA is required to examine the arrangements by which such decisions are made, monitored and reviewed.

TIAA may also conduct any special reviews requested by senior management, audit committee or the nominated officer (being the post responsible for the day to day liaison with the TIAA), provided such reviews do not compromise the audit service's objectivity or independence, or the achievement of the approved audit plan.

Standards and Approach

TIAA's work will be performed with due professional care, in accordance with the requirements of the PSIAS.

Access

TIAA has unrestricted access to all documents, records, assets, personnel and premises of Norfolk and Suffolk Police and is authorised to obtain such information and explanations as they consider necessary to form their opinion.

Independence

TIAA has no executive role, nor does it have any responsibility for the development, implementation or operation of systems. However, it may provide independent and objective advice on risk management, control, governance processes and related matters, subject to resource constraints. For day to day administrative purposes only, TIAA reports to a nominated officer within Norfolk and Suffolk Police and the reporting arrangements must take account of the nature of audit work undertaken. TIAA has a right of direct access to the chair of the Audit Committee and the responsible accounting officer (being the post charged with financial responsibility).

To preserve the objectivity and impartiality of TIAA's professional judgement, responsibility for implementing audit recommendations rests with Norfolk and Suffolk Police's management.

Consultancy activities are only undertaken with distinct regard for potential conflict of interest. In this role we will act in an advisory capacity and the nature and scope of the work will be agreed in advance and strictly adhered to. The objective of any consultancy work is to add value and improve governance, risk management and control processes. Internal audit will never take or assume management responsibility.

Irregularities, Including Fraud and Corruption

TIAA will without delay report any, serious weaknesses, significant fraud, major accounting and other breakdowns subject to the requirements of the Proceeds of Crime Act 2003 to the nominated officer.

TIAA will be informed when evidence of potential irregularity, including fraud, corruption or any impropriety, is discovered so that he or she can consider the adequacy of the relevant controls, evaluate the implication of the fraud on the risk management, control and governance processes and consider making recommendations as appropriate. The role of TIAA is not to investigate the irregularity unless commissioned to do so.