Data Protection

Manual of Guidance (Part II – Audit)

Second Consultation Draft: 1st July 2007

Prepared by the ACPO Data Protection & Freedom of Information Portfolio Group (National Audit Group)

Supercedes : ACPO Data Protection Audit Manual Version 1. February 1998.
This Manual may be disclosed to the public in its entirety

NOT PROTECTIVELY MARKED

1 Manual of Guidance Part II explained

1.1 Preface

This Data Protection Manual of Guidance (DPMOG) Part II – Audit, has been produced by the National Audit group to assist all Police Forces' comply with Section 3.6 and 7.7. of the Manual of Guidance Part I - Standards, which requires Forces to nominate an individual to co-ordinate a programme of Data Protection compliance audits.

The Information Commissioner has produced his own Data Protection Audit Manual, which looks at compliance with the Act as a whole, rather than just concentrating on data quality issues. Forces are also encouraged to adopt the practices of the Information Commissioner's Manual whilst co-ordinating a programme of compliance audits.

The key features of the DPMOG Part II – Audit are:

> *It replaces the ACPO Data Protection Audit Manual version 1 – February 1998.*
>
> *It helps achieve compliance with the Statutory Code of Practice on the Management of Police Information 2005 (MOPI Statutory CoP) and the Guidance on Management of Police Information 2006 ('MOPI Guidance')[1];*
>
> *It provides ACPO approved baseline standards for all Forces to follow in order to achieve greater uniformity in auditing police information systems such as: the Police National Computer system, Local crime/intelligence recording systems, Command and control systems, Personnel Systems etc.*
>
> *It is aimed primarily at Data Protection Audit staff to undertake an annual audit programme. However there are benefits in providing this manual to individual force System Owners to assist them undertake their daily monitoring activities and/or self-inspections to assist achieve compliance with the Manual of Police Information Code of Practice (and Guidance).*

The DP MOG Part II – Audit, will be regularly updated and adapted to reflect decisions made by ACPO, views of the Information Commissioner (where appropriate) and the evolution of the legislation as it is interpreted, challenged or reviewed. All modifications to the DP MOG Part II – Audit, will be the responsibility of the ACPO Portfolio Holder for Data Protection Audit.

1.2 Structure

The DP MOG Part II of this Manual has been divided into 6 Chapters and a series of Appendices:

> *Chapter 1 explains the structure of the DP MOG Part II, maintenance and appreciations.*
>
> *Chapter 2 provides a content, which will enable electronic searching.*
>
> *Chapter 3 provides an introduction to Data Protection Auditing, explains the terminology, objectives and benefits.*
>
> *Chapter 4 contains detailed information regarding the audit processes to be followed.*
>
> *Chapter 5 provides detail of transaction validation audits.*
>
> *Chapter 6 provides an insight into external audits undertaken by Her Majesty's Inspectorate of Constabularies (HMIC).*
>
> *The Appendices include established toolkits that have been prepared and approved by the National Data Protection Audit Group and must be used as baseline audit standards.*
>
> *It is anticipated that future versions of DP MOG Part II – Audit, will develop and produce new toolkits through liaison with Regional Audit Groups.*

1.3 Version Control

This is the Second consultation draft. It supersedes the first consultation draft in October 2005 and incorporates the changes made as a result of the consultation.

1.4 Further Enquiries

Any enquiries, comments, suggestions or criticisms regarding the DPMOG Part II – Audit, must be directed to the Secretary of the ACPO Data Protection Portfolio Group, namely Jason Russell – jason.russell@hampshire.pnn.police.uk
or the National Data Protection Audit Group Member with responsibility for producing the DP MOG Part II - Audit, namely Anne Chafer (Chair) – data.protection@leicestershire.pnn.police.uk and / or Angela Middleton (Secretary) – angela.middleton@leicestershire.pnn.police.uk.

1.5 Personal Acknowledgement

The production of this Manual was a collaborative effort, with valuable contributions from a number of staff from across the Police Service and Her Majesty's Inspectorate of Constabularies. Particular thanks go to those members of the National Data Protection Audit Group and Regional Data Protection Groups.

2 Contents

1 Manual of Guidance Part II explained 2

1.1 Preface 2
1.2 Structure 2
1.3 Version Control
1.4 Further Enquiries 2
1.5 Personal Acknowledgement 2

2 Contents 3

3 Introduction to Data Protection Auditing 4

3.1 Legislation 4
3.2 Introduction 4
3.3 Why should forces audit? 4
3.4 What is an internal audit? 4
3.5 Audit Terminology 4
3.6 The Auditor 4
3.6.1 Audit Staff 4
3.6.2 System Development/Documentation 4

4 Audit Practice and Methodology 6

4.1 Audit Programme (Plan) 6
4.2 Audit Phases 7
4.2.1 Planning and Preparation 7
4.2.2 Execution 7
4.2.3 Reporting 8
4.2.4 Follow Up (Review) 8

5 Transaction Validation Audits

5.1.1 Introduction 9
5.1.2 Method 9
5.1.3 Sample size – Access to data/transaction checks 9
5.1.4 Monitoring of record update /creation 9
5.1.5 Retention of audit documentation 9
5.1.6 Supporting/substantiating force record 9

Appendices

Appendix A Sampling Methodology
Appendix B Table One - Confidence Level (C) 90%
Appendix C Table Two – Confidence Level (C) 95%
Appendix D Chart One – Confidence Level (C)) 90%
Appendix E Chart Two – Confidence Level (C)) 95%
Appendix F Random Number Table
Appendix G Error Classification
Appendix H* Audit Record Sheets
Appendix I Audit Risk Analysis
Appendix J Annual Audit Programme (Plan)
Appendix K Audit Report
Appendix L Information Available from HDC

***Appendix H Annex**

Annex H1 Audit Working Papers
Annex H2 Urgent Matters / Brough Forward
Annex H3 Data Protection Officer Review Sheet
Annex H4 Audit Control Sheet
Annex H5 Audit Test Matrix
Annex H6 Supporting Documentation

Audit Toolkits

PNC Transaction Audit Process
PNC Correction Reports
PNC Destroyed Reports
PNC Disposal History
PNC Disqualified Drivers
PNC Found Reports
PNC Impending Prosecutions
PNC Information Reports
PNC Lost/Stolen Reports
PNC Removed Reports
PNC Restricted Reports
PNC Seen Reports
PNC Stolen Property
PNC Warning Signals and Information Markers
PNC Warrants

3 Introduction to Data Protection Auditing

3.1 Legislation

Section 4(4) of the Data Protection Act 1998 requires that the 'Data Controller' must comply with the Data Protection Principles, subject to exemptions, in relation to all Personal Data with respect to which he is the Data Controller.

3.2 Introduction

In order to help ensure compliance with the provisions of the Data Protection Act 1998 forces are required to institute a programme of Data Protection compliance audits. They must also conduct regular transaction validation audits, designed to discourage or identify misuse of Personal Data.

The Information Commissioner has produced a Data Protection Audit Manual, which looks at compliance with the Act as a whole, rather than just concentrating on data quality issues. Forces should adopt the practices of the Information Commissioner's Audit Manual, however such practices will not be included within the DP MOG Part II – Audit as a compulsory measure.

Success in implementing the DP MOG Part II – Audit, will be dependant upon resources available within individual police forces. Therefore, it is imperative that forces appoint sufficient, trained resources to adopt the baseline requirements of the DP MOG Part II – Audit.

Many forces will, prior to the introduction of the DP MOG Part II – Audit, already have auditing procedures in place. Forces should however be aware that the DP MOG will be used by Her Majesty's Inspectorate of Constabularies (HMIC) as an authoritative reference document containing criteria against which they will be audited; forces should therefore revise and update their current procedures in the light of the guidance contained within the DP MOG.

3.3 Why should forces audit?

It is important that forces must comply with the DP MOG Part II – Audit, as it will assist forces to:

Comply with the Data Protection Act 1998, and associated legislation including the Human Rights Act 1998 and the Freedom of Information Act 2000.

Comply with national/local standards and best practice.

Provide a more effective, efficient and economic use of police information to aid and improve all aspects of operational policing, resulting in better use of public money and services.

Improve and maintain high quality, accurate, reliable and timely police information to assist operational practices. Thus improving customer satisfaction, by reducing the likelihood of errors, which may lead to litigation/action being taken by individuals and/or the Information Commissioner against forces.

Identify data protection risks in information assets and identify 'danger areas' that need priority attention.

Provide information for other audits, inspections and reviews such as best value and information security.

Act as a conduit for best practice where appropriate.

Assesses whether effective staffing and reporting structures are in place.

Increase the level of data protection awareness among management and staff.

Identify examples of 'good practice' for dissemination throughout the Force.

Ensure documented reports are provided to and viewed by senior management to assess levels of compliance and that any other issues that may arise are brought to notice.

Contributes to forces planning processes and financial management.

Secure a continual service improvement

3.4 What is an Internal Audit?

Internal Audits look at how organisations manage their risks by providing appropriate senior members with information about identified risks and how well they are or are not being managed.

Internal Audits give an independent view of whether internal controls such as policies and procedures are adequately managing risk.

The official Institute of Internal Auditors (IIA) defines internal auditing as follows:

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".

(Refer to www.iia.org.uk/about/internalaudit)

3.5 Audit Terminology

For the purpose of this document:

Audit: means the examination of specific procedures and data (in accordance with the guidelines in this manual), with the objective of measuring the effectiveness of the supervision and monitoring procedures by recording the occurrence of inappropriate access and errors.

Monitoring: Monitoring includes the day-to-day examination (a system owner's self inspection/quality control checks) of access procedures and data at the discretion of the system owner with the objective of identifying misuse, or errors so that corrective action may be taken. Monitoring is not an activity undertaken by the Auditors but an action for the system owner. Data Protection Compliance Auditing, Data Quality Auditing and Monitoring

3.6 The Auditor

3.6.1 Audit Staff

Auditors should not be managed by senior staff on the sites they are auditing (i.e. they should be independent and avoid any conflict of interest) and must be able to audit in accordance with defined policy and to identify stated error conditions.

3.6.2 System Development/Documentation

It is assumed that Auditors will have an understanding of the information system development process. This document is designed to assist auditors to undertake minimum standards data quality auditing in respect of established information systems.

When auditing Police Information systems auditors will need to have a good knowledge of the system/process being audited and documentation, including:

National/mandatory documents:

ACPO DPMOG Part I – Standards

Code of Practice on the Management of Police Information (and supporting Guidance)

The PNC Code of Practice

Community Security Policy

PNC Code of Connection

ACPO information sharing protocols/processing agreements/Memorandum of Understandings (MOUs) /Service Level Agreements (SLAs)

Local documents:

System Manuals/User guides/Training

Information sharing protocols/ processing agreements/MOUs/SLAs

4 Audit Practice and methodology

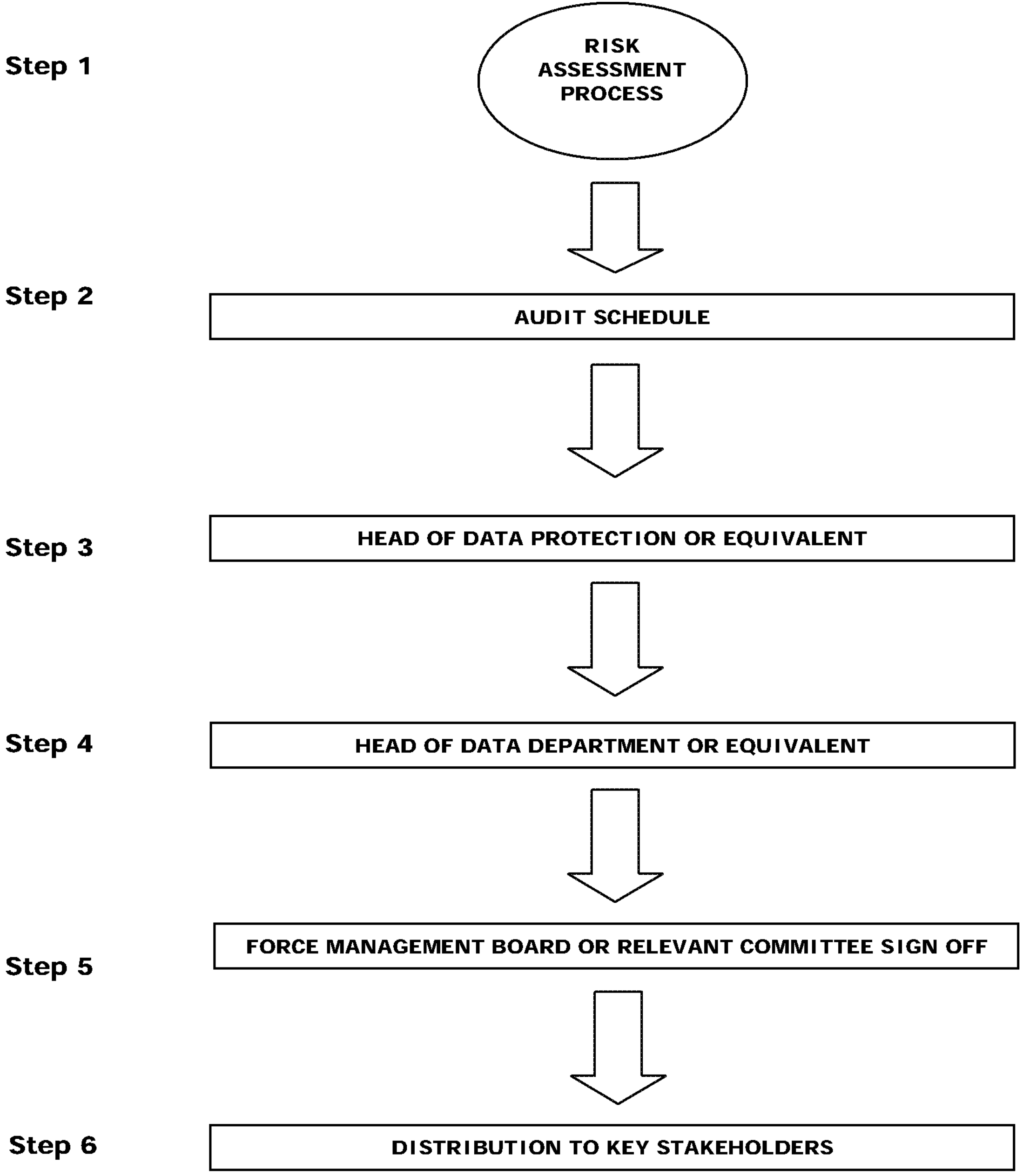
4.1 Audit Programme (Plan)

Forces must ensure a Data Protection Audit Programme is produced to detail the specific information to be audited, the frequency of such audits and the resources available to perform such audits.

This will be determined by a risk assessment (Appendix I) to identify the systems which present the greatest risk to the Force. However, it is acknowledged that due to certain constraints, the Audit programme may be subject to change by a Senior Officer should other matters take priority.

The Data Protection Audit Programme (Appendix J) should be written annually and signed off by the Data Protection Officer or higher rank where possible. The Data Protection Audit Programme and risk assessment documentation will be subject to inspection by external audit (HMIC).

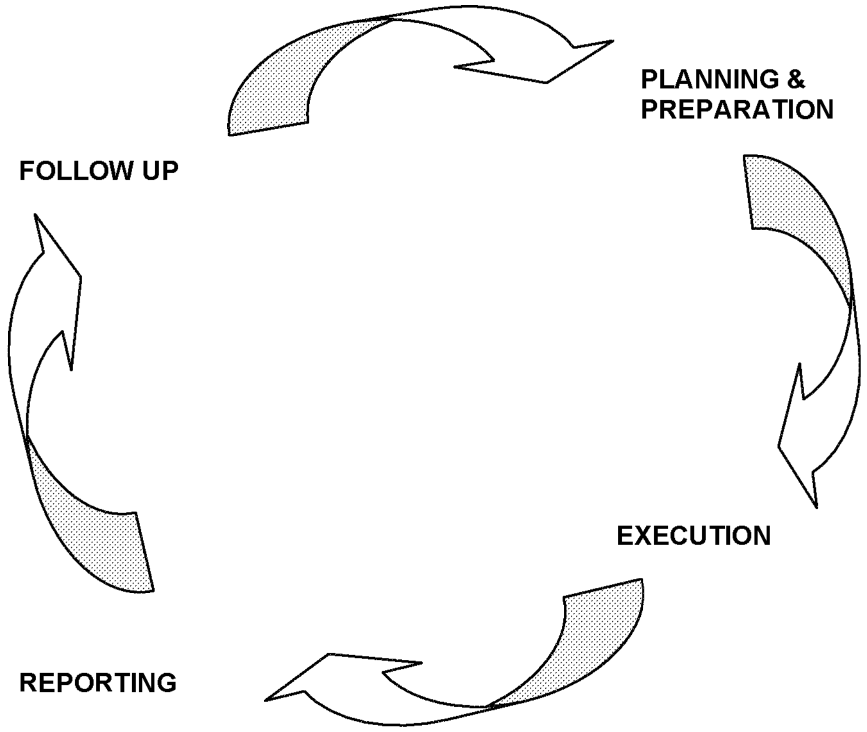
Example:


Step 1
RISK ASSESSMENT PROCESS
Step 2
AUDIT SCHEDULE
Step 3
HEAD OF DATA PROTECTION OR EQUIVALENT
Step 4
HEAD OF DATA DEPARTMENT OR EQUIVALENT
Step 5
FORCE MANAGEMENT BOARD OR RELEVANT COMMITTEE SIGN OFF
Step 6
DISTRIBUTION TO KEY STAKEHOLDERS

4.2 Audit Phases

Specific information audits should be subject to 4 distinct phases of an audit process, namely Planning, Execution, Reporting and Follow up.

Suggested Example



4.2.1 Planning and Preparation

This is often referred to as the time table of activities i.e. what needs to be done, when and by whom including:

Research - Acquire an understanding of policles, rules and guidance. As much information should be found out about the information being audited, as possible. This could be done by means of a questionnaire, interviewing key persons and reading policies, procedures, system manuals, guidance documents etc

Process maps – As much detail regarding the information flow and areas of risk from start to finish should be attained to assist the auditors understanding of the information management processes.

Terms of reference - This should be drafted to outline the scope, aims, approach and milestones of the audit and should be approved by the information system (asset) owner prior to the execution of the audit.

Conduct/Methods – This should be defined including the sample size (refer to Appendix A-F)

Prepare Audit Control Sheet (refer to Annex H4)

The audit programme should be signed-off by the auditor on completion

Test the Methodology – This must be tested to assess whether there are any modifications needed to the pre-defined toolkits. The methods may include site visits, fax/email, computer terminals and internal mail. When choosing the method to be used, resource implications and security issues should be taken into account. Site visits should, however, be seen as the ideal. Details of the specific records that are to be audited should not be given prior to the commencement of the audit. However it is normal practice to make the relevant personnel in the force aware that an audit will be taking place, and which of the above methods is to be adopted.

Resources/target date – The resources available to perform the audit and the target dates for each stage of the process should be identified.

4.2.2 Execution

Test the conditions – The specific toolkits detail specific tests which auditors must carry out in order to confirm the audit objectives.

Collect the Evidence – The auditor must obtain sufficient and appropriate audit evidence to provide them with a sound basis for their conclusions and recommendations. The documented evidence should be sufficient to support the audit conclusions and recommendations, and should be completed to a standard suitable for external audit. A suggested format is shown at Appendix J

Apply the toolkit - The specific toolkits detail specific tests which auditors must carry out in order to confirm the audit objectives. Refer to the Toolkits section of this Guidance.

Analyse the errors - Refer to relevant toolkit and Appendix G for error classification.

Correct the Errors - Procedures must be in place to correct errors that have been discovered during the audit. Major errors should be corrected immediately. Any corrective action taken should be documented.

A suggested format for the error-recording form is shown at Annex H5.

Close all meetings – Ensure that any outstanding meetings that have been arranged throughout the audit are now finalised and closed.

4.2.3 Reporting

Compile Audit Report

Results of the audit should be brought to the attention of both the Executive board and the responsible officers within the Section/Dept being audited, by means of a formal audit report (Appendix K). This report should contain the following:

Audit findings, to include:

- *conclusions;*
- *impact/risk of conclusions;*
- *recommendations/corrective action deemed necessary.*

Audit Methods, to include:

- *agreed action plans*
- *details of sample used;*
- *error rates;*
- *breakdown of errors; and*
- *year-on-year comparisons.*

A suggested report format is included at Appendix J.

An Executive response to this report, detailing proposed corrective action, should be required; the response and resultant action taken by the unit concerned should be noted. Recommendations made should be followed-up at subsequent audits, or in a post-audit review.

Publish Report

The audit report should be published ideally to a relevant committee i.e. Information Management Board which involves a senior or ACPO ranking Officer. When publishing the report ensure that relevant departments such as Training are included as the publishing of the report is an effective means of passing on and highlighting good and poor practice.

4.2.4 Follow Up (Review)

Identify evidence of implemented recommendations

Undertake any further action plan (Ideally, through a senior/ACPO ranking Officer)

All four phases of the audit should be included within the audit working papers (see examples at Appendix H)

5 Transaction Validation Audits

5.1.1 Introduction

The security of a database system depends, to a large extent, upon being able to retrospectively account for each transaction. The monitoring process and audit procedures test this capability.

The difference between auditing and monitoring has already been mentioned. The importance of effective monitoring as a means of reviewing procedures and enforcing policy cannot be overstated. A monitoring policy should be publicised within the Force.
It is important that the monitoring policy is seen to be enforced and appropriate action taken where necessary.

Transaction audits should be carried out on a regular basis and perform three important functions:

to deter and detect unauthorised access to systems;

to raise staff awareness of data protection issues, and maintain public confidence; and

to ensure all relevant transaction fields are completed to provide an adequate audit trail for retrospective investigations into transactions that have been carried out.

5.1.2 Method

While elements of transaction monitoring may be delegated to local supervisors, it is essential that the monitoring process is planned and controlled by Internal Audit/DPO. Where delegation does take place, control may be achieved by requiring supervisors to report results of monitoring checks back to the DPO, or by regular DPO inspection of monitoring logs. Where the DPO carries out the transaction-checking process directly, missing or unsatisfactory responses should be followed up.

When checking transactions the following areas should be examined:

transaction field inputs should be examined for quality;

there should be sufficient detail to be able to trace the inquiry back to the originator; and

the legitimacy of the check should be confirmed by questioning the originator or by checking any references to source documentation.

The validation of a transaction check must be authorised by a member of staff at a supervisory level.

Any errors found as a result of the transaction checks should be categorised and noted. The collation of results will enable recurrent errors, error trends and individuals involved in the errors to be identified, and permit corrective action to be taken. This process may be enhanced by circulation of the results e.g. within annual audit reports.

The audit guidelines stated earlier relate essentially to audit procedures; however the general methods e.g. planning, sampling and working papers is also generally applicable to monitoring procedures, where monitoring may be viewed as a 'rolling audit'.

5.1.3 Sample size – Access to data/transaction checks

Forces should ensure that the number of transactions that are checked is proportionate to the total number of transactions carried out. It is recommended that the minimum number of transactions checked on a daily basis should be commensurate with the total number of transactions carried out, subject to a minimum of three transactions per day. Clearly a Force, which carries out a large number of transactions, would be required to check more than the minimum of three transaction checks per day.

5.1.4 Monitoring of record update/creation

Procedures within forces regarding the update and creation of records vary widely; typical methods include:

centralised input by a dedicated data bureau;

input by control room personnel;

officer-entry; individual input by the case officer.

The level of risk increases as the process is decentralised and is carried out by non-specialist data input staff, resulting in errors such as data transcription, spelling, fields incorrectly completed, or mandatory fields not completed at all. The degree of monitoring required will therefore vary, from dip sampling to 100% checking before the record is added to the database. While the DPO will not necessarily be involved directly in this process, it is essential that the DPO should have input into the planning and controlling of the process, and be provided with details of the results of the checks for inclusion in annual audit reports.

As with access/transaction monitoring, the audit methods recommended previously should be applied to the monitoring of record update/creation.

5.1.5 Retention of audit documentation

For those applications subject to external audit, it will be necessary to retain audit working papers prepared since the previous external audit. It is appreciated that it may be impractical to retain all audit working papers relating to these applications for the period between external audits due to the large volume of print-outs involved.

However HMIC would regard the following as the minimum level of documentation which should be retained for potential examination by external audit:

annual/strategic audit plans including the supporting risk analysis;

audit plans and audit control sheets (for individual audits);

schedules showing summary detail of audit/monitoring work carried out;

detailed working papers supporting the audit conclusions (see below);

copies of audit reports; and, very importantly,

executive board/management responses to audit reports.

It is not necessary to retain detailed documentation relating to all audit/monitoring tests carried out on all tested items. Evidence of items, which are checked and found to be correct, may be documented in summary form (e.g. schedule/matrix of items tested with test results, or similar). However errors found during the audit must be fully documented, including copies of source documents etc., where applicable.

5.1.6 Supporting/substantiating force record

The force must have an originating or supporting/substantiating record to validate the computer records being audited. The supporting/substantiating force record may be in any form which is appropriate to the Force. This may include paper, computer or micro-fiche. It is important to note that the underlying force record is the definitive record of the facts, as it will usually be the first record to be updated when any changes occur.

Paperless systems (e.g. update creation of Phoenix records directly by case officers) present a problem in that no originating document may exist. The associated risks may be mitigated to some extent by ensuring that suitable monitoring controls are incorporated into the record update/creation procedures. The critical factor is the accuracy of the computer record.

All records on the system with information having the potential of resulting in the arrest of any person must show a reference on the system to a supporting/substantiating force record(s).

The supporting/substantiating force record (for reports on the system meeting the arrest criteria stated above) must be accessible at all times. This is tested in the audit procedure by allowing 30 minutes to locate the supporting/substantiating record. The supporting/substantiating force record for reports not having the potential of resulting in an arrest must be obtainable during normal office hours.

Appendices

Appendix A

SAMPLING METHODOLOGY

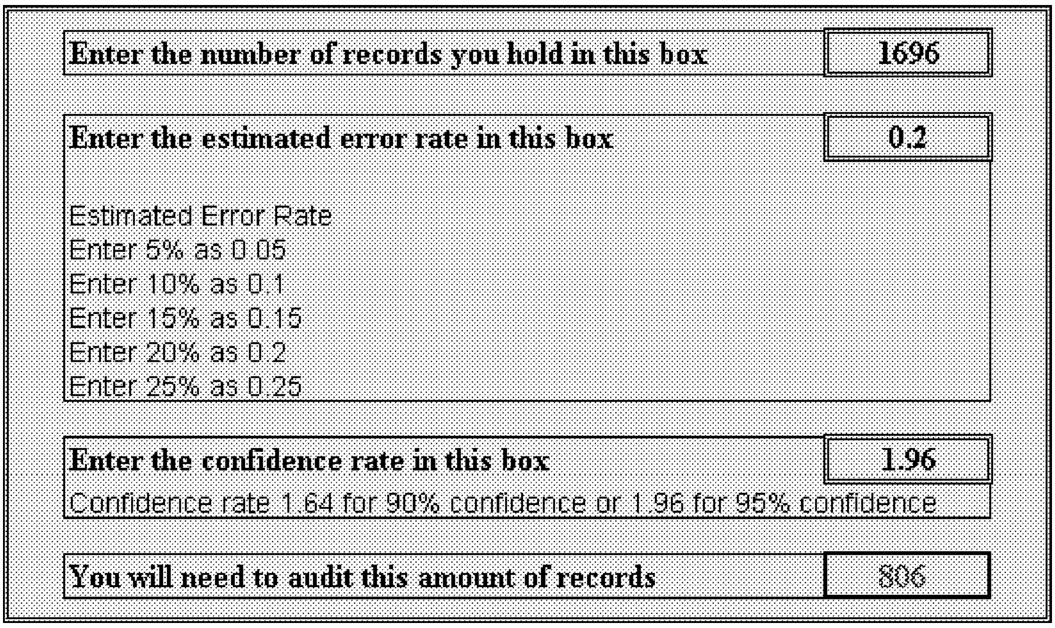
Unknown Error Rate

1. In cases where an estimate of the error rate is unknown a pilot audit of 200 records should be undertaken, irrespective of file size. From the results obtained the error rate and limits of accuracy can be calculated, this in turn will allow the auditor to decide whether it is necessary to sample additional records (See working examples below)

This method will allow forces to conduct audits of critical systems in a more timely and cost effective manner.

Known Error rate

2. Once antecedent history has been established estimates may be made with more reliability. By using the sampling software (see attached floppy disc) the auditor can work out exactly how many records need to be selected.



Enter the number of records you hold in this box	1696
Enter the estimated error rate in this box	0.2

Estimated Error Rate
Enter 5% as 0.05
Enter 10% as 0.1
Enter 15% as 0.15
Enter 20% as 0.2
Enter 25% as 0.25

Enter the confidence rate in this box	1.96

Confidence rate 1.64 for 90% confidence or 1.96 for 95% confidence

You will need to audit this amount of records	806

As can be seen from the above figure the auditor can select the desired error rate and confidence rate as required.

3. It is important that the entire population is identified to ensure that no items are omitted. Count the total number of records from which the sample will be taken - the computer may be able to do this. This represents the entire population from which a sample is to be selected, and is shown in the tables as **"file size"**.

4. Once the size of the sample has been determined, the sampled records should be selected from the total population using a random means, e.g. by using a random number generator or a sampling software package. It is important to ensure the records are randomly selected to eliminate bias in the sample. If bias is not eliminated at the selection stage the results of the audit will not be accurate and should not be used or relied upon.

5. If, during the course of the audit, more than 10% of the sampled records are discarded (because they have been amended or deleted) then the auditor should add more randomly selected records to

maintain the same sample size of records, or alternatively obtain a new sample of records. This situation may be avoided by ensuring that the audit is carried out as soon after the sample of records have been selected as possible.

6. The equation used to create the spreadsheet is shown below.

$$n = \frac{Z^2 Np(1-p)}{N E^2 + Z^2 p(1-p)}$$

n = sample size
Z = a value for the confidence level C.
95% = 1.96
90% = 1.64
N = file size
p = estimated error rate as a decimal (e.g. 20% is 0.2)
E = error range as a decimal (e.g. +/- 2% is 0.02)

Worked Examples

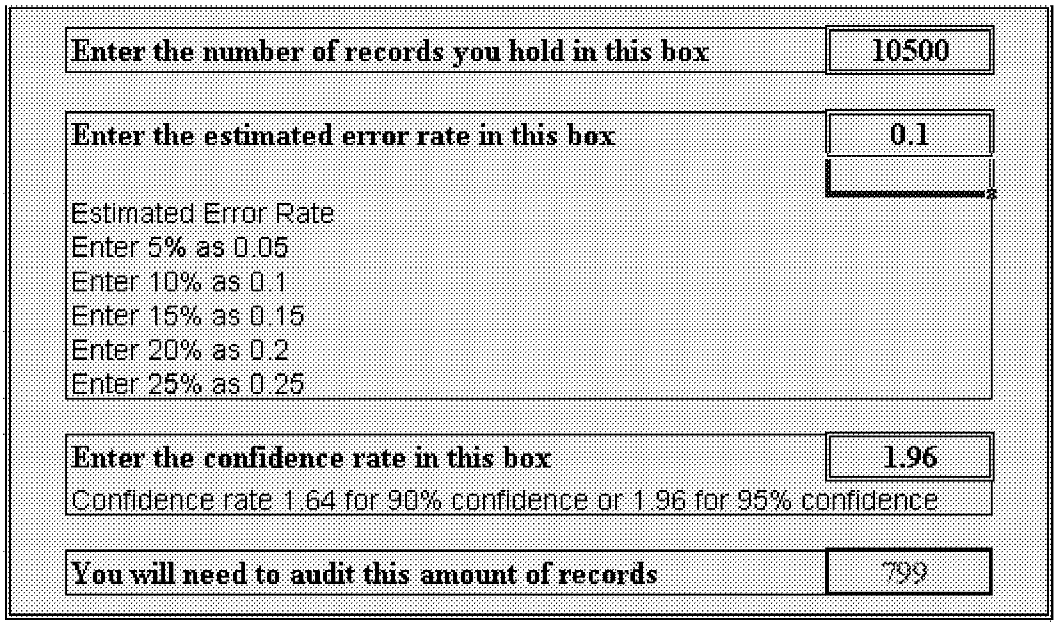
These working examples are designed to help the auditor to better understand the sampling methodology.

The examples are in three parts: Finding out the Sample Size (Error Rate Established), Pilot Audits and Using the Results.

Finding out the Sample Size

Step 1:
Firstly the population size of the records to be audited should be established i.e. determine the total number of records from which a sample will be taken.

For this example a population size of 10,500 will be used. This represents the file size (N).



Enter the number of records you hold in this box	10500
Enter the estimated error rate in this box Estimated Error Rate Enter 5% as 0.05 Enter 10% as 0.1 Enter 15% as 0.15 Enter 20% as 0.2 Enter 25% as 0.25	0.1
Enter the confidence rate in this box Confidence rate 1.64 for 90% confidence or 1.96 for 95% confidence	1.96
You will need to audit this amount of records	799

Step 2:
We will need to estimate the error rate of the records, (p) preferably, this should be estimated by using previous audit results. If the records have not been audited before then auditors should use the Pilot Audit method shown below.

When using this sampling theory the error range (E) is assumed to be + or - 2%. This means that if we estimate the error rate to be 10% (as above) we are estimating that the error rate lies within + or - 2% of 10% (or making the estimated error rate lie within the range 8% and 12%).

Step 3:
Select the confidence level (C) that will be used i.e. either 95% or 90% confidence. If possible it is always preferable to use 95% confidence as this gives a higher level of assurance that the results accurately reflect the population.

> For this example the 95% confidence level will be used. We will then be able to say with 95% confidence that the sample size used (and therefore the results concluded from the sample) are representative of the population.

Step 4:
As can be seen from the above diagram this returns the figure of 799, once the sample size has been found using the steps above the given number of records should be selected from the population of records. These records should be selected randomly to eliminate bias from the sample.

Pilot Audit Method

Step 1:

In cases where the error rate is unknown a pilot audit of 200 records should be undertaken, irrespective of file size.

A confidence level of 95% and a 2% error rate is used to calculate the number of records.

Step 2:

On completion of the audit from the results obtained the error rate and limits of accuracy can be calculated, this in turn will allow the auditor to decide whether it is necessary to sample additional records.

The following example is an audit of Correction Reports that had no established error rate (e.g. no previous audit experience). Using the previous practice of auditing at 95% confidence with an error rate of 20% for a population of 1200 records this would have required auditing 674 records. If each record took 4 minutes to audit then this would take approximately 44.9 hours or 6.1 staff days

By utilising the pilot audit approach this reduces the amount of records by 474 records, a saving of 31.6 hours or 4.3 staff days. On completion of the pilot audit if this revealed an error rate of 7.5% the auditor could choose to sample more records. Using the sampling methodology of 95% confidence and an error rate of 7.5% for a population of 1200 this means that 428 records need to be audited. As 200 records had already been audited only a further 228 records need to be checked, a saving of some 16.4 hours or 2.2 days.

Step 3:

These records should be selected randomly to eliminate bias from the sample.

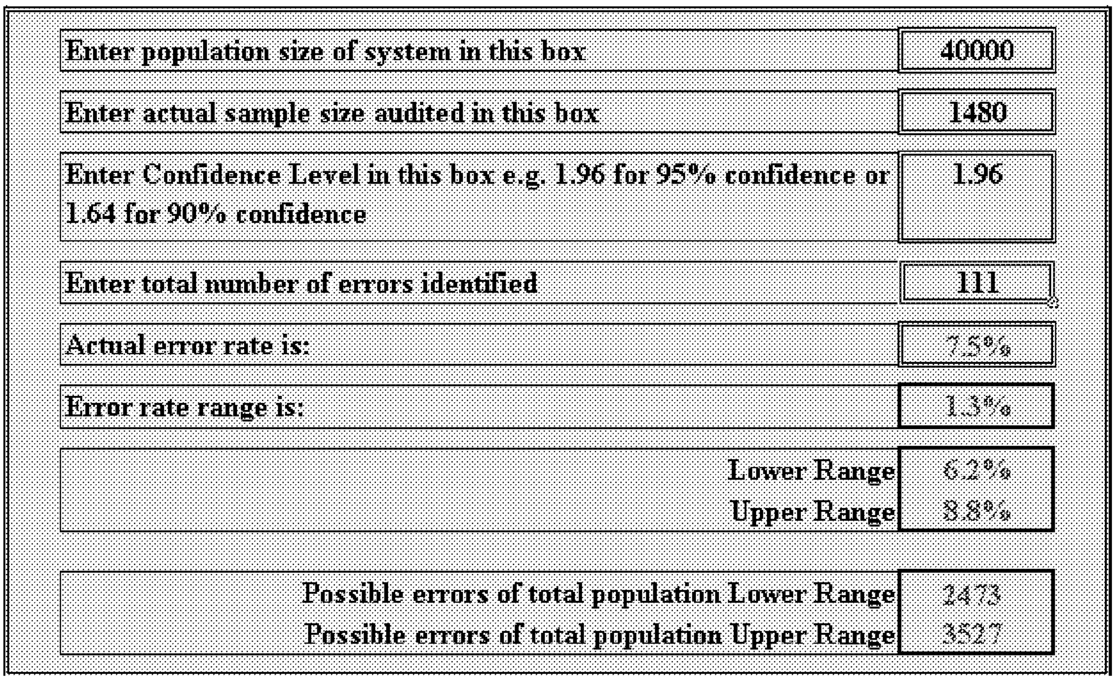
<u>Using the Results</u>

Once the audit has been carried out and the results are known they must be accurately reported. This means that to be accurate we say that the error rate lies in a range. We can calculate the range, **E**, by using the following equation:

$$E = Z\left(\sqrt{\frac{(N - n)p(1 - p)}{Nn}}\right)$$

where:

N = population size
n = sample size used
Z = a value for the confidence level C
when C = 95% then Z = 1.96
when C = 90% then Z = 1.64
p = actual error rate as a decimal



Enter population size of system in this box	40000
Enter actual sample size audited in this box	1480
Enter Confidence Level in this box e.g. 1.96 for 95% confidence or 1.64 for 90% confidence	1.96
Enter total number of errors identified	111
Actual error rate is:	7.5%
Error rate range is:	1.3%
Lower Range	6.2%
Upper Range	8.8%
Possible errors of total population Lower Range	2473
Possible errors of total population Upper Range	3527

From a population of 40,000 records, 1,480 records were audited at a 95% confidence and 111 errors were identified, this generates an error rate of 7.5%. This in turn gives a value for E of 1.3%.

It can then be stated that the error rate lies within the range (Lower and Upper) 6.2% to 8.8%. Alternatively, we could say the error rate found is 7.5% ± 1.3%.

From the error rate range it can be calculated that errors within the overall population could be between 2473 – 3527.

Another worked Example

The example is in two parts: ‘Finding out the Sample Size’ and ‘Using the Results’.

Finding out the Sample Size

Step 1:
Firstly the population size of the records to be audited should be established i.e. determine the total number of records from which a sample will be taken.

For this example a population size of 10,500 will be used. This represents the file size (**N**).

Step 2:
Select the confidence level (**C**), which will be used i.e. either 95% or 90% confidence. If possible it is always preferable to use 95% confidence as this gives a higher level of assurance that the results accurately reflect the population.

For this example the 95% confidence level will be used. We will then be able to say with 95% confidence that the sample size used (and therefore the results concluded from the sample) are representative of the population.

Step 3:
We will need to estimate the error rate of the records (p) selecting either a 5%, 10% or 20% error rate. Preferably, this should be estimated by using previous audit results. If the records have not been audited before it is better to over-estimate the error rate than to under-estimate it.

For this example we will assume that these records have not been audited before; we will therefore select a high estimated error rate, in this case 20%.

NB. When using this sampling theory the error range (E) is assumed to be + or - 2%. This means that if we estimate the error rate to be 20% (as above) we are estimating that the error rate lies within + or - 2% of 20%

(or making the estimated error rate lie within the range 18% and 22%).

Step 4:
Use the tables, charts or the formula to select your sample size given that:

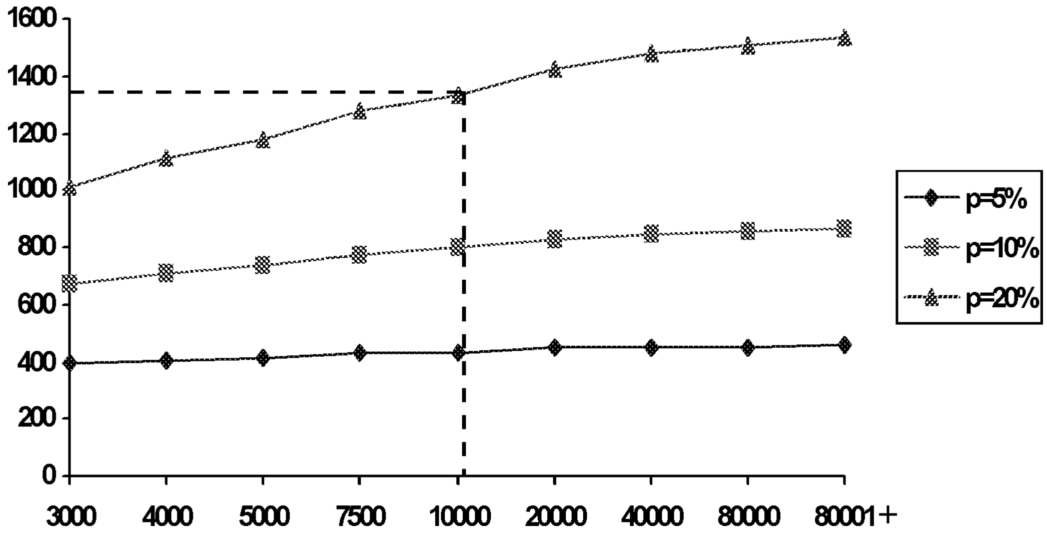
N = population size = 10,500
C = confidence level = 95% therefore Z = 1.96
p = estimated error rate as a decimal = 0.2 (i.e. 20%)
E = estimated error range as a decimal = 0.02 (i.e. 2%)

a) Using the Tables
To use the tables you first need to decide which confidence level will be used. For this example we will need to refer to the 95% confidence tables at Appendix F.

To find out the sample size first look down the left hand column to find the population size, which is 10,500.

In this example the left hand column does not show the population size of 10,500 and only has 10,000 or 20,000. It is always preferable to use the larger number and to have a sample size that is too large rather than one which is too small. One, which is too small, can adversely affect the validity of the results. So we will use the next highest population size of 20,000. To find out our sample size use the row which contains the population size and the column which contains the estimated error rate of p = 20% to identify the sample size, which in this example is 1427.

b) Using the Charts
To use the charts select the 95% confidence chart at Appendix F and pin-point the population size of 10,500 on the horizontal axis. Follow this point vertically up to the p = 20% line. Trace an imaginary line horizontally from this point to the vertical axis. At the point where this imaginary line crosses the vertical axis is the value of the sample size. This is calculated to be approximately 1350 (see the diagram below).



c) Using the Formula
To obtain a precise sample size use the following formula (also see Annex (i)):

$$n = \frac{Z^2 Np(1-p)}{N E^2 + Z^2 p(1-p)}$$

The parameters to use in the equation would be:

N = population size = 10,500

C = confidence level = 95% therefore Z = 1.96
p = estimated error rate as a decimal = 0.2 (i.e. 20%)
E = estimated error range as a decimal = 0.02 (i.e. 2%)

Using the above parameters we get the sample size of n = 1340 (rounded to the nearest integer).

Step 5:
Once the sample size has been found using one of the three methods in Step 4 (above) the given number of records should be selected from the population of records. These records should be selected randomly to eliminate bias from the sample.

Using the Results

Once the audit has been carried out and the results are known they must be accurately reported. This means that to be accurate we say that the error rate lies in a range. We can calculate the range, **E**, by using the following equation:

$$E = Z\left(\sqrt{\frac{(N - n)p(1 - p)}{Nn}}\right)$$

where:

N = population size
n = sample size used
Z = a value for the confidence level C
when C = 95% then Z = 1.96
when C = 90% then Z = 1.64
p = actual error rate as a decimal

For this example suppose the error rate found from the audit was 11.4% and the sample size used was 1,427 from Step 4 (a) above. The parameters to use in the equation are therefore:

N = 10,500
n = 1,427
Z = 1.96
p = 0.114 (i.e. 11.4%)

This gives a value for E which is E = 0.015 (to 3 decimal places). Remember that this value is the error range as a decimal so the actual error range would be ▯1.5% (i.e. 0.015).

The error range can be calculated by saying that the error rate lies in the range:

(p - E) < Error rate < (p + E)

where:

p = actual error rate = 11.4%
E = error range = 1.5%

So the error range is:

(11.4% - 1.5%) < Error rate < (11.4% + 1.5%)
9.9% < Error rate < 12.9%

The error rate then lies within the range 9.9% to 12.9%. Alternatively, we could say the error rate found is 11.4% + or - 1.5%.

Appendix B

TABLE ONE - CONFIDENCE LEVEL (C) 90%

FILE SIZE (N)	SAMPLE SIZE (n)		
	p = 5%	p = 10%	p = 20%
50	43	46	48
100	76	86	91
150	102	120	132
200	123	150	169
250	140	177	203
300	155	201	235
350	167	222	264
400	178	241	292
450	187	258	317
500	195	274	341
600	208	301	385
800	228	345	459
1000	242	377	518
1200	252	402	567
1400	260	423	608
1600	266	439	643
1800	271	453	673
2000	275	465	700
3000	289	504	792
4000	296	526	848
5000	300	540	885
7500	306	564	941
10000	310	571	971
20000	314	587	1021
40000	317	596	1048
80000	318	601	1062
80000 +	319	605	1075

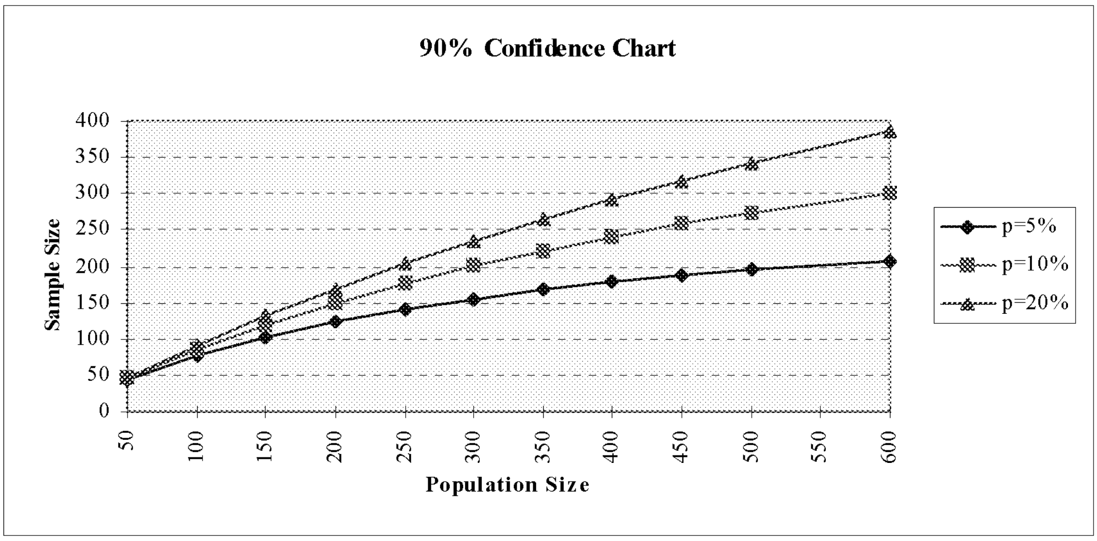
Appendix C

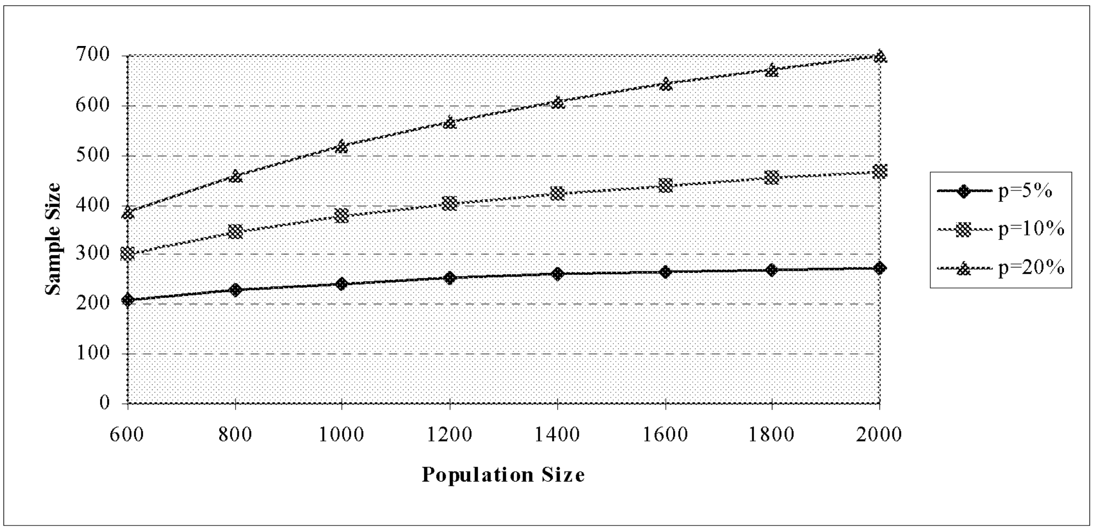
TABLE TWO - CONFIDENCE LEVEL (C) 95%

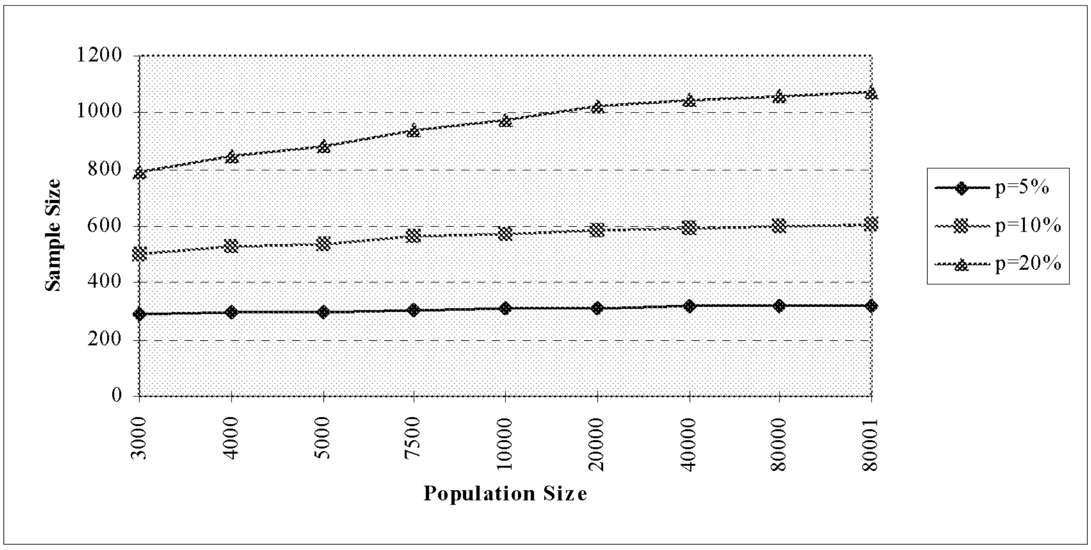
FILE SIZE (N)	SAMPLE SIZE (n)		
	p = 5%	p = 10%	p = 20%
50	45	47	48
100	82	90	94
150	113	128	137
200	139	162	177
250	161	194	215
300	181	223	251
350	198	249	285
400	213	273	317
450	227	296	348
500	239	317	377
600	259	354	432
800	291	415	526
1000	313	464	606
1200	331	502	674
1400	344	534	733
1600	355	561	784
1800	364	584	829
2000	371	604	869
3000	396	671	1016
4000	409	711	1110
5000	418	737	1175
7500	430	775	1275
10000	436	796	1332
20000	446	829	1427
40000	451	846	1480
80000	454	855	1508
80000 +	456	864	1536

Appendix D

CHART ONE - CONFIDENCE LEVEL (C) 90%

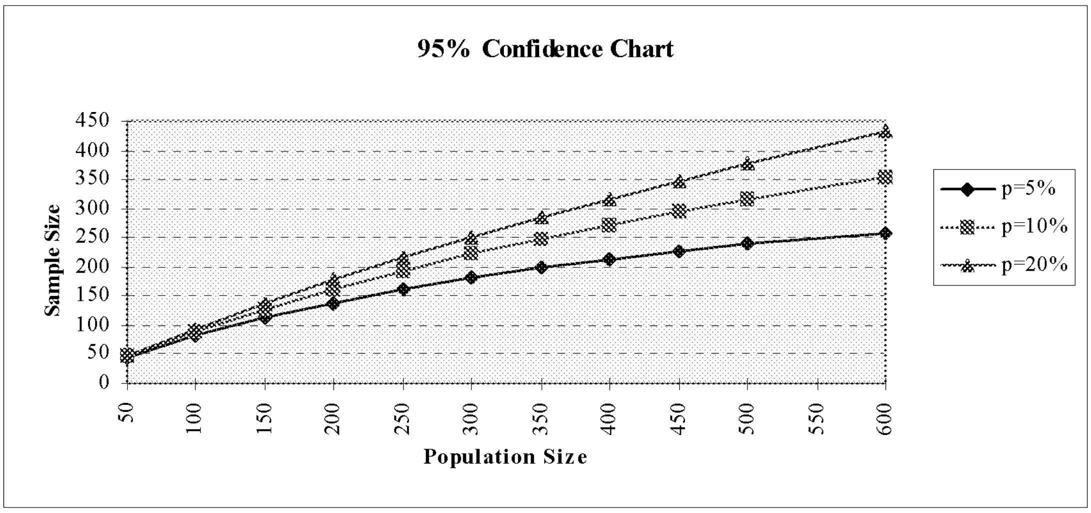


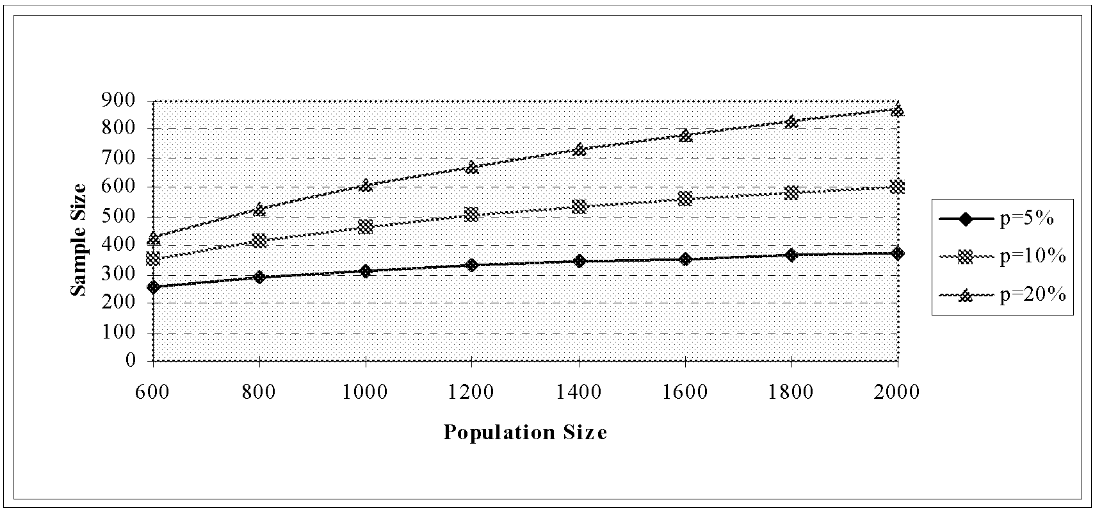


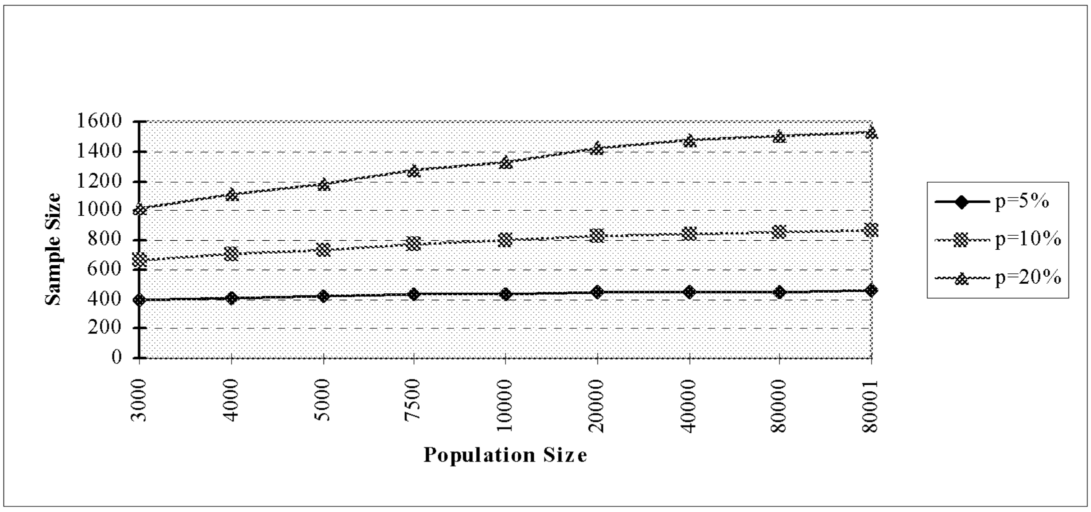


Appendix E

CHART TWO - CONFIDENCE LEVEL (C) 95%







Appendix F

RANDOM NUMBER TABLE - 1000 Random Numbers

	00-04	05-09	10-14	15-19	20-24	25-29	30-34	35-39	40-44
00	78889	54373	46608	78283	07723	94977	76576	69760	43586
01	58282	55626	14113	53967	29465	04725	53167	16140	66444
02	30303	77755	44118	58702	95318	82413	81438	30423	36164
03	97357	73154	53615	66416	72176	89513	17644	67249	23811
04	08369	61645	38732	09440	37511	21415	27823	26261	36822
05	19456	92473	57602	46582	18006	63284	83988	18732	48625
06	07730	46179	62312	89395	16809	21494	37792	17265	18757
07	16701	58463	29824	24717	71722	10398	53761	26216	68987
08	82896	83893	74549	45889	11511	63105	18641	53136	42106
09	66551	93814	38673	40645	62753	88735	63397	68376	37421
10	62654	95146	66230	41737	98356	35173	84566	01445	34442
11	69591	37036	73353	82987	80267	58636	64075	25301	69099
12	32867	47258	34551	28588	57137	43278	66485	85816	28326
13	28343	32188	63597	45642	91295	32662	49277	17336	35795
14	25562	49527	87142	65475	73563	35166	35543	12558	82146
15	44683	55622	10191	85061	48048	81317	62615	82424	58621
16	43019	39374	73208	74980	76773	78908	67446	94144	78402
17	55211	03239	25106	49868	61911	55136	37586	17226	33854
18	43171	25725	83625	23105	74176	38572	64727	74484	94886
19	33364	09132	15485	84143	10693	44846	26174	33378	79078

Appendix G

ERROR CLASSIFICATION

General

As a general rule errors will fall into three main categories: Major, Intermediate and Minor.

Pre defined toolkits, will be used for specific information systems .

Major Errors

- Those which could reasonably be expected to lead to the wrongful arrest of a person;
- Spelling mistakes that affect the capability of successfully locating records e.g. incorrect VRM;
- May put police personnel at risk;
- Cause adverse media attention or publicity, etc.;
- Could lead to an individual being refused employment as a result of inaccuracies being disclosed during authorised vetting checks;

Intermediate Errors

- Those which could cause unnecessary and unreasonable delay in locating case papers etc.;
- Could reasonably be expected to cause minor inconvenience to the subject;
- The substantiating force record cannot be located within 30 minutes, but is subsequently produced within 24 hours.

Minor Errors

- Those, which have little consequence, do not affect any computer processing, or will be circumvented by normal work practices. Examples of these will include spelling mistakes not categorised as major errors, times of incidents, value of property, slight variations in height etc.
- Inability to locate force record.

(It should be noted that most of these occurrences could lead to financial compensation being paid).

Appendix H

Audit Record Sheets

Annex H1	**-**	**Working Papers**
Annex H2	**-**	**Urgent Matters / Brought Forward**
Annex H3	**-**	**Data Protection Officer Review**
Annex H4	**-**	**Audit Control Sheet**
Annex H5	**-**	**Audit Test Matrix**
Annex H6	**-**	**Supporting Documentation**

Appendix I

AUDIT RISK ANALYSIS

The following are some guidelines to be followed when using the Risk Assessment Process Template. The process template can be used to either risk assess individual information systems / manual filing systems or risk assessing specific data sets across several information systems / manual filing systems.

Risk assessment timing.

A risk assessment should be completed as part of the audit planning phase and should be completed for all systems storing personal data. If a risk assessment has been previously undertaken for a system it should be reviewed in the following circumstances:

- An existing system has undergone a significant change.
- A change in force policy impacting on the personal data or system.
- As the result of an audit.
- Reviewed periodically, annually for example.

New systems should be risk assessed and if possible a process should exist for the notification of new systems to the Data Protection Officer and Auditors.

Personnel involved.

A Data Protection risk assessment should be undertaken by a Data Protection Officer or Auditor combined with the system owner or an individual delegated by the system owner with sufficient knowledge of the system.

The risk assessment process.

A meeting should be arranged with either the system owner or the nominated officer. It may be helpful to use an Aide Memoire covering the topics in the risk assessment to learn more about the system. These topics should be covered in a consultation prior to starting the risk assessment process. This information will aide the assessors when evaluating the risks and assigning appropriate scores. The Aide Memoire should cover questions such as: (This is not a definitive list and can be amended accordingly):

- How is the information stored? Electronically? Manually?
- What personal data is held?
- What is the data used for?
- Who uses the data, how many users are there and where are they located?
- What is the source of the data?
- What is the typical lifecycle of a record? i.e. why and how would it be updated and by whom?
- Are there any Operating Rules in place for the system?
- Who is the data disclosed to? Are there Information Sharing Protocols in place?
- Is there a retention policy in place covering the data? Is it adhered to?

Scoring the risk categories.

Within the risk categories there are a number of statements with scores next to them. In consultation with the system owner / nominated officer, identify which statement is closest to the system. The scores are 10, 7, 4 and 0. If you judge that the risk lies between these scores, you should choose an intermediate score. If some categories are of more importance to your individual force than others, a weighting system to adjust the scoring may be more appropriate.

Once you have agreed a score for a category, mark it accordingly and record any major factors that influenced your scoring under the appropriate box. This will provide an audit trail for the score and will be helpful when checking all assessments for consistency, as well as when a conducting a review. If there is additional documentation to support a score it is recommended that this is retained within the audit risk assessment working material.

The maximum score for a system is 130 (unless a weighting system has been used). Record all the scores in the matrix on the last page of the risk assessment documents. Identify the overall risk level for the system: High (>=80), Medium (40-79), or Low (0-39). The result should then be fed into your audit planning process accordingly.

Once the score has been agreed it is recommended that it is signed off by those who conducted the assessment and retained in the risk assessment working material.

Risk Assessment

Information Asset:	
System Owner:	
Location/Dept:	
Auditor:	
Consulted:	
Assessment Date:	
Expected Review Date:	
Final Score:	

This Risk Assessment process will be completed for every system that contains personal data. Assessments should be conducted when a system is newly created, is subject to significant changes in the system, policy or procedures, as part of audit planning and process and as a result of periodic review.

1. Importance of Operational Information

Importance of data to force operations and / or core business activities.

Score	Scoring Criteria
10	Critical to day-to-day operations and/or core business activities. An operation would not go ahead without it.
7	The absence of this information would create a significant delay in the implementation or success / effectiveness of an operation and/or core business activity.
4	The absence of this information would not delay an operation or core business activity as a workaround could be put in place.
0	No impact.

Reason:

2. Inaccurate Information

Inaccurate information could result in financial damage to or / poor public relations or image of the constabulary, or jeopardise operational matters.

Score	Scoring Criteria
10	Highly damaging, external impact, legal implications and/or financial damage.
7	Embarrassing, internal operational impact.
4	Internal administrative inconvenience, negligible impact.
0	No potential liability.

Reason:

3. Record Amendment

Data that undergo constant amendment are more prone to errors.

Score	Scoring Criteria
10	Individual record / data is updated weekly or more often
7	Individual record / data is updated monthly or more often
4	Individual record / data is updated less often than each month
0	Individual record / data was created but not updated since

Reason:

4. System enhancement / new system

Data transferred or recently imported to a new system or platform, whether automatic or manual.

Score	Scoring Criteria
10	New / existing system with data transferred/imported, no data integrity checks carried out before/after change, or unsatisfactory integrity check results.
7	New / existing system with data transferred/imported, limited data integrity checks carried out before/after change producing satisfactory results.
4	Minor changes made to existing system. Data not transferred or imported
0	No recent changes or planned changes in the near future.

Reason:

5. Legislation / Guidance / Procedures

New or amendments to existing legislation / guidance / administrative procedures on the way data is recorded, stored or managed will impact upon the risk levels.

Score	Scoring Criteria
10	New or amended legislation / guidance impacting on the data has been introduced
7	New or amended legislation / guidance impacting on the data is to be implemented in the next 12 months.
4	New or amended legislation / guidance impacting on the data is to be implemented in excess of 12 months.
0	New or amended legislation / guidance impacting on the data is not planned or expected.

Reason:

6. Past Audit Experience

Hindsight experience of previous audits can be used for assessing potential or actual risk, based on the number of Major errors and/or total errors across all categories.

Score	Scoring Criteria
10	Red Performance, Major error rate >= 10%, or Overall error rate >=20%, or the system has not been subject to audit in the last 5 years.
7	Amber Performance, Major error rate >= 5%, and <10%, or the Overall error rate >=10% and <20%.
4	Green Performance, Major error rate <=5%, or Overall error rate <=10%.
0	No material errors found.

Note: Error rates shown are suggested error rates for risk analysis purposes only, and should not be regarded as 'acceptable' or 'national' standard for error rates.

Reason:

7. Information Classification

Assessment of system / data based on the Government Protective Marking Scheme Baseline Measures. Systems that do not meet the required criteria for Impact, Storage & Retention, Distribution / Transmission and IT Systems should be scored more highly.

Score	Scoring Criteria
10	Top Secret or Highly damaging, immediate impact on business or national public image.
7	Secret or Seriously embarrassing, external impact, legal implications, some financial or operational damage.
4	Confidential or Embarrassing, largely internal impact, small financial and operational impact.
0	Restricted or Mildly embarrassing, negligible impact.

Reason:

8. Disclosure / Information Sharing

How likely is this information to be disclosed or shared with external agencies or third parties (including Subject Access and FOI disclosures). Where no Information Sharing Protocol or Legislation exists, the system / information should be scored more highly.

Score	Scoring Criteria
10	Information is regularly disclosed (weekly) or requests for disclosure are received from an external agency or third party.
7	Information is disclosed monthly or requests for disclosure are received from an external agency or third party.
4	Information is disclosed quarterly or requests for disclosure are received from an external agency or third party.
0	Information is not disclosed or no requests for disclosure from external agencies are received or third party.

Reason:

9. Impact on the Data Subject

This risk is the amount of damage or distress that could be caused to the data subject on unlawful or accidental disclosure of their personal data (in the worst case scenario). The likelihood of legal action, compensation and lasting effects should be considered.

Score	Scoring Criteria
10	Very High impact for potential damage or distress to the Data Subject.
7	High impact / or high potential for damage or distress to the Data Subject
4	Moderate impact / potential for damage or distress to the Data Subject
0	No or Negligible impact on the Data Subject

Reason:

10. Information Retention and Weeding Rules

Controlling adherence to Principle 5.

Score	Scoring Criteria
10	There are no weeding rules or information policies in place
7	Weeding rules are in place but are not enforced at all
4	Weeding rules are in place but there is limited adherence
0	Weeding rules are in place and adhered to

Reason:

11. Number of Users

Number of users accessing the system / record for view or update purposes.

Score	Scoring Criteria
10	System / information is accessed by 50% or more personnel
7	System / information is accessed by 25% - 49% personnel
4	System / information is accessed by 10% - 24% personnel
0	System / information is accessed by 9% or less personnel

Reason:

12. Location of Users

Location of users. Geographic or departmental separation increases the risk of local variations in training and procedures.

Score	Scoring Criteria
10	Users are split between more than 5 locations or departments
7	Users are split between more than 3 locations or departments
4	Users are split between more than 2 locations or departments
0	Users are in a single location

Reason:

13. Data relating to children or vulnerable adults

Due to the potential use of data relating to children or vulnerable adults it is deemed a high risk area and as such requires it's own risk assessment category.

Score	Scoring Criteria
10	The information system retains data specifically relating to children or vulnerable adults.
7	The information system retains data on non-vulnerable and vulnerable categories equally.
4	Data relating to children and vulnerable adults is retained but they are not the main focus of the data.
0	The data does not relate to children or vulnerable adults.

Reason:

Final Scores

System:

RISK ASSESSMENT SCORE FORM	
Key Risk Characteristic	
1. Importance of Operational Information	
2. Inaccurate Information	
3. Record Amendment	
4. System Enhancement / New System	
5. Legislation / Guidance / Procedures	
6. Past Audit Experience	
7. Information Classification	
8. Disclosure / Information Sharing	
9. Impact on the Data Subject	
10. Information Retention and Weeding Rules	
11. Number of Users	
12. Location of Users	
13. Data relating to children or vulnerable adults	
Total Scores (max 130)	

Overall Risk Rating:

High Risk:	Score of 80 and above
Medium Risk:	Score of 40 – 79
Low Risk:	Score of 0 – 39

Signatures

Auditor:

Date:

System Owner:

Date:

Appendix J

EXAMPLE DATA PROTECTION AUDIT PLAN TEMPLATE

Audit	Risk Assessment Rating	Planned Audit Dates	Status	Comments

Appendix K

Example

xxxx CONSTABULARY

Data Protection/Information Compliance Section
(Or equivalent)

AUDIT REPORT

DEPARTMENT:	**FORCEWIDE**
SYSTEM:	**PNC**
AUDIT:	**Sex Offenders Register**

Audit Date:	**1 May 2005**
Auditor(s):	**A.N.Other** **Information Compliance Auditor**

TO: Information Compliance Manager
(NB. For onward transmission to the Information Compliance Board/Senior Management Board)

FROM: **A.N.Other - Information Compliance Auditor**

DATE: 10 June 2005

5.2 TABLE OF CONTENTS

TABLE OF CONTENTS 2

LIST OF FIGURES Error! Bookmark not defined.

FOREWORD 3

EXECUTIVE SUMMARY 4

AUDIT REPORT 5

1 Introduction 5
2 Audit Purpose 5
3 Audit Scope 5
4 Audit Methodology 5
5 Audit Tests 5
6 Results 5
6.1 Previous Audit Results 5
6.2 Audit Results 6
7 Findings 7
7.1 Previous Audit Findings 7
7.2 Audit Findings 7
7.3 General Issues 7
8 Conclusion 7
9 Recommendations 7

APPENDIX A - Methodology Flow Diagram. 9

APPENDIX B - Error Classification. 10

APPENDIX C – SUMMARY OF ERRORS 12

APPENDIX D - Recommendations – Management Response 14

5.3 FOREWORD

....Constabulary is required to ensure that data held within Police information systems are obtained, used and disclosed in accordance with the Data Protection Act 1998 (DPA 98), other relevant legislation and national/force policy.

To comply with the statutory requirements of the Data Protection Act 1998, proper procedures must be in place to ensure that personal data held in force information systems is compliant with the provisions of the act. This includes compliance with the eight principles of Data Protection which require personal data to be:

- Processed fairly and lawfully (must have a legitimate reason)
- Obtained only for one or more specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in accordance with the data subjects rights
- Awarded appropriate security measures
- Retained within the European Economic Area unless adequate protection can be Guaranteed from other areas

5.4 EXECUTIVE SUMMARY

….Constabulary is required to ensure that data held within Police information systems are obtained, used and disclosed in accordance with the Data Protection Act 1998 (DPA 1998), other relevant legislation and national/force policy. To comply with the statutory requirements of the DPA 1998, proper procedures must be in place to ensure that personal data held in force information systems is compliant with the provisions of the act. In order to achieve this compliance the ACPO Data Protection Manual requires that Information Compliance audits are conducted. The personal data selected for this audit is that which is held by ….Constabulary on the Police National Computer WANTED/MISSING and INFORMATION MARKER applications which contain data elements associated with the Sex Offenders Register.

Audit Aims

The aims of the audit are:

a. To ensure compliance with the relevant principles of the DPA 1998 as defined by the audit scope.
b. To assist management in formulating policies and good practice.
c. To comply with the requirements of the Strategic Audit Plan.
d. To identify errors occurring and recommending corrective action to be taken to ensure compliance.
e. To support Officers and Staff in the conduct of their duties in respect of Information Compliance.
f. To ensure that a 100% review of personal data associated with …. owned Sex Offenders PNC data was conducted in conjunction with the introduction of the VISOR system.

Audit Scope

The audit scope was limited to checking for compliance with the 1st, 3rd and 4th principles of the DPA 98 which state that:

Principle 1 *"Personal data shall be processed fairly and lawfully."*

Principle 3 *"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are maintained."*

Principle 4 *"Personal data shall be accurate and, where necessary, kept up to date."*

Audit Results

5.4.1.1.1.1.1.1 Audit Findings

Audit Recommendations

The auditor therefore recommends: -

Appendix <x> Management Response should be completed and returned to the Information Compliance Section by <date>

5.5 FULL AUDIT REPORT

6 Introduction

...... is required to ensure that data held within Police information systems are obtained, used and disclosed in accordance with the Data Protection Act 1998 (DPA 98), other relevant legislation and national/force policy. To comply with the statutory requirements of the DPA 1998, proper procedures must be in place to ensure that personal data held in force information systems is compliant with the provisions of the act. The system selected for this audit is the Police National Computer WANTED/MISSING (WM) and INFORMATION MARKER (IM) data elements associated with the PNC Sex Offenders Register.

7 Audit Purpose

The aims of this audit are:

a. To ensure compliance with the relevant principles of the DPA 1998 as defined by the audit scope.
b. To assist management in formulating policies and good practice. To comply with the requirements of the Strategic Audit Plan.
c. To identify errors occurring and recommending corrective action to be taken to ensure compliance.
d. To support Officers and Staff in the conduct of their duties in respect of Information Compliance.
e. To ensure that a 100% review of personal data associated with .... owned Sex Offenders PNC data was conducted in conjunction with the introduction of the VISOR system.

8 Audit Scope

The audit scope was limited to checking for compliance with the 1st, 3rd and 4th principles of the DPA 98 which state that:

Principle 1 *"Personal data shall be processed fairly and lawfully."*

Principle 3 *"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are maintained."*

Principle 4 *"Personal data shall be accurate and, where necessary, kept up to date."*

9 Audit Methodology (Toolkit)

A 100% listing of ...... owned Sex Offenders was requested from Hendon Data Centre and resulted in a floppy disc of 424 Sex Offender entries being supplied. The procedure adopted at appendix ......(Toolkit) was used to ensure that the results could be compared like for like.

The information was examined to identify ....

10 Audit Tests (Toolkit)

a. Can the force record be located?
b. Is the Force Record still Valid?
c. Do the details on the system accurately reflect the force record?

Application of the above tests results in three error types a. Major , b. Intermediate and c. Minor. These three error types are further divided to allow for specific sub categories of error and are listed at Appendix B.

11 Results

11.1 Previous Audit Results

The audit conducted in 2002 had the following results:

Overall a total of .... errors were revealed from the total sample size of 273 records. This represents an overall error rate of .....%. Of the 273 records audited ....contained 2 errors, this results in approx ...of the records containing .....errors. A summary of errors and error rates based on each category sample is shown below:

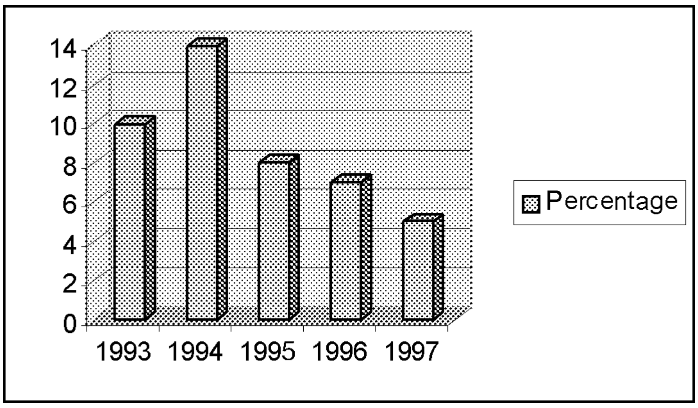
Major error: (Overall Error Rate .....)

Intermediate errors: (Overall Error Rate ...)

Minor errors: (Overall Error Rate .....)

Example of other year comparisons:

YEAR	NO. OF RECORDS AUDITED	NO. OF INCORRECT RECORDS	ERROR PERCENTAGE
2002	**350**	**35**	**10%**
2003	**402**	**56**	**14%**
2004	**520**	**40**	**8%**
2004	**607**	**45**	**7%**
2005	**725**	**35**	**5**



Ideal to also include comparison by Division etc. if appropriate.

11.2 Audit Results

Overall a total of ...... errors were revealed from the total sample size of ..... records. This represents an overall error rate of ..... Of the ....records audited ....

Major errors: (Overall Error Rate ...%)

Intermediate errors: (Overall Error Rate .....%)

Minor errors: (Overall Error Rate ......%)

12 Findings

12.1 Previous Audit Findings

13 Previous Audit Conclusion

13.1 This Audit Findings

13.2 General Issues

14 Conclusion

15 Recommendations

The auditor therefore recommends: -

Appendix <x> Management Response should be completed and returned to the Information Compliance Section by <date>.

The auditor's thanks are given to <names, depts,> for their assistance during the course of this audit.

Appendix xxx

Management Response/Schedule of Audit Findings

Action Points	Priority	Impact/Risk	Recommendations	Management Response
1 Data Accuracy				
1.1 Record no longer valid				
In one instance it was found that a warrant for a person recorded as Wanted on Warrant had been withdrawn, however the PNC had not been updated to reflect this.	**High**	The person to whom the record related could have been arrested during the period that the record was incorrectly retained on PNC. This leaves the force open to a complaint of wrongful/unlawful arrest, and therefore potentially liable for resultant damages.	DPO **recommends** that the procedures for updating PNC W/M records re withdrawn warrants be reviewed, and that the system of dip-checks currently in place to monitor data accuracy be extended. **By End May 2006**	
1.2 Incorrect spelling of names	**High**		Also that bureau staff should be made aware of the implications and potential liabilities of incorrect data on W/M records. **By End May 2006**	
etc., etc.				

15.1 APPENDIX A - Methodology Flow Diagram.

15.2 APPENDIX B - Error Classification.

15.2.1.1.1 Major Errors

CATEGORY	DESCRIPTION OF ERROR
A1	Case file/Source documentation missing, location unknown
A2	Incorrect surname and/or forename
A3	Current registered address incorrect/missing
A4	Information Marker missing
A5	Order Type Incorrect
A6	Weed Date incorrect/missing
A7	Current Registration date missing/incorrect
A8	Offenders status incorrect/missing
A9	PNC ID incorrect
A9	Other. (Major error not previously defined.)

15.2.1.1.2 Intermediate Errors

CATEGORY	DESCRIPTION OF ERROR
B1	Case Papers missing from files but location known
B2	Alias missing/incorrect
B3	Nickname Missing Incorrect
B4	2nd Registered address missing/incorrect
B5	Force Reference Nominal Number incorrect
B6	Other (Intermediate error not previously defined.)

15.2.1.1.3 Minor Errors

CATEGORY	DESCRIPTION OF ERROR
C1	Case files/ Source document location incorrect
C2	House Number missing from address
C3	Post Code missing/incorrect
C4	AS reference missing/incorrect
C5	Report date missing / incorrect
C6	Place of issue missing/incorrect
C7	Spelling mistakes other than name/address
C8	D.O.B. incorrect
C9	Other. (Minor error not previously defined.)

15.3 APPENDIX C - SUMMARY OF ERRORS

Information System:	PNC
Audit Category:	SEX OFFENDERS REGISTER
System Owner:	HEAD OF CJS
Nominated Officer:	PNC LIAISON OFFICER
Audit Reference:	SO/FEB/05

SER	PNCID	ERROR TYPE	REMARKS	ACTIONS
5		Minor Error C1: Case File location incorrect.	C1: PNC shows case paper location as …. actual location is …..	
6		Minor Error C1: Case File location incorrect.	As above	
8		Minor Error C1: Case File location incorrect.	As above	
10		Minor Error C1: Case File location incorrect.	As above	
12		Minor Error C1: Case File location incorrect.	As above	
16		Minor Error C2: Incorrect house number in address.	C5: PNC shows 51 Form 130 shows 56	Amended by PNC Bureau during Audit
21		Minor Error C1: Case File location incorrect.	C1: PNC shows case paper location as …. actual location is …..	
28		Minor Error C1: Case File location incorrect.	As above	
29		Minor Error C1: Case File location incorrect.	As above	
31		Minor Error C1: Case File location incorrect.	As above	
33		Minor Error C1: Case File location incorrect.	As above	
34		Minor Error C1: Case File location incorrect.	As above	

SER	PNCID	ERROR TYPE	REMARKS	ACTIONS
35		Minor Error C1: Case file location incorrect.	C1: Nominal now resides in ...Constabulary PNC Bureau not notified of change.	
38		Minor Error C5: Report date incorrect . Weed date correct.	C5: PNC shows IM and WM caution date = 29/11/01. Form 130 shows 17-11-01 for caution date.	Amended by PNC Bureau during Audit
41		Minor Error C1: Case File location incorrect.	C1: PNC shows case paper location as ….actual location is ...	
42		Minor Error C8: Other.	C8: Alias forename missing. "Stephen" shown on form 130 dated 09/02/05	Amended by PNC Bureau during Audit
43		Minor Error C1: Case File location incorrect.	C1: Nominal was in….Hospital Transferred to ….Hospital in 2002. PNC Bureau not notified. ...Constabulary not aware of move.	Norfolk notified by auditor on 15 April 2005

15.4 APPENDIX D - Recommendations – Management Response

INFORMATION COMPLIANCE AUDIT

1 Data Accuracy *1.1 Record no longer valid* In one instance it was found that a warrant for a person recorded as Wanted on Warrant had been withdrawn, however the PNC had not been updated to reflect this. *1.2 Incorrect spelling of names* etc., etc.	**High** **High**	The person to whom the record related could have been arrested during the period that the record was incorrectly retained on PNC. This leaves the force open to a complaint of wrongful/unlawful arrest, and therefore potentially liable for resultant damages.	DPO **recommends** that the procedures for updating PNC W/M records re withdrawn warrants be reviewed, and that the system of dip-checks currently in place to monitor data accuracy be extended. **By End May 2006** Also that bureau staff should be made aware of the implications and potential liabilities of incorrect data on W/M records. **By End May 2006**

Appendix L

Information Available from HDC

This information can be obtained from the Data Control Centre at Hendon. Print-outs or floppy discs (indicated by 'D' after the batch number) will be despatched with a covering letter which gives details of the batch search number which has produced the data. Forces that request the same search criteria should quote this number in future enquiries.

It should be noted, the capability to obtain printout of certain indices, currently VODS and Property Searching, exists locally and may therefore obviate the need to contact Hendon Data Centre.

Vehicle & Property File

Printouts (or discs) may be requested using the following parameters:

(a) Any one or more of the vehicle classes:

i. Lost or Stolen
ii. Found
iii. Information
iv. Seen
v. Correction
vi. Removed
vii. Restricted

or any one or more of the property classes:

i. Lost or Stolen
ii. Found
iii. Property Type (Plant, Trailers, Animals, Marine, Firearms, All)

(b) By:

i. Whole force i.e. by 2-figure PNC code, e.g. 01
ii. Division within a force i.e. by 3-figure PNC code, e.g. 01A
iii. Station within a division i.e. by 4-figure PNC code, e.g. 01AD

(c) All records i.e. 100% of the records meeting the criteria in (a) or (b) above.
OR
A randomly selected audit printout of records meeting the criteria selected in (a) & (b).

n.b. HDC will calculate this file size by using the formula in Appendix A (E = 0.02, p = 0.05, 0.1 or 0.2, Z = 1.64 or 1.96). The sample size provided by HDC should be confirmed as correct by comparing the given sample size with the sample size calculated using the formula in Appendix A.

Printout Format
The printout contains the full details of the report type requested. However it does not contain any other police reports that the vehicle may have attached to it. A change request has been submitted to printout all attached reports.

Printout Order
The printout is in report owner groupings and the records within these groupings are in report type order and within these groupings are in report creation date order.

Wanted/Missing and Disqualified Drivers

Printouts may be requested using the following parameters;

(a) Any one or all of the Wanted/Missing classes, i.e.

i. Detained
ii. Wanted

iii. Order
iv. Missing
v. Found
vi. Desert
vii. Abscond
viii. Recall
ix. Locate
x. Non-payment of fines (though not a class)

OR Disqualified Drivers (Batch No. NP 230 J)
OR Information Markers

(b) Whole force i.e. by 2 figure PNC code, NOT 4 figure code.

(c) All records i.e. 100% of the records meeting the criteria in (a) or (b) above.
OR
A randomly selected audit printout of records meeting the criteria selected in (a) & (b). (Warning- the formula used may not be the recommended formula stated at Appendix A, and may result in a statistically invalid sample. The sample size provided by HDC should be confirmed as correct by comparing the given sample size with the sample size calculated using the formula in Appendix A.)

Printout Format
100% of records selected will only print the report for the class selected. The audit printout will print additional person details. However neither show details of any relevant Detained reports i.e. those that post-date the Wanted/Missing report.

Printout Order
The printout is in 4 figure PNC code groupings and the records within these groupings may be arranged chronologically or alphabetically.

Impending Prosecution

A printout is available for all i.e. (100%) Impending Prosecution reports owned by a force by 2 figure PNC code.
Selection is possible by 4 figure PNC code.

A randomly selected audit printout is available. (Warning- the formula used may not be the recommended formula stated at Appendix A, and may result in a statistically invalid sample. The sample size provided by HDC should be confirmed as correct by comparing the given sample size with the sample size calculated using the formula in Appendix A.)

Warning Signals

A printout is available for all (i.e. 100%) Warning Signals owned by a force, by 2 figure PNC code.

Three change requests have been made:

-That selection be possible by 4 figure PNC code.
-That selection be possible by type of warning signal.
-That a randomly selected audit printout be made available.

Printout Order
The printout is in 4 figure PNC code groupings and the records within these groupings may be arranged chronologically or alphabetically.

Transaction Log

The #TE transaction gives a flexible search and printout option. All forces can carry out the #TE locally; Data Control can also carry out off-line transaction logs (UT 500 J) for all force terminals for the last eleven months. This can be restricted to a single terminal or time period if required.

Annex H1

Audit Working Papers

Audit of:
Lead Auditor:
Audit Dates:

Ref:	Activity	Completed

Annex H2

Urgent Matters / Brought Forward

Audit of:
Lead Auditor:
Audit Dates:

Ref	Urgent Matters / Brought Forward	Completed
	This section highlights points resulting from the previous audit, or which have come to notice since then, which may impact on the current audit.	
	e.g.	
1	At previous audit (May 2005) J Division had inadequate procedures in place to check newly-created records back to originator / source documentation to confirm accuracy. Audit recommendation to introduce new procedures was accepted, to be implemented by October 2005. This has been done. Review: Adequate procedures are now in place – Satisfactory.	

Annex H3

Data Protection Officer Review Sheet

Audit of:
Lead Auditor:
Date:
Reviewed By:

Ref	Review Comments	Reply
	This section is a part of the audit management process, to enable the DPO to comment on matters contained in the file which require clarification or further information. It also provides evidence that the file has been subject to quality review.	
	e.g.	
1	**Record Validation** You have indicated that new procedures are in place to validate records, but the file contains no reference to what these procedures entail. Please provide an outline of the new procedures.	Now attached @ Encl. 3.x

Annex H4

AUDIT CONTROL SHEET

Audit of:
Lead Auditor:
Audit Dates:

Audit Phase	Milestone	Audit Timeline (BELOW ARE EXAMPLES ONLY)	Target Completion Date	Actual Completion Date	Reviewed By
Planning	Risk Assessment Completed	- 4 weeks			
	Liaison Letter sent	- 4 weeks			
	Initial meeting with owner	- 4 weeks			
	Terms of reference drafted	- 3 weeks			
	Process mapping	- 2 weeks			
	Terms of Reference Agreed	- 2 weeks			
	Sample identified and requested	- 2 weeks			
	Audit Programme Completed	- 1 weeks			
Execution	Interviews Held	0			
	Audit Tests Undertaken	0			
	Results analysis	+ 1 week			
	Closing meeting with owner	+ 1 week			
Reporting	Draft Report Completed	+ 3 weeks			
	Consultation Phase	+ 6 weeks			
	Final Report Distributed	+ 7 weeks			
	Actions Updated on spreadsheet	+ 7 weeks			

Annex H5

Audit Test Matrix

Audit Test Ref	File Reference	Name	PNCID	No Error	1	2	3	4	5	Major	Inter	Minor	Comments / Findings / Description of error.

Note:

The columns to the left of the matrix only contain sufficient information for the record to be identified. An auditor may wish to add, delete or rename columns according to own requirements.

For ease of counting, cataloguing and analysing results auditors might find that the Audit Test Matrix is best created in a Spreadsheet format rather than a Word format.

A cross in a column under 'No Error' would indicate that the Audit Test for the specific sample was successful and that no error was identified.

A cross in one of the columns '1 – 5' would indicate that a specific test has been failed. A sample case can fail more than one test. If this is true then additional columns would have to be created. For each test failure the auditor would also place a cross on the 'Major, Inter or Minor' column and would substantiate the fail in the 'Comments / Findings / Description of error' column.

Annex H6

Supporting Documentation

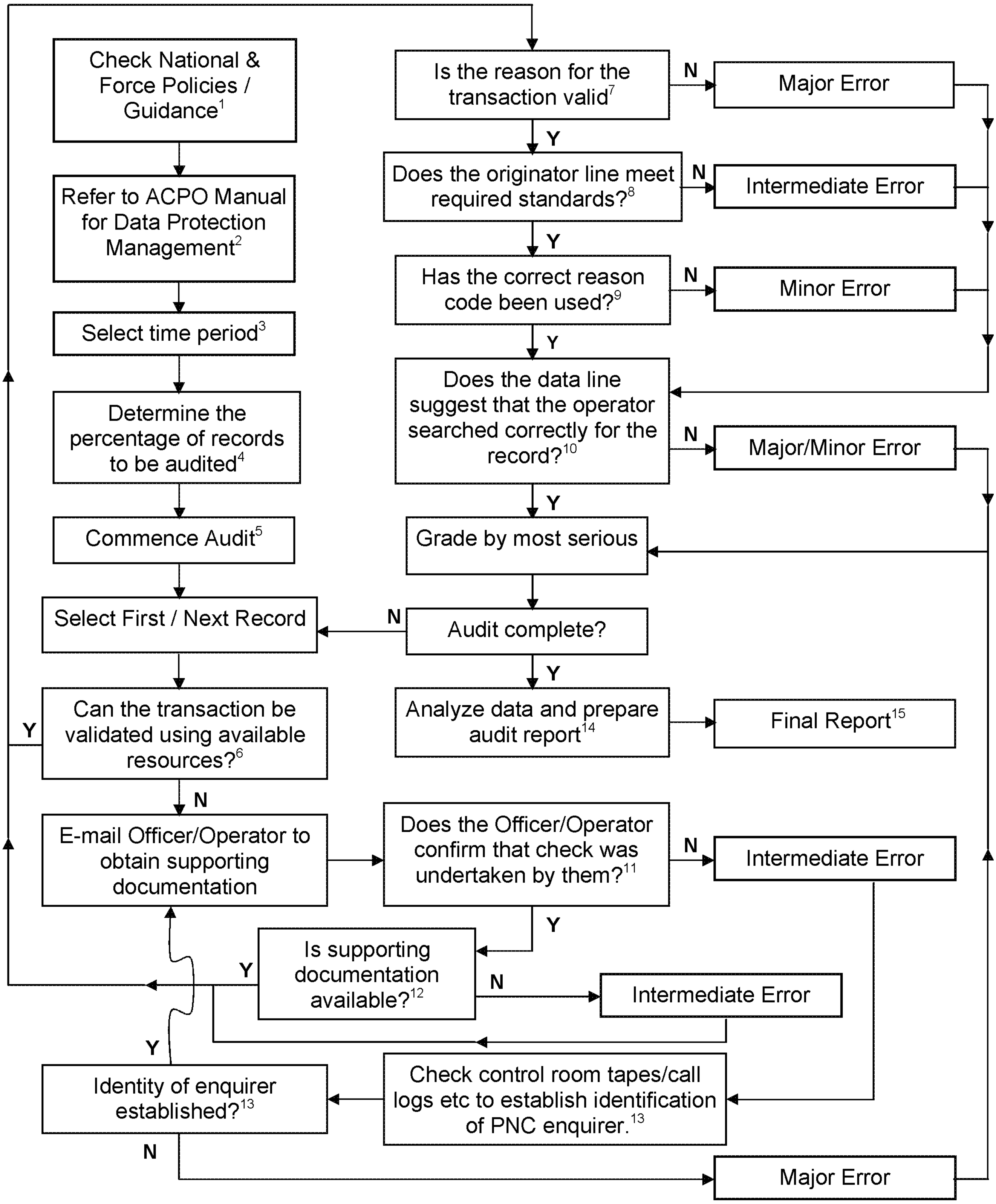
Audit of:
Lead Auditor:
Date:

Ref	Supporting Documentation	Reviewed
	This is where the auditor would record what Supporting Documentation is required for the audit and when it was reviewed.	
	e.g.	
1	Force Policy	Date
2	PNC Manual	Date
3	Force Procedure	Date
4	ACPO Guidance	Date
5	Previous Audit Report	Date

Audit Toolkits

PNC TRANSACTION AUDIT PROCESS ACTIVITY FLOW CHART

(To be used in conjunction with Reference Guide)


Check National & Force Policies / Guidance[1]
Refer to ACPO Manual for Data Protection Management[2]
Select time period[3]
Determine the percentage of records to be audited[4]
Commence Audit[5]
Select First / Next Record
Can the transaction be validated using available resources?[6]
Y
N
E-mail Officer/Operator to obtain supporting documentation
Is the reason for the transaction valid[7]
N
Major Error
Y
Does the originator line meet required standards?[8]
N
Intermediate Error
Y
Has the correct reason code been used?[9]
N
Minor Error
Y
Does the data line suggest that the operator searched correctly for the record?[10]
N
Major/Minor Error
Y
Grade by most serious
Audit complete?
N
Y
Analyze data and prepare audit report[14]
Final Report[15]
Does the Officer/Operator confirm that check was undertaken by them?[11]
N
Intermediate Error
Y
Is supporting documentation available?[12]
Y
N
Intermediate Error
Check control room tapes/call logs etc to establish identification of PNC enquirer.[13]
Identity of enquirer established?[13]
Y
N
Major Error

PNC TRANSACTION AUDIT PROCESS ACTIVITY FLOW CHART (To be used in conjunction with Activity Flow Chart)

1. **Check National and Force policies/guidance**
   This is to ensure compliance with national circulations, local policy and the guidelines in PNC Manuals, particularly the PNC Manual Volume 1, Chapter 1, Section 7.

2. **Refer to ACPO Manual.**
   To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

3 **Select time period**
   Select a time period to select a sample from, for example, the last three months worth. It should be noted that a #TE will only produce the last 12 months. However, the force PNC Bureau may hold transactions further back than this.

4. **Determine the percentage of records to be audited.**
   The audit sample size should be based on the sample methodology explained in the ACPO Data Protection Audit Manual.

5. **Commence Audit**
   Schedule visits with relevant departments and set time scales.

6. **Can the transaction be validated using available resources?**
   In order to substantiate the reason for the check without contacting the officer, in-force systems should be interrogated. For example, the crime, custody or incident recording systems would provide justification for the transaction.

7. **Is the reason for the transaction valid?**
   Has PNC been misused? If so it is a major error.

8. **Does the originator line meet required standards?**
   As per PNC manual "A minimum of four characters is required, but it is essential that the identity of the person requesting the check, the reason for it and their location are all included."

9. **Has the correct reason code been used?**
   As per the PNC manual, "a 2-character field, the first of which is used to indicate a National Reason Code. Organisations may use the second character to break down the national coding further." If incorrect, this is a minor error.

10. **Does the data line suggest that the operator searched correctly for the record?**
    Has the operator used the incorrect search string? This would only be major error if the search results did not contain the correct record. A slightly misspelled name or incorrect DOB which still hits the correct record is only a minor error.

11. **Does the Officer/Operator confirm that the check was undertaken by them?**
    If they do not, an error has occurred on the originator line, which should contain the correct details of the enquirer. This is an intermediate error at this stage as the enquiry may still be identified through further enquiries.

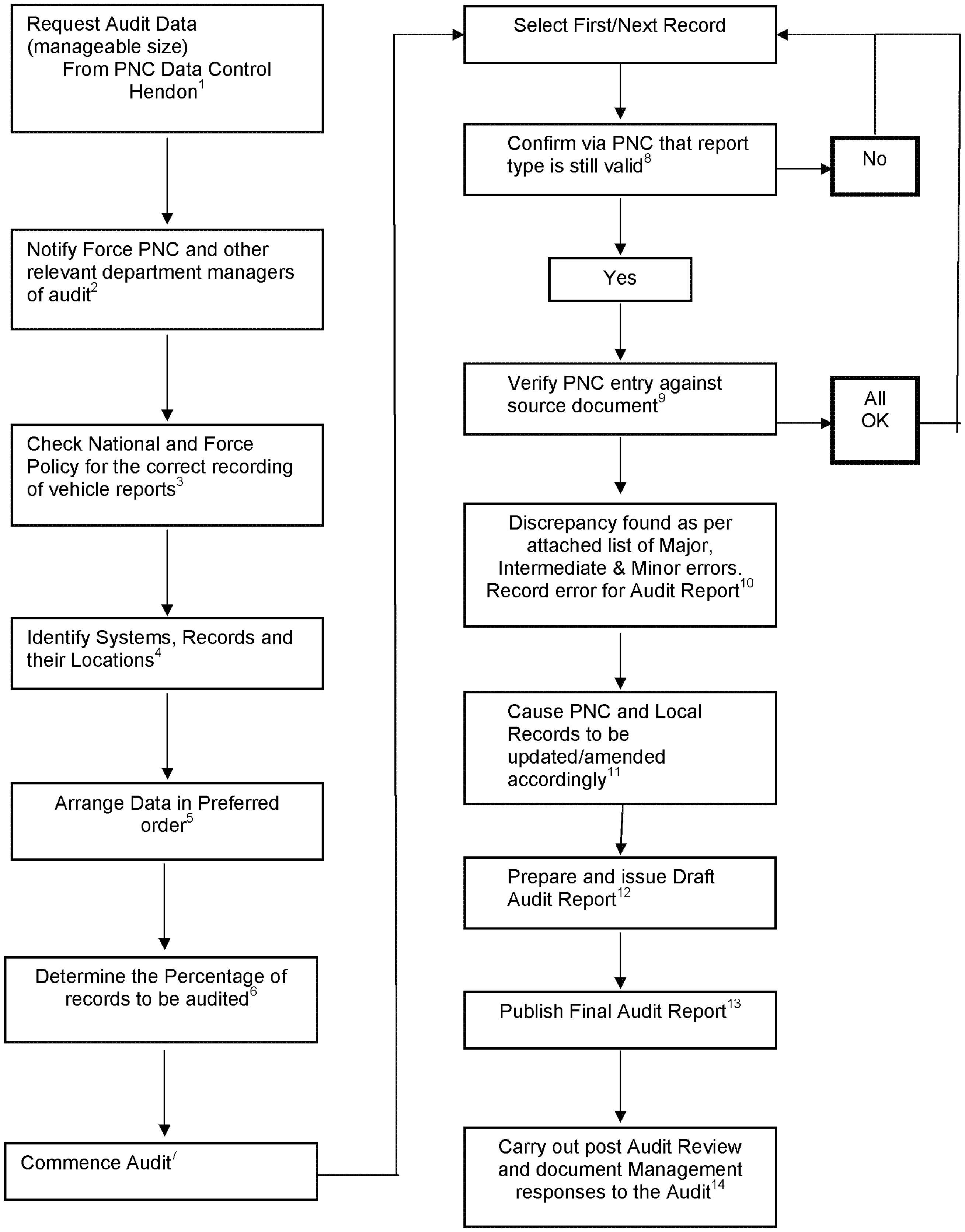
12. **Is supporting documentation available?**
    The officer will have to provide supporting documentation, such as a copy of the pocket note book entry or incident number. If no supporting documentation is available then this is an intermediate error.

13. **Check control room tapes/call logs etc to establish identification of PNC enquirer?**
    If the officer states that they did not requested the check, control room tapes must be checked in order to establish the identity of the enquirer. If this is not established, it is a major error.

14. **Analyse data and prepare audit report**
    Categorise and calculate total errors and percentages. Enter into a chart in order to best present the data. Write an audit report based upon audit findings.

15. **Final Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should include a comprehensive list of errors.

CORRECTION VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)



Request Audit Data (manageable size) From PNC Data Control Hendon[1]

Notify Force PNC and other relevant department managers of audit[2]

Check National and Force Policy for the correct recording of vehicle reports[3]

Identify Systems, Records and their Locations[4]

Arrange Data in Preferred order[5]

Determine the Percentage of records to be audited[6]

Commence Audit[7]

Select First/Next Record

Confirm via PNC that report type is still valid[8]

No

Yes

Verify PNC entry against source document[9]

All OK

Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]

Cause PNC and Local Records to be updated/amended accordingly[11]

Prepare and issue Draft Audit Report[12]

Publish Final Audit Report[13]

Carry out post Audit Review and document Management responses to the Audit[14]

CORRECTION VEHICLE AUDIT PROCESS
REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

CORRECTION VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- **N**o source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Correction report
- Incorrect VRM
- Incorrect or no Force Reference

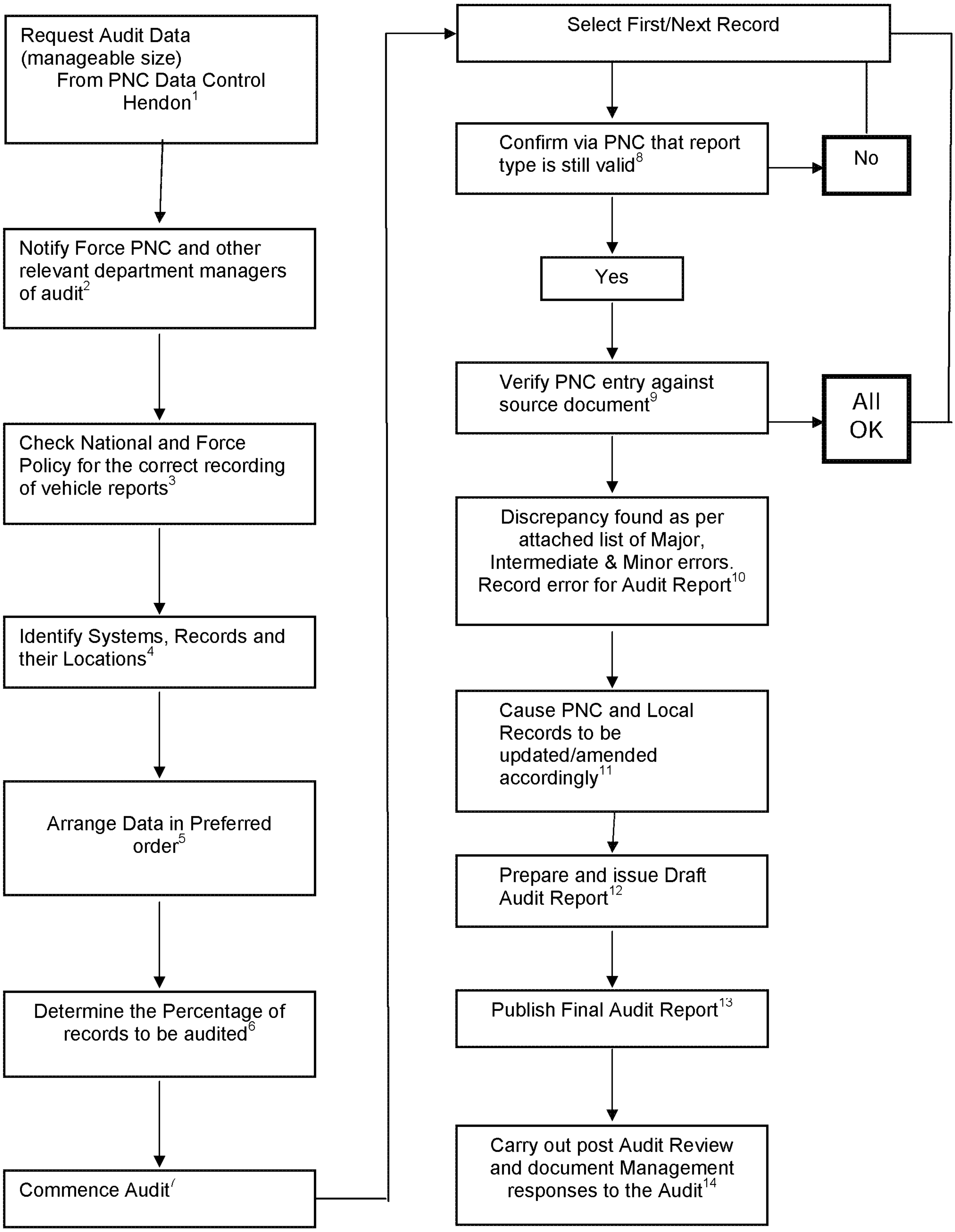
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

DESTROYED VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (manageable size) From PNC Data Control Hendon[1]
Notify Force PNC and other relevant department managers of audit[2]
Check National and Force Policy for the correct recording of vehicle reports[3]
Identify Systems, Records and their Locations[4]
Arrange Data in Preferred order[5]
Determine the Percentage of records to be audited[6]
Commence Audit[7]
Select First/Next Record
Confirm via PNC that report type is still valid[8]
No
Yes
Verify PNC entry against source document[9]
All OK
Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]
Cause PNC and Local Records to be updated/amended accordingly[11]
Prepare and issue Draft Audit Report[12]
Publish Final Audit Report[13]
Carry out post Audit Review and document Management responses to the Audit[14]

DESTROYED VEHICLE AUDIT PROCESS REFERENCE GUIDE (To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

DESTROYED VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- No source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Destroyed report
- Incorrect VRM
- Incorrect or no Force Reference

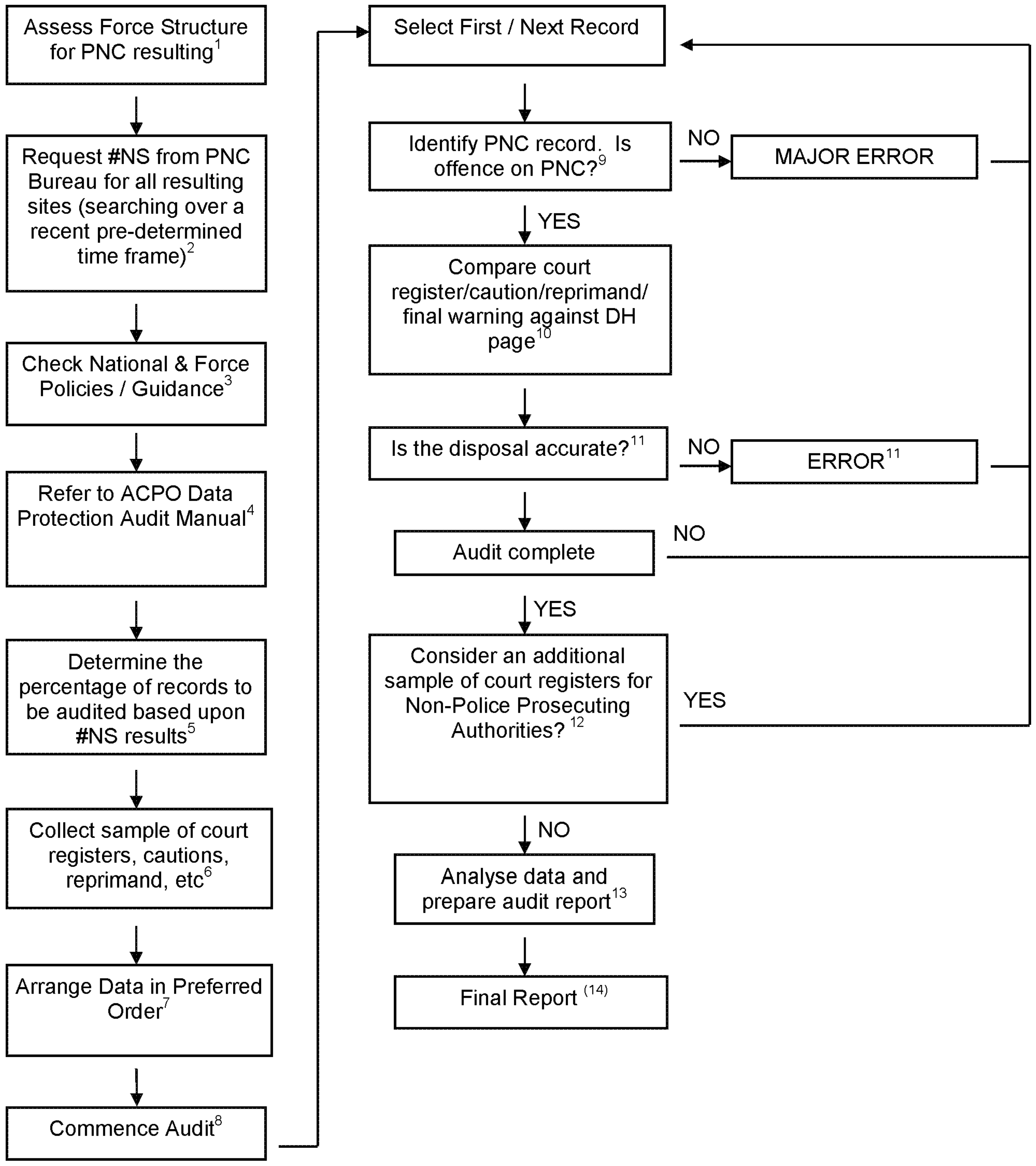
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

DISPOSAL HISTORY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Assess Force Structure for PNC resulting[1]
Request #NS from PNC Bureau for all resulting sites (searching over a recent pre-determined time frame)[2]
Check National & Force Policies / Guidance[3]
Refer to ACPO Data Protection Audit Manual[4]
Determine the percentage of records to be audited based upon #NS results[5]
Collect sample of court registers, cautions, reprimand, etc[6]
Arrange Data in Preferred Order[7]
Commence Audit[8]
Select First / Next Record
Identify PNC record. Is offence on PNC?[9]
NO
MAJOR ERROR
YES
Compare court register/caution/reprimand/ final warning against DH page[10]
Is the disposal accurate?[11]
NO
ERROR[11]
Audit complete
NO
YES
Consider an additional sample of court registers for Non-Police Prosecuting Authorities? [12]
YES
NO
Analyse data and prepare audit report[13]
Final Report (14)

DISPOSAL HISTORY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Activity Flow Chart)

1. **Assess Force Structure for PNC resulting.**
   How many resulting sites are there?

2. **Request #NS from PNC Bureau for all resulting sites (searching over a recent pre-determined time frame).**
   The #NS transaction will provide statistics on the number of results entered onto the DH page. It will also break down the type of results into court, Caution, Reprimand, Final Warning, NFA etc.
   It is necessary to search using a time frame such one month or a whole year, in order to assess current performance of staff entering results.

3. **Check National and Force policies/guidance**
   This is to ensure compliance with the guidelines in PNC Manual for stolen property, other national circulations and local policy.

4. **Refer to ACPO Manual.**
   To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Determine the percentage of records to be audited based upon #NS results.**
   The audit sample size should be calculated using the sample methodology described in the ACPO Data Protection Audit Manual.

6. **Collect sample of court registers, cautions, reprimands, etc.**
   If court registers are not held electronically then visit relevant locations in order to copy required sample of registers, caution, etc.
   Note that offences must be recordable.

7. **Arrange data in preferred order**
   Sort the data into your preferred audit sequence e.g. by division or court.

8. **Commence Audit**
   Ensure that access to PNC terminal is available in order to undertake the audit. Set time scales.

9. **Identify PNC record. Is offence on PNC?**
   Search PNC using the name and date of birth, if offence not on the PNC record as an impending or disposal then mark as a major error.

10. **Compare court register/caution/reprimand/ final warning against DH page.**
    If the entry on PNC does not accurately reflect what is recorded on the source document then refer to error classifications.

11. **Is the disposal accurate?**
    Refer to error classifications.

12. **Consider additional sample of court registers for Non-Police Prosecuting Authorities?**
    If these results are entered onto PNC by your force then it maybe necessary to obtain an additional sample of court registers for offences that belong to external authorities.
    For example:
    Selling for human consumption food which fails to comply with food safety requirements
    Food Safety Act 1990 section 8(a)

    Delay or open postal packet or mailbag
    Postal Services Act 2000 section 83(1) + s.83(6)

    Attempting to travel without paying rail fare
    Regulation of Railways Act 1889 section 5(3)(a)

    Contravening condition of waste management licence
    Environmental Protection Act 1990 section 33(6)

    Permitting act resulting in cruelty to animal
    Protection of Animals Act 1911 section 1

    Making a false statement or representation in order to obtain benefit or payment
    Social Security Administration Act 1992 section 112(1)(a)

    Supplying goods to which false trade description applied
    Trade Descriptions Act 1968 section 1(1)(b)

    Breach of community service order
    Criminal Justice Act 1991 section 14

13. **Analyse data and prepare audit report**
    Categorise and calculate total errors and percentages. Enter into a chart in order to best present the data. Write an audit report based around audit findings.

14. **Final Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should include a comprehensive list of errors.

DISPOSAL HISTORY AUDIT
ERROR CLASSIFICATION

MAJOR

- Recordable offence not on PNC
- Non-Recordable Offence not added to composite
- Incorrect offence
- Refer to court case not added to record
- Incorrect sentence (disposal date) date
- Offence incorrect
- Disqualification period incorrect
- Imprisonment Incorrect/Missing
- Consecutive/Concurrent Incorrect
- Attempt not added to offence

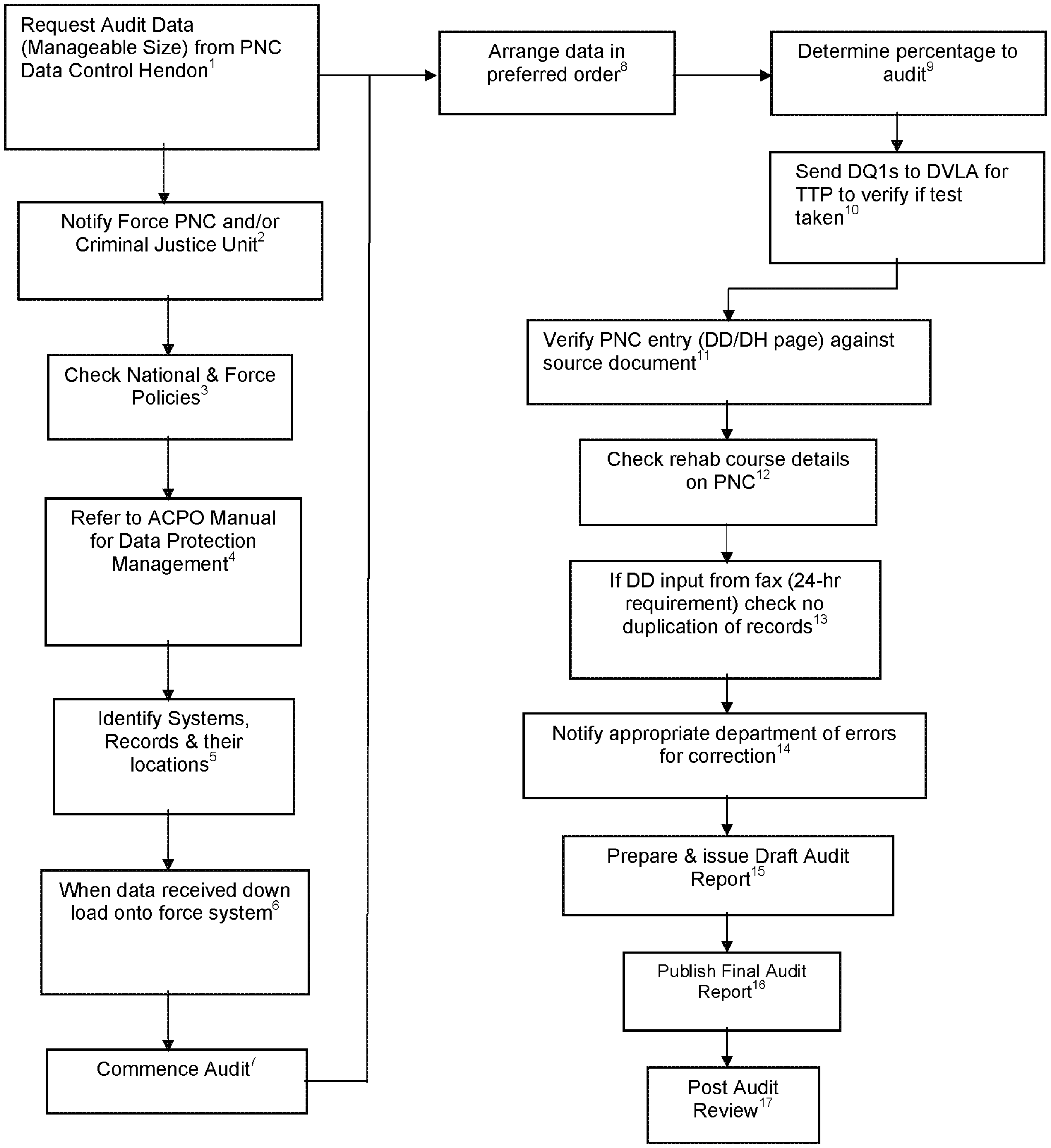
INTERMEDIATE

- Court incorrect
- Name and DOB incorrect
- Detained until court rises not added to result

MINOR

- Endorsement points not added
- Compensation entered as costs
- Compensation not added/incorrect
- Forfeiture (weapon not stated)
- Community Service order not added/incorrect
- Probation Order not added/incorrect
- Conditional discharge not entered/incorrect

DISQUALIFIED DRIVERS FLOWCHART
(To be used in conjunction with Reference Guide)



Request Audit Data (Manageable Size) from PNC Data Control Hendon[1]

Notify Force PNC and/or Criminal Justice Unit[2]

Check National & Force Policies[3]

Refer to ACPO Manual for Data Protection Management[4]

Identify Systems, Records & their locations[5]

When data received down load onto force system[6]

Commence Audit[7]

Arrange data in preferred order[8]

Determine percentage to audit[9]

Send DQ1s to DVLA for TTP to verify if test taken[10]

Verify PNC entry (DD/DH page) against source document[11]

Check rehab course details on PNC[12]

If DD input from fax (24-hr requirement) check no duplication of records[13]

Notify appropriate department of errors for correction[14]

Prepare & issue Draft Audit Report[15]

Publish Final Audit Report[16]

Post Audit Review[17]

DISQUALIFIED DRIVERS AUDIT
REFERENCE GUIDE
(To be used in coniunction with Activitv Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable sizes. E.g. by Division or District**
   Nominated officers either must make requests by fax or e-mail to PITO at Hendon.

2. **Notify Force PNC and/or Criminal Justice Unit**
   Courtesy call in order to inform PNC bureau and/or CJU Managers an audit will be taking place.

3. **Check National and Force Policies**
   What are the guidelines for the recording of disqualified drivers?

4. **Refer to ACPO Manual**
   To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Identify Systems, Records and their Location**
   Systems and records required in order to conduct the audit are: PNC, local Force system(s), Court registers and DVLA records

6. **When Received, Download Data on to Force System**
   Transfer data from the disk received from Hendon onto Force system, save e-mail onto relevant disc drive. Not applicable if paper records requested.

7. **Commence Audit**
   Confirm schedule of visits.

8. **Arrange Data in Preferred Order**
   Sort the data into your audit sequence - e.g. Till Test Passed (TTP), standard Disqualified

9. **Determine Percentage of Records to Audit**
   100% or statistically valid sample.

10. **Send Forms DQ1 to DVLA**
    For sentences, which impose a disqualification to run TTP, the driver record should be checked to establish whether a test has been taken and passed. Compare DVLA printout against PNC entry.

11. **Check against Source Document**
    If Court Register unavailable, obtain verification from Magistrates Court (or Public Records office) or Crown Courts.

12. **Check Rehab Course Details on PNC**
    If Rehabilitation Course offered as an incentive to reduce disqualification period, check DH page and verify certificate of attendance. If attended check the reduction in disqualified period is correctly reflected.

13. **Duplicate Records**
    Records created from faxed information from courts (24hr requirement to input disqualification) need to be verified to prevent duplication of records.

14. **Errors**
    When errors occur, notify appropriate department for correction.

15. **Draft Audit Report**
    A draft report should be prepared to include a list of errors; the overall error rate; method of audit; conclusion and recommendations and an executive summary (see ACPO Manual). Send to relevant managers for their comments.

16. **Final Report**
    On receipt of comments a final report should be prepared and sent to the relevant persons.

17. **Post Audit Review**
    Carry out Post Audit Review within schedule determined by report.

DISQUALIFIED DRIVERS ERROR CLASSIFICATION

MAJOR

- Not disqualified until test passed
- No longer valid – test passed
- Unable to substantiate record within 24 hours
- Disqualification date incorrect (interim imposed/rehab course taken)
- Incorrect or missing information on DH Page (Recordable offences only)
- Duplicated entries

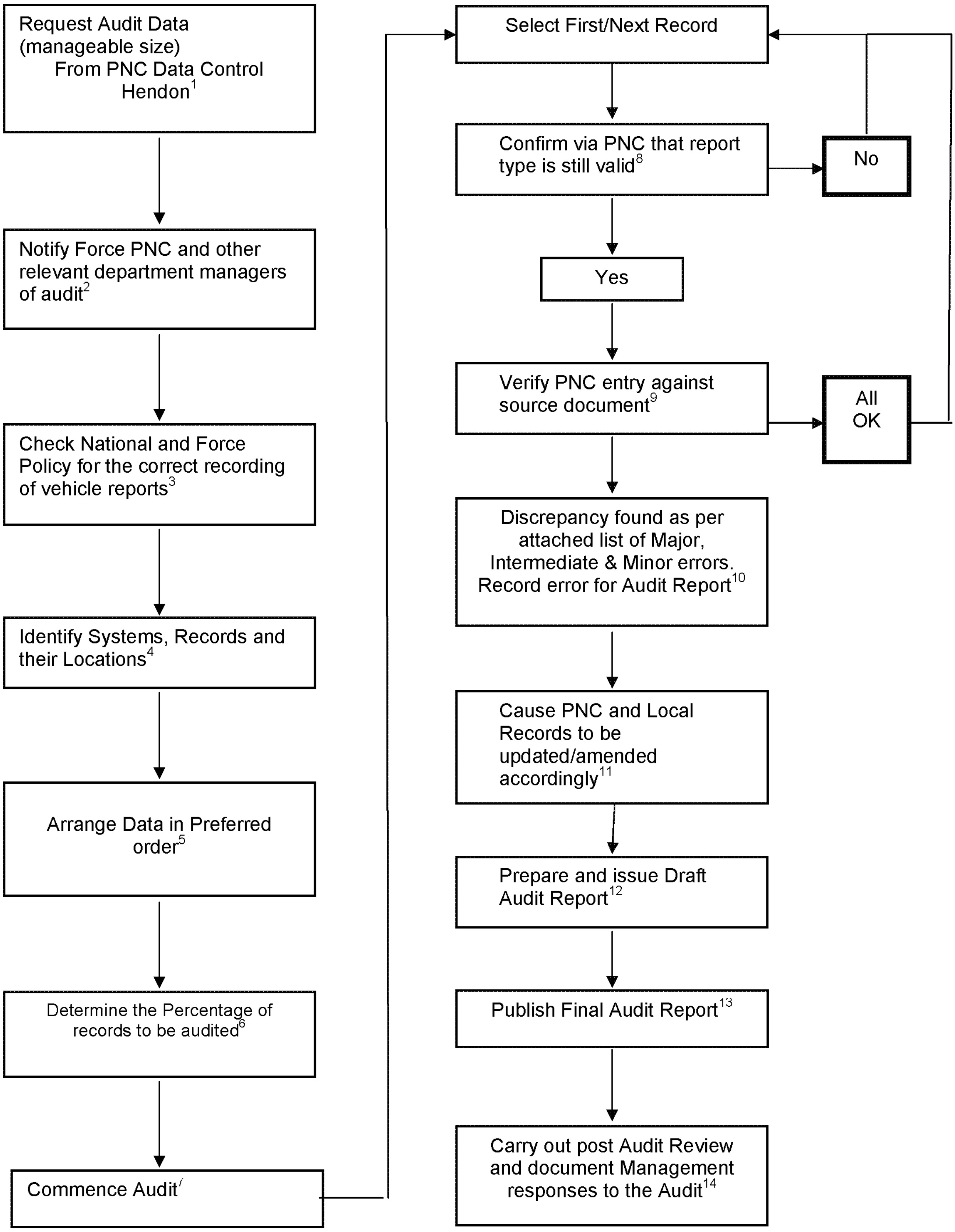
INTERMEDIATE

- Incorrect Force Reference (could impede location of paperwork)
- Differing Court information between DD/DH Page
- Unable to locate record within 30 minutes

MINOR

- Incorrect data (spelling etc)

FOUND VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide


Request Audit Data (manageable size) From PNC Data Control Hendon[1]
Notify Force PNC and other relevant department managers of audit[2]
Check National and Force Policy for the correct recording of vehicle reports[3]
Identify Systems, Records and their Locations[4]
Arrange Data in Preferred order[5]
Determine the Percentage of records to be audited[6]
Commence Audit[7]
Select First/Next Record
Confirm via PNC that report type is still valid[8]
No
Yes
Verify PNC entry against source document[9]
All OK
Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]
Cause PNC and Local Records to be updated/amended accordingly[11]
Prepare and issue Draft Audit Report[12]
Publish Final Audit Report[13]
Carry out post Audit Review and document Management responses to the Audit[14]

FOUND VEHICLE AUDIT PROCESS REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
   This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
   Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
   Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
   This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
   Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
   When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
   Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
    Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
    Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
    Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
    After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

FOUND VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- **N**o source Document
- Vehicle Recovered **N**ot Cancelled
- Wrong Report Type e.g. Lost/Stolen report instead of Found report
- Incorrect VRM
- Incorrect or no Force Reference

INTERMEDIATE

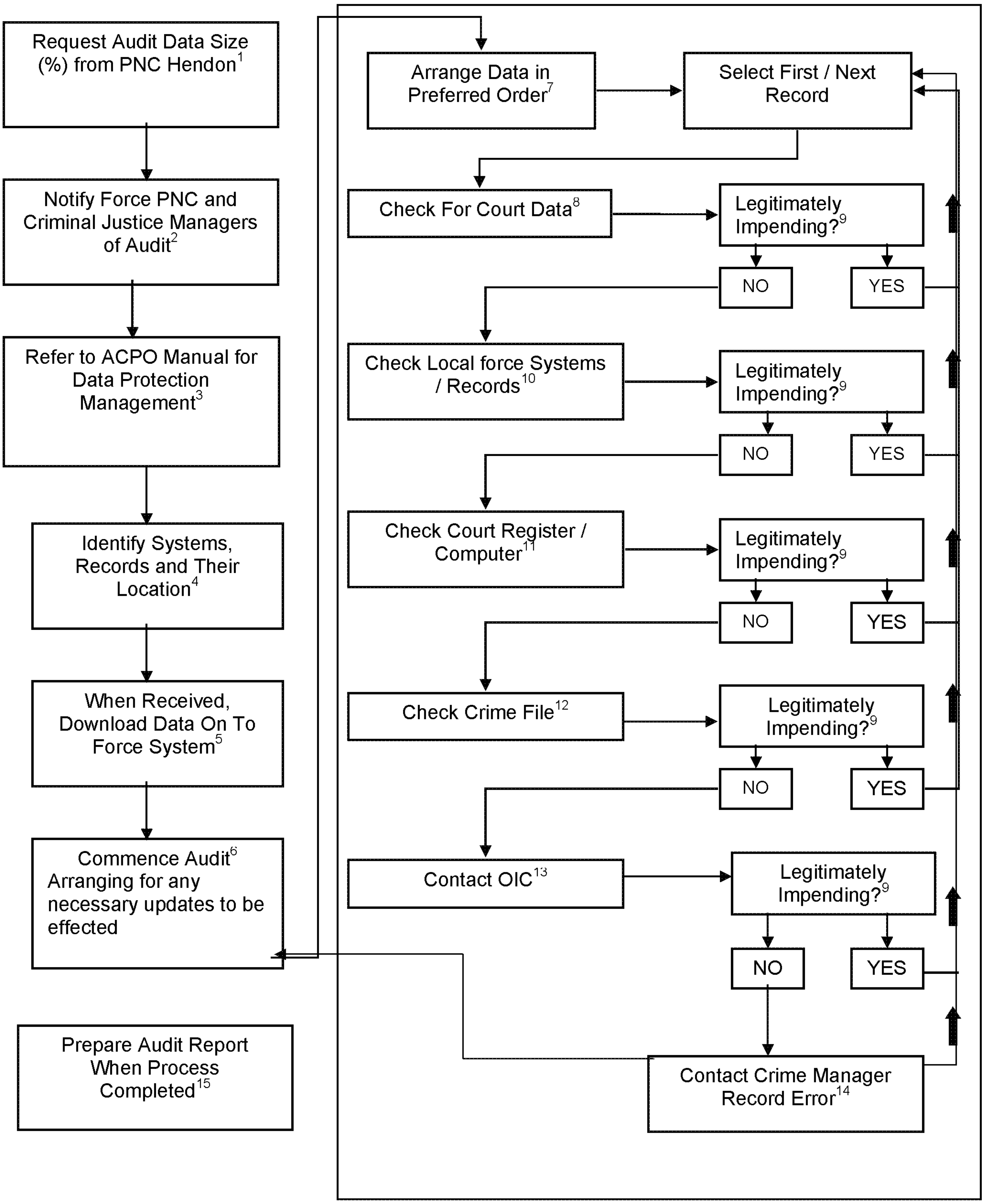
- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

For Distribution to CPs

IMPENDING PROSECUTION AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)



Request Audit Data Size (%) from PNC Hendon[1]
Notify Force PNC and Criminal Justice Managers of Audit[2]
Refer to ACPO Manual for Data Protection Management[3]
Identify Systems, Records and Their Location[4]
When Received, Download Data On To Force System[5]
Commence Audit[6] Arranging for any necessary updates to be effected
Prepare Audit Report When Process Completed[15]
Arrange Data in Preferred Order[7]
Select First / Next Record
Check For Court Data[8]
Legitimately Impending?[9]
NO
YES
Check Local force Systems / Records[10]
Legitimately Impending?[9]
NO
YES
Check Court Register / Computer[11]
Legitimately Impending?[9]
NO
YES
Check Crime File[12]
Legitimately Impending?[9]
NO
YES
Contact OIC[13]
Legitimately Impending?[9]
NO
YES
Contact Crime Manager Record Error[14]

IMPENDING PROSECUTION AUDIT PROCESS REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data Size (%) from PNC Hendon**
   Nominated officers, either must make requests by fax or e-mail, to PITO at Hendon.

2. **Notify Force PNC and Criminal Justice Managers of Audit**
   Courtesy call in order to inform PNC and CJD managers that audit will be taking place.

3 **Refer to ACPO Manual**
   To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

4. **Identify Systems, Records and Their Location**
   Systems and records required in order to conduct the audit are PNC; Local Force System(s); Crime Files; Court Registers/ Computer Records.

5. **When Received, Download Data On To Force System**
   Transfer data from disc received from Hendon onto Force system, save e-mail onto relevant disc drive.

6. **Commence Audit**
   Confirm schedule of visits with CJD Managers.
   Arrange for any updates to be effected.

7. **Arrange Data In Preferred Order**
   Sort the data into your preferred audit sequence - e.g. alphabetical, crimes by date or crime number. Start at Step 8 for each record.

8. **Check For Court Data**
   To establish whether the record is an outstanding IP and to match data from the crime file and PNC record.

9. **Is It Legitimately Impending?**
   Check the date of Court appearance, if not shown or Court date has passed, move on to next step.

10. **Check Local Force Systems / Records**
    Local systems & records may show current IP situation e.g. file is with CPS. If no further information can be gained move on to next step.

11. **Check Court Register / Computer**
    The Court register may be able to provide either an updated court date or information as to whether the case is still being continued. If you have access to the Court computer system this can be checked in order to ascertain if a next appearance date has been entered. If no further information can be gained move on to next step.

12. **Check Crime File**
    The crime file may well be able to provide details about the current stage the case has reached. If not, continue to next step.

13. **Contact OIC**
    The OIC may be able to inform you of the current situation.

14. **Contact Crime Manager / Record Error**
    Once confirmed that a record is no longer impending the appropriate Crime Manager should be informed and an error record created for the audit report.

15. **Prepare Audit Report**
    The report should contain a list of errors; the overall error rate; method of audit; conclusion and recommendations and an executive summary. (See ACPO Manual).

IMPENDING PROSECUTION AUDIT
ERROR CLASSIFICATION

MAJOR

- Court result received but not resulted
- Partly/Incorrectly resulted cases
- Incorrect name details
- No supporting source document
- Caution certificate missing from crime file
- NFA cases not updated on PNC
- Record not updated to show disposal etc
- Variations of bail and conditions not updated

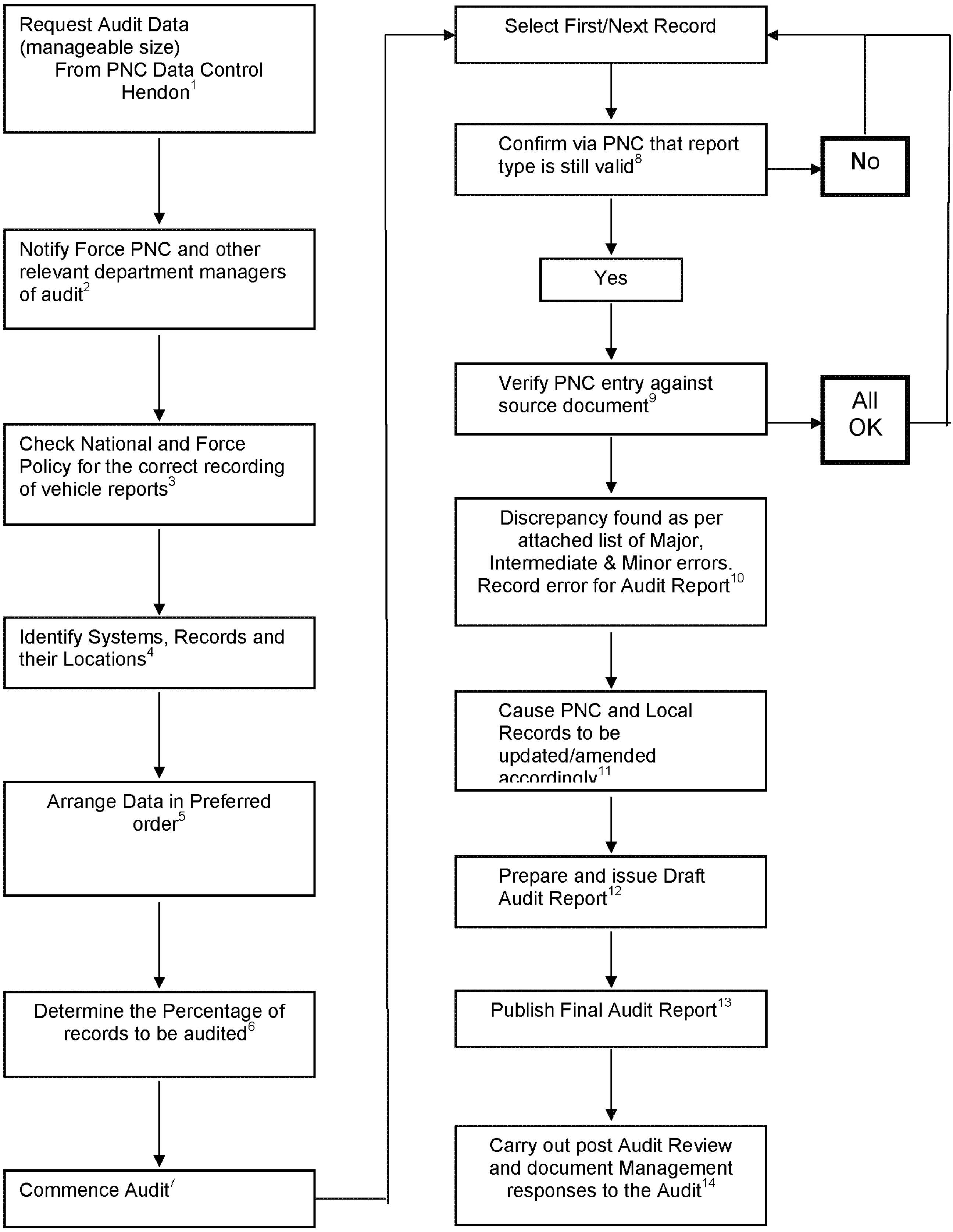
INTERMEDIATE

- Missing documentation not found within 30 minutes but located within 24 hours

MINOR

- Spelling mistakes

INFORMATION VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (manageable size) From PNC Data Control Hendon[1]
Notify Force PNC and other relevant department managers of audit[2]
Check National and Force Policy for the correct recording of vehicle reports[3]
Identify Systems, Records and their Locations[4]
Arrange Data in Preferred order[5]
Determine the Percentage of records to be audited[6]
Commence Audit[7]
Select First/Next Record
Confirm via PNC that report type is still valid[8]
No
Yes
Verify PNC entry against source document[9]
All OK
Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]
Cause PNC and Local Records to be updated/amended accordingly[11]
Prepare and issue Draft Audit Report[12]
Publish Final Audit Report[13]
Carry out post Audit Review and document Management responses to the Audit[14]

INFORMATION VEHICLE AUDIT PROCESS
REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
   This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
   Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
   Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
   This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
   Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
   When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
   Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
    Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
    Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
    Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
    After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

INFORMATION VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- No source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Information report
- Incorrect VRM
- Incorrect or no Force Reference
- Report no longer valid e.g. missing person located but report on vehicle not cancelled.
- Report entered for a non-policing purpose e.g. civil proceedings

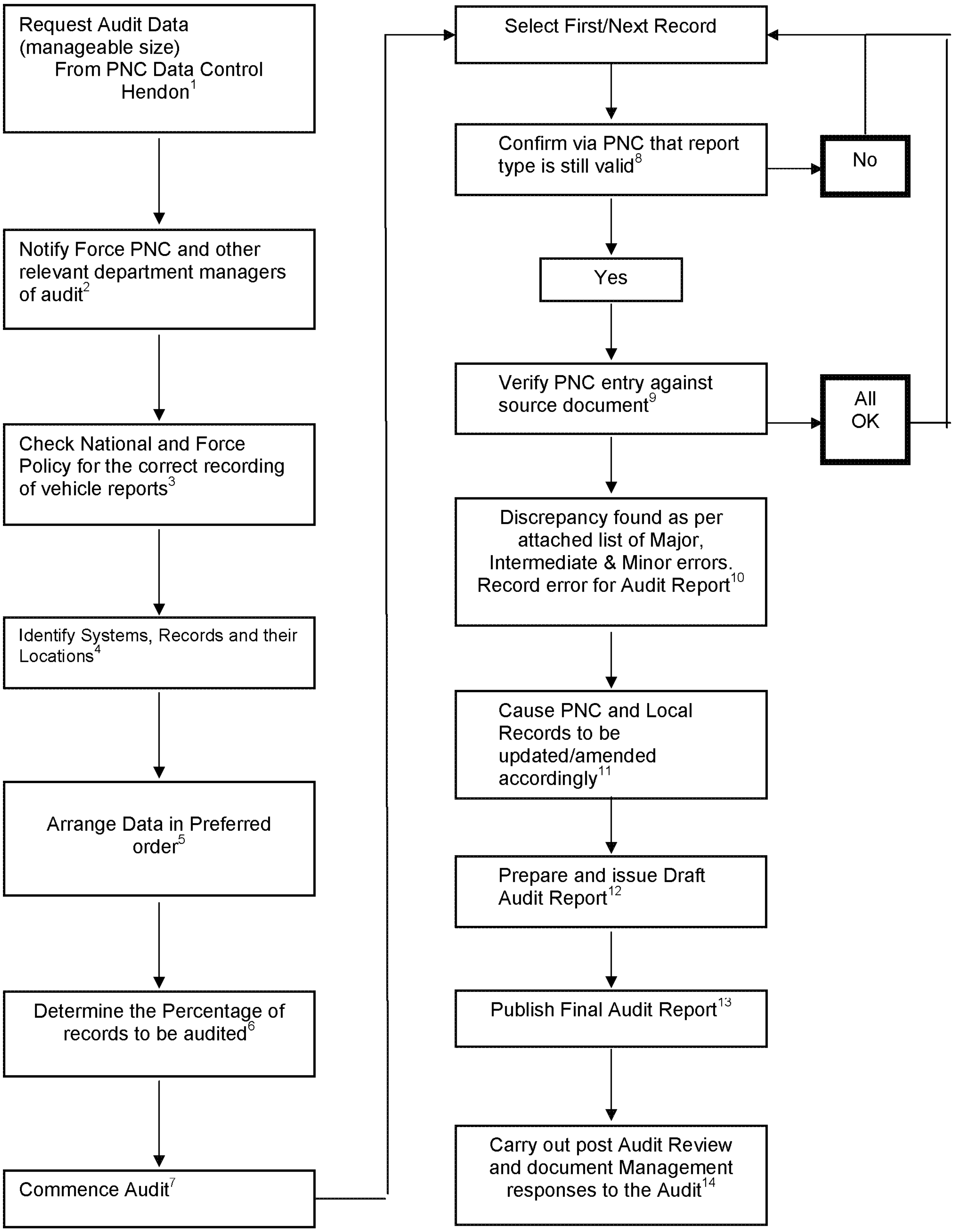
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

LOST/STOLEN VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)



Request Audit Data (manageable size) From PNC Data Control Hendon[1]

Notify Force PNC and other relevant department managers of audit[2]

Check National and Force Policy for the correct recording of vehicle reports[3]

Identify Systems, Records and their Locations[4]

Arrange Data in Preferred order[5]

Determine the Percentage of records to be audited[6]

Commence Audit[7]

Select First/Next Record

Confirm via PNC that report type is still valid[8]

No

Yes

Verify PNC entry against source document[9]

All OK

Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]

Cause PNC and Local Records to be updated/amended accordingly[11]

Prepare and issue Draft Audit Report[12]

Publish Final Audit Report[13]

Carry out post Audit Review and document Management responses to the Audit[14]

LOST/STOLEN VEHICLE AUDIT PROCESS REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
   This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
   Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
   Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
   This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
   Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
   When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
   Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
    Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
    Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
    Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
    After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

LOST/STOLEN VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- **N**o source Document
- Vehicle Recovered **N**ot Cancelled
- Wrong Report Type e.g. Information report instead of Lost/Stolen report
- Incorrect VRM
- Incorrect or no Force Reference

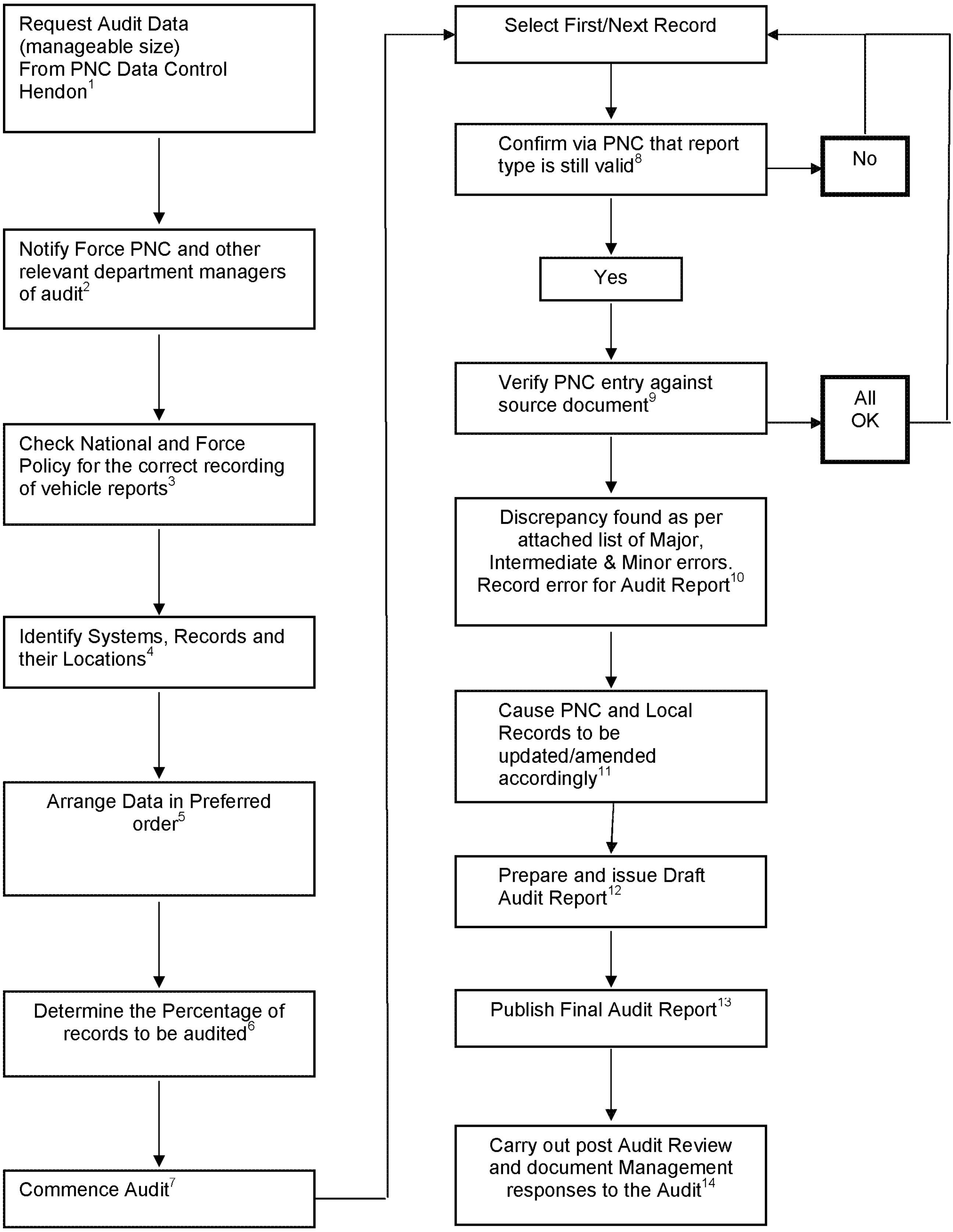
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

REMOVED VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (manageable size) From PNC Data Control Hendon[1]
Notify Force PNC and other relevant department managers of audit[2]
Check National and Force Policy for the correct recording of vehicle reports[3]
Identify Systems, Records and their Locations[4]
Arrange Data in Preferred order[5]
Determine the Percentage of records to be audited[6]
Commence Audit[7]
Select First/Next Record
Confirm via PNC that report type is still valid[8]
No
Yes
Verify PNC entry against source document[9]
All OK
Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]
Cause PNC and Local Records to be updated/amended accordingly[11]
Prepare and issue Draft Audit Report[12]
Publish Final Audit Report[13]
Carry out post Audit Review and document Management responses to the Audit[14]

REMOVED VEHICLE AUDIT PROCESS REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
   This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
   Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
   Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
   This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
   Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
   When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
   Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
    Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
    Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
    Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
    After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

REMOVED VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- No source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Removed report
- Incorrect VRM
- Incorrect or no Force Reference

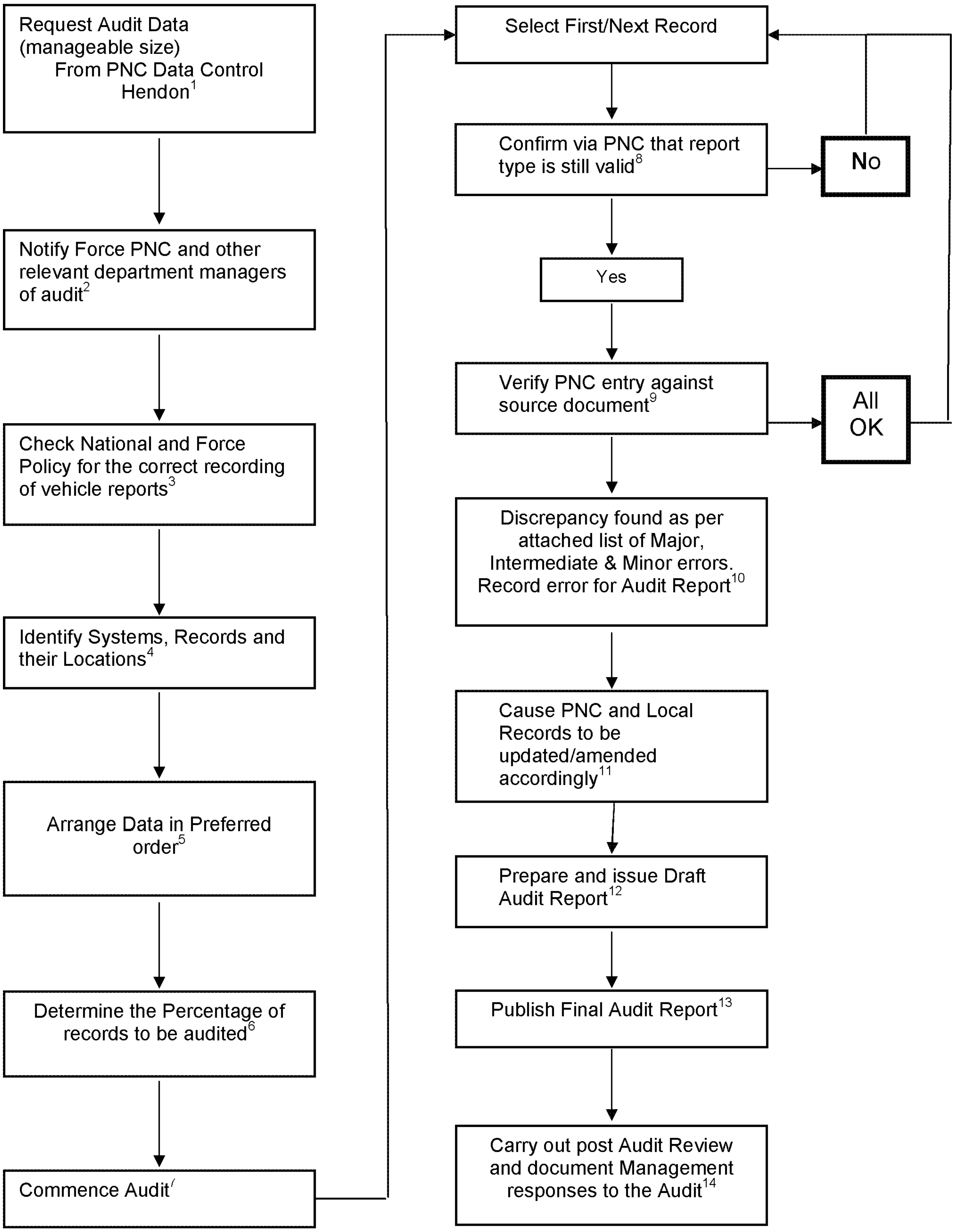
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

RESTRICTED VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)



Request Audit Data (manageable size) From PNC Data Control Hendon[1]

Notify Force PNC and other relevant department managers of audit[2]

Check National and Force Policy for the correct recording of vehicle reports[3]

Identify Systems, Records and their Locations[4]

Arrange Data in Preferred order[5]

Determine the Percentage of records to be audited[6]

Commence Audit[7]

Select First/Next Record

Confirm via PNC that report type is still valid[8]

Verify PNC entry against source document[9]

Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]

Cause PNC and Local Records to be updated/amended accordingly[11]

Prepare and issue Draft Audit Report[12]

Publish Final Audit Report[13]

Carry out post Audit Review and document Management responses to the Audit[14]

RESTRICTED VEHICLE AUDIT PROCESS
REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

RESTRICTED VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- No source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Restricted report
- Incorrect VRM
- Incorrect or no Force Reference
- Report no longer valid e.g. missing person located but report on vehicle not cancelled.

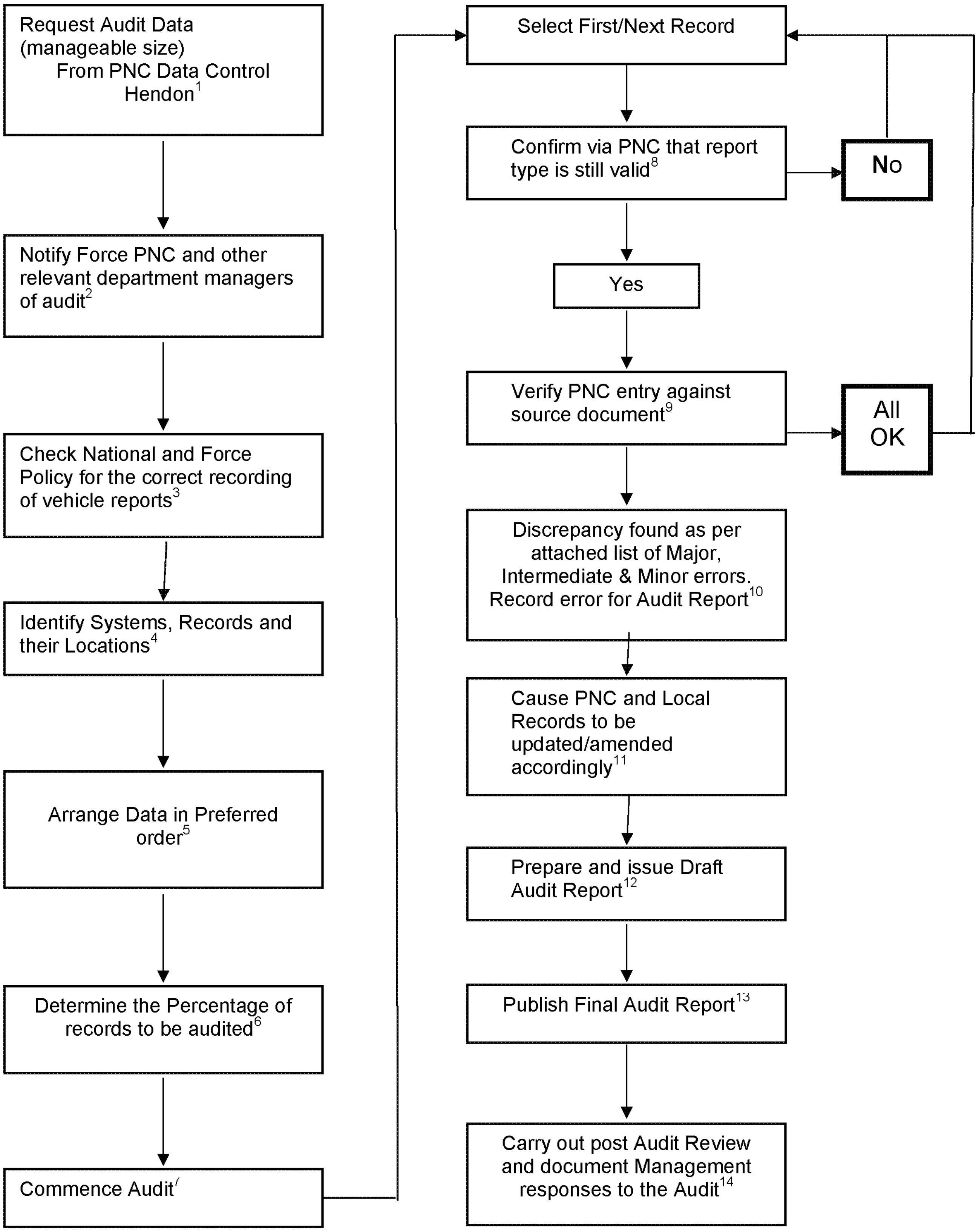
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

SEEN VEHICLE AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (manageable size) From PNC Data Control Hendon[1]
Notify Force PNC and other relevant department managers of audit[2]
Check National and Force Policy for the correct recording of vehicle reports[3]
Identify Systems, Records and their Locations[4]
Arrange Data in Preferred order[5]
Determine the Percentage of records to be audited[6]
Commence Audit[7]
Select First/Next Record
Confirm via PNC that report type is still valid[8]
No
Yes
Verify PNC entry against source document[9]
All OK
Discrepancy found as per attached list of Major, Intermediate & Minor errors. Record error for Audit Report[10]
Cause PNC and Local Records to be updated/amended accordingly[11]
Prepare and issue Draft Audit Report[12]
Publish Final Audit Report[13]
Carry out post Audit Review and document Management responses to the Audit[14]

SEEN VEHICLE AUDIT PROCESS
REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable size** e.g. by Division or District or record types. Requests must be made by nominated officer by fax or email to the PNC Service Desk (020 8358 5050) for the attention of Data Control at Hendon.

2. **Notify appropriate department(s) of the audit** e.g. Force PNC, the Administrative office holding the original paperwork e.g. CJU, PNC Cabinet.

3. **Check National and Force Policies/Procedures.**
This is to ensure compliance with the guidelines in the PNC Manual for vehicle reports, and local Force policy and procedures.

4. **Identify Systems, Records and their location**.
Is the audit to be just of PNC or are local systems to be part of the audit.

5. **Arrange the Data in preferred order**.
Sort the data into your audit sequence e.g. Lost/Stolen, Found, Information etc.

6. **Determine the percentage of the records to be part of the audit**.
This can be achieved by utilising the sample calculation given in the ACPO Audit Manual.

7. **Commence Audit**
Confirm schedule of visits with the relevant department managers.

8. **Check PNC entry is still circulated**
When the audit commences check PNC entry to establish the vehicle report is still circulated.

9. **Verify PNC against source document**
Check that the source document is available and compare the accuracy of the PNC circulation.

10. **Any Discrepancy**
Record any discrepancies that are found for inclusion on the audit report.

11. **Cause PNC and Local Records to be amended/updated**
Contact the relevant department with a list of the errors for correction.

12. **Prepare and Issue Draft Audit Report**
The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should also include a comprehensive list of errors. Send the report to the relevant managers for their comments.

13. **Final Report**
Prepare and publish the final Audit Report. It may have been necessary to amend the draft report following any replies received from the draft report reading.

14. **Audit Review**
After appropriate time period carry out a post audit review of recommendation and follow up to management responses.

SEEN VEHICLE AUDIT PROCESS
ERROR CLASSIFICATION

MAJOR

- No source Document
- Wrong Report Type e.g. Lost/Stolen report instead of Seen report
- Incorrect VRM
- Incorrect or no Force Reference

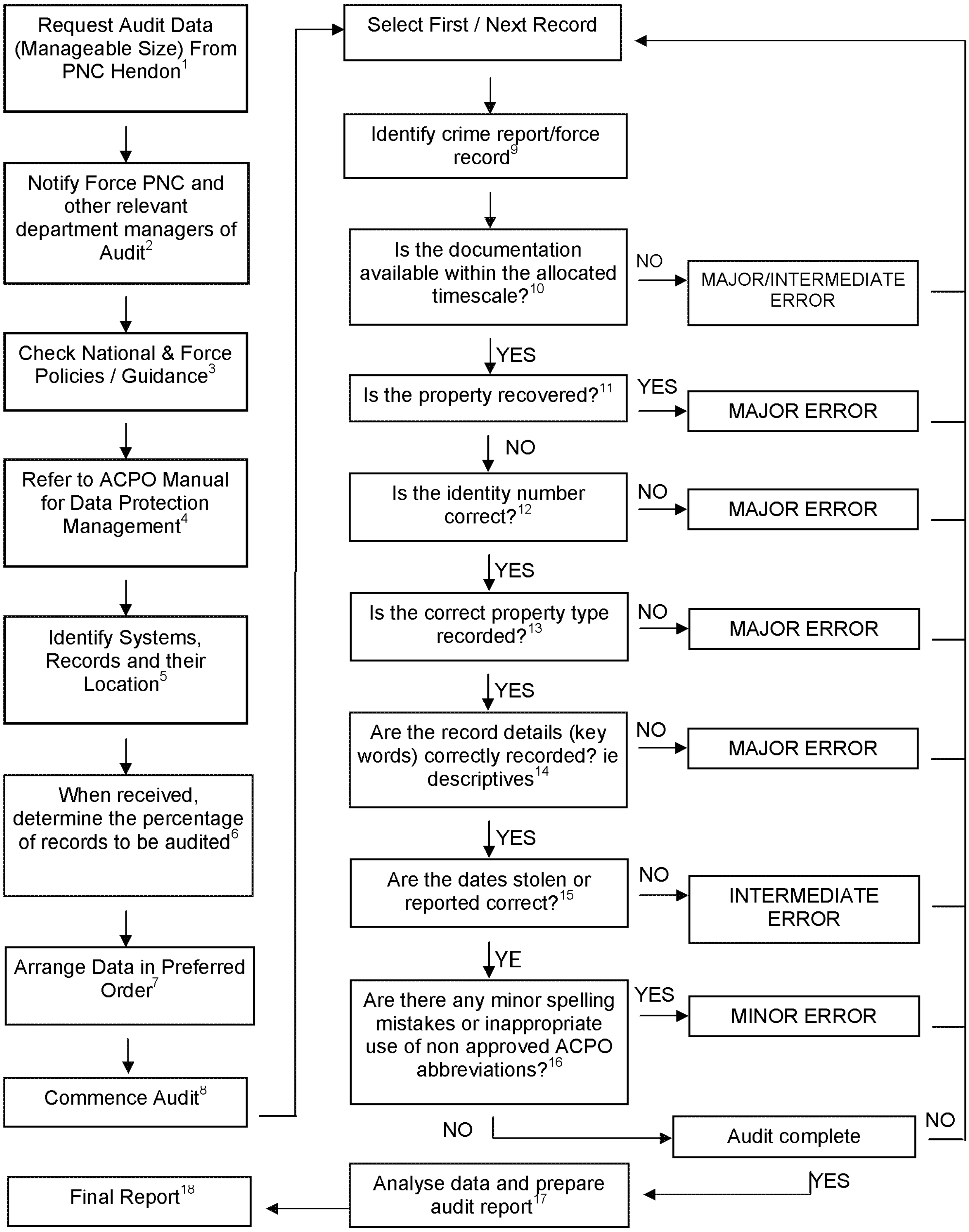
INTERMEDIATE

- Source Document not located within 30 minutes.
- Incorrect text entry on PNC according to Force Policy

MINOR

- Spelling or typing mistakes
- Use of non-approved Abbreviations

STOLEN PROPERTY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (Manageable Size) From PNC Hendon[1]
Notify Force PNC and other relevant department managers of Audit[2]
Check National & Force Policies / Guidance[3]
Refer to ACPO Manual for Data Protection Management[4]
Identify Systems, Records and their Location[5]
When received, determine the percentage of records to be audited[6]
Arrange Data in Preferred Order[7]
Commence Audit[8]
Select First / Next Record
Identify crime report/force record[9]
Is the documentation available within the allocated timescale?[10]
NO
MAJOR/INTERMEDIATE ERROR
YES
Is the property recovered?[11]
YES
MAJOR ERROR
NO
Is the identity number correct?[12]
NO
MAJOR ERROR
YES
Is the correct property type recorded?[13]
NO
MAJOR ERROR
YES
Are the record details (key words) correctly recorded? ie descriptives[14]
NO
MAJOR ERROR
YES
Are the dates stolen or reported correct?[15]
NO
INTERMEDIATE ERROR
YE
Are there any minor spelling mistakes or inappropriate use of non approved ACPO abbreviations?[16]
YES
MINOR ERROR
NO
Audit complete
NO
YES
Analyse data and prepare audit report[17]
Final Report[18]

STOLEN PROPERTY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Activity Flow Chart)

1. **Request audit data from PNC Hendon in manageable sizes e.g. by Division or District.**
e.g. by Division or District or record types such as Plant, Trailers, Animals, Marine, Firearms, Engines or all. Requests must be made by nominated officers, by fax or e-mail to PNC Service Desk (020 8358 5050) for attention of Data Control.

2. **Notify Appropriate department(s) of audit e.g. Force PNC, Criminal Justice Managers.**
Courtesy call in order to notify appropriate managers that audit will be taking place.

3. **Check National and Force policies/guidance**
This is to ensure compliance with the guidelines in PNC Manual for stolen property, other national circulations and local policy.

4. **Refer to ACPO Manual.**
To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Identify systems, records and their location.**
Is the audit to be just of PNC or are local systems to be part of the audit.

6. **When received determine the percentage of records to be audited.**
The audit sample size should be based on the sample methodology explained in the ACPO Data Protection Audit Manual.

7. **Arrange data in preferred order**
Sort the data into your preferred audit sequence e.g. by property type, year reported, etc concentrating on most problematic first.

8. **Commence Audit**
Schedule visits with relevant departments and set time scales.

9. **Identify crime report or force record**
This should be the crime report. However certain items such as stolen firearms maybe recorded on a separate system.

10. **Is the documentation available within the allocated timescale?**
If cannot be located within 30 minutes but subsequently produced within 24 hours.

11. **Is the property recovered?**
Does the force record show that the item is recovered. If so ensure that a Found report is added to the PNC record and log the error.

12. **Is the identity number correct?**
Ensure that the identification number of the property is correct by checking it against the force record.

13. **Is the correct property type recorded?**
e.g Engine, Plant, Trailer, Animal, Marine or Firearm.

14. **Are the record details (key words) correctly recorded?**
The descriptive details such as colour and model.

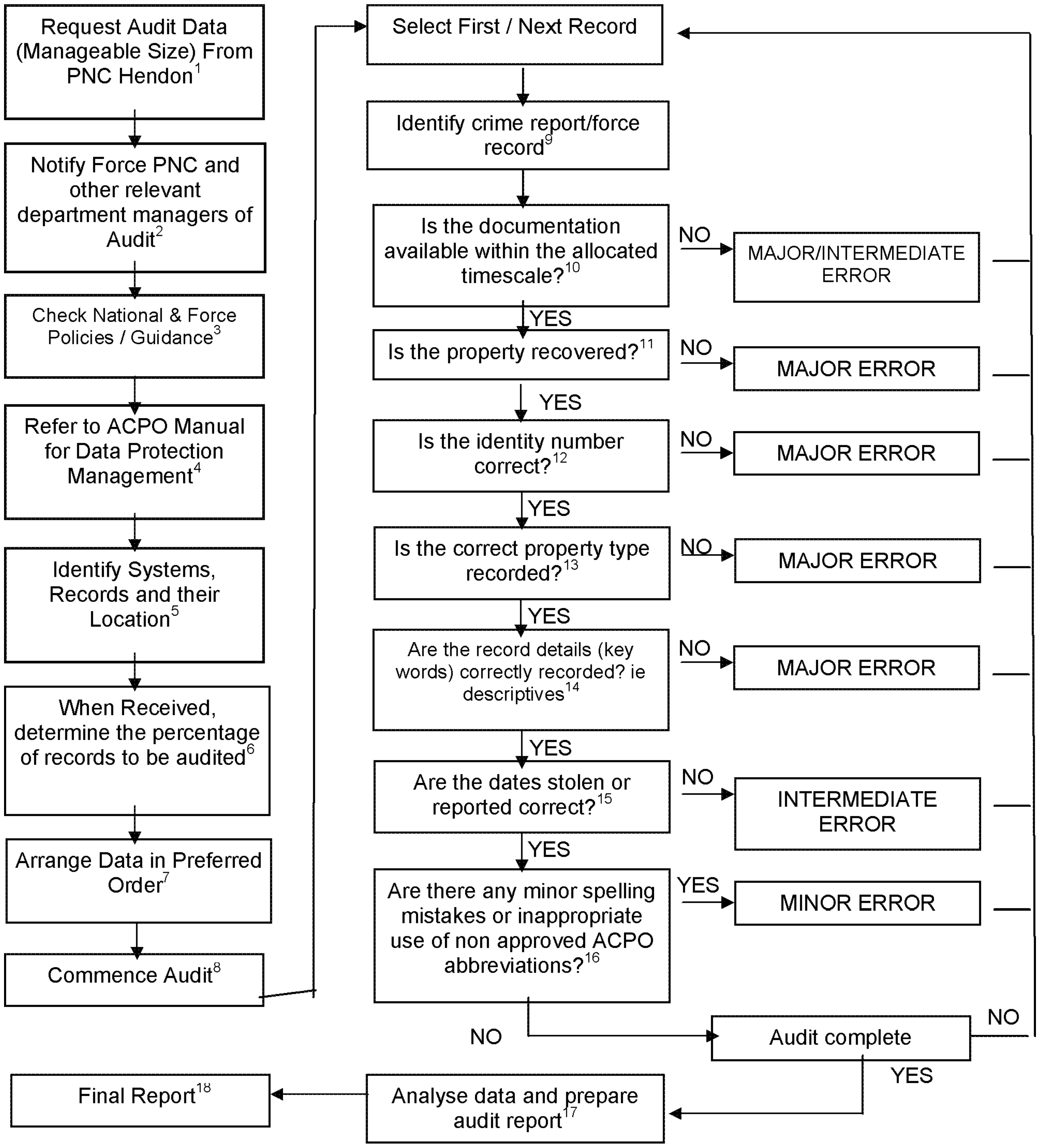
15. **Are the dates stolen or reported correct?**
Does PNC reflect the force record.

16. **Are there any minor spelling mistakes or inappropriate use of non approved ACPO abbreviations?**
Log as minor errors any such discrepancy.

17. **Analyse data and prepare audit report**
Categorise and calculate total errors and percentages. Enter into a chart in order to best present the data. Write an audit report based upon audit findings.

18. **Final Report**
The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should include a comprehensive list of errors.

FOUND PROPERTY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (Manageable Size) From PNC Hendon[1]
Notify Force PNC and other relevant department managers of Audit[2]
Check National & Force Policies / Guidance[3]
Refer to ACPO Manual for Data Protection Management[4]
Identify Systems, Records and their Location[5]
When Received, determine the percentage of records to be audited[6]
Arrange Data in Preferred Order[7]
Commence Audit[8]
Select First / Next Record
Identify crime report/force record[9]
Is the documentation available within the allocated timescale?[10]
NO
MAJOR/INTERMEDIATE ERROR
YES
Is the property recovered?[11]
NO
MAJOR ERROR
YES
Is the identity number correct?[12]
NO
MAJOR ERROR
YES
Is the correct property type recorded?[13]
NO
MAJOR ERROR
YES
Are the record details (key words) correctly recorded? ie descriptives[14]
NO
MAJOR ERROR
YES
Are the dates stolen or reported correct?[15]
NO
INTERMEDIATE ERROR
YES
Are there any minor spelling mistakes or inappropriate use of non approved ACPO abbreviations?[16]
YES
MINOR ERROR
NO
Audit complete
NO
YES
Analyse data and prepare audit report[17]
Final Report[18]

FOUND PROPERTY AUDIT PROCESS ACTIVITY FLOW CHART
(To be used in conjunction with Activity Flow Chart)

1. **Request audit data from PNC Hendon in manageable sizes e.g. by Division or District.**
   e.g. by Division or District or record types such as Plant, Trailers, Animals, Marine, Firearms, Engines or all. Requests must be made by nominated officers, by fax or e-mail to PNC Service Desk (020 8358 5050) for attention of Data Control.

2. **Notify Appropriate department(s) of audit e.g. Force PNC, Criminal Justice Managers.**
   Courtesy call in order to notify appropriate managers that audit will be taking place.

3. **Check National and Force policies/guidance**
   This is to ensure compliance with the guidelines in PNC Manual for stolen property, other national circulations and local policy.

4. **Refer to ACPO Manual.**
   To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Identify systems, records and their location.**
   Is the audit to be just of PNC or are local systems to be part of the audit.

6. **When received determine the percentage of records to be audited.**
   The audit sample size should be based on the sample methodology explained in the ACPO Data Protection Audit Manual.

7. **Arrange data in preferred order**
   Sort the data into your preferred audit sequence e.g. by property type, year reported, etc concentrating on most problematic first.

8. **Commence Audit**
   Schedule visits with relevant departments and set time scales.

9. **Identify crime report or force record**
   This should be the crime report. However certain items such as stolen firearms maybe recorded on a separate system.

10. **Is the documentation available within the allocated timescale?** If cannot be located within 30 minutes but subsequently produced within 24 hours.

11. **Is the property recovered?**
    Does the force record show that the item is recovered. If not then is found report correct?

12. **Is the identity number correct?**
    Ensure that the identification number of the property is correct by checking it against the force record.

13. **Is the correct property type recorded?**
    e.g Engine, Plant, Trailer, Animal, Marine or Firearm.

14. **Are the record details (key words) correctly recorded?**
    The descriptive details such as colour and model.

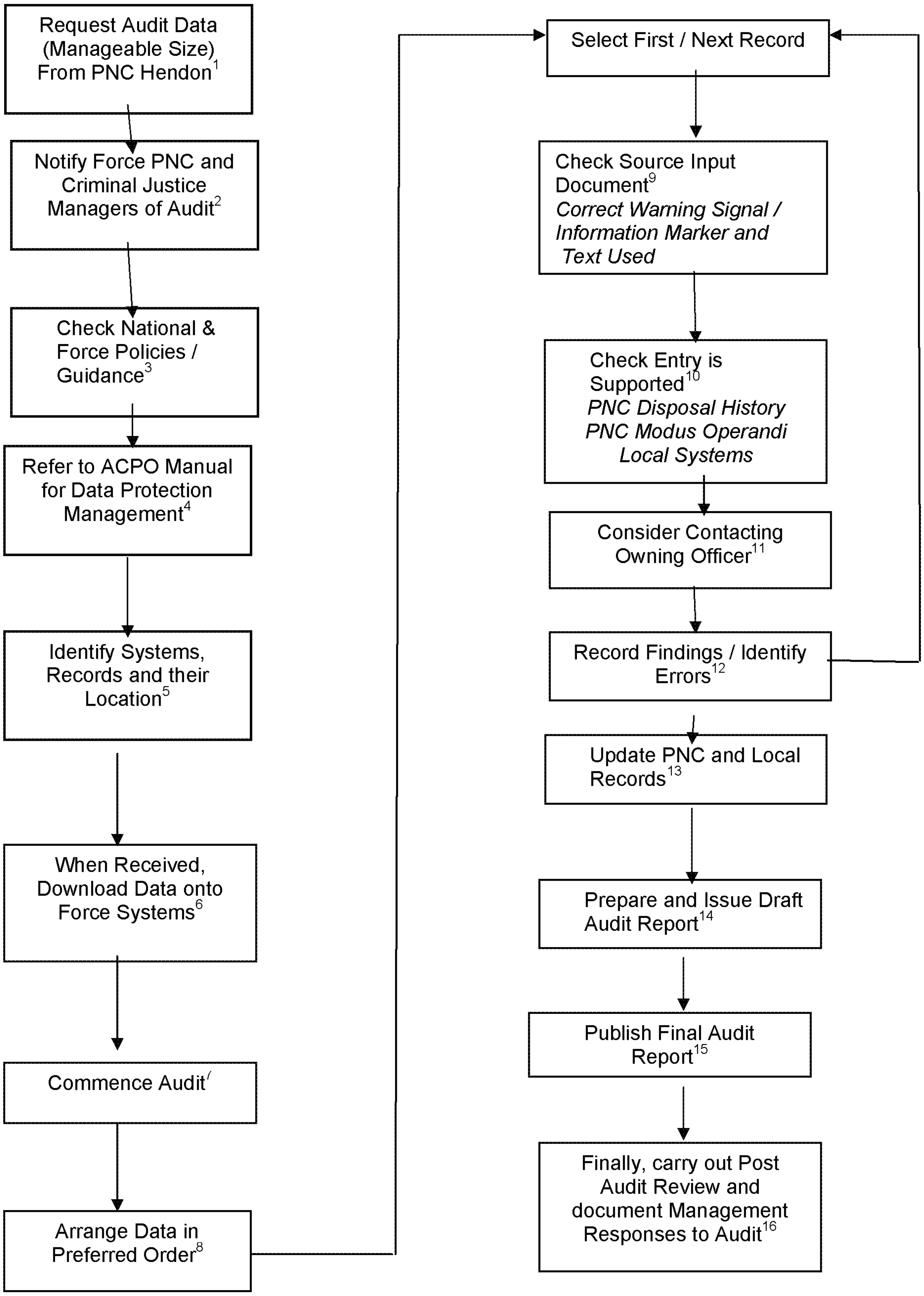
15. **Are the dates stolen or reported correct?**
    Does PNC reflect the force record.

16. **Are there any minor spelling mistakes or inappropriate use of non approved ACPO abbreviations?**
    Log as minor errors any such discrepancy.

17. **Analyse data and prepare audit report**
    Categorise and calculate total errors and percentages. Enter into a chart in order to best present the data. Write an audit report based upon audit findings.

18. **Final Report**
    The report should contain an executive summary, detailing the overall error rate; method of audit; conclusion and recommendations. The report should include a comprehensive list of errors.

WARNING SIGNALS & INFORMATION MARKERS AUDIT PROCESS ACTIVITY FLOW CHART (To be used in conjunction with Reference Guide)


Request Audit Data (Manageable Size) From PNC Hendon[1]
Notify Force PNC and Criminal Justice Managers of Audit[2]
Check National & Force Policies / Guidance[3]
Refer to ACPO Manual for Data Protection Management[4]
Identify Systems, Records and their Location[5]
When Received, Download Data onto Force Systems[6]
Commence Audit[7]
Arrange Data in Preferred Order[8]
Select First / Next Record
Check Source Input Document[9] *Correct Warning Signal / Information Marker and Text Used*
Check Entry is Supported[10] *PNC Disposal History PNC Modus Operandi Local Systems*
Consider Contacting Owning Officer[11]
Record Findings / Identify Errors[12]
Update PNC and Local Records[13]
Prepare and Issue Draft Audit Report[14]
Publish Final Audit Report[15]
Finally, carry out Post Audit Review and document Management Responses to Audit[16]

WARNING SIGNALS & INFORMATION MARKERS AUDIT ERROR CLASSIFICATION

MAJOR

- Incorrect Report Type Used Against Individual
- Incorrect Text
- No Supporting Evidence To Substantiate Entry
- Insufficient Supporting Evidence To Substantiate Entry

INTERMEDIATE

- Incorrect Supporting Evidence
- Sex Offender marker remains on PNC record when requirement to register has expired
- No or incorrect reference number

MINOR

- Spelling Mistakes

WARNING SIGNALS & INFORMATION MARKERS AUDIT PROCESS REFERENCE GUIDE
(To be used in conjunction with activity Flow Chart)

1. **Request audit data from PNC Hendon in manageable sizes e.g. by Division or District.** Requests must be made by nominated officers, by fax or e-mail to PITO Data Control, Hendon.

2. **Notify Appropriate department(s) of audit e.g. Force PNC, Criminal Justice Managers.** Courtesy call in order to notify appropriate managers that audit will be taking place.

3. **Check National and Force policies/guidance** To ensure compliance with the guidelines in PNC Manual, other national circulations and local policy.

4. **Refer to ACPO Manual** To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Identify systems, records and their location.** PNC, local force systems, source input documents. (SID)

6. **When received, download data onto force system.** Transfer data from disk received from Hendon onto force system (if on disk use notepad rather than word), save e-mail onto relevant disk drive. Not applicable if paper records requested.

7. **Commence Audit** Confirm schedule of visits with holders of records.

8. **Arrange data in preferred order** Sort the data into your preferred audit sequence e.g. by date – oldest first or marker/signal type concentrating on most problematic first. Note (Information Marker) Persistent Offender marker automatically created and deleted – no need to audit.

9. **Check Source Input Document** Does SID support entry and confirm that the correct warning signal/information marker has been used? Note. (Warning signals) Contagious must not be used for HIV+/AIDS. Compulsory completion of text field is not a national standard, but good practice to include any relevant information to support entry. May also indicate evidence of previous review.

10. **Entry Supported** Check PNC disposal history for relevant conviction and local systems in support of record. Note: M.O. text may assist if no disposal history to support record. OD page may have additional information. Could also consider cross checking information against local system entry as dual audit. (Information Marker) The Sex Offender marker should not remain if the associated Wanted Missing report has been deleted.

11. **Contact 'owning' officer** Consider contacting 'Owning' officer who may have personal knowledge of the nominal, to confirm relevance and timeliness if necessary.

12. **Record Findings / Identify Errors** Classify errors.

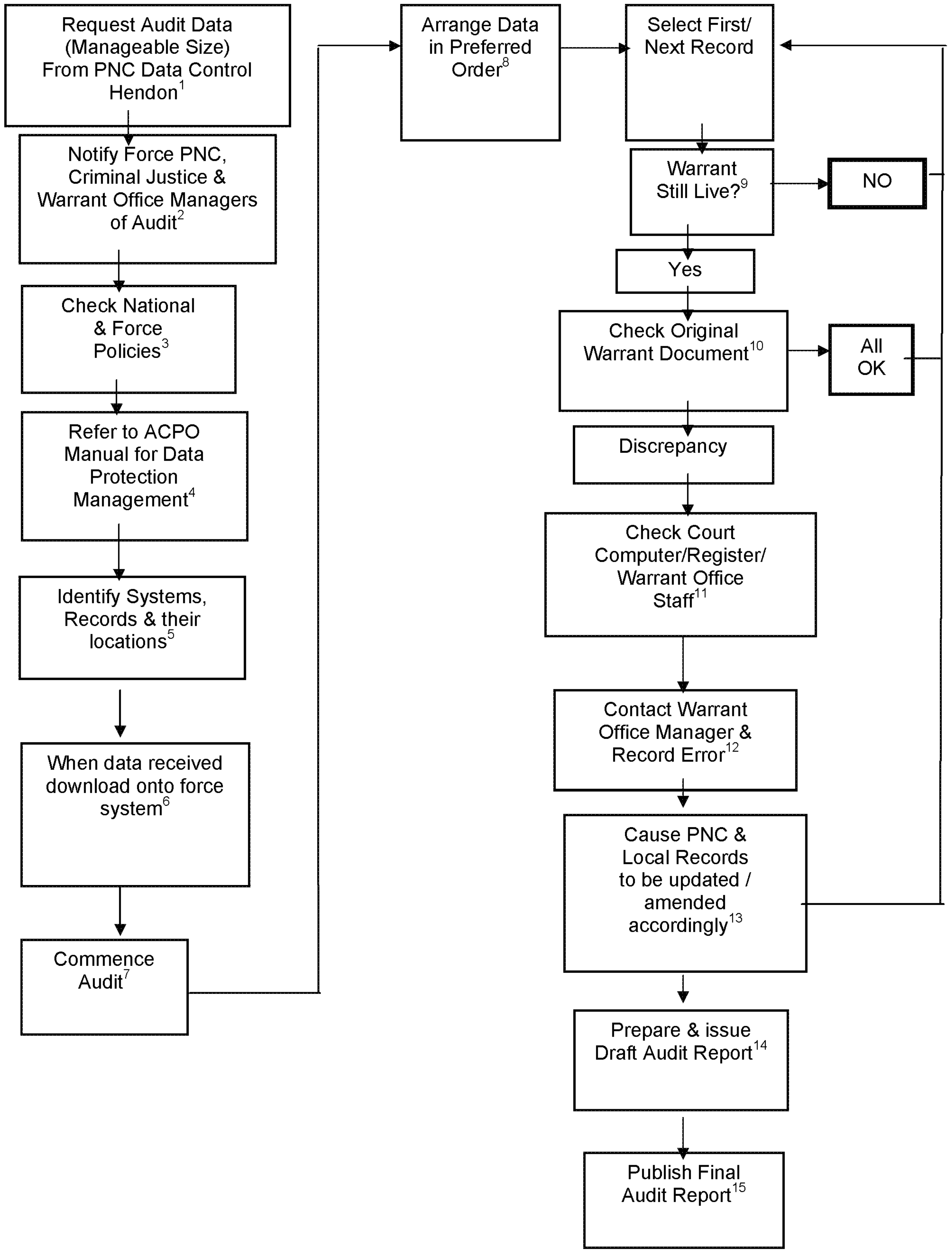
13. **Update PNC and Local Records** Where necessary cause PNC and any local systems to be updated accordingly.

14. **Prepare Draft Audit Report** The report should contain a list of errors; the overall error rate; method of audit; conclusion and recommendations and an executive summary (see ACPO Manual). Send to relevant managers for their comments

15. **Final Report** Prepare and publish final report.

16. **Audit Review** After appropriate time period carry out post audit review of recommendations and follow up to management responses.

WARRANT AUDIT PROCESS
ACTIVITY FLOW CHART
(To be used in conjunction with Reference Guide)


Request Audit Data (Manageable Size) From PNC Data Control Hendon[1]
Notify Force PNC, Criminal Justice & Warrant Office Managers of Audit[2]
Check National & Force Policies[3]
Refer to ACPO Manual for Data Protection Management[4]
Identify Systems, Records & their locations[5]
When data received download onto force system[6]
Commence Audit[7]
Arrange Data in Preferred Order[8]
Select First/ Next Record
Warrant Still Live?[9]
NO
Yes
Check Original Warrant Document[10]
All OK
Discrepancy
Check Court Computer/Register/ Warrant Office Staff[11]
Contact Warrant Office Manager & Record Error[12]
Cause PNC & Local Records to be updated / amended accordingly[13]
Prepare & issue Draft Audit Report[14]
Publish Final Audit Report[15]

WARRANT AUDIT PROCESS
REFERENCE GUIDE
(To be used in conjunction with Activity Flow Chart)

1. **Request Audit Data from PNC Hendon in manageable sizes. E.g. by Division or District**
Nominated officers either must make requests by fax or e-mail to PITO at Hendon.

2. **Notify Force PNC, Criminal Justice and Warrant Office Managers of Audit**
Courtesy call in order to inform PNC, CJD and Warrant Office Managers an audit will be taking place.

3. **Check National and Force Policies**
What are the guidelines for the
Input of "Wanted on Warrant" reports.

4. **Refer to ACPO Manual**
To ensure compliance with national requirements, follow guidance set out in the ACPO Manual for Data Protection Management.

5. **Identify Systems, Records and Their Location**
Systems and records required in order to conduct the audit are PNC; Local Force system(s); Court registers/ computer records.

6. **When Received, Download Data On To Force System**
Transfer data from the disk received from Hendon onto Force system, save e-mail onto relevant disc drive. Not applicable if paper records requested.

7. **Commence Audit**
Confirm schedule of visits with Warrants Office Managers.

8. **Arrange Data In Preferred Order**
Sort the data into your audit sequence - e.g. **WARRANT**, arrest, locate trace, Mispers, Sex Offenders, and Court Orders.

9. **Check Warrant is Still Live**
When data received establish whether the warrant is still live and matches the PNC record.

10. **Check Warrant**
Physically check there is an **ORIGINAL** warrant document held and the information held on the PNC and any local systems is identical.

11. **Any Discrepancy**
If you have access to the Court computer system this can be checked in order to ascertain the validity of the warrant and the information thereon, otherwise the Court register should provide you with the answers. Alternatively speak to a member of the warrants office staff, who may have knowledge of ongoing situations.

12. **Contact Warrant Office Manager / Record Error**
Once an error has been established and confirmed, the appropriate Warrants Office Manager to be informed and the error recorded for the audit report.

13. **Update PNC & Local Records**
Where necessary cause PNC and any local systems to be updated accordingly.

14. **Draft Audit Report**
A draft report should be prepared to include a list of errors; the overall error rate; method of audit; conclusion and recommendations and an executive summary (see ACPO Manual). Send to relevant managers for their comments.

15. **Final Report**
On receipt of comments a final report should be prepared and sent to the relevant persons.

WARRANT AUDIT
ERROR CLASSIFICATION

MAJOR

- Warrant not Cancelled
- Warrant live but not on PNC
- Warrant Not Found
- Duplicate PNC File
- Incorrect Information that effects the execution of the warrant
- Limitations of proceedings apply

INTERMEDIATE

- Warrant not traced within 30 minutes, but located within 24 hours
- Local warrant system incorrect
- No X Reference e.g. Information report omitted from vehicle

MINOR

- Spelling mistakes
- Non-Approved ACPO Abbreviations
- Confirmed Dead (Still WM)