Home Office

National Standards for Compliance and Audit of Law Enforcement ANPR

Version 2.0
September 2020

1 Purpose of Compliance and Audit

Consistent management of NAS is essential to ensure that data is accurate and to maximise the benefits for law enforcement purposes. Public confidence in the system is essential and robust standards with clear records of compliance with those standards is importance to ensure support for ANPR systems is maintained.

Audit is one part of a larger suite of security controls and measures which includes, governance, physical, personnel, technical and procedural controls. The NAS is designed to provide a security regime that supports and compliments the business and technical needs. It is important that business audit standards, policy and governance are also in place which requires a robust compliance audit regime to be in place.

2 Applicability

These Audit Standards apply to national law enforcement ANPR capability (NAC) operated by the police and other law enforcement agencies (hereinafter called LEA), throughout the UK, that connect to or receive data from the National ANPR Service (NAS).

Audit is conducted with reference to National Standards for Policing and Law Enforcement (NASPLE)

LEAs must ensure compliance by their agency with the requirements of all parts of NASPLE.

3 Audit Governance and Roles

The National Strategic lead as lead controller must ensure that audit standards are in place to provide for effective governance of NAS taking account of threats and risks.

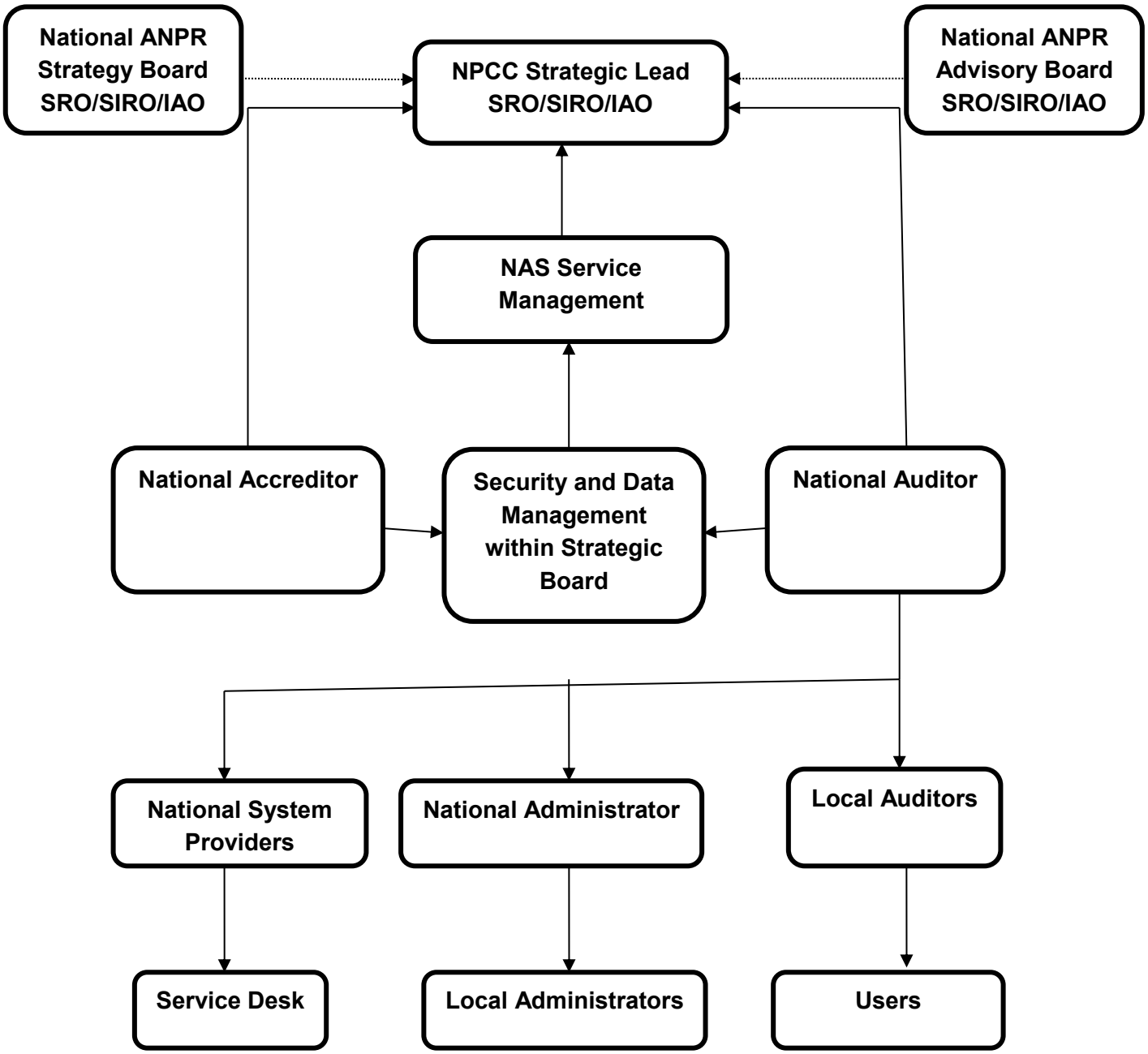
Staff conducting audits must have current security clearance to levels as detailed in NASPLE Part 3.

Staff with user access permissions to NAS may not conduct audits.

LEA must ensure that audit of any access to NAS using administrative permissions is conducted by staff who do not themselves have administrative responsibility for NAS.

3.1 Governance Model

The below governance model is in place for NAS:



4 Data Standards Audit

Accurate data is essential to ensure legislative compliance and to enable the benefits that can be obtained from ANPR to be optimised. The following elements of NASPLE Part 1 are included for audit.

4.1.1 Data Security

Every 6 months LEA to review a sample of reports that have been obtained by that LEA from NAS for compliance with the requirements of the Government Security Classification Policy (GSCP) requirements for OFFICIAL – SENSITIVE data. (NAS configuration should ensure that all reports are appropriately marked)

4.1.2 Time

LEAs must record evidence of the accuracy of time recording for all camera that submit data to their management server. Records confirmation of time accuracy must be reviewed at Least once every 7 days. A record of review and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.1.3 Location

The accuracy of the recording of location for a read record from all camera with the exception of mobile camera must be confirmed on installation and thereafter reviewed at Least once every 6 months by the LEA manging that camera. A record of all reviews and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.2 Reporting of Data Standards

Every 12 months LEA must provide the national auditor with a report to include details of the number of cameras operated by the LEA, the number tested during the preceding 12 months, information of the accuracy for recording time and location for each camera tested and details of any maintenance conducted following testing.

5 Infrastructure Standards Audit

5.1 ANPR Infrastructure Development

Compliance with NASPLE Part 2 is important to ensure that ANPR systems are developed and maintained in conformance with relevant legislation and that the benefits that can be obtained from the NAS are optimised. The following elements of NASPLE Part 2 are included for audit.

5.1.1 Static ANPR Systems - Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of

performance evaluation as required by NASPLE Section 8.14 LEAs to retain records of all reviews for a period of 2 years.

5.1.2 **Moveable ANPR Systems** - Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.1.3 **Multi Lane ANPR Systems** - Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.1.4 **CCTV Integrated ANPR Systems** - Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.1.5 **Mobile ANPR Systems** - Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.1.6 **Covert Systems** – Audit of deployments of ANPR systems authorised within provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) to be completed in accordance with arrangements for compliance and review of RIPA and RIPSA deployments as appropriate.

6 LEA Local System Audit

6.1.1 **Local Systems** - Audit of local data storage to be completed by the LEA every 6 months to confirm that the period of retention is consistent with NASPLE Part 2 and that data is not transferred or used in other systems except as authorised by NASPLE.

6.1.2 **Mobile Systems Data Transfer** – Review of records for transfer of data from Mobile ANPR Systems to be completed by the LEA every 7 days to confirm

compliance with NASPLE Part 2. LEAs to retain records of all reviews for a period of 2 years.

6.1.3 Support and Maintenance – Records for failure of any component of infrastructure to be reviewed by the LEA every 7 days to support compliance with requirements for reinstatement of capability as detailed in NASPLE section 8.14.

7 Vehicle of Interest (VOI) lists Audit

7.1.1 Compliance with the requirement for deletion of lists from NAS 28 days after the latest date of revision to be reviewed by the LEA every 14 days.

7.1.2 Lists held on Mobile ANPR Systems to be reviewed by the LEA at Least once every 7 days to ensure that they remain the current version of any VOI list.

7.1.3 LEA to maintain a record for the review of all VOI lists and retain those records for a period of 2 years.

8 Data Access and Management Standards Audit

8.1 Policy

Annually, the local auditor to confirm that a current written policy is in place in accordance with NASPLE Part 3.

8.2 Audit of provisions for Data Access

8.2.1 The identity of the senior manager as required by NASPLE Section 9.3.6.1 to be confirmed by the local auditor annually

8.2.2 Evidence of the management of staff authorisations and permissions to be audited by the LEA for compliance with authorisation and removal procedures to include:

- Annually 5% of all new staff authorisations that have been approved during the previous 12 months
- Annually review a sample of staff authorisations where the privileges have changed during the previous 12 months
- All staff who have not accessed NAS for a period of 90 days within the 14 days immediately following the expiry of that period.
- All accounts for staff that have left the LEA within 48 hours of them leaving an LEA to ensure that access permissions have been ceased.

- Annually all staff with administrative access to ensure that this remains appropriate and is not combined with user access permissions.

- Monthly to review records for all failed 'log on' attempts. A record of all reviews conducted to be retained for a period of 2 years

8.2.3 LEA audit to be conducted every 6 months to confirm the deletion of data in accordance with NASPLE with an annual review of 5% of all cases where data is retained beyond standard deletion times to ensure continued retention remains appropriate, both for NAS and other systems.

8.2.4 LEA to audit of instances of data access to ensure access is appropriate within terms of NASPLE with reference to the justification and authority where required as follows:

- LEAs must establish provisions for audit of ANPR data where the period for the search includes data that entered the NAS 90 days or less prior to the search, that is proportionate in each case taking account of their assessment of the potential risk of non-compliance with NASPLE and for the misuse of data. The audit to be completed quarterly.[1]

- To audit 5% of searches across a sample covering 30 consecutive days since the previous audit where those searches cover data that was captured more than 90 days prior to the date of search. The audit to be completed quarterly.
- All instances of access to data preserved under provisions of the Criminal Procedure and Investigations Act 1996 (CPIA)

8.2.5 As a minimum, the following elements of data access must be reviewed as part of the audit:

- That any search was properly authorised where required with evidence of authorisation recorded

- That the timescales for the search were appropriate in that they were no greater than was necessary and proportionate in the circumstances of the investigation

- That the reason, purpose and justification for the search was fully recorded within NAS

[1] In most cases a sample of 2% of all instances where the period included in the search extends for 90 days or less prior to the date of the search being conducted for a sample of 30 consecutive days in a period since the previous audit (Quarterly) is likely to be appropriate. Depending upon the level of risk a lessor or greater sample may be appropriate. The rationale for determining the data sample should be documented in all cases.

8.2.6 In respect of access to data preserved under provisions of the CPIA that any access was solely for the investigation for which it was preserved.

8.2.7 LEAs to audit 10% of records of the disclosure of data otherwise than in accordance with CPIA or similar procedures in Scotland in respect of the justification, the date and time of the disclosure and the identification of both the person disclosing and the recipient of the data. (NASPLE section 9.4.3.7)

8.2.8 LEAs are responsible for dealing with any non-compliance with standards that are identified during audit and must report all non-compliance and a copy of the audit report to the national auditor within 28 days of the non-compliance being identified.

8.2.9 All LEAs must maintain a record of audits that are conducted to include:

- A statement of the findings for all audit activity
- A report of the extent of non-compliance
- A report of action taken in relation to non-compliance

8.2.10 Records of audit will be retained for a period of 2 years and made available to the national auditor on request.

8.3 Audit of Changes to Read Records

8.3.1 LEAs to review a sample of changes to 'read' records every 6 months to confirm the validity of the change. Records of review to be retained for a period of 2 years.

8.3.2 Audit of Access by System Providers, National Administrators and Local Auditors

8.3.3 The National Auditor will audit access to NAS by system providers, national administrators and local auditors, reporting details of any audit that is conducted for the information of controllers to the extent determined by those post holders.

8.3.4 The National Auditor will conduct a NAS system audit every 6 months to confirm data is deleted in line with the requirements of NASPLE Part 2.

8.3.5 Audit of access to NAS by a user with 'Super Administrator' permissions will be conducted for each occasion that the system is accessed when those permissions are enabled for that user by the National Auditor.

Glossary of Terms, Abbreviations and Definitions

ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture and ANPR read.
CPIA	Criminal Procedure and Investigations Act 1996
DPA	Data Protection Act 2018
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS))
GPS	Global Positioning System
JPEG	Joint Photographic Expert Group image format
NAS	National ANPR Service
NAC	National Law Enforcement ANPR Capability
NPCC	National Police Chiefs' Council
NASPLE	National ANPR Standards for Policing and Law Enforcement
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities
Read	The interpretation of a VRM by an ANPR system
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
VRM	Vehicle Registration Mark

Document Revisions

Version 2.0	September 2020	Update of links within text, Minor revision of section 7

This publication is available at www.gov.uk/government/publications and www.npcc.police.uk/anpr

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk .