tiaa

INTERNAL AUDIT

Norfolk and Suffolk Police and Crime Commissioners and Chief Constables

3 Year Strategic Internal Audit Plan 2015/16 to 2017/18 and Annual Internal Audit Plan 2015/16

June 2015

Three Year Strategic Internal Audit Plan 2015/16 to 2017/18 and Annual Internal Audit Plan 2015/16

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 2015/16 TO 2017/18 AND ANNUAL INTERNAL AUDIT PLAN 2015/16

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:	21 May 2015

Annex A

Internal Audit Strategic Plan – 2015/16 – 2017/18

System	Type of review	2015/16	2016/17	2017/18
Strategic				
Governance – Strategic Control and Corporate Governance	Assurance		12	
Governance – Strategic Planning	Assurance		12	
Governance – Performance Management	Assurance	15		15
Governance – Transformation and Change Management	Assurance		12	
Governance – Ethical Standards	Assurance	12		
Risk				
Risk Management – Embedding	Assurance	12		12
Risk Management – Mitigating Controls	Assurance		15	
Risk Management – Business Continuity	Assurance		12	
Risk Management – RAID log	Assurance	15		12
ICT				
ICT – Cyber Security	Assurance	10		12
ICT – Network Security	Assurance	12		12
ICT – t-Police	Assurance	12		
ICT - ITIL Framework Gap Analysis	Assurance	10		
ICT – Data Assurance	Assurance		12	
ICT – Internet/email/Social Networking	Assurance		12	
ICT – Change Management	Assurance		10	

tiaa

System	Type of review	2015/16	2016/17	2017/18
ICT – Disaster Recovery	Assurance		10	
Finance				
Payroll	Assurance	10	10	10
Accounts Payable	Assurance	10	10	10
Accounts Receivable	Assurance	10	10	10
Purchase Ordering	Assurance	12	10	10
Purchase Cards	Assurance	10	10	10
General Ledger	Assurance	10	10	10
Treasury Management	Assurance	10		
Capital Expenditure	Assurance	10		10
Budgetary Control	Assurance		12	
Fixed Assets	Assurance		10	
Pensions Administration	Assurance		10	
Expenses and Additional Payments	Assurance		10	
Operational				
Estates Management - Strategy	Assurance		12	
Estates Management – Duty of Care	Assurance			12
Estates Management – Maintenance and Repair	Assurance	8 (Norfolk)		15
Fleet Management - Strategy	Assurance		12	
Fleet Management - Procurement	Assurance			12
Fleet Management – Fuel Usage	Assurance			12
Fleet Management – Maintenance and Repair	Assurance		12	
HR – Absence Management	Assurance	10 (Suffolk)		10
HR - Strategy	Assurance		10	
HR - Recruitment	Assurance	12 (Norfolk)		12
HR – Learning and Development	Assurance			10

System	Type of review	2015/16	2016/17	2017/18
Duty Management System	Assurance	15		12
Communications	Assurance		10	
Mobile Devices	Assurance	15		12
Digital Data	Assurance		15	
Firearms Management	Assurance			12
Commissioners Grants	Assurance	18 (two audits)		16
Proceeds of Crime	Assurance	15		12
Contract Review	Assurance	12	12	12
Police Stations	Assurance	7 (Suffolk)		
Other				
Contingency		10	10	10
Follow Up		8	8	8
Audit Management (to include: audit planning, client liaison, external audit, annual report, Audit Committee)		20	20	20
Totals		330	330	330

Internal Audit Annual Plan – 2015/16

Quarter	Audit	Type	Days	Scope
Q2	Governance – Performance Management	Assurance	15	Scope 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. Rationale Key area of Governance, reviews included every other year of the plan. Lead Officer Head of JPAD
Q2	Governance – Ethical Standards	Assurance	12	Scope The Policing Protocol makes clear at section 10 that 'All parties will abide by the seven principles set out in Standards in Public Life: First Report of the Committee on Standards in Public Life (a) (known as the "Nolan Principles").' The review will focus on how the PCC and Chief Constable demonstrate adherence to the Seven Principles of Public Life: Selflessness, Integrity, Objectivity, Accountability, Openness, Honesty and Leadership. Rationale Reputationally a high risk area. Lead Officers Head of PSD
Q3	Risk Management – Embedding (the risk culture)	Assurance	12	Scope The review will appraise how the OPCC and Force have engaged with risk management and how well these are embedded. Key staff will be interviewed to assess how they use risk management in their everyday activities. Rationale The embedding of risk management is the important element in how risks are managed by the organisation on a day to day basis.

Quarter	Audit	Type	Days	Scope
				<u>Lead Officers</u> Head of Organisational Development
Q3	Risk Management – Risk, Assurance, Issues, Dependencies (RAID) log	Assurance	15	<u>Scope</u> The review will appraise the effectiveness of the RAID log in managing risk. <u>Rationale</u> An important area for the Force. Agreed with the CFOs. <u>Lead Officers</u> Head of CDC
Q2	ICT – Cyber Security	Assurance	10	<u>Scope</u> The review will focus on the "10 steps to cyber security" which is Government guidance and the use of Cyber Essentials. <u>Rationale</u> A high ICT risk. Agreed with the Director of ICT <u>Lead Officers</u> Director of ICT
Q3	ICT – Network Security	Assurance	12	<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;

Quarter	Audit	Type	Days	Scope
				Default login accounts;
				Discretionary access controls.
				The scope of the review does not include consideration of the merits of the types of hardware and software used, the access rights to the individual software; or the depreciation policies
				Rationale
				Rolling programme of technical ICT reviews. Agreed with the Director of ICT
				Lead Officers
				Director of ICT
Q3	ICT – t-Police	Assurance	12	Scope
				The review will be a post implementation review to include the following:
				. The business requirements have been met;
				The expected benefits have been realised;
				The system is considered usable;
				Stakeholders expectations have been met;
				No unexpected impacts on the organisation;
				Change management, installation and accreditation processes were performed effectively
				and efficiently.
				Rationale
				An important system. Review agreed with the Director of ICT
				Lead Officers
				Director of ICT
				Head of Organisational Development
Q4	Information Technology Infrastructure Library (ITIL) Framework Gap Analysis	Assurance	10	(ITIL is a method of organising the system and network management departments of large organisations. ITIL defines the work processes involved and the interfaces between them.)
				Scope
				The review will be a gap analysis to confirm that the Forces are compliant with the ITIL framework. To include:

Quarter	Audit	Type	Days	Scope
				Service Desk and Change and Problem Management
				Rationale
				The Forces need to demonstrate compliance with the ITIL framework. Review agreed with the Director of ICT.
				Lead Officers
				Director of ICT
Q3	Payroll	Assurance	10	Scope
				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 removal of staff, severance payments or reimbursement of travel and subsistence expenses, or pension arrangements.
				Rationale
				Key Audit risk area - completed annually due to large percentage of overall budget.
				Lead Officers
				Chief Finance Officers
Q3	Accounts Payable	Assurance	10	Scope
				The review considers the arrangements for authorising and paying expenditure incurred by the organisation and the arrangement for control of the organisation's cheques and automated payments. The scope does not include providing an assurance that the expenditure was necessary or that value for money was achieved from the expenditure committed.
				Rationale
				Key Audit risk area - completed annually.
				Lead Officers
				Chief Finance Officers
Q3	Accounts Receivable	Assurance	10	Scope
				The review considers the raising of debtor accounts, collection of income, receipting, storage and banking of income received by the organisation. The scope of the review does not include identification of the activities giving rise to income for the organisation, the basis of calculating the rates to be charged or that all income receivable has been identified.

Quarter	Audit	Type	Days	Scope
				Rationale Key Audit risk area - completed annually. Lead Officers Chief Finance Officers
Q3	Purchase Ordering	Assurance	12	Scope To examine a number of orders placed to confirm compliance with the Force's Purchasing procedures when goods and/or services are procured. Ensure compliance with operating procedures for Purchasing Review the system and procedures for contract procurement To verify that internal controls are in place and working to manage the purchase ordering procedures Rationale A high risk area for the Force. Agreed with the CFOs Lead Officers Chief Finance Officers
Q3	Purchase Cards	Assurance	10	Scope The review will focus on the distribution and use of purchasing cards to confirm that: Cards are issued to appropriate staff/Officers Spending Limits are proportionate and appropriate Purchases are in accordance with agreed procedures Statements are reconciled and correctly allocated to budgets Rationale A high risk area for the Force. Agreed with the CFOs Lead Officers Chief Finance Officers
Q3	General Ledger	Assurance	10	Scope The review considers the arrangements for providing an effective audit trail for data entered onto the general ledger and the appropriateness of the reports generated. The scope of the

Quarter	Audit	Type	Days	Scope
				review does not extend to the budgetary control arrangements and bank reconciliations. Rationale Key Audit risk area - completed bi-annually. Lead Officers Chief Finance Officers
Q3	Treasury Management	Assurance	10	Scope The review considers the arrangements for controlling the investment and borrowing arrangements; compliance with the organisation's overall policy; banking arrangements; reconciliations and the reporting to committee. The scope of the review does not include consideration of the appropriateness of any individual financial institution or broker or of individual investment decisions made by the organisation. Rationale Key financial risk area - completed bi-annually. Lead Officers Chief Finance Officers
Q3	Capital Expenditure	Assurance	10	Scope The review considers the arrangements for accounting for the capital programme. The scope of the review does not include consideration of the funding arrangements or the specification of the projects Rationale Key Audit risk area - completed bi-annually. Lead Officers Head of Finance
Q2	Estates Management – Maintenance and Repair	Assurance	8 (Norfolk only)	Scope The review will appraise the effectiveness, efficiency and timeliness of the maintenance and repair work/programme for the Estate Rationale An important area for the PCC. Agreed with the CFOs Lead Officers

Quarter	Audit	Type	Days	Scope
				Head of Estates
Q3	HR – Absence Management	Assurance	10 (Suffolk only)	<u>Scope</u> The review will consider the arrangements for: recording, reporting and monitoring absence. The scope of the review will also consider the arrangements to promote wellbeing and reduce absence. <u>Rationale</u> Review of HR Management arrangements included in each year of the plan. Suffolk specifically requested this audit <u>Lead Officers</u> Director of HR
Q3	HR - Recruitment	Assurance	12 (Norfolk only)	<u>Scope</u> The review will consider the arrangements for advertising, shortlisting, interviewing and appointing staff/Officers. In addition, the review will also review the need/business case which supports the recruitment requirements. <u>Rationale</u> An important area for the PCC. Agreed with CFO <u>Lead Officers</u> Director of HR
Late Q3	Duty Management System	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

tiaa

Quarter	Audit	Type	Days	Scope
Late Q3	Mobile Devices	Assurance	15	Scope The review will appraise the process for progressing the use and development of mobile devices. In addition, the benefits realisation will be examined. Rationale An important area for the Forces. Agreed with the CFOs Lead Officers T/Assistant Chief Constable
Q4	Commissioners Grants /PCC Commissioning	Assurance	18 (Two Audits – Norfolk and Suffolk)	Scope The review will consider the arrangements for the assessing, awarding and compliance monitoring process for the grants issued by the Commissioners. Rationale An important area requiring high levels of governance and probity. Lead Officers Chief Executives (OPCC)
Q2	Proceeds of Crime	Assurance	15	Scope The review will appraise the effectiveness of managing the Proceeds of Crime. In particular the review will focus on the securing and monitoring of the proceeds of crime which is held by the Forces Rationale Reputationally a high risk for the PCC and Chief Constable Lead Officers Head of PSD
Q4	Contract Review	Assurance	12	Scope The review considers the identification of: the arrangements for the letting, management and monitoring of contracts entered into by the organisation. The scope of the review does not include consideration of the funding arrangements or the specification of the contracts. Rationale A key risk area - Large value contracts being let.

Quarter	Audit	Type	Days	Scope
				Lead Officers Head of Procurement and Supplies
Q2	Police Stations	Assurance	7 (Suffolk only)	Scope The review considers the controls and security surrounding the management and running of a sample of Police Stations Rationale A key risk area Lead Officers Officers in Charge
	Contingency		10	Only to be used with the express permission of the Chief Finance Officers
Late Q4	Follow up work		8	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	**330**	

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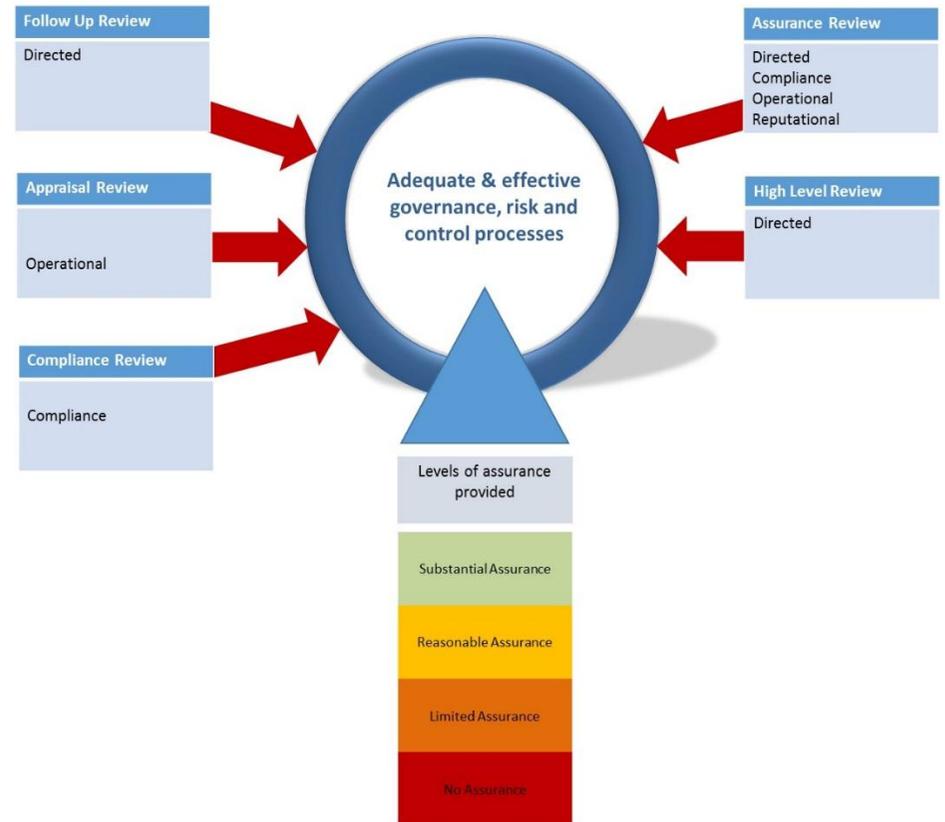
Operational Risk: Failure to identify opportunities to operate more efficiently or to be prepared for forthcoming changes.

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

tiaa

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.