Downloaded from lawaccent.com - For personal use only.
Redistribution without permission is prohibited.

info@lawaccent.com

Regulatory Readiness: How to Prepare for NDPC Audit Returns Submission

The Nigeria Data Protection Commission (NDPC) 2023 (which establishes the NDPC) and the GAID 2025 provide the framework for organisations to ensure accountability in handling personal data. Preparing for NDPC audit returns is more than a regulatory obligation; it's a reflection of an organization's commitment to privacy, risk management, and operational integrity. Below, I explore how organizations can approach audit readiness strategically and systematically.

1. Understanding NDPC Audit Requirements

Before you begin any preparation, it is crucial to understand what NDPC expects:

- Who Must Submit: Annual Compliance Audit Returns are required for Data Controllers/Processors of Major Importance especially those classified as Ultra ?High Level or Extra?High Level.
  Non-compliance can lead to penalties, reputational damage, or legal sanctions.
- Audit Objectives: NDPC audits are designed to assess whether personal data is collected, processed, a
- Submission Timeline: The deadline for filing audit returns is 31 March each year while new entities subm
- Documentation Expectations: Organizations are required to provide supporting evidence of their compli

2. Conduct a Comprehensive Internal Audit

Internal auditing is the foundation of regulatory readiness. It ensures your organization knows its current compliance status before submitting audit returns:

- Policy Review: Verify that your data protection policies, privacy notices, and internal standard operating
- Data Inventory and Mapping: Catalog all personal data collected, its source, storage location, processing
- Risk Assessment: Identify potential risks to personal data, including unauthorized access, leaks, or oper
- Gap Analysis: Determine areas where existing practices fall short of NDPC requirements. Early identifica

Example: If your organization collects customer data for marketing but lacks a formal consent mechanism, this gap must be addressed before submission to avoid non-compliance.

3. Engage Key Stakeholders

Successful NDPC audit preparation requires coordination among multiple teams:

- Data Protection Officer (DPO): Leads compliance efforts, oversees audits, and ensures all documentatio
- IT and Security Teams: Provide evidence of technical safeguards, system monitoring, incident response
- Legal and Compliance Units: Verify that internal policies comply with NDPC regulations and provide guid
- Management and Board: Ensure resource allocation, policy enforcement, and top-down accountability fo

4. Document Evidence Properly

NDPC audit returns require substantial evidence to prove compliance. Well-organized documentation simplifies the review process:

- Records of Processing Activities (RPA): Document every instance of personal data collection, storage, p
- Consent Forms and Privacy Notices: Demonstrate that all data subjects have been adequately informed
- Incident and Breach Reports: Include records of previous data breaches, actions taken, and preventive m
- Training and Awareness Records: Show that employees have been trained on data protection laws and

5. Test Your Systems and Controls

Audit readiness is not only about paperwork, it also involves verifying that operational systems effectively protect data:

- System Testing: Regularly test IT systems, access permissions, and encryption methods to ensure comp
- Third-Party Verification: Check that vendors and service providers handling personal data comply with c
- Incident Simulations: Conduct mock scenarios to test incident response readiness, including data breach

Example: If your CRM system allows data export, ensure only authorized personnel have access, and logs are maintained for all data actions.

6. Establish a Compliance Timeline

A clear, actionable timeline ensures submission is on time and accurate:

1. Initial Assessment (1–2 weeks): Identify compliance gaps and assign responsibilities.
2. Document Compilation (2–3 weeks): Gather supporting evidence including RPAs, consent forms, and tra
3. Internal Review (1 week): Verify the accuracy and completeness of documents with management and D
4. Submission Preparation (1 week): Finalize forms, attach documentation, and conduct final checks.
5. Submission Deadline: Ensure filings are completed before the official NDPC deadline to avoid penalties. Late filing typically attracts surcharges or fines, and ?compliance may trigger administrative sanctions up to ?10m or 2% of prior? year gross revenue (whichever is greater) under enforcement practice tied to the NDPA/GAID framework

Tip: Use a Gantt chart or project management tool to track progress and ensure accountability.

7. Leverage Technology for Audit Readiness

Modern technology can significantly streamline NDPC audit preparation:

- Compliance Management Tools: Centralize all documentation, track deadlines, and generate automated
- Data Mapping Software: Maintain an up-to-date inventory of all personal data and processing activities.
- Risk Assessment Tools: Identify vulnerabilities in real time and implement corrective measures quickly.
- Training Platforms: Track employee compliance and provide refresher courses on data protection laws.

Example: A cloud-based compliance platform can alert the DPO when documents are missing or outdated, reducing human error.

8. Maintain Continuous Compliance

Regulatory readiness is a continuous process, not a one-time event:

- Ongoing Monitoring: Conduct regular internal audits, spot checks, and system reviews.

- Policy Updates: Adjust policies and procedures as NDPC guidance evolves or business operations char
- Training: Provide regular training for new employees and refresher sessions for existing staff.
- Regulatory Engagement: Stay informed about NDPC circulars, guidelines, and best practices to maintai

Conclusion

Preparing for NDPC audit returns requires a structured, strategic approach combining internal audits, stakeholder engagement, accurate documentation, system verification, and continuous monitoring. Organizations that adopt a proactive compliance strategy not only meet regulatory obligations but also enhance reputation, build trust, and mitigate operational risks. By investing in proper preparation and leveraging technology, businesses can navigate NDPC audits confidently and maintain a culture of data protection excellence.

AUTHORS

OLUMIDE OYELEKE

PRACTICE MANAGER

Phone: +234 911 100 6744

Email: olumide@lawaccent.com

SPECIALIZATION:

Data Protection