The 2025 State of Cyber Governance

A Comprehensive Analysis of New Regulatory Frameworks for an IS Auditor

1. Introduction: The Paradigm Shift to Resilience and Sovereignty

The fiscal year 2025 has marked a definitive inflection point in the trajectory of India's digital governance. For the better part of the last decade, the regulatory landscape was characterized by a patchwork of advisories—reactive measures often precipitated by specific incidents. However, the period from January 2025 to the present represents a structural maturation. The regulatory discourse has shifted from a checklist-based "compliance" model to a dynamic "resilience" model, underpinned by a rigorous enforcement of data sovereignty.

For the professional holding a Diploma in Information System Audit (DISSA), this shift is not merely academic; it fundamentally alters the engagement model. The auditor is no longer a passive verifier of control existence but an active assessor of control efficacy under stress. The simultaneous release of the **CERT-In Comprehensive Cyber Security Audit Guidelines**, the **SEBI Cyber Security and Cyber Resilience Framework (CSCRF)**, the **RBI Master Directions on Payment Aggregators**, and the **MeitY India AI Governance Guidelines** creates a complex, interlocking mesh of obligations.

This report serves as an exhaustive analysis of these developments. It synthesizes the disparate regulatory threads into a coherent fabric of audit assurance, providing the DISSA auditor with the theoretical grounding, practical methodologies, and strategic foresight required to navigate this new era. The analysis is driven by the central thesis that **regulatory compliance in 2025 is synonymous with operational resilience and fiduciary accountability.**

2. The Auditor as Data Fiduciary

CERT-In Comprehensive Guidelines (July 2025)

In a move that has redefined the liability landscape for audit firms, the Indian Computer Emergency Response Team (CERT-In) released the *Comprehensive Cyber Security Audit Policy Guidelines Version 1.0* on July 25, 2025. This document transcends the traditional scope of audit methodologies to regulate the auditor's own infrastructure and data handling practices.

2.1 The Jurisprudence of Audit Data

The most profound change introduced by the July 2025 guidelines is the reclassification of the auditor's role vis-à-vis the Digital Personal Data Protection Act (DPDPA). Historically, auditors operated under a "service provider" construct. The new guidelines, however, explicitly position the **Auditor Entity as a Data Fiduciary** regarding the data collected during the audit process.

This distinction is critical. As a Data Fiduciary, the auditor is not merely processing data on behalf of the Auditee (the Data Principal in this context); the auditor determines the purpose and means of processing that data to reach an audit opinion. Consequently, the auditor assumes direct liability for the security, privacy, and sovereignty of that evidence.

So, auditors are now directly liable under the Digital Personal Data Protection Act (DPDPA) for the security of the evidence you collect. Auditors are no longer just "checking" the client's compliance; they must demonstrate their own.

2.1.1 Data Localization and Sovereignty Mandates

The guidelines impose a strict data localization requirement that permits no ambiguity. All audit-related data must be stored on systems located **exclusively within India**. This requirement challenges the operational models of many global audit firms that rely on centralized, cloud-based audit management platforms often hosted in jurisdictionally agnostic locations like Ireland or Singapore.

For the DISSA auditor, this necessitates a rigorous validation of their own toolchain. Before an audit engagement begins, the auditor must verify the tenancy of their storage solutions.

Storage Component	Pre-2025 Practice	2025 Mandatory Requirement	Audit Implication

Cloud Storage	Global instances (e.g., OneDrive Global)	India-specific instances (e.g., AWS Mumbai Region)	Auditor must obtain "Data Residency Certificates" from their CSP.
SaaS Tools	Tools uploading logs to US/EU for analysis	Tools processing data locally or on Indian servers	Usage of foreign-hosted vulnerability scanners is a violation unless configured for local processing.
Cross-Border Sharing	Seamless sharing with Global Centers of Excellence	**Prohibited** without explicit written consent	Cross-border data transfer impact assessments must be conducted for internal peer reviews.

The prohibition on cross-border sharing extends to the auditor's own global headquarters. If a DISSA professional in Mumbai wishes to share audit working papers with a subject matter expert in London for quality review, this is now a regulated data transfer requiring specific consent from the Auditee.

2.2 Operational Security Protocols for Auditors

The guidelines do not merely suggest security; they mandate specific technical controls for the auditor's environment. The auditor must implement "Reasonable Security Safeguards" that mirror the rigor expected of the auditee.

2.2.1 Encryption and Storage Limitation

The entire dataset collected during the audit—ranging from configuration files and log dumps to interview notes—must be stored in **encrypted form**. This applies to data at rest on servers and, crucially, on mobile devices. The common practice of carrying unencrypted audit evidence on laptops is now a direct violation of CERT-In guidelines.

Furthermore, the principle of **Storage Limitation** is enforced through mandatory data destruction protocols. Upon the completion of the audit process, all data residing on mobile devices (laptops, tablets, external drives) must be **forensically wiped**. The guidelines specify that simple deletion is insufficient; the data must be rendered irretrievable to prevent recovery through forensic methods.

Auditor's Output Requirement: The auditor is now required to issue a **Certificate of Data Destruction** to the Auditee, formally attesting that all temporary data stores have been sanitized. This certificate becomes part of the Auditee's own compliance documentation.

2.2.2 Incident Management Obligations

In a reversal of roles, the auditor is subject to strict incident reporting norms. If the audit firm suffers a security breach involving Auditee data, the auditor must intimate the Auditee "without undue delay". This requirement compels audit firms to maintain their own 24x7 incident response capabilities. The reputational risk is severe; a breach in an audit firm undermines the credibility of every opinion they have issued.

2.3 Strategic Learning Material: The Pre-Audit Governance Framework

To comply with these rigorous standards, DISSA auditors must adopt a "Pre-Audit Governance Framework." This involves a preparatory phase before any testing begins.

Learning Exercise: Drafting the Data Handling Agreement

Scenario: You are the Lead Auditor for a mid-sized bank. You need to download 50GB of firewall logs for analysis.

- **Step 1 (Scope):** Verify the "Data Minimization" principle. Do you need 50GB, or is a representative sample of 5GB sufficient? The guidelines mandate the scope be limited to the "consolidated and updated asset inventory".
- **Step 2 (Transport):** Define the transfer mechanism. Email is insecure. A secure, India-hosted SFTP server with forced TLS 1.3 encryption is the standard.
- **Step 3 (Access):** Define the "Need-to-Know." Only the specific auditors assigned to the network review should have access to the logs. Transitioning employees must have access revoked immediately.
- **Step 4 (Destruction):** Agree on the retention period. If the contract is silent, the default retention is **1 year**, after which the logs must be destroyed.

2.4 Operational Mandates for the Auditor's Infrastructure

Before you send an engagement letter, your firm's infrastructure must meet three non-negotiable criteria.

A. Absolute Data Localization

The guidelines explicitly prohibit the storage of "Auditee-related data" outside India.

- **The Requirement:** Data must be stored *exclusively* on systems located within India.
- **Common Audit Pitfalls:**

    - **Cloud Storage:** Using global instances of Google Drive, Dropbox, or OneDrive where data residency is not pinned to an Indian region (e.g., ap-south-1 Mumbai).
    - **SaaS Tools:** Using vulnerability scanners (like certain cloud-based Jira or Trello instances) that process data on US/EU servers.
- **Audit Procedure (Internal):** You must obtain a "Data Residency Certificate" from your Cloud Service Provider (CSP) confirming that your specific tenant allows data storage *only* in Indian data centers.

B. The Cross-Border "Consent Barrier"

Sharing data with overseas entities is now restricted by default.

- **The Restriction:** You cannot share audit data with "overseas entities or partners" without **specific written consent** from the Auditee.
- **Impact on Global Firms:** If you are part of a global network (e.g., Big 4) and wish to send logs to a "Center of Excellence" in London or New York for analysis, you are violating the guidelines unless the Auditee explicitly signs off on this transfer.
- **Exception:** Disclosure mandated by law or regulatory bodies.

C. Encryption and Device Security

- **Mobile Device Mandate:** The entire dataset stored on mobile devices (laptops, external hard drives, tablets) must be stored in **encrypted form**.
- **Access Control:** Access to this data must be restricted. Crucially, employees who are "due for transition or retirement" must have their access revoked immediately. This prevents the common issue of a departing auditor taking a copy of the "Work In Progress" folder.

2.5 The Audit Lifecycle: Mandatory Protocols

Phase	Activity	New 2025 Requirement
1. Scoping	**Data Minimization**	The scope must be limited to the "consolidated and updated asset inventory" provided by the Auditee. You cannot fish for data outside this list.
2. Fieldwork	**Sensitive Audits**	For Critical Ministries/Departments, you must use the **MeitY Comprehensive Audit Program Checklist**, which comprises **282 control points**.[2]

3. Reporting	**Breach Notification**	If *your* laptop is stolen or *your* email is hacked containing client data, you must intimate the Auditee **"without undue delay"**.
4. Closure	**Forensic Wiping**	Simple deletion is illegal. Data on mobile devices must be wiped such that it is **"not retrievable through forensic methods"**.

2.6 Use Case: The "Global Expert" Trap

Scenario:

You are auditing a large Indian Fintech. You encounter a complex proprietary encryption algorithm you cannot crack. You decide to email the code snippet to your firm's cryptography expert based in Singapore for advice.

Analysis under 2025 Guidelines:

1. **Violation:** You transferred "Auditee-related data" to an "overseas entity" (Singapore).
2. **Liability:** If the Singapore expert's email is compromised, *you* (the Indian Auditor) are liable as the Data Fiduciary for the breach.
3. **Correct Procedure:**
    - Check your Engagement Letter. Does it have a "Cross-Border Data Transfer" clause?
    - If No: You must formally request written permission from the Fintech's CISO *before* sending the email.
    - If Yes: Ensure the transfer uses an encrypted channel.

3. Democratizing Defense: CERT-In 15 Elemental Controls for MSMEs (Sept 2025)

While the audit guidelines tighten the standards for assessors, the **15 Elemental Cyber Defense Controls for MSMEs**, released in September 2025, aim to raise the floor for the assessed. Recognizing that Micro, Small, and Medium Enterprises (MSMEs) constitute the vulnerable underbelly of the national supply chain, CERT-In has transitioned from "suggestive advisories" to a "mandatory baseline" for a significant portion of the economy.

3.1 The Strategic Intent: Supply Chain Hardening

The rationale behind this framework is the interconnectedness of modern digital ecosystems. A vulnerability in a small payroll processor (an MSME) can serve as a vector to compromise a large bank. By mandating these controls, CERT-In is effectively creating a "Trust Tier" of MSMEs eligible for government tenders and corporate integration.

The framework is structured around **15 Elemental Controls** which are further mapped to **45 Baseline Recommendations**. For the DISSA auditor, this simplifies the engagement. The audit criteria are no longer the exhaustive ISO 27001 standard, which is often cost-prohibitive for MSMEs, but a targeted list of "Must-Haves."

3.2 Detailed Analysis of the 15 Elemental Controls

The controls are categorized into Technical, Operational, and Organizational measures. An auditor must verify these controls are not just present, but *effective*.

3.2.1 Technical Hygiene and Asset Governance

1. Effective Asset Management (EAM):

The foundation of the framework is visibility. An MSME cannot protect what it does not know it owns.

- *Requirement:* Establish and maintain an asset management framework.
- *Audit Insight:* The auditor should look for a "Living Inventory." A spreadsheet updated last year is a finding. Automated discovery tools are preferred, but for smaller entities, a strictly managed manual process is acceptable if verified by physical inspection.

2. Secure Configurations (SC):

This control mandates the hardening of default settings.

- *Requirement:* Secure configuration of hardware and software.
- *Audit Insight:* The most common failure point in MSMEs is the "Default Admin" syndrome. The auditor must sample network devices (routers, switches) and verify that default credentials (admin/admin) have been changed and that unused ports are logically disabled.

3. Patch Management (PM):

- *Requirement:* Regular updates to fix security flaws.
- *Audit Insight:* Auditors must verify the *window of exposure*. It is not enough to patch; the patch must be applied within a reasonable timeframe (e.g., 7 days for critical vulnerabilities) after release.

4. Endpoint & Mobile Security (EMS):

- *Requirement:* Protection of end-user devices.
- *Audit Insight:* With the prevalence of BYOD (Bring Your Own Device) in MSMEs, this is critical. The auditor must check for Containerization (separating corporate data from personal data) and the presence of active, updated Anti-Malware solutions that cannot be disabled by the user.

3.2.2 Network and Perimeter Defense

5. Network and Email Security (NES):

- *Requirement:* Safeguarding communication channels.
- *Audit Insight:* Email is the primary attack vector. The auditor must verify the implementation of domain authentication protocols: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC. Absence of these is a critical finding as it allows domain spoofing.

6. Access Control and Identity Management (ACIM):

- *Requirement:* Restricting access based on roles.
- *Audit Insight:* The "Least Privilege" principle. Auditors should review the list of users with "Administrator" rights. In many MSMEs, the CEO often retains full admin rights despite lacking technical necessity—this is a high-risk configuration that must be flagged.

7. Robust Password Policy (RPP):

- *Requirement:* Strengthening authentication practices.

- *Audit Insight:* Beyond length and complexity, auditors should check for *rotation* policies and the prohibition of common passwords.

3.2.3 Operational Resilience

8. Logging and Monitoring (LM):

- *Requirement:* Tracking suspicious activity.
- *Audit Insight:* The critical compliance metric here is **Retention**. CERT-In mandates a **180-day retention period** for logs within Indian jurisdiction. An MSME keeping logs for only 30 days is non-compliant.

9. Incident Management (IM):

- *Requirement:* Capabilities to detect and respond.
- *Audit Insight:* Does the MSME have a "Cyber Crisis Management Plan"? Even a simple one-page document listing emergency contacts (CISO, IT Vendor, CERT-In) is acceptable, provided it is known to the staff.

10. Data Protection, Backup, and Recovery (DPBP):

- *Requirement:* Safeguarding sensitive data.
- *Audit Insight:* The "3-2-1 Rule" of backup (3 copies, 2 media types, 1 offsite) should be the benchmark. The auditor must witness a *Restore Test*. A backup that has never been restored is theoretically non-existent.

3.2.4 Organizational and Cultural Controls

11. Awareness and Training (AT):

- *Requirement:* Culture as a defense multiplier.
- *Audit Insight:* Documented attendance at security training sessions. Phishing simulation results are excellent evidence of effectiveness.

12. Third-Party Risk Management (TPRM):

- *Requirement:* Managing vendor risks.
- *Audit Insight:* Does the MSME hold its vendors to the same standards? Review vendor contracts for "Right to Audit" clauses.

13. Governance and Compliance (GC):

- *Requirement:* Accountability.
- *Audit Insight:* Identification of a "Security Officer." In small firms, this may be the owner, but the role must be formally acknowledged.

14. Physical Security (PS):

- *Requirement:* Protecting infrastructure.
- *Audit Insight:* Physical access controls to server rooms/racks. Biometrics or keyed locks with access logs.

15. Vulnerability Audits and Assessments (VAA):

- *Requirement:* Regular health checks.
- *Audit Insight:* Review of past VAPT reports and, crucially, the "Action Taken Report" (ATR) closing the findings.

3.3 The Regulatory Context: From Advisory to Mandatory

On **September 1, 2025**, CERT-In operationalized this framework.

- **The Mandate:** It is no longer optional. MSMEs are now required to undergo **annual baseline audits** by CERT-In empaneled auditors.
- **The Scope:** It applies to the "Digital Supply Chain." If a small payroll processor, logistics firm, or cloud integrator wants to do business with a regulated entity (like a Bank or Insurer), they must demonstrate compliance with these 15 controls.
- **The Structure:** The framework consists of **15 Elemental Controls** which are further mapped to **45 Baseline Recommendations**.

3.4. Strategic Audit Methodology: "The Baseline Approach"

When auditing an MSME, do not use the ISO 27001 checklist. It is too heavy.

- **Step 1:** Request the **Self-Assessment Report**. The guidelines encourage MSMEs to conduct self-assessments first.
- **Step 2:** Focus on **Implementation** over **Documentation**. An MSME might not have a 50-page "Access Policy" document (which is fine), but they *must* have MFA enabled (which is critical).

- **Step 3:** Check for **Cloud Shadow IT**. MSMEs often use free tools (WeTransfer, personal Gmail) for business data. This is a major violation of the *Data Protection (DPBP)* control.

3.5. Case Study: The "Supply Chain" Audit

Scenario:

You are the Internal Auditor for a large automobile manufacturer. You are tasked with auditing "FastLogistics," a small trucking company (MSME) that delivers your parts. FastLogistics has access to your inventory system via an API.

Audit Findings based on the 15 Controls:

1. **Observation:** FastLogistics uses a generic email address (logistics@gmail.com) for business communication.
    - **Verdict:** Violation of **Network & Email Security (NES)**. They lack domain-based security (SPF/DKIM), making them a prime target for Business Email Compromise (BEC).
2. **Observation:** The API key to your inventory system is saved in a text file on the dispatcher's desktop.
    - **Verdict:** Violation of **Secure Configurations (SC)** and **Data Protection (DPDP)**.
3. **Observation:** They have an Antivirus installed, but the license expired 3 months ago.
    - **Verdict:** Violation of **Endpoint Security (EMS)** and **Patch Management (PM)**.

Auditor's Recommendation:

Instead of demanding an ISO certification, you issue a "Conditional Pass": FastLogistics must implement domain-based email (e.g., @fastlogistics.in), renew the Antivirus, and move the API key to a secure vault within 30 days, or their API access will be revoked.

4. The Architecture of Resilience: SEBI CSCRF (April 2025)

The Securities and Exchange Board of India (SEBI) has traditionally been at the forefront of technology regulation. With the **Cyber Security and Cyber Resilience Framework (CSCRF)**, effective **April 30, 2025**, SEBI has deprecated a decade of fragmented circulars in favor of a unified, principal-based architecture.

Unlike previous circulars that focused on "prevention," CSCRF mandates "resilience"—the ability to recover from an attack. For the DISSA auditor, this requires moving beyond binary checklists (Yes/No) to calculating a quantitative **Cyber Capability Index (CCI)** and auditing complex artifacts like the **Software Bill of Materials (SBOM)**.

4.1 Structural Evolution: The Five-Pillar Model

The CSCRF is built upon standard global frameworks (like NIST) but adapted for the Indian capital markets. It moves beyond "Prevention" to emphasize "Resilience"—the ability to withstand and recover from attacks.

Pillar	Focus Area	Key Auditor Check
Governance	Accountability & Oversight	CISO must report directly to MD/CEO (Direct Accountability).
Identify	Asset & Risk Visibility	Comprehensive Inventory and Classification of Assets (Critical vs. Non-Critical).
Protect	Defense Mechanisms	Implementation of Data Leakage Prevention (DLP) and Encryption (Data at Rest/Transit).
Detect & Respond	Operational Agility	Integration with a 24x7 Security Operations Center (SOC).
Recover	Business Continuity	Defined RTO/RPO metrics validated through actual drills.

4.2 The Cyber Capability Index (CCI)

A novel introduction in the CSCRF is the **Cyber Capability Index (CCI)**. This is a quantitative metric designed to measure the maturity of a Regulated Entity (RE).

- **The Concept:** Instead of a binary "Compliant/Non-Compliant," the CCI provides a score (e.g., 0-100).

- **Audit Role:** The DISSA auditor is responsible for calculating this index based on the implementation percentage of various controls. This allows SEBI to benchmark entities across the sector.
- **Strategic Implication:** REs with low CCI scores will likely face heightened scrutiny and potentially higher capital requirements.

4.3 Supply Chain Integrity: The SBOM Mandate

One of the most technically advanced requirements in the CSCRF is the management of the **Software Bill of Materials (SBOM)**. This directly addresses risks arising from third-party libraries (e.g., the Log4j vulnerability).

Deep Dive: Auditing the SBOM

The auditor must verify compliance with Annexure-X of the CSCRF.

1. **Component Inventory:** The RE must maintain a list of all open-source and third-party components used in their critical applications.
2. **Hash Verification:** The SBOM must include SHA-256 hashes to verify the integrity of these components.
3. **Vulnerability Mapping:** The inventory must be cross-referenced with the CVE (Common Vulnerabilities and Exposures) database to identify known risks.
4. **Executive Sign-off:** The SBOM declaration must be signed by the MD/CEO, ensuring top-level awareness of software supply chain risks.

4.4 Cloud Adoption and STQC Certification

The CSCRF clarifies the stance on cloud computing. While cloud adoption is permitted, it is tightly regulated.

- **STQC Mandate:** REs must verify that their Cloud Service Providers (CSPs) use data centers that are **STQC (Standardisation Testing and Quality Certification)** certified.
- **Geographic Confinement:** Data must reside within India.
- **Audit Check:** The auditor must review the Service Level Agreement (SLA) with the CSP. Does it explicitly guarantee data residency? Does the RE retain the "Right to Audit" the cloud environment?

4.5 Case Study: The "SBOM" Investigation

Scenario:

You are auditing a mid-sized Stock Broker. They use a mobile trading app developed by a third-party vendor.

Audit Steps:

1. **The Request:** You ask for the SBOM of the mobile app (Version 3.0).
2. **The Pushback:** The broker says, "The vendor considers the code proprietary and won't share the SBOM."
3. **The Regulation:** SEBI CSCRF **Annexure X** mandates that REs *must* obtain assurance on the composition of software.
4. **The Finding:**
    - **Observation:** The RE failed to obtain an SBOM or a "Vulnerability Free Certificate" listing components.
    - **Risk:** If the app uses an outdated library (e.g., openssl with a Heartbleed flaw), the broker has no way of knowing.
    - **Impact on CCI:** The score for the "Identify" and "Supply Chain" domains is significantly reduced.
5. **Recommendation:** The broker must mandate the vendor to provide the SBOM as a condition of the contract, or implement a Software Composition Analysis (SCA) tool to generate it themselves.

5. The Expansion of Regulatory Nets: RBI Guidelines 2025

The Reserve Bank of India (RBI) has continued its aggressive stance on digital security, particularly in the payments space. The most significant development in 2025 is the **Master Directions on Regulation of Payment Aggregators**, updated **September 15, 2025**.

5.1 Unifying the Payment Ecosystem: PA-O and PA-P

The 2025 Master Direction eliminates the regulatory arbitrage between Online Payment Aggregators (PA-O) and Physical Payment Aggregators (PA-P). Entities that deploy Point-of-Sale (POS) terminals and QR codes at physical merchant locations are now fully regulated "Payment Aggregators" subject to the same cybersecurity rigor as online gateways.

Use Case: The "Offline" Fintech

Consider a Fintech startup providing soundboxes and QR codes to kirana stores. Previously, they might have operated with light oversight. Under the 2025 guidelines:

- They must have a **Board-approved Information Security Policy**.
- They must conduct **Background Checks** on merchants to prevent fraud.
- They are subject to **System Audits** by CERT-In empaneled auditors.

5.2 Critical Compliance Requirements

5.2.1 The "Secure by Design" Philosophy

The Master Directions mandate that applications be **"Secure by Design"**. This requires the integration of security into the Software Development Life Cycle (SDLC).

- **Audit Test:** The auditor should look for evidence of security reviews at the *design* phase, not just testing at the *deployment* phase. This includes Threat Modeling artifacts and Static Application Security Testing (SAST) reports.

5.2.2 Source Code Escrow

To mitigate vendor risk, PAs using third-party applications must ensure business continuity.

- **Requirement:** Obtain the source code or establish an **Escrow Arrangement**.
- **Audit Test:** Verify the Escrow Agreement. Is it active? When was the last time the source code deposited in the escrow was updated? If the vendor releases version 2.0 but the escrow holds version 1.0, the control has failed.

5.2.3 The "6-Hour" Incident Reporting Rule

The RBI enforces a stringent incident reporting timeline.

- **Requirement:** Unusual incidents (cyberattacks, outages, fraud) must be reported to the RBI within **6 hours** of detection.
- **Operational Challenge:** This demands a highly mature Incident Response process.
- **Audit Insight:** Auditors must review the "Incident Register." Compare the timestamp of "Detection" with the timestamp of the "Report to RBI." A delay beyond 6 hours is a regulatory violation.

5.3 IT Governance Master Direction (2025 Context)

While the *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices* was initiated earlier, its full implementation is the cornerstone of 2025 audits.

- **Governance Structure:** It mandates a **Board-level IT Strategy Committee** (ITSC) headed by an Independent Director. This separates IT *strategy* (Board) from IT *execution* (Management).
- **Audit Implications:** The auditor must review the minutes of the ITSC meetings. Are they discussing cyber risk, or just budgets? The depth of discussion is a key indicator of governance maturity.

5.4 Deep Dive: Critical Audit Components

A. Baseline Technology Recommendations (Annexure 1)

The Master Direction references **Annexure 1** as the non-negotiable technical baseline. As an auditor, this is your checklist.

Control Area	DISSA Audit Test
Data Sovereignty	**The "Residency" Check:** Verify that *all* payment data (end-to-end transaction details) is stored strictly within India. If the PA processes cross-border payments (PA-CB), verify that foreign data is deleted from Indian systems within the stipulated window (usually 24 hours) after settlement, retaining only transaction logs.

Merchant Compliance	**The "PCI-DSS" Check:** PAs cannot store Card-on-File data. They must use Tokenization. Audit the database: If you see a 16-digit card number, it is a critical finding. Check if the *merchants* connected to the PA are compliant or if the PA is enforcing security on them.
Fraud Prevention	**The "Velocity" Check:** Does the PA's system flag abnormal transaction velocities? (e.g., A small *Kirana* store suddenly processing ₹50 Lakhs in an hour). The auditor must test the efficacy of the Fraud Risk Management (FRM) engine.

B. Source Code Escrow & "Secure by Design"

To mitigate vendor risk, RBI mandates strict controls over third-party software.

- **Requirement:** If the PA uses a third-party application for critical functions (e.g., the switching software), they must own the source code OR have a **Source Code Escrow** arrangement.
- **The Audit Test:**
    1. **Review the Agreement:** Is there a tripartite agreement between the PA, the Software Vendor, and the Escrow Agent?
    2. **Verify Deposit:** Contact the Escrow Agent. When was the last time the source code was updated? If the live app is v4.0 but the escrow has v2.0, the control is ineffective.
    3. **Secure by Design:** Review the SDLC policy. Evidence of **Static Application Security Testing (SAST)** implies security was checked *during* coding, not just after.

C. The "6-Hour" Incident Reporting Rule

- **The Rule:** All unusual cyber incidents (ransomware, settlement manipulation, outages) must be reported to the RBI (CSITE cell) within **6 hours** of detection.
- **Audit Strategy:**
    - Pull the "Incident Log" for the last year.
    - Select a sample incident (e.g., "Database connectivity failure" on Jan 12th at 10:00 AM).
    - Check the "Reporting Timestamp" to RBI. If it is after 4:00 PM (16:00 hrs), it is a regulatory violation.

5.5 Case Study: The "Offline" QR Code Security Audit

Scenario:

You are auditing "QuickPay," a Fintech (PA-P) that deploys QR codes to street vendors.

Audit Findings:

1. **Observation:** QuickPay prints static QR codes on stickers. Malicious actors have been pasting their own QR stickers over QuickPay's stickers at merchant shops (Quishing).
    - **Regulatory Gap:** Failure in **Merchant Infrastructure Security** (Annexure 1).
    - **Recommendation:** QuickPay must implement a "Verified Merchant" registry or move to dynamic QRs on digital screens.
2. **Observation:** The sales team onboards merchants using a mobile app. The app stores the merchant's Aadhaar card photo in the sales agent's phone gallery.
    - **Regulatory Gap:** Violation of **Data Privacy** and **Storage Limitation** (RBI & DPDPA).
    - **Recommendation:** The app must capture the image directly to the server without saving it to the local gallery (Containerization).
3. **Observation:** QuickPay uses a cloud provider in Singapore for "faster analytics."
    - **Regulatory Gap:** Critical violation of **Payment Data Localization** norms. All data must be in India.

6. Auditing the Algorithm: India AI Governance Guidelines (MeitY - Nov 2025)

On November 5, 2025, the Ministry of Electronics and Information Technology (MeitY) unveiled the **India AI Governance Guidelines**. This framework represents India's distinct approach to AI regulation—prioritizing innovation and "Do No Harm" over heavy-handed legislation, yet establishing clear guardrails that require auditing.

Unlike the European Union's strict "AI Act," India's approach is **risk-based and sectoral**.

- **The Philosophy:** "Innovation over Restraint." The goal is to promote AI adoption while mitigating specific harms like bias, privacy violations, and manipulation.
- **Sectoral Enforcement:** There is no single "AI Regulator." Instead, SEBI regulates AI in trading, RBI in lending, and the National Health Authority in healthcare. You, as the auditor, act as the verification arm for these sectoral mandates.

6.1 The "Sutras" of Ethical AI

The framework is anchored in **Seven Guiding Principles (Sutras), f**or an auditor, these are the **Control Objectives**.

Sutra (Principle)	Audit Objective	The "DISSA" Audit Test
1. Trust	Ensure reliability and predictability.	**Test:** Review the model's accuracy metrics (Precision/Recall). Has the model been tested against "out-of-distribution" data (data it hasn't seen before)?
2. People First	Human oversight is non-negotiable.	**Test:** "Human-in-the-loop" check. If the AI recommends rejecting a loan, does a human officer review the decision before final rejection?
3. Fairness & Equity	Preventing algorithmic discrimination.	**Test:** Request the **Bias Assessment Report**. Has the model been tested for disparate impact across gender, religion, and pincodes?
4. Accountability	Defining liability.	**Test:** Review the Vendor Contract. If the third-party AI creates a financial loss, who pays? The contract must explicitly assign liability to a human or legal entity.
5. Understandable by Design	Transparency & Explainability (XAI).	**Test: "The Why Test."** Pick a specific output (e.g., User X classified as High Risk). Can the

		system explain *which* features (age, income, history) contributed to this score?
6. Safety & Resilience	Security against manipulation.	**Test: Adversarial Attack Testing.** Can the model be fooled by injecting noise into the input data (e.g., pixel manipulation in KYC images)?
7. Innovation over Restraint	Proportionality.	**Test:** Ensure controls do not stifle the core function. (Auditor judgment required).

6.2 The Action Plan: A Roadmap for Auditors

The guidelines lay out a phased implementation plan:

- **Short-Term:** Establishment of governance institutions and risk frameworks. Adoption of voluntary commitments by industry.
- **Medium-Term:** Publication of common standards and operationalization of AI incident reporting systems.
- **Long-Term:** Evolution of laws based on emerging capabilities.

For the auditor, the **Short-Term** actions are the immediate focus. Organizations are expected to adopt "voluntary commitments," which effectively become the audit criteria in the absence of hard law.

6.3 Algorithmic Auditing: New Methodologies

The guidelines introduce concepts that require new audit testing procedures.

1. Transparency and Disclosure:

- *Requirement:* Users must be informed when they are interacting with an AI system.
- *Audit Test:* Verify that chatbots, automated call systems, and robo-advisors explicitly declare their non-human nature at the start of the interaction.

2. Explainability (XAI):

- *Requirement:* Employ methods to explain AI decisions (e.g., loan denial).
- *Audit Test:* Review the model validation reports. Does the organization use techniques like SHAP (SHapley Additive exPlanations) or LIME to interpret model outputs? Can they explain *why* a specific decision was made?

3. Bias Mitigation:

- *Requirement:* Ensure fairness and equity.
- *Audit Test:* Examine the training data. Was it representative? Review "Bias Assessment Reports" that test the model against protected categories (gender, religion, region) to ensure no discriminatory patterns exist.

6.4 Practical Guidelines for Industry (Part 4)

MeitY provides specific instructions for the industry, which serve as your audit checklist.

- **Labeling & Disclosure:**
    - **Requirement:** Users must know they are interacting with an AI.
    - **Audit Test:** Initiate a chat with the customer support bot. Does the *first* message state, "I am an automated assistant"? If not, it violates the **Trust** Sutra.
- **Techno-Legal Solutions:**
    - **Requirement:** Use of Privacy Enhancing Technologies (PETs).
    - **Audit Test:** Verify if training data was anonymized or if techniques like **Federated Learning** (training on local devices without moving data) were used to protect privacy.

6.5 Case Study: The Algorithmic Bias Audit

Scenario:

You are auditing a "Neo-Bank" that uses a proprietary Machine Learning model to approve instant micro-loans.

Audit Investigation:

1. **Data Review:** You analyze the training data and find that 90% of the "successful repayment" examples are from Tier-1 cities.
    - **Risk:** The model is likely to reject applicants from rural areas (Tier-3) regardless of their actual creditworthiness because it hasn't "learned" from them.

2. **Outcome Analysis:** You sample 100 rejections. You find that applicants from a specific pincode are rejected at a rate 3x higher than others, despite similar income levels.
    - **Finding:** This is **"Digital Redlining"** and violates the **Fairness & Equity** principle.
3. **Explainability Check:** You ask the data science team, "Why was Mr. A rejected?"
    - **Response:** "The Neural Network is a black box; we don't know exactly."
    - **Verdict: Critical Non-Compliance** with the **Understandable by Design** principle.
4. **Recommendation:** The auditor mandates the implementation of **SHAP (SHapley Additive exPlanations)** or **LIME** values to interpret model decisions and requires retraining the model with a more diverse dataset.

7. The Privacy Assurance Audit

Regulatory Source: *Digital Personal Data Protection (DPDP) Rules, 2025 (Notified Nov 13, 2025)*

7.1 Learning Objective

To transition the IS Auditor from a "Security-First" mindset to a "Privacy-First" mindset. While security protects the *data*, privacy protects the *individual*. The 2025 Rules have operationalized the DPDPA 2023, making **Data Protection Impact Assessments (DPIA)** and **Independent Data Audits** mandatory for Significant Data Fiduciaries (SDFs).

7.2 The Regulatory Context: The "Fiduciary" Era

- **Effective Date:** The Rules were notified on November 13, 2025. While some provisions are immediate, SDF obligations (like audits) have a phased implementation (approx. 12-18 months), but auditors must start "Readiness Assessments" now.
- **The Shift:** The law moves from "ownership of data" to "fiduciary duty." The organization does not own the customer's data; it holds it in trust.
- **Audit Mandate: Rule 12** explicitly mandates that every **Significant Data Fiduciary (SDF)** must undertake an **Independent Data Audit** and a **DPIA** annually.

7.3 Deep Dive: Critical Audit Components

A. Auditing the "Consent Artifact" (Rule 3 & 4)

Consent is the lawful basis for processing. It must be free, specific, informed, unconditional, and unambiguous.

- **The "DISSA" Audit Test:**
    1. **The "Notice" Review:** Check the Privacy Notice presented *before* consent. Does it specify:
        - The exact personal data being collected?
        - The specific purpose? (e.g., "For delivering food" vs "For improving services").
        - The contact details of the Data Protection Officer (DPO)?

2. **The "bundled" Check:** Try to sign up. If checking "I agree to Terms" *automatically* checks "I agree to share data with partners," it is a **Dark Pattern** and illegal. Consent must be a separate, affirmative action.
3. **The "Withdrawal" Simulation:** Go to the app settings. Can you withdraw consent as easily as you gave it? (e.g., One click vs. sending an email). If it's harder, it's a non-compliance.

B. Auditing the "Consent Manager" Integration

The Rules introduce "Consent Managers" (CMs)—platforms that allow users to manage consent centrally.

- **Requirement:** Data Fiduciaries must be interoperable with registered Consent Managers.
- **Audit Check:** Ask the IT team: "If a user revokes consent via a Consent Manager app, does your system automatically stop processing their data in real-time?"
    - *Pass:* The API receives the signal and locks the data.
    - *Fail:* The signal is received but requires a manual email to the DB admin to delete data.

C. The Data Protection Impact Assessment (DPIA)

- **Requirement:** Before starting any new high-risk processing (e.g., Facial Recognition for attendance), an SDF must conduct a DPIA.
- **Audit Strategy:** Review the DPIA Report. It must contain:
    - Mapping of data flows.
    - Assessment of "Harm" to the Data Principal (financial loss, reputational injury).
    - Mitigation strategies (e.g., Tokenization, Aggregation).

D. The "72-Hour" Breach Notification

- **Rule:** Personal data breaches must be reported to the **Data Protection Board (DPB)** and the *affected users*.
- **Audit Check:**
    - **Drill Evidence:** Ask for logs of the last "Breach Drill." Did they generate the notification draft within timeline?

- **User Notification:** Does the draft notification explain *what* happened in plain English, or does it use vague legal jargon? (The latter is non-compliant).

7.4 Case Study: The "Legitimate Use" Trap

Scenario: You are auditing an Insurance Company (likely an SDF). They are sending "Happy Birthday" emails to policyholders and also pitching a new "Cancer Rider" policy in the same email. They claim this is "Legitimate Use" (Section 7) related to the policy.

Audit Investigation:

1. **Analysis:** "Legitimate Use" covers issuing the policy and sending premium reminders.
2. **The Gap:** Cross-selling a *new* product (Cancer Rider) is "Marketing," not "Service Delivery."
3. **Finding:** This processing requires **explicit consent**. Using data collected for the main policy to sell a rider without separate consent is "Purpose Limitation" violation.
4. **Verdict: Major Non-Compliance**. The company must scrub the marketing list or obtain fresh consent.

8. Critical Sector Resilience (Power & Non-Bank PSOs)

Regulatory Source: *CEA (Cyber Security in Power Sector) Regulations, 2025* & *RBI Master Directions on Cyber Resilience for Non-Bank PSOs (April 2025)*

8.1 Learning Objective

To audit **Critical Information Infrastructure (CII)**. This module covers "Kinetic Cyber"—where a hack causes physical damage (power cuts) or systemic financial collapse (payment failure). The focus is on **Architecture (Air Gaps)** and **Supply Chain (Trusted Sources)**.

8.2 Deep Dive: Power Sector Regulations (CEA 2025)

The Central Electricity Authority (CEA) regulations apply to Generation, Transmission, and Distribution companies (DISCOMs).

A. The "Air-Gap" & Zoning Audit

- **The Rule:** IT (Information Technology - Email, HR systems) and OT (Operational Technology - SCADA, PLCs) must be isolated.
- **The "DISSA" Audit Test:**
    - **Physical Inspection:** Go to the Control Room. Trace the cables from the SCADA server.
    - **The "Ping" Test:** Can you ping the Corporate Email Server from the SCADA Operator Console?
        - *Result:* If "Yes," the Air Gap is bridged. This is a **Critical Vulnerability**.
    - **Data Diode Check:** If data moves from OT to IT (for billing), is it via a hardware Data Diode (one-way traffic) or just a firewall? (Data Diodes are the gold standard).

B. The "Trusted Source" Procurement Audit

- **The Rule:** Equipment connecting to the grid (Smart Meters, RTUs) must be bought from "Trusted Sources" designated by the Ministry of Power to prevent hardware trojans.
- **Audit Check:**
    - Select a sample of newly procured Smart Meters.
    - Check the "Country of Origin" and "OEM Vendor."

- Verify if the vendor is on the "Restricted List" (e.g., from land-border sharing countries without prior permission).
- *Finding:* If non-compliant equipment is found, it must be ripped and replaced.

C. CISO & CSIRT-Power Alignment

- **Requirement:** Every power utility must have a CISO who reports to the Board and coordinates with **CSIRT-Power** (Computer Security Incident Response Team for Power).
- **Audit Check:** Review the CISO's reporting line. If the CISO reports to the CIO (IT Head), it is a conflict of interest and a regulatory violation.

8.3 Deep Dive: Non-Bank PSO Resilience (RBI - April 2025 Deadline)

This applies to Payment Aggregators, Wallets (PPIs), and Clearing Houses.

A. Managing "Unregulated" Vendors

- **The Risk:** PSOs often outsource KYC or Cloud hosting to unregulated tech firms.
- **The Rule:** The PSO is **fully liable** for the cyber resilience of its unregulated vendors.
- **The Audit Test:**
  - Ask for the **"Vendor Audit Report"**.
  - *Scenario:* The PSO says, "Our cloud provider is a global giant; we can't audit them."
  - *Verdict:* **Non-Compliance.** The PSO must obtain a "Third-Party Assurance Report" (e.g., SOC2 Type II) from the vendor that specifically covers the India region.

B. The "Secure by Design" Certification

- **Requirement:** Before any new payment app version goes live, it must be certified "free from vulnerabilities."
- **Audit Check:**
  - Select the latest app release (e.g., v5.2).
  - Ask for the **"Final VAPT Sign-off"** dated *before* the release date.
  - *Finding:* If the VAPT report is dated 2 days *after* the release, the control failed.

8.4 Case Study: The "Smart Meter" Hardware Trojan

Scenario: You are the auditor for a State Transmission Utility (STU). They have deployed 50,000 new Smart Meters to industrial clients.

Audit Investigation:

1. **Traffic Analysis:** You review the firewall logs of the "Head End System" (HES) that manages the meters.
2. **Anomaly:** You notice that every night at 3:00 AM, the meters send a 5KB packet to an unknown IP address not listed in the configuration.
3. **Investigation:** The IP traces back to a server in a foreign jurisdiction.
4. **Finding:** This is a potential "Command & Control" beacon (Hardware Trojan).
5. **Regulatory Violation:** Violation of **CEA Cyber Security Regulations** (Supply Chain Security) and **Data Localization** norms.
6. **Action:** Immediate quarantine of the meters and reporting to **CSIRT-Power** and **CERT-In**.

Synthesis: The Integrated Audit Strategy

The 2025 regulatory environment is dense, but it allows for an integrated audit strategy. While the bodies (CERT-In, RBI, SEBI) are different, the underlying themes are convergent.

Theme 1: Supply Chain Accountability

- *CERT-In:* MSME controls.
- *SEBI:* SBOM and SBOM certification.
- *RBI:* Vendor Risk Management and Escrow.
- *Audit Strategy:* Assess the "Extended Enterprise." The security of the entity is only as strong as its weakest vendor.

Theme 2: Operational Resilience

- *CERT-In:* 6-hour reporting.
- *SEBI:* Recover pillar, RTO/RPO.
- *RBI:* CCMP and 6-hour reporting.
- *Audit Strategy:* Move from "Document Review" to "Drill Observation." Witness the incident response simulation.

Theme 3: Data Sovereignty

- *CERT-In:* Auditor data localization.
- *SEBI:* Cloud data residency.
- *RBI:* Payment data localization.
- *Audit Strategy:* Verify the physical location of data storage. "Cloud" is not an acceptable answer; "Mumbai Region" is.

Conclusion

For the DISSA certified auditor, the regulations of 2025 present both a challenge and an opportunity. The challenge lies in the technical depth required—auditing an SBOM or an AI algorithm requires skills far beyond checking password policies. The opportunity, however, is the elevation of the audit function. The auditor is no longer a back-office compliance officer but a critical guardian of the digital economy's resilience. By mastering these frameworks—CERT-In's fiduciary mandates, SEBI's resilience pillars, RBI's governance strictures, and MeitY's ethical guardrails—the auditor ensures that India's digital infrastructure is not just compliant, but robust, sovereign, and trustworthy.