Compliance audit

Briefing note about audit and compliance for data protection purposes.

10 mins read

First published 4 August 2022

The General Data Protection Regulations 2016/679 (GDPR) and the Data Protection Act 2018 (DPA) emphasise the principle of **accountability** when processing any information that falls within the definition of personal data. Personal data is any information relating to an identified or identifiable natural person who can be identified directly or indirectly in particular by reference to an identifier.

Forces ensure they are accountable and comply with data protection legislation through a number of activities, at different **lines of defence**. These activities include auditing, monitoring and self-inspection. This briefing note defines and outlines these activities and who is responsible for them.

Audit

??????Purpose of information management compliance auditing

Information management compliance auditing helps ensure that the privacy and subject rights of individuals are adhered to by the **force controller**. The audit process is designed to check compliance with legal, regulatory, contractual and procedural obligations.

These include, but are not limited to:

- **Data Protection Act 2018** and **UK GDPR**
- **Computer Misuse Act 1990**
- **Human Rights Act 1998**
- **Freedom of Information Act 2000**
- **Regulation of Investigatory Powers Act 2000**
- Home Office (2005) Code of Practice for the Management of Police Information (to be updated)
- **Police Code of Ethics**
- national and local standards, policies and good practice

- codes of connection (CoCos) – for example, the Police National Computer (PNC) and Police National Database (PND)
- memoranda of understanding (MoUs) with government departments
- ISO 27001 or ISO 27701

ISO 27001 is the international standard for information security. ISO/IEC 27701:2019 is a privacy extension to the international information security management standard

Compliance auditors ensure the requirements for audits are met, in order to demonstrate compliance with the requirements above.

Definition of compliance auditing

The **Chartered Institute of Internal Auditors (CIIA)** defines compliance auditing as:

> *the requirement to examine and evaluate defined activities of an organisation to measure adherence to legal, regulatory, contractual and procedural obligations*
>
> **Chartered Institute of Internal Audit (CIIA)**

Independence

The degree of an auditor's independence is defined by whether the audit is internal or external. An external audit has greater independence than an internal audit, where the auditor is employed by the organisation.

Nonetheless, anyone employed in forces to perform an audit function should pay regard to the **CIIA Code of Ethics,** whether a member of the CIIA or not.

Three lines of defence

Forces should use the CIIA **three lines of defence for risk management and control in organisations**, in respect of the auditor role.

First line of defence

This comprises of functions that own and manage risk.

The outputs from the first line of defence are reported to senior management. These are:

- day-to-day management of risk
- application of internal controls

Second line of defence

This comprises of functions that oversee or specialise in compliance or the management of risk.

The outputs from the second line of defence are reported to senior management. These are:

- financial controls
- security controls
- risk management
- quality
- inspection
- compliance

Third line of defence

This comprises of functions that provide independent assurance.

The outputs from the third line of defence are reported to the governing body or audit board, with copies to senior management. This is internal audit.

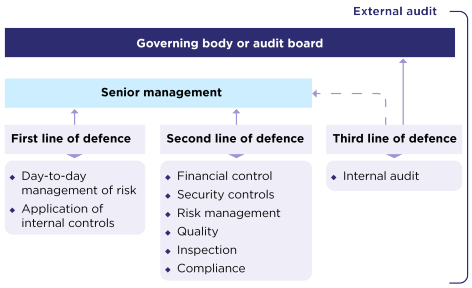

Figure 1: Three lines of defence

Many compliance officers employed by forces undertake the second line of defence because they are employed within the business unit that owns the information (for example, within a crime desk) and they report to the business management team. These are considered **self-inspections** as

opposed to audits, because the officer is not independent.

However, if the officer is located within the information management team or largely reports to the audit board, they are acting as an internal compliance auditor and can be designated as such. The audit board is responsible for oversight of the audit process. The board can be configured in any way designated by the chief officer and therefore will differ from force to force. The audit board is chaired or led by the individual responsible for audit. In most cases, this will be the senior information risk owner (SIRO).

The expertise of the compliance auditor should be used by project teams during the development and at the initiation of new systems and applications that process personal data. This will ensure that audit requirements are addressed at an early stage. The compliance auditor can make recommendations to the project team to ensure that privacy mandated by data protection legislation is built into the design. Their knowledge and views of privacy risk can also assist the **information asset owner** or business owner when completing the **data protection impact assessment** (DPIA) for such projects.

Force roles and responsibilities relevant to the compliance auditor

The following force roles are relevant to the compliance auditor.

- **Controller** – under the UK GDPR, the chief constable is the data controller for their respective force. The controller is responsible for all of the personal data being processed within the force, and should therefore ensure that policies, procedures and monitoring are in place to protect personal data from unlawful and unfair processing. The compliance auditor undertakes the audit testing to confirm that the mechanisms in place are providing the required protection.
- **Senior information risk owner (SIRO)** – the SIRO within a force is responsible for information risk and, as a consequence, is usually responsible for approving the strategic audit programme and plan, along with ownership of the compliance audit process. Where the SIRO delegates the compliance audit responsibility, they should ensure that processes are in place to make them aware of any issues arising from the audit that pose a risk to the force.
- **Information asset owner (IAO)** – the IAO has the senior role for ensuring an information asset(s) under their control is appropriately managed. The IAO, sometimes referred to as the business owner, has responsibility for a specific asset that supports a specific business function. Their

responsibilities in relation to the compliance audit are outlined in **Information compliance assurance**.

- **Data protection officer (DPO)** – the DPO's primary role is to support their force's compliance with GDPR and to ensure that the data subjects' rights are upheld. UK GDPR requires that the DPO must be adequately resourced, including the compliance audit function. Compliance auditors can provide assurance and advice to the DPO. They can assist in the development of new systems and provide advice on privacy by design, in respect of enabling the ability to audit. They can also provide support by delivering training on privacy and data quality.

More detail on force roles and responsibilities that are relevant to the compliance auditor are contained in the **authorised professional practice (APP) on Information management**.

Force obligations in relation to compliance auditors

The chair of the force information governance board or equivalent should ensure that the compliance auditor:

- is providing support to the DPO in securing force compliance with UK GDPR and the DPA, including monitoring compliance with policies put in place by the controller and related audits
- has a good working knowledge of the force and its strategy
- develops a good understanding of police systems in general and operational requirements and procedures, as well as local and national requirements
- has a good understanding of the role of the Information Commissioner's Office (ICO) and the ICO audits
- has a good understanding of external influences – for example, the Home Office, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), and the Office of the Police and Crime Commissioner
- is in a position in the organisation where they can remain independent and not subject to any influence in relation to their auditing role, and where they can avoid any conflict of interest
- is not managed by senior staff on the sites they are auditing, which would make it impossible to ensure total independence
- is made aware of instances where other organisations use, store or retain force information, necessitating a site visit
- is given the required resource to assist in undertaking audits where specific expert knowledge is required

- receives training on, and is permitted access to, any systems or data to undertake and fulfil their compliance audit role
- receives training in respect of the legislation they will be auditing against
- receives training in how to interpret police records
- is able to gain a basic understanding of the procedures of the other organisations or agencies that provide, or are in receipt of, information from the force

Information compliance audit

The value of an information compliance audit is that it will enable a compliance auditor to do the following.

- Provide an independent view to the DPO and controller of the adequacy of supervision and monitoring practices put in place by the IAO or business owner to ensure compliance with privacy legislation, particularly data protection legislation, given the obligation of accountability placed on the controller under **Article 5(2) UK GDPR**.
- Provide an independent view of the adequacy of internal controls, such as policies and procedures, and whether or not they are being applied **(Principle 3 UK GDPR)**.
- Assess whether supervisors are effectively monitoring and dip-sampling staff's work to ensure that information is accurate, relevant and up to date, in compliance with **Principle 4 UK GDPR**.
- Identify specific information that is not held or processed in accordance with the data protection legislation **(Principle 1 and 2 UK GDPR)**.
- Ensure the SIRO and the IAO or business owner are aware of any risks that may result in potential breaches of legislation or loss of public confidence **(Principles 1 to 6 UK GDPR)**.
- Identify any operational risks in information assets so that these can be brought to the attention of the IAO, business owner or SIRO for appropriate action to be taken.
- Ensure that forces maintain high-quality, accurate, reliable and timely police information that assists operational practices and results in better use of public money and services **(Principle 4 UK GDPR)**.
- Assist with reducing the occurrence of inaccurate information being supplied under the subject access provision of data protection legislation **(Principle 4 UK GDPR)**.
- Assist with reducing the possibility of litigation arising from inaccurate information **(Principles 1 to 6 UK GDPR)**.
- Provide evidence of compliance auditing to the ICO and external auditors, such as HMICFRS.

- Provide evidence of compliance with all the CoCos and MoUs the controller has signed up to.
- Identify examples of good practice.
- Highlight issues to the DPO that can be addressed by further training or improved supervision (**Principle 1 to 6** and **Article 37 UK GDPR**).
- Provide the following to the ICO, HMICFRS or other regulatory body:
  - reports, including their findings and recommendations, on plans detailing how findings and recommendations will be addressed
  - evidence that the SIRO has acknowledged and signed off the action plan

Information compliance assurance

The information compliance audit should be designed to test to ensure the following.

- The IAO or business owner has collated, processed and used personal data within their asset, lawfully and fairly (Principle 1 UK GDPR). This includes working with the systems administrator to ensure that only people who have an identified business need to access the system in order to carry out their current role are permitted to do so (**Principle 6 UK GDPR**). A designated system administrator within the IT department is responsible for the system and facilitates the physical access to the system.
- The IAO or business owner has a comprehensive understanding of which legislation is applicable to their asset. Although the asset will be held by the police force, the data protection legislation controlling the processing may not fall under the DPA Part 3. For example, where processing relates to human resources or membership of the force gym, the processing of personal data will fall under the UK GDPR.
- Where the IAO or business owner has authorised any information sharing and disclosure of personal data involving their asset, they have ensured that it is in accordance with legislation, by documenting the means and purpose in an information sharing agreement (ISA). It should also test, where necessary, that the risk of sharing has been assessed by completing a data DPIA, as required under **Article 35 of the UK GDPR**.
- Appropriate physical and technical security has been applied to the asset to protect the personal data from loss or unauthorised access or unauthorised disclosure (**Principle 6 UK GDPR**).
- Any access to the IAO or business owner’s asset requested by non-police users is supported by a business case and, if access is approved, will test to ensure there is evidence of:
  - appropriate security vetting

- a data processing contract (if appropriate)
- a signed confidentiality agreement
- training in place (**Principles 1,2 and 6 UK GDPR**)

- The IAO or business owner has assigned the correct access levels to any system they have been assigned to and these access levels are maintained at all times by regular monitoring (**Principle 6 UK GDPR**).
- The IAO or business owner is able to identify unlawful access or use of information held (**Principle 1,2 and 6 UK GDPR**).
- Information is accurate, relevant and up to date as a result of regular monitoring put in place by the IAO or business owner (**Principle 4 UK GDPR**).
- Information is adequate and relevant in terms of the purpose for which it is being processed, as a result of regular monitoring put in place by the IAO or business owner. (**Principle 3 UK GDPR**).
- Processes are in place to rectify any errors and that the monitoring put in place by the IAO or business owner confirms adherence to such processes (**Principle 4 UK GDPR**).
- Appropriate physical and technical security is in place. The IAO or business owner is responsible for ensuring that access is withdrawn when it is no longer required (**Principle 6 UK GDPR**).
- Information is being shared lawfully and fairly and, where appropriate, transparently by the users of the asset (**Principles 1, 2 and 6 UK GDPR**).

Pre-compliance audit work

Risk assessment

The controller should carry out a risk assessment that sets out:

- the nature and severity of risks associated with each set of personal data
- actions to mitigate those risks
- contingency plans to deal with the risks should they arise (for example, loss of personal data)

The College has developed **principles for taking and reviewing risk**.

Risk assessment process

Each system holding personal data should be subject of a risk assessment by the IAO or business owner and should be prioritised to identify the level of risk posed to the force. For example, poor-

quality personal data held within a system related to protection of children may pose a considerable risk to their protection.

The risk assessment process should be based on the likelihood of an event occurring, scored against the impact that such an event would have on 13 impact factors (see **risk assessment score form**).

Completion of the risk assessment

The risk assessment should be completed by the compliance auditor in conjunction with the IAO or business owner.

It provides the compliance auditor with the opportunity to:

- discuss the role of compliance audit and the responsibilities surrounding the ownership of a system
- emphasise the need for recommendations identified during the compliance audit to be acted on
- emphasise the need for the IAO or business owner to appreciate the importance of their role to ensure that the controller is complying with the legal requirements of the DPA, Home Office (2005) Code of Practice for the Management of Information and any other relevant legislation and agreements
- discuss how the audit process can improve investigations and performance
- take into account the implications of any existing privacy impact assessments (PIAs) or DPIAs, information sharing agreements, data processing contracts crown contracts and other relevant documents

Risk assessment outcome

The results of the risk assessments should be used to identify high-risk systems and to assist in preparing an appropriate audit plan.

The force SIRO should set a benchmark, in consultation with the DPO, so that any system assessed over a certain score is audited and placed in the audit plan for attention during the ensuing period. The order in which the audits take place depends on:

- the risk assessment score or risk level identified

- the ability of the compliance auditor to access the particular data (for example. system access and appropriate training)
- the availability of third-party assistance to access data if required
- the resources available to carry out the compliance audit task

The SIRO or DPO may determine that information or systems with a very high-risk score should be audited as a matter of urgency.

Audit plan

Example of an audit plan (to access, log in to the Knowledge Hub).

On completion of the risk assessments, details and a timetable of the compliance audits to be carried out are included in an audit plan. Forces can determine the specific time period covered by the audit plan.

The audit plan should be submitted to the senior person with responsibility for compliance audit for their written approval, and should also be brought to the attention of the SIRO (if this is not the same officer). Amendments to the audit plan must be similarly approved and documented.

If a force has insufficient resources available to carry out all of the high-risk audits, this should be brought to the attention of the SIRO, to enable the issue to be added to the force risk register.

Practical audit phase

The audit plan shows which audits have to be undertaken and when they are due. There are four phases to each audit:

- planning
- testing
- reporting
- post-audit review

Planning the audit

This includes:

- communicating with the IAO or business owner
- agreeing a single point of contact, usually the information asset assistant
- obtaining results of the day-to-day monitoring undertaken by the IAO or business owner
- acquiring an understanding of the relevant policies, procedures and guidance documents
- liaising, where appropriate, with the head of the force's professional standards department to identify any issues
- setting the terms of reference
- obtaining access to relevant systems and any necessary training through the system administrator on the authorisation of the IAO or business owner
- determining the assurance rating (**very limited, limited, reasonable, high**)
- determining a sample size for the audit
- creating an audit documentation sheet to record the findings, including data to identify the record, assurance rating and comments

The information asset assistant is the role designated by the IAO or business owner to oversee the day-to-day management of the information asset. It is a role that is usually undertaken by a user of the asset, who also holds a supervisory role, enabling them to access data input by users.

Communication with the business owner or IAO

Details of the specific records to be audited should not be disclosed before the audit begins. However, the IAO or business owner should be made aware of the audit and should be requested to nominate a liaison officer. The IAO or business owner should be informed of the length of the audit and any specific assistance required from their staff. These discussions provide the compliance auditor with the opportunity to acquire an understanding of:

- the system and/or process
- the information held
- the way the information is used
- any relevant legislation, CoCo and/or MoU that governs its use

Compliance auditors should obtain:

- as much background information as possible relating to the area to be audited
- policies (usually written in force by the IAO or business owner, but may be national policies)

- procedures (usually written in-force), to give specific guidance on the practical use of the information
- rules (usually written in-force), to provide information on specific rules appertaining to the system or the data
- guidance (usually written in-force, but could have been issued nationally)
- system operating procedures (SYOPS), which contain detailed information about how the whole system should be operated on a day-to-day basis
- CoCos, which usually detail how a system is to be used, access controls, dissemination of information (usually produced by external business owners, external system owners or IAOs)
- MoUs, which are legally binding once signed by the controller – many government organisations use these rather than CoCos

Compliance auditors should consider developing a questionnaire for business owners or key stakeholders to complete, to assist with this phase.

Terms of reference

These should outline the following:

- scope – the extent of the audit
- aims and the objectives of the audit
- approach – how it will be undertaken
- milestones – start and finish dates, submission of interim report(s)
- methodology test required to meet the audit objective – having decided on the method of approach, a number of tests should be undertaken to assess whether any modifications are needed, and information on this test should be included in the terms of reference

Resource implications and security issues should be considered when choosing the audit method to be used. Site visits should be included where practical.

Process maps

A process map shows the flow of information from start to finish and enables the compliance auditor to fully understand the information management process associated with the system being audited. If no process map exists, it should be created. The maps – as well as any previous audit reports, monitoring reports and issues identified – provide the compliance auditor with a good

understanding of the systems and/or processes to be audited and assist in drawing up the terms of reference.

Testing phase

The following steps should be taken when conducting the audit test:

1. Select a random sample (see **sampling methodology**, table one – confidence level (C) 90%, table two – confidence level (C) 95%, chart one – confidence level (C) 90%, chart two – confidence level (C) 95%, random number table – 1,000 random numbers).
2. Collect the evidence.
3. Analyse the findings and identify the level of assurance.
4. Submit any urgent issues or errors to the business owner for immediate correction (**as per error guidance and classification document**).

Supporting and substantiating force records

Forces should check for original, supporting or substantiating information to verify the records being audited. The supporting or substantiating information may be in any form that is appropriate to the force. The underlying information is the definitive record of the facts, as it is usually the first record to be updated when any changes occur.

Where paperless systems are used, the associated risks may be mitigated to some extent by ensuring that suitable monitoring controls are incorporated into the record update and creation procedures. The critical factor is the quality of the computer record.

All records containing personal data that may result in the detention of a person must show a reference on a policing system – for example, the PNC, PND or local intelligence systems – to a supporting or substantiating force record. See the Home Office's PNC user manual. The supporting or substantiating record must be accessible at all times. The accessibility of these records is tested in the audit procedure by allowing 30 minutes to locate them (Ibid).

The supporting or substantiating force record for reports without the potential to result in an arrest must be available during normal office hours.

Reporting the audit findings

This includes:

- collating audit findings and ratings
- compiling a draft audit report
- arranging a meeting with the appropriate IAO or business owner to discuss the findings and audit recommendations
- approval for circulation from the SIRO or audit owner
- a response from the IAO or business owner that includes an action plan to address the audit recommendations within the agreed timescales
- the final report, which should be published and circulated according to force policy
- closure by the SIRO or force audit owner

The responsibility for compliance audit ultimately sits with the controller but is delegated to the SIRO, who is defined as the audit owner (the individual who has overall responsibility for compliance audit). However, delegation differs from force to force. Some forces have designated it to other senior individuals within the force, such as the Head of Finance or IT.

Post-audit review

The action plan drawn up in response to the audit recommendations should be followed up at a post-audit review or in a subsequent audit. This should include reviewing evidence from any previous action plan and/or conducting a follow-up review.

Retention of audit documentation

HMICFRS regards the following as the minimum amount of documentation that should be retained for potential examination by external audit:

- strategic audit plans, including the supporting risk analysis
- audit plans and audit control sheets for individual audits
- schedules showing summary detail of audit and monitoring work carried out
- detailed working papers supporting the audit conclusions
- copies of compliance audit reports
- executive board and management responses to compliance audit reports

- detailed evidence supporting audit findings revealing inaccurate or incorrect information, or indicating where action is necessary for future compliance

It is not necessary to retain detailed documentation relating to all audit and monitoring tests carried out on all tested items. Evidence of items that are checked and found to be correct may be documented in summary form (for example, a schedule or matrix of items tested with test results). Audit documentation must be retained in accordance with the local and/or national retention schedule.

Monitoring

Monitoring is the day-to-day examination of procedures and processes for access to, and use of, personal data. It should be initiated by the IAO or business owner with the objective of identifying misuse, errors or general non-compliance with legislation, policy, processes or procedures to ensure that corrective action can be taken immediately. It may also highlight training requirements.

As monitoring is a self-inspection and quality control process, it is undertaken by the relevant business area and is not recognised as an independent audit. It is the IAO or business owner's responsibility to ensure that personal data held complies with the requirements of data protection legislation. Day-to-day monitoring activity should be recorded and retained, then produced in the event of a breach, misuse or data quality issues being identified. This enables ongoing errors to be identified so that action can be taken.

Monitoring records are also referred to when undertaking a risk assessment of the system or process and will be referred to by the compliance auditor during the scoping exercise prior to conducting an audit.

Monitoring should be carried out to assess how correct access levels to the system have been assigned and maintained. A monitoring report should include:

- when the system was last checked and the method that was used
- details of results and any recommended action on whether:
  - there has been any unlawful access to or use of information held on the system
  - information is accurate, adequate, relevant and up to date

- there is a process in place to rectify any mistakes and whether this process is being adhered to
- appropriate physical and technical security is in place
- information is being shared lawfully within and between forces
- information sharing agreements have been put in place in relation to ongoing sharing with partners and these agreements are being complied with
- data processing contracts are in place, up to date and being adhered to

A monitoring policy should be publicised within the force. The monitoring policy should be enforced, and action should be taken where required.

Monitoring of record creation and update

Procedures within forces regarding the creation and update of records vary widely. Typical methods include:

- centralised input by a dedicated data bureau
- input by the control or operations room personnel
- input by relevant departmental staff

- officer entry – individual input by the officer in the case (OIC)

The level of risk increases as the process is decentralised and carried out by non-dedicated data input staff. This may result in errors, such as in data transcription, misspellings, fields incorrectly completed or mandatory fields not completed. The degree of monitoring required will, therefore, vary from dip-sampling to 100% checking before the record is added to the database.

The IAO or business owner is responsible for ensuring that force policy and compliance processes and procedures are being adhered to, and for providing assurances of this to the SIRO.

Regional audit groups

Due to the need for independence, the role of the compliance auditor within a force can feel very isolated. Having the opportunity to network with other compliance auditors to share and discuss good practice enables new skill sets to be developed. This is especially the case where forces only have one compliance auditor.

Regional compliance audit groups enable compliance auditors to:

- share good practice and lessons learned with compliance audit colleagues
- work together to develop new compliance audits
- establish regional standards for recording privacy risk
- share information about training courses
- discuss opportunities to carry out joint compliance audits within and between forces
- discuss opportunities to undertake peer compliance audits
- share information relating to privacy risks, identified during compliance audits
- undertake work around the development of the Police Service Compliance Audit Guidance
- provide feedback to the National Compliance Audit Working Group
- have a forum for discussing issues arising from the National Compliance Audit Working Group
- discuss approaches to undertaking compliance audits on national systems
- discuss implications on compliance auditing resulting from changes in legislation

Transaction validation monitoring

Due to the high volume of assurance work required in forces that falls into the definition of compliance audit, some work that does not require the same degree of independence can be delegated to the business area. Transaction validation monitoring (TVM) is a process used to monitor the lawful use of personal data provided to the police by other agencies that are accessed via PNC or PND.

The integrity of a system depends upon the ability to account for each transaction undertaken by a user. The TVM process tests this capability.

TVM should be carried out on a regular basis in order to:

- deter and detect unauthorised access to, and use of, the system and/or personal data
- ensure all relevant transaction fields are completed, to provide an adequate audit trail for retrospective investigations into transactions
- give the necessary assurance to any third-party provider of a system containing personal data that such information is being processed in compliance with the CoCo, SYOPS, MoU or other relevant document
- provide evidence of the controller’s accountability

- provide the opportunity to raise staff awareness of operating procedures and adherence to policy and procedure

The TVM process must be planned and controlled by the person carrying responsibility for the TVM process. As this is not an audit, it does not require independence and can be delegated to local supervisors. Where this takes place, control is maintained by requiring supervisors to record and report results of TVMs undertaken. Any missing or unsatisfactory responses from a system, process or procedure should be followed up and escalated by the local supervisor, as appropriate.

The TVM process should check the following:

- transaction fields – content should be examined for quality
- sufficiency of detail – there should be sufficient detail to be able to trace the enquiry back to the originator
- legitimacy – the legitimacy of the check should be confirmed by asking the user questions, or checking any references to source documentation

Chief officers should ensure their force is able to carry out the TVM requirements stipulated in any CoCo or SYOPS, as required by the provider of the system.

Any issues found as a result of the TVM process should be collated, categorised and recorded. This enables recurrent issues, trends and individuals responsible for errors to be identified, enabling corrective action to be taken.

The TVM process will be validated by the compliance auditor, who will be responsible for dip sampling the TVM results and submitting a report of findings to the SIRO. The monitoring report compiled by the local supervisor, together with the dip sample report submitted by the compliance auditor, will provide evidence of **accountability** and assurance of compliance with the SYOPS, CoCo, MoU or other relevant document.

Sample size of data and transaction checks

Forces should ensure that the number of transactions, when undertaking TVM, complies with the relevant SYOP. The SYOP usually specifies the number of checks required or states that the number of checks undertaken must be proportionate to the total number of transactions carried out.

Self-validation

Self-validation can be a useful exercise to increase assurance capability. It can be used by the compliance auditor or by the IAO or business owner. The following are two examples of its application.

Example 1: Checking for compliance on any system

Self-validation can be applied to monitor compliance and identify inconsistencies or misuse on a system by its users. To do this, the compliance auditor or the IAO or business owner selects a random sample of checks undertaken by users. Those users who undertook the checks originally are then sent a form giving the details of the check.

Users are then required to provide the reason for accessing the data. This rationale is checked by their supervisor, who confirms, after further enquiries, whether or not the check was for a lawful purpose. For example, further enquiries can be to review a pocketbook, Pronto or an incident log (this list is not exhaustive). The completed form is then sent back to the compliance auditor. Inconsistencies can then be escalated as per force policy.

Example 2: Checking for compliance in PNC entries

Self-validation can be used when auditing PNC entries to identify inconsistencies and misuse, and to escalate these as per force policy. To do this, details of all locate and trace entries are obtained from the Hendon Data Centre. The relevant OIC or business area is sent the details of the locate/trace entry, together with a questionnaire, to check the accuracy of the information and to confirm that the circulation is still required. The completed form is then sent back to the compliance auditor to identify any inconsistencies.

The compliance auditor will maintain control of the self-validation process. They will dip sample the appropriate number of responses to verify the information provided and submit the report of findings to the SIRO or individual responsible for audit. Again, this provides evidence of the controller's **accountability**.

Self-inspection

A self-inspection is an activity carried out by staff working in the particular area to be examined. For example, an officer working in an intelligence unit where the PNC's wanted and arrest files are managed could undertake a self-inspection of those files.

The objective of self-inspection is to identify any processes or procedures that are not being followed and to recommend a course of action to rectify the situation. A self-inspection is always carried out under either the indirect supervision of a compliance auditor or an independent observer within the organisation who has an understanding of data protection and the legal responsibilities of the controller.

A self-inspection may be required where insufficient independent audit resources are available to undertake audits identified as high-risk. Following the risk assessment process, forces may wish to consider self-inspection as a means of providing some assurance to the controller of the force's compliance with the requirements of the data protection principles, other legislation, SYOPS or MoU.

The information and/or process for self-inspection is selected in the same way as for a compliance audit. The IAO or business owner responsible for the area to be inspected is provided with a self-inspection package and is responsible for nominating an individual to carry out the self-inspection process.

Self-inspection package

The basic contents of the self-inspection package include:

- guidance on undertaking the self-inspection
- instructions on documentation relating to the system or process being inspected
- self-inspection questionnaires
- an interim report template
- previous audit reports and action plans

A PNC-based self-inspection requires the compliance auditor to obtain the relevant information from the Hendon Data Centre and provide advice on the number of records to be inspected, to ensure the viability of the sample size.

The compliance auditor provides guidance and support, and answers any queries raised during the self-inspection.

The person carrying out the self-inspection should submit the findings to the compliance auditor and the IAO or business owner before the final audit report is completed. The content of the final

audit report will be agreed between the person undertaking the self-inspection and the compliance auditor.

After implementing the recommendations of the self-inspection, the IAO or business owner may repeat the inspection to identify whether or not the actions taken have improved the processes and reduced the previous issues or errors identified. These new findings are recorded and a report is sent to the compliance auditor, who will include the findings in their report to the SIRO.

All self-inspections should be followed up by a dip-sample audit undertaken by a compliance auditor. This validates the self-inspection and provides assurance to the IAO or business owner and the controller that the action plan implemented as a result of the self-inspection has been applied. The dissemination of the dip-sample results or report will be agreed with the IAIO or business owner.

National systems

There are a number of national systems with designated national auditors. These include the Child Abuse Image Database (CAID), PNC, PND, and National ANPR Standards for Policing and Law Enforcement Database (NASPLE).

The controller is responsible for ensuring that an IAO or business owner is appointed in their force for each system. Their role will be to authorise access to users in their force and to ensure that policies and procedures detailing permitted use are in place.

The national auditor will send out requests to forces for TVM or compliance audits to be undertaken to provide assurance of legitimate use. The outcome of these audits should be recorded in an audit report back to the national auditor and a copy submitted to the SIRO.

In addition, forces are permitted access to the Driver Validation Service (DVS) owned by the Driver Vehicle Licencing Agency (DVLA), the passport system owned by the Border Agency and the insurance database owned by the Motor Insurers' Bureau. Forces with access to these systems are required to undertake compliance audits as dictated by the CoCo and/or the MoU. The results are then sent back to the respective organisations, so that assurance of legitimate use can be provided to their SIRO.

- **Go back to the APP on Information management**

Tags

Information management