VIRTUAL CAIM

COMPLIANCE AUDIT

ISO/IEC 27001:2022 and DPDP Readiness Audit

Prepared for Example Finserv Ltd. (fictional client). Independent readiness audit of the information security management system and personal data protection practices.

SAMPLE REPORT - fictional engagement, sanitized

SAMPLE

Report ID	VC-SAMPLE-CMP-2026-001
Client	Example Finserv Ltd. (fictional NBFC)
Audit dates	Stage-1 style document review 5 to 9 October 2026; on-site and technical sampling 12 to 23 October 2026
Report date / version	30 October 2026 / v1.0 (Final)
Nature of audit	Pre-certification readiness audit. Not a certification audit.
Classification	Confidential (sample). Fictional data throughout.

Document control

Audit criteria	ISO/IEC 27001:2022 including Amendment 1:2024; Statement of Applicability v3.2; Digital Personal Data Protection Act, 2023 and the Rules as notified; client policies
Audit team	Lead Auditor, 2 Auditors, 1 technical expert (names and credentials in the audit plan, sample)
Independent reviewer	One reviewer, not part of the audit team (sample)
Distribution	CISO and ISMS Manager. Shared from an official mailbox through an encrypted channel.
Draft and final dates	Draft 27 October 2026, final 30 October 2026

Version history

Version	Date	Status	Description
0.1	16 Oct 2026	Draft	Interim note of Major nonconformity shared with CISO at the end of fieldwork week 1
0.9	27 Oct 2026	Draft	Full draft for factual accuracy
1.0	30 Oct 2026	Final	Issued

Contents

1. Executive summary 3
2. Scope, criteria and approach 4
3. Management system conformity (clauses 4 to 10) 5
4. Annex A control conformity (selected controls) 7
5. Nonconformities and corrective action plan 8
6. DPDP Act readiness 11
7. Certification-readiness verdict 13
8. Roadmap 13
Annex A. Evidence register 14
Annex B. Glossary 14
Annex C. Sign-off 14

IMPORTANT NOTE

This is a readiness audit by Virtual Caim. It is not an ISO/IEC 27001 certificate. Certification is granted by an accredited certification body after its own Stage 1 and Stage 2 audits. A readiness audit tells you how likely that outcome is and what to fix first.

SAMPLE

1. Executive summary

Example Finserv has a working ISMS with real strengths: committed leadership, a sound risk method, good technical controls and a responsive security team. Most gaps are about evidence, testing and keeping records current. One Major nonconformity (internal audit) must be closed before a certification body visits.

1	4	10	50%
MAJOR NONCONFORMITY	MINOR NONCONFORMITIES	OBSERVATIONS	DPDP READINESS
NC-01, internal audit	NC-02 to NC-05	improvement opportunities	weighted over assessable obligations

Of the 25 clause areas assessed, 15 conform fully, 8 conform with observations, 1 carries a minor nonconformity and 1 a major nonconformity. Of the 33 Annex A controls sampled, 19 conform fully.

Strengths

- Board-level ownership of information security, with a quarterly report from the CISO.
- Risk assessment covers 64 assets and is repeated after significant change.
- Strong endpoint, identity and monitoring controls: MFA on remote access, EDR on 98% of endpoints, 24x7 SOC.
- Pre-release penetration testing by a CERT-In empanelled auditor for every internet-facing release.

What needs attention

- **Assurance loop.** Internal audits skipped the technology controls and the DR site (NC-01). Without them the management review is working with less evidence than it should.
- **Proving that controls work.** Backup restore and DR tests (NC-03), log retention (NC-04) and supplier assessments (NC-05) need records.
- **Personal data.** The DPDP Act adds duties that the ISMS does not yet cover: granular consent, rights handling, and a Board and Data Principal breach notification step. Several obligations commence in phases under the Rules (see section 6).

VERDICT IN ONE LINE

CONDITIONALLY READY. Ready for a certification body Stage 1 after NC-01 and NC-02 are closed, and for Stage 2 after NC-03 to NC-05 are closed and one full management review cycle has used the corrected inputs. Estimated 10 to 12 weeks.

SAMPLE

2. Scope, criteria and approach

2.1 Audit scope and objectives

- Scope of the ISMS: design, development, operation and support of the retail lending platform and its supporting infrastructure, at the head office and one data centre, including the DSA portal and cloud-hosted workloads.
- Objectives: determine conformity to ISO/IEC 27001:2022 clauses 4 to 10 and selected Annex A controls, assess readiness against the DPDP Act, and give a verdict on certification readiness with a corrective action plan.
- Locations: head office, primary data centre. The disaster recovery site was in scope for document review only because of a facility access constraint (noted as a limitation).

2.2 Criteria

Criteria	Version	Use
ISO/IEC 27001:2022 with Amendment 1:2024	2022 and 2024	Clauses 4 to 10 and Annex A
Statement of Applicability	v3.2	Control selection and status
Digital Personal Data Protection Act, 2023	2023	Obligations of Data Fiduciaries, rights of Data Principals
DPDP Rules, 2025	Nov 2025	Procedural detail, phased commencement
CERT-In Directions	28 Apr 2022	Logging, time synchronisation, incident reporting
Client policies and procedures	Current	Internal requirements

2.3 Approach and sampling

Method	What we did	Sample
Document review	Policies, procedures, registers, records	63 documents
Interviews	Top management, ISMS manager, control and process owners, HR, procurement, IT	22 people
Observation	Operational practice, physical areas, SOC dashboard	6 walkthroughs
Technical sampling	Configuration checks on logging, retention, NTP, access, backup, TLS	22 log sources, 20 change records, 25 leavers, 10 supplier contracts, 8 releases
Evidence testing	Re-performance of reviews and approvals	Per control

Sampling followed a risk-based approach: higher criticality systems and processes were sampled more heavily. Sample sizes are stated in the evidence for each finding. Audit time was 24 auditor-days over 2 weeks.

2.4 Classification of results

Result	Meaning
Conforms	Requirement met with objective evidence
Observation	Met, but an improvement opportunity or an early risk was noted
Minor NC	A requirement is not fully met; isolated or limited lapse. Corrective action required
Major NC	Requirement not met, or a systemic failure that undermines the ISMS or its ability to achieve intended outcomes. Corrective action required before certification
N/A	Not applicable or not yet in force

2.5 Limitations

- Findings are based on a sample and on evidence made available at the time of the audit.
- DR site assessed by documents only.
- DPDP assessment is a readiness view and not legal advice. Commencement of different provisions follows the Government's notification and the Rules.

3. Management system conformity (clauses 4 to 10)

Clause	Requirement	Evidence examined and result	Result
4.1	Understanding the organisation and its context	Context register reviewed (v2.1, dated Mar 2026), covers regulatory, technology and market issues. Climate change considered as a relevant issue as required by Amendment 1:2024; record present.	Conforms
4.2	Needs and expectations of interested parties	Interested-party register lists regulators (RBI, CERT-In, DPB), customers, partners, DSAs, auditors. Requirements mapped. Climate-related requirements assessed.	Conforms
4.3	Scope of the ISMS	Scope statement covers lending platform, back-office and supporting infrastructure at two locations. One cloud service and DSA portal described as boundary interfaces.	Conforms
4.4	ISMS and its processes	Process map available; interactions defined. Two process owners were unable to explain inputs and outputs.	Observation
5.1	Leadership and commitment	Board minutes show approval of the policy and budget; CISO reports quarterly.	Conforms
5.2	Information security policy	Policy v4.0 approved and communicated. Staff interviews (9 of 9) aware of the policy.	Conforms
5.3	Roles, responsibilities and authorities	RACI in place for CISO, ISMS manager, asset and risk owners. Deputy for CISO not formally named.	Observation
6.1.1	Actions to address risks and opportunities	Risk methodology and criteria documented, aligned to enterprise risk appetite.	Conforms
6.1.2	Information security risk assessment	Risk register covers 64 assets and 118 risks; assessed in January 2026. Repeatable scoring method in use.	Conforms
6.1.3	Information security risk treatment	Treatment plan approved. Statement of Applicability (v3.2) lists all 93 controls, but 14 inclusion or exclusion decisions have no rationale and 6 controls are marked implemented without evidence reference.	Minor NC
6.2	Information security objectives and planning to achieve them	9 objectives, measurable, owners and dates assigned, tracked quarterly.	Conforms
6.3	Planning of changes	Change procedure refers to ISMS impact. Two of five sampled changes lacked ISMS impact notes (introduced as a clause by Amendment 1:2024).	Observation
7.1	Resources	Security budget approved; tooling in place.	Conforms
7.2	Competence	Competence matrix and training records for ISMS roles. 3 of 12 certificates expired.	Observation
7.3	Awareness	Induction and annual training; completion 91% (target 95%).	Observation
7.4	Communication	Communication plan defines what, when, whom and how. Evidence of use present.	Conforms
7.5	Documented information	Document control system in place, version history intact, access controlled.	Conforms
8.1	Operational planning and control	Operational controls documented; outsourced processes identified (SOC, cloud).	Conforms
8.2	Information security risk assessment (operation)	Risk assessment repeated after the platform release in June 2026.	Conforms
8.3	Information security risk treatment (operation)	Treatment plan tracked monthly; 79% actions closed against schedule.	Conforms
9.1	Monitoring, measurement, analysis and evaluation	Metrics defined for 9 objectives; 7 reported quarterly, 2 not reported in Q2.	Observation

Clause	Requirement	Evidence examined and result	Result
9.2	Internal audit	Audit programme exists but the technology controls (Annex A.8) and the disaster recovery site were not audited in the last 12 months. Auditor independence not evidenced for two audits. See NC-01.	Major NC
9.3	Management review	Reviews held in Feb and Aug 2026 with required agenda items. Inputs lacked internal audit results (see NC-01).	Observation
10.1	Continual improvement	Improvement log with 22 entries, 15 closed.	Conforms
10.2	Nonconformity and corrective action	Corrective action procedure followed for 11 of 12 sampled incidents; root cause recorded in 9.	Observation

SAMPLE

4. Annex A control conformity (selected controls)

The 93 controls of Annex A are grouped into organisational (37), people (8), physical (14) and technological (34) themes. We sampled the controls most relevant to a lending business and the risks in the risk register. Controls not listed were reviewed through the SoA only.

Control	Title	Evidence examined and result	Result
A.5.1	Policies for information security	Policy set reviewed annually; approved by management.	Conforms
A.5.7	Threat intelligence	Subscription to CERT-In advisories and a commercial feed; monthly review recorded.	Conforms
A.5.9	Inventory of information and other associated assets	Asset register covers 94% of sampled items. Cloud assets reconciled quarterly.	Observation
A.5.15	Access control	Access control policy in place; role matrix for lending platform reviewed.	Conforms
A.5.16	Identity management	Joiner, mover, leaver process followed for 24 of 25 sampled leavers within 24 hours.	Observation
A.5.18	Access rights	Quarterly access reviews performed for 3 of 4 critical systems; the DSA portal review was skipped in Q2.	Observation
A.5.19	Information security in supplier relationships	Supplier policy exists. 6 of 25 critical suppliers lack a security assessment on file. See NC-05.	Minor NC
A.5.23	Information security for use of cloud services	Cloud shared-responsibility matrix documented; configuration reviews quarterly.	Conforms
A.5.24	Incident management planning and preparation	Incident response plan v3.0, roles named, tested by tabletop in April 2026.	Conforms
A.5.26	Response to information security incidents	5 of 5 sampled incidents handled per procedure, with lessons learned.	Conforms
A.5.29	Information security during disruption	BCP security requirements included. Alternate site controls reviewed.	Conforms
A.5.30	ICT readiness for business continuity	Disaster recovery test for the core lending system not performed in the last 12 months. See NC-03.	Minor NC
A.5.31	Legal, statutory, regulatory and contractual requirements	Register includes IT Act, CERT-In Directions, RBI directions, DPDP Act. Owner assigned.	Conforms
A.5.34	Privacy and protection of PII	Privacy policy and notice exist. No record of processing activities that maps to DPDP requirements. See section 6.	Observation
A.6.3	Information security awareness, education and training	Phishing simulation conducted quarterly; click rate 6.2%, down from 9.8%.	Conforms
A.6.8	Information security event reporting	Staff know the reporting channel. 214 reports in 12 months.	Conforms
A.7.2	Physical entry	Badge access logs reviewed monthly at the data centre; visitor logs complete.	Conforms
A.7.4	Physical security monitoring	CCTV retention is 30 days. Policy asks for 90 days.	Observation
A.8.1	User endpoint devices	Endpoint standard enforced through MDM on 97% of devices.	Conforms
A.8.2	Privileged access rights	Privileged access managed through a vault with approval and session recording. 2 dormant admin accounts found.	Observation
A.8.5	Secure authentication	MFA enforced for remote access and administrators. Legacy authentication still allowed on one protocol.	Observation
A.8.7	Protection against malware	EDR on 98% of endpoints; email gateway sandboxing active.	Conforms

Control	Title	Evidence examined and result	Result
A.8.8	Management of technical vulnerabilities	Monthly scans, annual penetration test by an empanelled auditor. Critical patches closed within SLA in 19 of 21 cases.	Observation
A.8.9	Configuration management	Hardening baselines exist for operating systems and databases; drift checks monthly.	Conforms
A.8.13	Information backup	Backups run daily with success monitoring. Restore test for the core lending database not evidenced for the last 12 months. See NC-03.	Minor NC
A.8.15	Logging	Logs centralised in SIEM. Retention is 90 days for 6 of 22 sampled sources, against the organisation's own 180 day requirement. See NC-04.	Minor NC
A.8.16	Monitoring activities	24x7 monitoring by an external SOC; monthly reports reviewed.	Conforms
A.8.20	Networks security	Segmentation between corporate, production and DSA zones verified on firewall rules.	Conforms
A.8.24	Use of cryptography	Cryptography standard in place; TLS 1.2 or above on tested services; key management procedure documented.	Conforms
A.8.25	Secure development life cycle	SDLC policy with security gates. Security sign-off recorded for 7 of 8 sampled releases.	Observation
A.8.28	Secure coding	Secure coding guidelines issued; static analysis in the pipeline for two of five repositories.	Observation
A.8.29	Security testing in development and acceptance	Pre-release VAPT performed for all internet-facing releases in the last 12 months.	Conforms
A.8.32	Change management	Change records sampled (n=20) show approvals and rollback plans. One emergency change closed late.	Conforms

Summary of 33 sampled controls: 19 conform, 10 conform with observations, 4 minor nonconformities (NC-02 to NC-05 in part), 0 major.

5. Nonconformities and corrective action plan

Each nonconformity is stated against the requirement, supported by evidence and root cause analysis, and paired with a corrective action plan. Closure will be verified by Virtual Caim before the certification body is booked.

NC-01 Clause 9.2 Internal audit — Major NC

Requirement	The organisation shall conduct internal audits at planned intervals (clause 9.2.1) and plan, establish, implement and maintain an audit programme covering all in-scope processes (9.2.2).
Evidence	The 2026 audit programme lists 14 audits. 9 were completed. The technology controls (Annex A.8) and the disaster recovery site were not audited. Internal audit report IA-2026-04 was signed by the process owner who also owned the audited process (objectivity not evidenced). Management review of August 2026 did not receive audit results as an input.
Root cause	Audit planning relied on the ISMS manager's availability, and no back-up auditor was trained. No tracker flagged slipping audits to top management.
Corrective action plan	1. Appoint and train two additional internal auditors, one of them from outside the IT function. 2. Re-baseline the programme with a monthly tracker reported to the CISO. 3. Complete the A.8 and DR site audits. 4. Add audit results to the management review input checklist.
Owner / due	ISMS manager / 45 days
Verification	Re-audit evidence and updated programme

NC-02 Clause 6.1.3(d) Statement of Applicability Minor NC

Requirement	The organisation shall produce a Statement of Applicability with the necessary controls, justification for inclusion, whether implemented, and justification for exclusions of Annex A controls.
Evidence	SoA v3.2: 14 of 93 controls have no inclusion or exclusion rationale. 6 controls are marked Implemented without an evidence reference.
Root cause	SoA was updated by copying the 2013 mapping and not reviewed line by line after the 2022 transition.
Corrective action plan	1. Review all 93 controls with control owners. 2. Record rationale and evidence for each. 3. Approve SoA v3.3 through management review.
Owner / due	CISO / 30 days
Verification	SoA v3.3 sampled by auditor

NC-03 Annex A.8.13 Information backup and A.5.30 ICT readiness for business continuity Minor NC

Requirement	Backup copies shall be tested regularly (A.8.13). ICT readiness shall be planned, implemented, maintained and tested (A.5.30).
Evidence	No restore test evidence for the core lending database in the last 12 months. Last disaster recovery failover test dated September 2025. Recovery time objective is 4 hours; no evidence it was met.
Root cause	Test schedule depended on a business freeze that was repeatedly postponed.
Corrective action plan	1. Run a restore test within 30 days and record time taken. 2. Schedule a DR failover test with business sign-off for Q1. 3. Record results against the RTO and RPO in the BCP.
Owner / due	Head of IT / 30 days (restore), 90 days (DR)
Verification	Test reports with timings

NC-04 Annex A.8.15 Logging Minor NC

Requirement	Logs recording activities, exceptions, faults and relevant events shall be produced, stored, protected and analysed. The organisation's own policy sets 180 days of retention, in line with the CERT-In Directions of 28 April 2022.
Evidence	6 of 22 sampled log sources keep 90 days (legacy ERP, three branch devices, two application servers). NTP source for two branch routers could not be shown to trace to NIC or NPL servers.
Root cause	Retention was configured per system at deployment and not reviewed against the 2022 Directions.
Corrective action plan	1. Raise retention to 180 days and confirm storage within India. 2. Standardise NTP to the corporate source traceable to NIC or NPL. 3. Add retention and NTP checks to the monthly control review.
Owner / due	Head of IT, SOC lead / 30 days
Verification	Configuration screenshots, SIEM retention report

NC-05 Annex A.5.19 and A.5.20 Supplier relationships Minor NC

Requirement	Processes shall be defined and implemented to manage the information security risks of the use of suppliers, and relevant requirements shall be agreed in supplier agreements.
Evidence	6 of 25 critical suppliers have no security assessment on file. 4 of 10 sampled contracts do not include breach notification timelines or data return and deletion terms.
Root cause	Supplier assessments were done at onboarding only and the template predates the DPDP Act.
Corrective action plan	1. Complete assessments for the 6 suppliers. 2. Adopt a contract security and data protection schedule with breach notification timelines. 3. Review critical suppliers annually.
Owner / due	Procurement and CISO / 60 days
Verification	Assessment reports, signed addenda

SAMPLE

Observations and opportunities for improvement

Ref	Observation	Suggestion
OFI-01	Process owners unable to explain inputs and outputs (4.4)	Brief owners and add process map to induction
OFI-02	Deputy for CISO not named (5.3)	Name a deputy
OFI-03	3 of 12 competence certificates expired (7.2)	Renewal tracker
OFI-04	Awareness completion 91% (7.3)	Escalate to managers monthly
OFI-05	Two objectives not reported in Q2 (9.1)	Add to dashboard
OFI-06	Two dormant admin accounts (A.8.2)	Disable and add monthly check
OFI-07	Legacy authentication allowed on one protocol (A.8.5)	Disable after impact check
OFI-08	Static analysis on two of five repositories (A.8.28)	Extend coverage
OFI-09	CCTV retention 30 days against 90 day policy (A.7.4)	Align policy or storage
OFI-10	Asset register coverage 94% (A.5.9)	Reconcile with cloud inventory

SAMPLE

6. DPDP Act readiness

The Digital Personal Data Protection Act, 2023 sets duties for a Data Fiduciary, rights for Data Principals and penalties administered by the Data Protection Board of India after inquiry. The Rules were notified in November 2025 with phased commencement; most operative duties, including security safeguards and breach intimation procedure, are scheduled to apply from May 2027. The practical advice is to build now, because consent, rights and breach processes take months to change.

Provision	Obligation (summary)	Position found	Status	Action
s.4	Lawful purpose: personal data may be processed only with consent or for certain legitimate uses	Purpose register exists for lending and collections. Marketing purposes not separated.	Partly	Separate marketing purpose and record lawful basis per purpose
s.5, Rule 3	Notice: itemised description of data and purpose, with how to exercise rights and complain	Privacy notice published in English only. Does not list rights process or Board complaint route.	Partly	Update notice; offer English or an Eighth Schedule language
s.6	Consent: free, specific, informed, unconditional, unambiguous; withdrawal as easy as giving	Consent captured as a bundled tick box at onboarding. No withdrawal flow in the mobile app.	Gap	Granular consent, withdrawal in app and portal, consent log with version
s.7	Certain legitimate uses (for example, voluntary provision, compliance with law)	Legal basis for regulatory reporting and KYC retention documented.	Met	Keep register current
s.8(1), 8(2)	Data Fiduciary is responsible for compliance, including for processing by a Data Processor under a valid contract	Processor list has 18 entries. 4 of 10 sampled contracts lack DPDP terms (see NC-05).	Partly	Contract schedule, annual processor review
s.8(3)	Ensure completeness, accuracy and consistency where data is used to decide about the Data Principal or disclosed	Correction workflow for customer master data present; credit decisions use verified sources.	Met	Evidence sampling each year
s.8(4)	Appropriate technical and organisational measures to ensure compliance	ISMS controls assessed in sections 3 and 4. Privacy governance has no owner outside IT.	Partly	Name a privacy owner and add DPDP to the ISMS risk method
s.8(5), Rule 6	Reasonable security safeguards to prevent a personal data breach	Controls broadly strong (encryption, access control, MFA, logging). Gaps in log retention and restore testing.	Partly	Close NC-03 and NC-04; confirm vendor log retention for Rule 6 expectations
s.8(6), Rule 7	Intimate a personal data breach to the Board and affected Data Principals, in the prescribed form and manner	Incident plan covers CERT-In 6 hour reporting. No Board and Data Principal notification steps or templates.	Gap	Add breach assessment, notification templates and decision tree; tabletop
s.8(7), 8(8)	Erase personal data when consent is withdrawn or the purpose is no longer served, unless law requires retention; ensure processors also erase	Retention schedule exists for 11 of 18 data categories. No automated deletion in lending data store.	Partly	Complete retention schedule; deletion jobs; processor attestations
s.8(9)	Publish business contact information of the DPO or a person able to answer Data Principals	Grievance email published on the website; person not named.	Partly	Publish contact details of the named person
s.8(10), s.13	Effective grievance redressal mechanism; right of grievance redressal	Complaint handling exists for RBI Ombudsman matters; no DPDP-specific path or time-bound response.	Partly	Define DPDP grievance flow with response timeline

Provision	Obligation (summary)	Position found	Status	Action
s.9	Children: verifiable parental consent; no tracking or targeted advertising directed at children	Products are for adults. Age check at onboarding in place.	Met	Document the age-gating decision
s.10, Rule 13	Significant Data Fiduciary (if notified): DPO in India, independent data auditor, periodic impact assessment	Not notified at the date of the audit. Volume and sensitivity could qualify in future.	Check	Prepare DPIA method and auditor shortlist in advance
s.11 to s.14	Rights of Data Principals: access to information, correction and erasure, grievance, nomination	Access and correction handled through branch and email, no tracked workflow, no nomination option.	Gap	Build a rights request workflow with identity verification and SLA
s.16	Transfer of personal data outside India permitted except to countries restricted by the Government	No offshore processing identified. One SaaS tool hosts HR data in a non-India region.	Check	Confirm hosting location and sectoral rules (RBI localisation expectations)

Readiness score: Met counts 1, Partly 0.5, Gap 0, over 14 assessable obligations = 50%. Items marked Check are excluded. The score is an internal planning aid, not a legal conclusion.

Penalty exposure (for planning)

Failure	Maximum penalty under the Schedule
Failure to take reasonable security safeguards (section 8(5))	Up to Rs 250 crore
Failure to give the Board and affected Data Principals notice of a personal data breach (section 8(6))	Up to Rs 200 crore

Penalties are imposed by the Board after inquiry, considering factors listed in the Act. Other breaches carry separate ceilings in the Schedule.

Where ISO/IEC 27001 helps and where it does not

- **Helps:** risk assessment, access control, logging, supplier management and incident response give a base for Rules on safeguards and breach handling.
- **Does not cover:** consent management, notices, rights requests, children's data, retention and erasure duties. ISO/IEC 27701 is one option for a privacy information management system on top of the ISMS, or the same controls can be built into the current ISMS risk method.

SAMPLE

7. Certification-readiness verdict

VERDICT: CONDITIONALLY READY

The ISMS is mature enough for external certification once the Major nonconformity and the SoA finding are closed and the team has one clean management review. We do not recommend booking Stage 2 until all five nonconformities are closed with evidence.

Gate	Condition	Status	Earliest date
Gate 1: Stage 1 ready	NC-01 and NC-02 closed. SoA v3.3 approved.	Open	Week 6 (mid December 2026)
Gate 2: Stage 2 ready	NC-03, NC-04, NC-05 closed. Management review held with audit results as input.	Open	Week 12 (late January 2027)
Gate 3: DPDP foundation	Consent, rights workflow and breach notification path designed and tested	Open	Before May 2027 commencement

What the certification body will do

- **Stage 1:** a document and readiness review of the ISMS (scope, SoA, risk assessment, internal audit, management review).
- **Stage 2:** an on-site audit of implementation and effectiveness across the scope.
- **After certification:** surveillance audits in the following years and a recertification audit at the end of the three-year cycle.

Likelihood by area



Likelihood values are the auditors' judgement of readiness at the audit date and are shown to help planning. They are not statistical measures.

8. Roadmap

Wave	Timeline	Actions	Owner
1	0 to 30 days	NC-02 SoA review; NC-03 restore test; NC-04 retention and NTP; start NC-01 auditor appointments	CISO, Head of IT
2	31 to 60 days	NC-01 audits completed; NC-05 supplier assessments and contract schedule; internal audit report to management	ISMS manager, Procurement
3	61 to 90 days	DR failover test; management review with audit input; DPDP consent and rights design	CISO, Compliance
4	90 to 120 days	Book certification body; DPDP breach notification tabletop; privacy owner appointed	CISO, Compliance

Follow-up audit

After each nonconformity is reported closed, Virtual Caim performs a follow-up check of the evidence and issues a closure statement. For production-impacting controls, the check includes technical verification. The follow-up is scheduled by the Lead Auditor in agreement with the CISO.

Annex A. Evidence register

Ref	Evidence	Related result
EV-01	Context and interested parties registers v2.1	4.1, 4.2
EV-02	ISMS scope statement and process map	4.3, 4.4
EV-03	Board minutes (Feb, Aug 2026)	5.1, 9.3
EV-04	Risk register export and method	6.1.2
EV-05	Statement of Applicability v3.2	6.1.3, NC-02
EV-06	Internal audit programme and reports IA-2026-01 to 14	9.2, NC-01
EV-07	Restore test and DR test records	A.8.13, A.5.30, NC-03
EV-08	SIEM retention report, NTP configuration extracts	A.8.15, NC-04
EV-09	Supplier register, assessments, contracts (10 sampled)	A.5.19, NC-05
EV-10	Privacy notice, consent forms, processor list	DPDP s.5, s.6, s.8
EV-11	Incident plan and tabletop report (April 2026)	A.5.24, DPDP s.8(6)

Annex B. Glossary

Term	Meaning
ISMS	Information security management system
SoA	Statement of Applicability: list of Annex A controls, with inclusion, status and justification
NC	Nonconformity
OFI	Opportunity for improvement
Data Fiduciary	Person who determines the purpose and means of processing personal data (DPDP Act)
Data Principal	Individual to whom the personal data relates
Data Processor	Person who processes personal data on behalf of a Data Fiduciary
DPB	Data Protection Board of India
SDF	Significant Data Fiduciary, notified by the Central Government
DPIA	Data protection impact assessment
RTO, RPO	Recovery time objective, recovery point objective
NIC, NPL	National Informatics Centre, National Physical Laboratory (time sources named in the CERT-In Directions)

Annex C. Sign-off

The report is signed by the auditors who conducted the audit, reviewed and signed by a designated reviewer who is not part of the audit team, and authorised by the head of the auditing organisation. Blocks are shown for format only. This sample carries no signatures.

Lead Auditor and auditors	Independent reviewer	Head of auditing organisation
Sample	Sample	Sample

All names, systems, evidence and results in this document are fictional. ISO and IEC standards are the property of their publishers.