**DRAFT**

|  |  |
| --- | --- |
|  | **The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police** |
|  | **Audit Strategy and Annual Internal Audit Plan** |
|  | **2019/20** |

**February 2019**

**Internal Audit**

**Overview**

**Introduction**

The Audit Plan for 2019/20 has been informed by a risk assessment carried out across all our police clients (with members and senior management) and by an updated audit risk assessment to ensure that planned coverage for the year is focussed on the key audit risks, and that the coverage will enable a robust annual Head of Internal Audit Opinion to be provided.

**Key Emerging Themes**

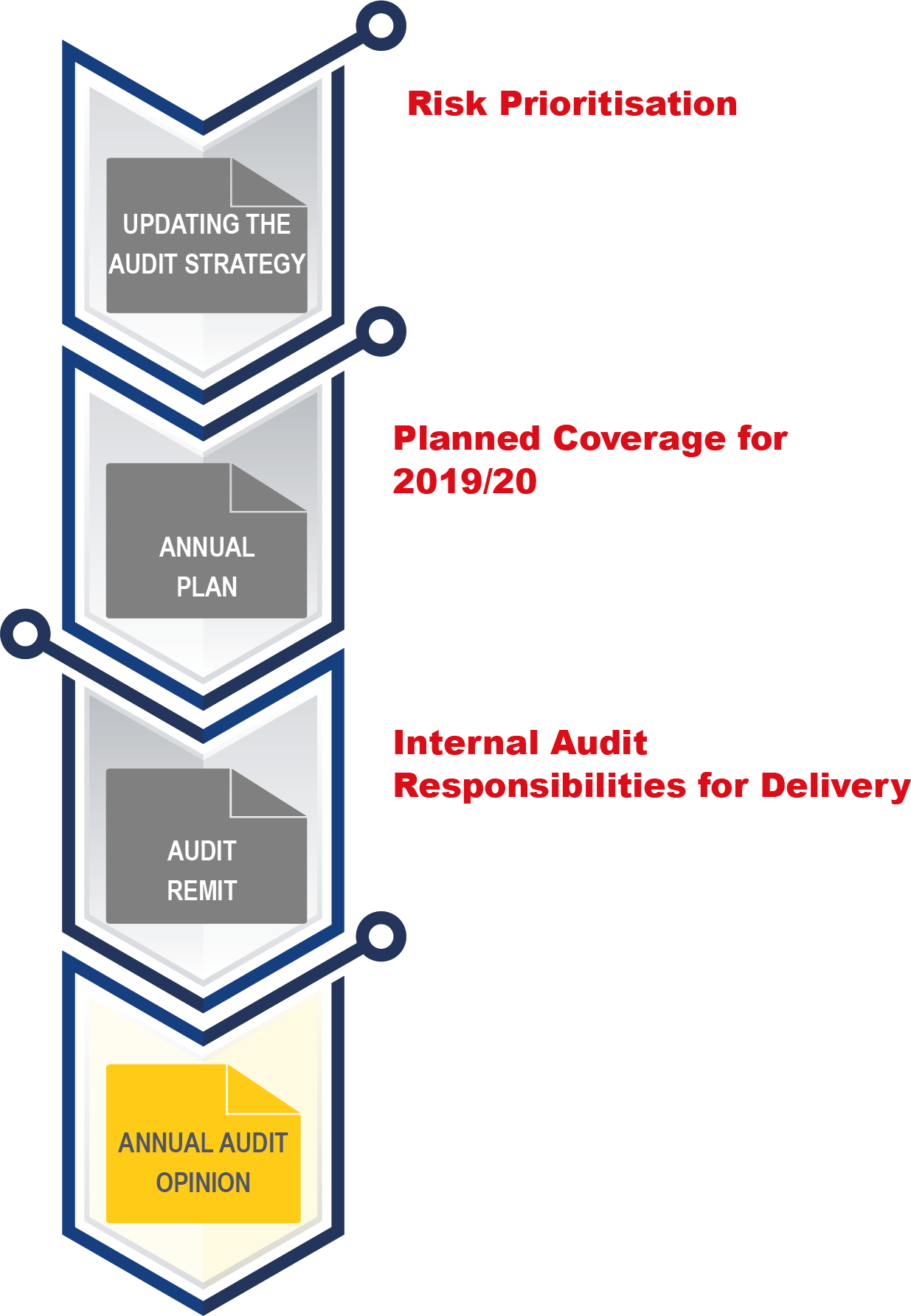
This year will be another challenging year for Police organisations in terms of income, regulation and also the pressures on service delivery. We have identified a number of key areas which require consideration when planning internal audit coverage.

* Collaboration – continuing collaboration across the public sectors
* Joint working – closer ties with the Fire and Rescue Service and other Forces
* Training – HR issues such as mental health and how training is addressing this previously under recognised issue
* HR Learning and Development – the continuing need to retain quality officers
* ICT – body worn cameras will continue to present issues particularly with storage and retrieval
* Transformation - Mobile and agile Police working are ongoing initiatives that raise risk awareness
* Governance – Changes to senior management within the Force may impact on the governance of the organisation

**Adequacy of the planned audit coverage**

The fundamental reviews identified in the audit plan for 2019/20 support the Head of Audit’s annual opinion on the overall adequacy and effectiveness of the organisation’s framework of governance, risk management and control as required by TIAA’s charter. The organisational reviews have been identified from your assurance framework, risk registers and key emerging themes.

*2019/20 Audit planning process*



**Internal Audit Plan**

**Audit Strategy Methodology**

We adopt a proprietary risk based approach (GUARD) to determining your audit needs each year which includes reviewing your risk register and risk management framework, previous internal audit work for the organisation, the regulatory framework and assessment of the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police, external audit recommendations together with key corporate documentation such as your business and corporate plan, standing orders, and financial regulations. The audit strategy is based predominantly on our understanding of the inherent risks facing the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police and those within the sector and has been developed with senior management.

**Risk Prioritisation**

Each year an updated risk assessment is carried out to ensure the audit strategy remains fully aligned with the key risks facing the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police. The resultant changes for 2019/20 which underpin your audit plan is set out at Annex A.

**Audit Strategy and Annual Plan**

Following the risk prioritisation review, the audit strategy has been updated (Annex B) and the annual plan (Annex C) sets out the reviews that will be carried out, the planned times and the scopes for each of these reviews.

The annual plan will be subject to ongoing review and could change as the risks change for the organisation and will be formally reviewed with senior management and the audit committee as an ongoing process throughout the year.

The overall agreed time for the delivery of the annual plan includes: research, preparation and issue of terms of reference, production and review of working papers and reports and site work. The annual plan has been prepared on the assumption that the expected controls will be in place.

The total number of days required to deliver the Audit Plan is as agreed in the contract between TIAA and the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police. This number of days is fixed and it is TIAA’s responsibility to deliver the Audit Plan for this number of days. Where the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police

agrees additional work the required number of days and the aggregate day rate will be agreed in advance with the Chief Finance Officers for the Police and Crime Commissioner and the Chief Constable for Cleveland Police and will be clearly set out in the terms of reference for the additional review(s).

**Audit Remit**

The audit remit (Annex D) formally defines internal audit’s purpose, authority and responsibility. It establishes internal audit’s position within the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police and defines the scope of internal audit activities.

**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 TIAA’s audit charter and the IIA UK & Ireland standards.

**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 TIAA’s audit charter and the IIA UK & Ireland standards. The annual report will include our opinion of the overall adequacy and effectiveness of the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police’s governance, risk management and operational control processes.

**Other Briefings:** During the year client briefing notes, benchmarking and lessons learned digests will be provided. These are designed to keep the organisation abreast of in-year developments which may impact on the governance, risk and control assurance framework.

**Assurance Mapping**

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 E.

**Liaison with the External Auditor**

We will liaise with the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police’s external auditor. Any matters in the areas included in the annual plan that are identified by the external auditor in their audit management letters will be included in the scope of the appropriate review.

**Performance**

The following performance targets will be used to measure the performance of internal audit in delivering the annual plan:

| **Area** | **Performance Measure** | **Target** |
| --- | --- | --- |
| Achievement of the plan | Completion of planned audits. | 100% |
| Audits completed in time allocation. | 100% |
| Reports Issued | Draft report issued within 10 working days of exit meeting. | 95% |
| Final report issued within 10 working days of receipt of responses. | 95% |
| Professional Standards | Compliance with TIAA’s audit charter and the IIA UK & Ireland Standards. | 100% |

**Conflict of Interest**

We are not aware of any conflicts of interest and should any arise we will manage them in line with TIAA’s audit charter and the IIA UK & Ireland standards, the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police’s requirements and TIAA’s internal policies.

**Limitations and Responsibility**

Substantive testing will only be carried out where a review assesses the internal controls to be providing ‘limited’ or ‘no’ assurance with the prior approval of the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police and additional time will be required to carry out such testing. The Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police is responsible for taking appropriate action to establish whether any loss or impropriety has arisen as a result of the control weaknesses.

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.

**Audit Committee Responsibility**

It is the responsibility of the audit committee to determine that the number of audit days to be provided and the planned audit coverage are sufficient to meet the committee’s requirements and the areas selected for review are appropriate to provide assurance against the key risks within the organisation.

**Release of Report**

The table below sets out the history of this plan.

|  |  |
| --- | --- |
| **Date plan issued:** | **14th February 2019** |

**Annex A: GUARD Risk Analysis**

**Changes for 2019/20**

In addition to the core audit work required to underpin the Head of Audit Annual Opinion (governance, risk management, core financial systems, network controls, follow up etc.) a GUARD assessment of key risks has been completed, to identify those that are most relevant to the organisation and where internal audit assurance would be best focussed. These are summarised below.

|  | **GUARD Risk Analysis** | | |  |
| --- | --- | --- | --- | --- |
| **Risk Areas** | **Registered Provider Specific** | **TIAA National Intelligence Assessment** | **Updated Guard Assessment** | **Cross Ref to Annual & Strategic Plan (Annex B, C)** |
| Data Protection Act 2018 – This will be an ongoing issue and source of risk for all organisations given the regulatory and public expectation about how data is held and protected, together with a likely increase in access requests.  How we intend to review this risk: We will assess the organisation’s arrangements for storing hardcopy and electronic information that is covered under the Act and how it is managed to ensure its accuracy and completeness. We will consider responsibilities for managing data including awareness among the wider staff base on processing and providing data. Our approach also includes the arrangements in place for effectively dealing with access requests within the prescribed timeframe. |  |  |  | N |
| Cybersecurity – All the indications are that there will continue to be more sophisticated hacking attempts designed to disrupt or deny services, often for no clear motive.  How we intend to review this risk: We will consider the practical and technical security measures that the organisation has deployed to minimise the risk of succumbing to a cyber incident. We will also consider the extent to which staff awareness has been addressed to minimise the risk of behaviours giving rise to a cyber incident. |  |  |  | N |
| Funding pressure – despite improvements in the funding for Police services this will remain a high risk for some time.  How we intend to review this risk: We will consider the extent to which funding pressures impact upon the governance, risk and control framework for the organisation. |  |  |  | Y |
| Government consultation “Policing for the Future” (October 2018) – This wide-ranging report examines changing demands on policing, and considers the extent to which the service is able to meet the challenges that these create.  How we intend to review this risk – This is potentially an emerging risk on which TIAA will provide client briefing notes at key points during implementation, if appropriate. |  |  |  | N |
| **Client Specific Risks** | | | | |
| Risk- Data Assurance and Disaster Recovery - The maintenance of data and its recovery in the event of a disaster is essential to maintaining the records needed for appropriate policing  How we intend to review this risk - Both Data Assurance and Disaster Recovery are planned audits for 2019-20. |  |  |  | Y |
| Risk - Senior Management Changes - With changes to senior management governance arrangements can be overlooked so additional audit in this area will provide confidence that governance standards have not slipped.  How we intend to review this risk - A number of governance reviews are planned during 2019/20**.** |  |  |  | Y |

**Key to Risk Assessment Grades:**

|  |  |  |
| --- | --- | --- |
| **High** | **Medium** | **Low** |

|  |  |
| --- | --- |
| **RP Specific** | The control framework relating to the specific area has been identified as ‘High’ risk as per Assurance Framework, senior management, internal and external audit. ‘Medium’ priority determines that the control framework has been identified as reasonably vulnerable to control weaknesses based on discussions with management, internal and external audit. ‘Low’ priority means that review of the control framework has not revealed any significant issue. |
| **TIAA portfolio** | Across our client portfolio of similar types of police providers, our intelligence has tracked a large or growing (‘High’ priority); mid-range or flat line (‘Medium’ priority); or relatively low or decreasing (‘Low’ priority) number of control issues in this specific area for this type of organisation. |
| **National Policy/Issue** | National bodies have identified a growing or high level of control weaknesses (‘High’ priority); mid-range or flat line (‘Medium’ priority); or relatively low or decreasing (‘Low’ priority) in this specific area. There may also be a national policy emphasis on a specific area which will be reflected in this priority rating. |

**Annex B: Rolling Strategic Plan**

| **Fundamental Review Areas**  **To support the Head of Internal Audit opinion** | **Risk Ref.** | **Type** | **Yr1** | **Yr2** | **Yr3** |
| --- | --- | --- | --- | --- | --- |
| **Governance** |  |  |  |  |  |
| Key governance areas will be reviewed on a rotational basis each year such as strategic planning, strategic control, regulatory compliance, performance management, board assurance framework, partnership working, management of conflicts, health and safety, subsidiary governance and third party assurances. |  | Assurance |  |  |  |
| **Risk** |  |  |  |  |  |
| A robust risk management framework is critical to all organisations to ensure risks are effectively management and emerging risks identified our cyclical annual reviews will cover embedding risk, risk identification, risk mitigation and risk workshops. |  | Assurance | x |  |  |
| **Financial systems** |  |  |  |  |  |
| Robust financial systems are essential to financial well-being of any organisation. Our reviews of key financial systems are designed to ensure compliance with IIA standards and help protect against potential frauds. We will carry out a high level review of key financial systems each year supported by a rolling programme of financial system reviews such as payments, income, payroll, budgetary control/management reporting, and nominal ledger. |  | Assurance |  |  |  |
| **Estates and Fleet** |  |  |  |  |  |
| Estates and the Fleet will continue to receive audit coverage as key areas of expenditure for the Force. Following the move to the new Community Safety Hub and the many changes to the Estate no audits are planned in this area for 2019/20 |  | Assurance |  |  |  |
| **Services** |  |  |  |  |  |
| Each year a selection of services will be subject to audit to provide assurance across a range of important areas of activity. |  | Assurance |  |  |  |
| **ICT** |  |  |  |  |  |
| We will use our GUARD risk assessment to continue to review ICT risks and controls in place within the organisation. The rolling programme of reviews will include data protection, ICT governance, ICT management and business support, application reviews, network security, data quality and cyber security. |  | Assurance |  |  |  |
| **Follow Up** |  |  |  |  |  |
| We will undertake an annual follow up of all our recommendations. However, the Force themselves monitor all recommendations which are periodically reported to the Audit Committee. |  | Follow Up |  |  |  |

**Annex B: Rolling Strategic Plan**

| **Organisational Review Area** | **BAF / Risk Ref.** | **Type** | **2018/19** | **2019/20** | **2020/21** | **2021/22** |
| --- | --- | --- | --- | --- | --- | --- |
| **Governance** |  |  |  |  |  |  |
| Governance – Transformation and Change Management |  | Assurance |  |  |  |  |
| Governance – OPCC – SARC review |  | Assurance |  |  |  |  |
| Governance – Data Quality/Information Governance | 1539 | Assurance |  |  |  |  |
| Governance – Ethical Standards and Embedding Culture |  | Assurance |  |  |  |  |
| Governance – Performance Management |  | Assurance |  |  |  |  |
| Governance – Strategic Control and Corporate Governance |  | Assurance |  |  |  |  |
| **Risk Management** |  |  |  |  |  |  |
| Risk Management – Mitigating Controls |  | Assurance |  |  |  |  |
| Risk Management – Strategy/Policy |  | Assurance |  |  |  |  |
| Risk Management – Business Continuity |  | Assurance |  |  |  |  |
| **ICT** |  |  |  |  |  |  |
| ICT – Network Security |  | Assurance |  |  |  |  |
| ICT – Firewall |  | Assurance |  |  |  |  |
| ICT – Disaster Recovery |  | Assurance |  |  |  |  |
| ICT – Data Assurance | 1539 | Assurance |  |  |  |  |
| ICT – Cyber Security |  | Assurance |  |  |  |  |
| ICT – Business Continuity |  | Assurance |  |  |  |  |
| **Finance** |  |  |  |  |  |  |
| Key Financial Controls | 1435 | Assurance |  |  |  |  |
| Budgetary Control | 1435 | Assurance |  |  |  |  |
| Payroll | 1435 | Assurance |  |  |  |  |
| Overtime, Expenses and Additional Payments | 1435 | Compliance |  |  |  |  |
| Pensions Administration | 1435 | Assurance |  |  |  |  |
| Accounts Payable | 1435 | Compliance |  |  |  |  |
| Purchase Cards | 1435 | Assurance |  |  |  |  |
| **Estate Management** |  |  |  |  |  |  |
| Estate Management - Procurement |  | Assurance |  |  |  |  |
| Estate Management – Maintenance and Repairs |  | Assurance |  |  |  |  |
| Estate Management - Strategy |  | Appraisal |  |  |  |  |
| **Fleet Management** |  |  |  |  |  |  |
| Fleet Management - Procurement |  | Assurance |  |  |  |  |
| Fleet Management – Maintenance, Repairs, Disposal & Fuel Use |  | Assurance |  |  |  |  |
| **HR Management** |  |  |  |  |  |  |
| HR Management – Recruitment |  | Assurance |  |  |  |  |
| HR Management – Learning and Development |  | Assurance |  |  |  |  |
| HR Management – Absence Management & Occupational Health | 1439 | Assurance |  |  |  |  |
| **Services** |  |  |  |  |  |  |
| Seized Cash |  | Compliance |  |  |  |  |
| Lone Working |  | Assurance |  |  |  |  |
| Duty Management System |  | Assurance |  |  |  |  |
| Digital Data |  | Assurance |  |  |  |  |
| Commissioners Grants |  | Assurance |  |  |  |  |
| Proceeds of Crime |  | Assurance |  |  |  |  |
| Collaborations |  | Appraisal |  |  |  |  |
| Corporate Communications |  | Appraisal |  |  |  |  |
| FOI/Data Protection/Document Security |  | Assurance |  |  |  |  |
| Contingency- Audits that flow from the Force’s Corporate Risk Register |  | Assurance |  |  |  |  |
| **Management and Planning** |  |  |  |  |  |  |
| Follow up |  | F/Up |  |  |  |  |
| Strategic and Annual Plan 2019/20 |  |  |  |  |  |  |
| Annual Report 2019/20 |  |  |  |  |  |  |
| Audit Management |  |  |  |  |  |  |

**Annex C: Annual Plan – 2019/20**

| **Quarter** | **Audit** | **Type** | **Rationale and Scope** |
| --- | --- | --- | --- |
| 1 | Governance – Data Quality/Information Governance | Assurance | Rationale  Data management is an essential part of maintaining an efficient and effective Policing service.  Scope  The review will assess the adequacy and effectiveness of the internal controls in place at the Force for managing the Information Governance/Data Quality arrangements. The audit will focus on the following areas:   * An Information Governance framework is in place to ensure compliance with relevant legislation and operational requirements; * Roles and responsibilities have been clearly defined (e.g. SIRO, Information Governance Officers) and an information governance group (or similar) monitors ongoing information governance issues; * Policies and procedures are in place to govern the management of data and systems including a formally adopted information security and data quality policy; * Appropriate training is in place for those with information management responsibilities; * Data is captured in accordance with data quality policy requirements (e.g. timely, complete, accurate, relevant), with monitoring carried out to test compliance; * Up to date information asset registers and document retention schedules are in place; * Process controls exist to ensure that manual records are stored securely in structured filing systems and are available, if required; and * Data sharing and third party data processing protocols are in place which ensures that responsibilities for data transferred to and from third parties are clearly defined. |
| 1 | Commissioners Grants | Assurance | Rationale  Potentially a higher risk area for the Commissioner which will benefit from a regular internal audit  Scope  The review will consider the arrangements for the assessing, awarding and compliance monitoring process for the grants awarded by the Commissioner. |
| 2 | Governance – Ethical Standards and Embedding Culture | Assurance | Rationale  Ethical standards and appropriate culture are key essentials in maintaining an efficient and effective Policing service.  Scope  The audit will review the adequacy and effectiveness of the internal controls in place at the Force for identifying and maintaining ethical standards. In addition, the audit will review the culture within the Force and to make recommendations accordingly. The audit will focus on the following areas;   * Policies and procedures; * Roles and responsibilities; * Training and awareness; and * Systems and processes * Values and behaviour |
| 2 | ICT – Disaster Recovery | Assurance | Rationale  An important area for the Force that receives periodic audit coverage.  Scope  The scope of this audit will be to review the key controls in the following areas:   * ICT Continuity Framework (Including integration with the Forces Business Continuity Management Processes) * ICT Continuity Plans * Critical ICT resources * Maintenance of the ICT Continuity Plan * Testing of the ICT Continuity Plan * ICT Continuity Plan training * Distribution of the ICT Continuity Plan * ICT services recovery and resumption * Backup storage |
| 2 | ICT – Data Assurance | Assurance | Rationale  The management and maintenance of data is fundamental to the successful provision of a Police service.  Scope  The review will assess the adequacy and effectiveness of the internal controls in place at the Force for ensuring that data is managed in accordance with key principle retention and disposal of police information under the Code of Practice on the Management of Police Information. |
| 2 | HR – Learning and Development | Assurance | Rationale  An important area for the Force that receives periodic audit coverage  Scope  The audit will review whether an accurate record of Police Officer learning and development is maintained.  The audit will focus on the following key areas;   * Roles and responsibilities for maintaining accurate training records; * Appropriateness of the system for recording of police officer skills; * Accuracy of police officer training records maintained; * Appropriateness of the system to generate reminders for training that needs to be undertaken before training expires; * Management monitoring information. |
| 2 | Digital Data | Assurance | Rationale  An important area for the Force that receives periodic audit coverage  Scope  The audit will focus on the following key areas   * The aims and objectives of the Force for the management of digital data; * Identifying responsibilities for the maintenance of digital data; * Identifying the filing structure that will allow information to be efficiently retrieved by those with a right to do so for as long as the digital data needs to be kept; * The policy and guidelines about securing digital data: * Identifying retention periods, archival and disposal procedures for the various types of digital data held; * Determine how requests for information will be dealt with, ensuring that disclosure is properly controlled (under the Freedom of Information Act and/or the General Data Protection Regulations); |
| 2 | Collaborations | Assurance | Rationale  An important area for the Force that receives periodic audit coverage  Scope  The review considers the structure and agreements that are in place to include:   * the business planning of the collaborative working arrangements * the roles and responsibilities * the decision making processes and * the performance measurement and monitoring of the partners. |
| 3 | Governance – Performance Management | Assurance | Rationale:  Performance Management is an essential part of maintaining an efficient and effective Policing service.  Scope  The review will consider the arrangements in place for performance management and cover the following areas:   * An appropriate performance management system is in place. * Adequate staffing resources are assigned for performance management and training has been provided to staff on the system. * Reports are produced in accordance with nationally set targets (i.e. emergency response times and call handing). * Police and crime commissioners are provided with appropriate performance reports (which are in line with their police and crime commissioner plans). * There is an appropriate system in place which is capable of recording crimes in line with the National Crime Reporting Standard. * Adequate arrangements are in place for data integrity. |
| 3 | Key Financial Controls | Assurance | Rationale  This is a key audit risk area. The full audits for the financial systems will be undertaken on a systematic basis, however, to provide assurance that the key financial systems are adequately controlled an annual audit will be undertaken selecting a number of key financial systems.  Scope  To assess the adequacy and effectiveness of the internal controls in place at the Constabulary for managing the following key financial systems.   * Accounts Receivable * General Ledger * Treasury Management |
| 3 | Payroll | Assurance | Rationale  Payroll is a significant cost to the organisation and is seen as a key audit risk.  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. |
| 3 | Accounts Payable | Assurance | Rationale  This has a high number of transactions and expenditure involved and although it is subject to an annual key controls audit a detailed review from time to time is appropriate  Scope  The review will assess the adequacy and effectiveness of the internal controls in place at the Force for managing the Accounts Payable (Creditors) function. The audit will focus on the following key areas:   * Adequate policies and procedures are in place and accessible to all relevant staff; * System access is restricted to authorised personnel only; * New supplier set up/amendments to supplier details are subject to satisfactory segregation of duties; * Payments are supported by proper documentation, properly authorised, correctly coded, and subject to satisfactory segregation of duties; and * Regular reconciliations are carried out between the purchase ledger and the general ledger control account. |
| 3 | Proceeds of Crime | Assurance | Rationale  An important area for the Force that receives periodic audit coverage  Scope  The review will appraise the effectiveness of controls for managing the proceeds of crime and in particular the arrangements for securing and monitoring of the proceeds of crime which is held by the Force.  The audit will focus on the following key areas:   * Governance arrangements are in place to provide management with required levels of assurance; * Training and guidance is provided to staff; * Controls exist to ensure confiscated assets are appropriately held and managed.   The audit scope does not include visits to stations as these maybe undertaken as part of a separate audit. |
| 4 | Seized Cash | Compliance | Rationale  This is a focus area of the Audit Committee with concerns having been raised in previous years.  Scope  The review will consider the arrangements for the receiving, handling and disposal of seized cash to ensure that processes adopted by the organisation are being complied with. |
|  | CONTINGENCY –  Audits that flow from the Force’s Corporate Risk Register |  | Rationale  Scope |
| 1-4 | Follow-up | Follow up | Scope  The review ascertains whether management action has been taken to address the Priority 1 and 2 recommendations arising from selected internal audit work carried out at the organisation during the previous financial year. |
| 1 | Annual Plan | Management |  |
| 4 | Annual Report | Management |  |
| 1-4 | Management and Planning | Management |  |
|  |  | **Total days 110** |  |

**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 Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police framework of governance, risk management and control. TIAA is responsible for giving assurance to the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police “Governing Body” (being the body with overall responsibility for the organisation) on the adequacy and effectiveness of the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police risk management, control and governance processes.

**Scope**

All the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police 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 the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police 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 the board, 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.

**Access**

TIAA has unrestricted access to all documents, records, assets, personnel and premises of the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police and is authorised to obtain such information and explanations as they consider necessary to form their opinion. The collection of data for this purpose will be carried out in a manner prescribed by TIAA’s professional standards, Information Security and Information Governance policies.

**Annex D: Audit Remit**

**Standards and Approach**

TIAA's work will be performed with due professional care, in accordance with the requirements of the Public Sector Internal Audit Standards (PSIAS).

**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 the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland 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 the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police 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.

**Irregularities, Including Fraud and Corruption**

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

TIAA will be informed when evidence of potential irregularity, including fraud, corruption or any impropriety, is discovered so that TIAA 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.

**Corporate Assurance Risks**

We consider four corporate assurance risks; directed; compliance; operational and reputational, and tailor the type of audit accordingly. For all types of audit we also taken into account value for money considerations and any linkages to the organisational assurance framework. 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.



**Benchmarking**

Where a similar review is carried out at a number of our clients we will subsequent to the completion of the review at each of the clients, where relevant, provide a benchmarking and lessons learned digest. This digest will include operational effectiveness matters for the Police and Crime Commissioner for Cleveland and the Chief Constable Cleveland Police to consider.

**Annex E: Assurance Mapping**

**Types of Audit Review**

The annual plan includes a range of types of audit review. The different types of review focus on 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.

