Technology Update

Beyond the Audit

ISO 27001 as the Backbone of Trusted Digital Infrastructure

Edited by **MOHAN DAS VISWAM**

As India's digital governance accelerates, so do the risks of managing sensitive citizen data, vast IT infrastructure, and outsourced development. While most government apps undergo basic security audits, these often focus narrowly on code flaws—overlooking compliance gaps, weak controls, and unmonitored infrastructure.

This is where certifications like ISO/IEC 27001 matter. Unlike routine audits, ISO 27001 offers a holistic framework—covering cybersecurity, infrastructure, HR protocols, documentation, and legal compliance—within a unified Information Security Management System (ISMS). It's about designing secure, accountable, and resilient systems from the ground up.

This article explains why surface-level audits are no longer enough—and why ISO 27001 is now crucial for the credibility, sustainability, and public trust of e-governance platforms.

Case Study: DST Infrastructure Audit

In 2024, under the direction of MeitY, NIC initiated a large-scale cyber security infrastructure audit across several ministries and government departments at Central, State and District levels. Centre for Development of Advanced Computing (CDAC) had been entrusted to conduct Cyber Security Audit of Department of Science and Technology (DST) network in Technology Bhawan,

Naveen Kumar
Dy. Director General & HoG
naveenkumar@nic.in

Arpita Barman
Sr. Technical Director & HoD
arpita.barman@nic.in

Nadeem Akhtar
Scientist - C
nadeem.akhtar@nic.in

India's expanding digital governance needs more than routine audits, which often miss infrastructure gaps, weak access controls, and policy lapses. ISO/IEC 27001 offers a robust, enforceable framework with defined controls, ongoing audits, and role-based accountability. Drawing from real-world audits and case studies, it highlights how certification ensures legal compliance, operational resilience, and public trust. For government bodies handling sensitive data, ISO 27001 isn't optional—it's essential.

The audit aimed to assess the overall cybersecurity posture of DST's IT ecosystem—beyond just application-level vulnerabilities.

Scope of Audit

- Asset Identification and Discovery
- Network Architecture Review
- Endpoint Security and Configuration Review
- Internal and External VAPT (Vulnerability Assessment & Penetration Testing)
- System and Device Log Review
- Review of Cybersecurity Policies and Standard Operating Procedures (SOPs)
- Network Traffic Analysis
- Review of Network and Security Device Logs
- Risk Management Assessment
- Adherence to Best Practices and Auditor Recommendations

During the audit, teams from CDAC and NIC Cyber Security conducted a pre-audit assessment to understand the existing IT infrastructure as per Meity issued guidelines and, while the NIC team at DST shared details such as asset lists, network diagrams, configurations, security measures, whitelisted applications, logs, and incident history.

CDAC team collected and reviewed existing asset list, architecture diagram, and device configurations. Interacted with concern IT Team to understand current network infrastructure, network connectivity, followed practices, procedures, and configurations. The audit was conducted based on this information and further validated through onsite visits and system reviews.

CDAC submitted its audit report in April'25, highlighting vulnerabilities categorized as critical, high, medium, and low, which DST is expected to address. This was the initial step towards strengthening cyber security and will require follow-up after compliance actions are taken.

Findings

The exercise achieved most defined objectives and, for the first time, resulted in complete documentation of DST network, identifying key security gaps. This serves as a foundation for comprehensive gap analysis and implementation of the Cyber Crisis Management Plan.

The result? A clear, actionable roadmap to:

- Well documented assets and network details
- Streamline security processes
- Align with MeitY and CERT-In guidelines
- Support crisis management planning

Though the IT Infrastructure Audit is done, this audit cannot be considered as Information Security Audit as it has not covered other IT applications and portals used for implementation of its schemes and projects.

Mixed Response Across Departments

Some departments acted on the audit find-

ings; others treated it as a mere formality. Without mandatory certification, follow-through was weak—especially under the assumption that government cloud hosting made formal certification unnecessary. The audit revealed a hard truth: infrastructure vulnerabilities are real, often undocumented, and remain unaddressed without systematic certification.

The Limitations of Application

Application security audits have long been a standard requirement for government portals and e-governance platforms to be hosted in National Data Centers. These audits typically review code vulnerabilities, test for common cyber threats as per OWAPS guidelines and provide a certificate that clears the application for deployment—often seen as the final green signal.

However, these audits are not sufficient to ensure real-world security, compliance, or long-term sustainability. Here's why.

Common Gaps Observed

Despite years of mandated application security audits across ministries, several critical vulnerabilities and policy violations continue to go unchecked. These gaps highlight the limitations of conventional audits and the urgent need for structured certification frameworks like ISO 27001.

Limited Scope of Application Security Audit

Most application audits focus on code-level issues as per OWAPS guidelines —like SQL injection, XSS vulnerabilities, or insecure APIs—but rarely evaluate the application:

- Whether it follows government-approved security guidelines (like NISPG or eSAFE)
- Does meet data privacy laws such as the Digital Personal Data Protection (DPDP) Act, 2023
- If the system is designed for required performance and availability
- Do the system follow standard Change Management Policy?
- If disclaimers or user consent mechanisms exist before collecting personal data
- Whether change management or SOPs are documented and followed
- Whether the hosting system is hardened
- Any performance monitoring or reporting mechanism implemented

Insecure Authentication, Weak Identity and Access Management

Many applications continue to operate with:

- Poor Identity and password management
- Basic username-password logins (often without CAPTCHA),
- No multi-factor authentication (MFA),
- Default admin credentials or shared logins.
- Non enforcement of periodical password change.

Poor Design and Broken Workflows

Even when code is audited, functional flaws go unnoticed, leading to poor service delivery. For instance:

- Auto-logout mechanisms don't work
- Role-based approvals are bypassed
- Logging mechanisms are incomplete.
- No standard support and redressal mechanism.

Non-Compliance with Accessibility Laws

Despite completing STQC certification, many portals:

- Do not meet WCAG 2.1 guidelines,
- Do not comply to DBIM guidelines
- Violating of Web Accessibility Guidelines had forced the Supreme Court ruling to implement WCAG 2.1 on priority. Violation may lead to monthly penalty.

Absence of Confidentiality Safeguards

- Non maintenance of Non-Disclosure by implementing agencies and outsourced employees.
- No documentation exists for human resource onboarding, offboarding, or data access boundaries.

Lack of User Consent and Data Sharing Disclaimers

Applications routinely collect sensitive user data but:

- Do not display Terms of Use or data-sharing consent notices
- Do not have policies for cross-system data exchange, putting departments at risk under the DPDP Act

Poor Readiness for Legal Compliance

More than 80% of audited applications are not equipped to demonstrate:

- Data retention and deletion policies,
- Log monitoring or breach detection systems,
- Compliance with the DPDP Act or IT Act 2000.

ISO 27001: What It Covers

In a digital ecosystem where data is the lifeblood of governance, security must extend beyond code-level audits and isolated technical fixes—it demands an integrated, holistic approach. True resilience demands a structured, organization-wide commitment to protecting information at every stage of its lifecycle. That's where ISO/IEC 27001 steps in—not merely as a standard, but as a strategic framework for managing information security in a measurable, repeatable, and certifiable way.

Globally recognized and widely adopted across public and private sectors, ISO 27001 offers a blueprint for establishing a comprehensive Information Security Management System (ISMS). Unlike routine audits that often provide a narrow technical assessment, ISO 27001 looks at the entire organization—its people, policies, infrastructure, and technology—to ensure end-to-end accountability and risk management.

The ISO 27001 Certification Lifecycle

ISO 27001 certification is not a single event but a continuous lifecycle of building, validating, and improving an organization's Information Security Management System (ISMS). It integrates internal discipline with third-party oversight and evolves as your organization grows, changes, and faces new risks.

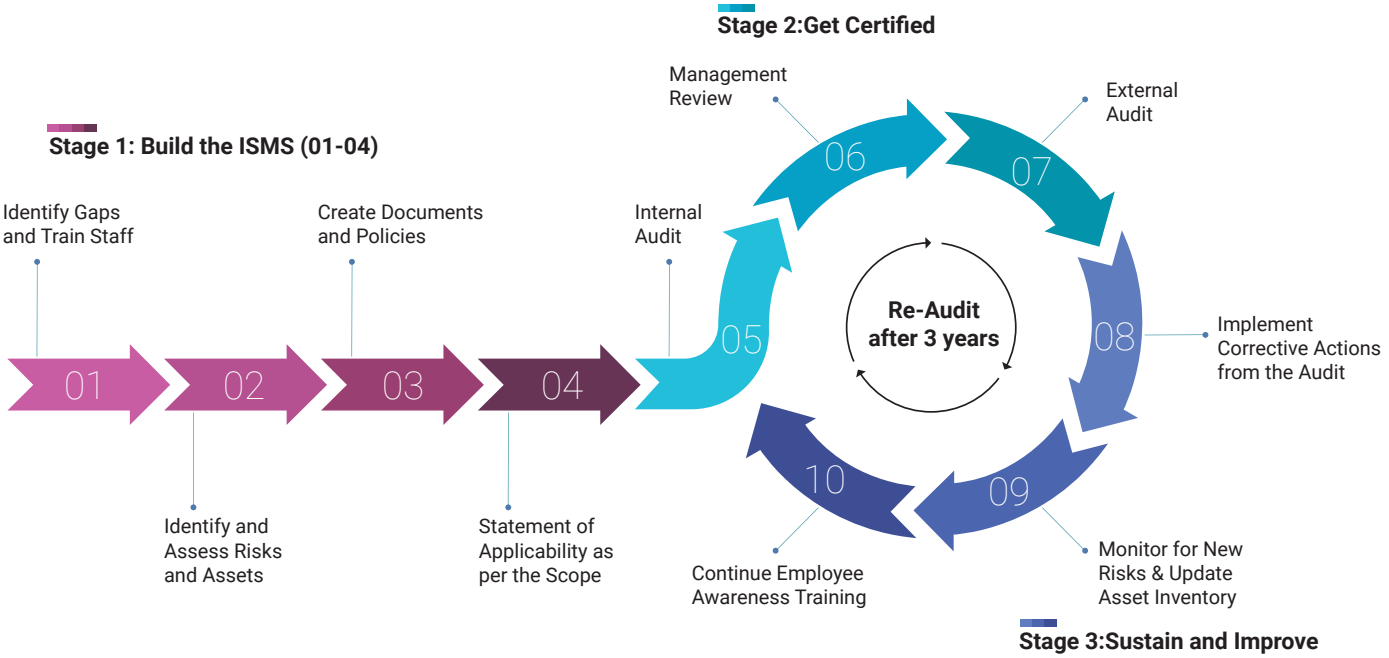
The Four Pillars of ISO 27001

The 2022 revision of ISO/IEC 27001 organizes 10 clauses, with 93 security controls into four well-defined domains, each covering a critical area of information security. This structured approach ensures that all dimensions of an organization—people, processes, infrastructure, and technology—are systematically secured. Clause 1 to 3 pertaining to Scope and References, Clause 4 Context of organization. See fig. 11.1 for breakdown of the domains and their focus areas:

▼ Fig : 11.1

ISO27001:2022 Domains and Controls

Domain	Clauses	Controls	Area
Organizational	5	37	Policies, Role &Responsibilities, Risk & Asset management, Access control and identity management, Supplier relationship security, Incident response, Business continuity, Compliance with legal and regulatory requirements
People	6	8	Pertaining to HR screening & qualifications before employment, T&C of Employment, ISMS Awareness, Training, Disciplinary Process, Responsibilities After Termination or Change of Employment, Confidentiality or Non-Disclosure, Remote Working, Information Security Event Reporting
Physical	7	14	Physical security perimeters like entry/ exit controls, physical security of the location, security monitoring, security of assets on-off premise, cabling security, equipment maintenance, secure disposal or reuse etc
Technological	8	34	Access Control, Securing sensitive data, both in transit and at rest, Endpoint Protection, Logging and Monitoring, Backup and Recovery, Secure Development, Configuration Management, Data Deletion and Masking, Web Filtering and Secure Coding etc



▲ Fig 11.2 **ISO 27001 Certification LifeCycle**

Clause 9 is related to Performance evaluation and Clause 10 for improvement.

The lifecycle can be broken down into three key stages:

Stage 1: Build the ISMS

This is the foundation phase where the organization prepares itself for certification:

A. Identify Gaps and Train Staff: Begin with a gap analysis and launch awareness training to build a security-first culture.

B. Identify and Assess Risks and Assets: Map critical assets and evaluate threats, vulnerabilities, and impacts through a detailed risk assessment.

C. Create Documents and Policies: Draft and finalize the necessary security policies, SOPs, access control guidelines, and risk treatment plans required for your ISMS.

D. Statement of Applicability (SoA) Making Controls Traceable: SoA is a key document that outlines which of the information security controls listed in Annexure A of the standard, the organization has chosen to implement—and which ones it hasn't, along with the reasons why. Organizations are required to provide clear documentation, demonstrate tested implementation, and justify why any control has been excluded or deferred.

Here's what the SoA typically includes:

- A list of all Annex A controls
- Whether each control is applicable or not
- Justification for inclusion or exclusion
- The current implementation status of each applicable control
- References to how each control is implemented (e.g., policies, procedures, tools)

Stage 2: Pass Your External Audit

E. Internal Audit and Management Review: Usually internal auditing is conducted by certified Lead Auditor or auditing agency. The team prepare the Audit Checklist as per the SoA and Implementation guidelines given in ISO27002. Identify non-conformities, address them, and review the Statement of Applicability (SoA).

The auditor coordinates with all the stakeholders and prepare as internal assessment report as per SoA. Typical Internal Assessment reports includes

- Clause and Sub-clause number as per the ISO27001 framework
- Standard Verbatim. Clause's exact description
- Audit point: The point to verify.
- Status: Whether the organisation is meeting this compliance. NC means Nonconformity, C means Conformity, Under process and Not Applicable.
- Stage: 1st time and consecutive post review.
- Department: Which department/ division is responsible for implementation.
- Supporting documents: Like MOA, MOU, SOP, Configuration, other relevant certificate etc.
- Document type: Internal External Issues document

During Internal Auditing following documents are prepared for submission to the ISO27001 Certifying bodies.

- Introduction: Purpose and scope as per Clauses 1–3.
- General Information: Overview of the organization, its business, and stakeholders.
- Internal Audit Report: Control verification status for Clauses 4–8.
- Supporting Documents: SOPs, ToRs, WOs, NDAs, and other relevant records.
- Clause-wise Conformance List: Control-wise status under Clauses 4–10, categorized by Organization, People, Physical, and Technology.
- Nonconformity List: Controls deemed non-applicable or accepted as risk by the organization.
- Corrective Actions: Measures planned for addressing nonconformities.

F. ISO 27001 External Audit: Undergo an external certification audit by an accredited body. This involves document checks, interviews, site inspections, and testing of your ISMS in practice. Passing this phase results in official certification. In India there are around 11 ISO27001 certifying bodies including STQC.

Stage 3: Sustain and Improve

Certification is only the beginning. Maintaining it requires active involvement:

- Implement corrective actions by addressing audit findings and refining security controls accordingly.
- Continuously monitor for new risks and update the risk register and asset inventory to reflect changes.
- Provide ongoing employee training on security protocols, phishing threats, and role-based responsibilities.
- Conduct regular internal audits with experts to test control effectiveness and identify emerging risks.

- Undergo annual surveillance audits and tri-annual re-certification to keep the ISMS aligned with evolving standards.

ISO 27002: Turning Policy into Practice

While ISO 27001 defines what needs to be done, its companion standard, ISO/IEC 27002, explains how to do it. This implementation guideline provides detailed instructions for implementation of ISO27001 Controls.

Think of ISO 27001 as the "security constitution" and ISO 27002 as the "operations manual." Together, they enable not just compliance—but security maturity.

Benefits of Certification Over Routine Audits

Routine audits are like snapshots—brief glimpses into a system's surface vulnerabilities. In contrast, certifications like ISO 27001 offer a full diagnostic scan, addressing the organization's security posture across people, processes, policies, and infrastructure.

Here's how certification goes beyond compliance and becomes a strategic enabler of secure governance:

Strengthened IT Governance

ISO 27001 requires departments to document, implement, and routinely review their policies and procedures. This improves:

- Accountability at every level,
- Role clarity for stakeholders,
- Alignment between business objectives and IT operations.
- Building trust and assurance

Enhanced Security Coverage

While routine audits test application-level code, ISO certification ensures:

- Infrastructure hardening (servers, VMs, firewalls)
- Log monitoring and retention,
- Secure access management across systems
- Physical and human safeguards are enforced.

It closes the loop on vulnerabilities that arise not from code—but from configuration, behavior, or oversight.

Legal and Regulatory Compliance

Certification helps departments proactively comply with:

- The Digital Personal Data Protection (DPDP) Act, 2023
- CERT-In and NISPG guidelines
- International standards like GDPR, WCAG 2.1, and ISO 27002.

These aren't just checklists—they're auditable commitments, enforceable during breach investigations or RTI responses.

Improved Operational Efficiency

Certifications mandate:

- Defined Standard Operating Procedures (SOPs)
- Change control, backup, and incident handling protocols
- Structured communication between development, deployment, and audit teams.

This reduces rework, improves service uptime, and helps systems evolve with fewer disruptions.

Better Risk Management

Every control under ISO 27001 maps to a risk treatment objective. This forces departments to:

- Acknowledge known risks
- Apply mitigation or accept them formally with justification
- Maintain a live risk register linked to measurable actions.

ISO does not eliminate all risks. It ensures risks are visible, owned, and managed.

End-to-End Data Integrity and Confidentiality

Certification includes hardening of:

- Hosting environments (e.g., patching and VM isolation)
- Admin-level access (with logs and justifications)
- Encryption standards and retention policies.

It ensures that even if application code is secure, the environment and operations remain secure too.

Recommendations for Government Agencies

To truly secure India's digital infrastructure and citizen-facing services, government departments must move from reactive audits to proactive certifications. Here are few Policy and Practice Recommendations:

- Mandate ISO 27001 for all major G2C and G2B platforms: Especially those handling financial transactions, personal data, or integration with external APIs.
- Include certification requirements in RFPs and vendor contracts: Third-party developers and data handlers must hold valid ISO 27001 / CMMI / WCAG certifications.
- Train internal teams in certification-readiness: Appoint internal ISO leads or auditors who can conduct pre-certification assessments and maintain compliance.
- Establish a central repository of SoAs and audit results: Enable transparency and knowledge-sharing across ministries.
- Integrate SOPs and ISO controls into Agile workflows: Encourage secure-by-design thinking rather than last-minute audits.
- Tie funding and renewals to certification compliance: Make ISO compliance a condition for continued budget allocation and hosting approvals.

Conclusion

In today's digital era, trust is as critical as technology. Citizens expect not only faster services but also secure, accountable systems that respect their data and rights. Routine audits may tick a box, but only certifications like ISO 27001 can guarantee that an organization has done the hard work—building security into its infrastructure, its people, its processes, and its mindset.

For India's digital governance to mature, security cannot remain an afterthought. It must be embedded, enforced, and externally validated. Certification is not just a stamp—it's a statement. A declaration that the government values privacy, accountability, and excellence in public service delivery.

▼ Fig : 11.3 : Audit vs. Certification: A Comparative Snapshot

Aspect	Routine Security Audit	ISO 27001 Certification
Scope	Code-level, application-specific	Organization-wide: people, process, tech
Depth of Evaluation	Surface-level testing	In-depth, control-by-control verification
Documentation Required	Minimal (audit report)	SoA, SOPs, risk register, internal audits
Validity	One-time pre-launch	Ongoing (annual reviews + recertification)
Enforceability	Advisory in nature	Legally recognized and auditable
Risk Management	Not always addressed	Central to certification process

Contact for more details

Arpita Barman
Senior Technical Director & HoD
Science and Technology (DST & DSIR) Informatics Division
NIC HQ, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: hod-mst@nic.gov.in, Phone: 011-24305400