THIRD-PARTY RISK ASSESSMENT REPORT

Odisha e-Registration System

Aadhaar e-KYC Authentication Infrastructure

VERSION HISTORY

Version #	Prepared By	Verified By	Reviewed BY	Approved BY	Approved Date	Reason
1.0	Prasanta Kumar Samal	Rashmi Mohanty	Sujay Kumar Pati	Debaranjan Mohanty	21/08/2026	For Aadhar e-KYC Audit

Table of Contents

1. Purpose

The purpose of this report is to identify, evaluate, and manage information security risks associated with third-party vendors and service providers supporting the Odisha e-Registration System and Aadhaar e-KYC Authentication infrastructure.

This assessment ensures that vendors having access to Aadhaar-related infrastructure, services, or information comply with organizational security policies and UIDAI Aadhaar Authentication Regulations.

2. Scope

This assessment covers all third-party organizations providing services related to:

- Hosting Infrastructure
- Network Connectivity
- Aadhaar Authentication
- SMS Services
- Email Services
- Payment Services
- Security Audit
- Application Support
- Managed Infrastructure Services

3. Objectives

The objectives are to:

- Identify security risks associated with vendors.
- Evaluate confidentiality, integrity, and availability risks.
- Assess compliance with contractual and regulatory obligations.
- Verify implementation of appropriate security controls.
- Recommend mitigation measures.
- Ensure compliance with UIDAI security requirements.

4. Assessment Methodology

The assessment follows these steps:

1. Identify vendors.
2. Determine services provided.
3. Assess access to Aadhaar ecosystem.
4. Identify security risks.
5. Evaluate likelihood and impact.
6. Review existing controls.
7. Determine residual risk.
8. Recommend mitigation actions.

5. Vendor Assessment Criteria

The following parameters were evaluated:

- Nature of Services
- Access to Aadhaar Systems
- Access to Aadhaar Data

- Confidentiality Agreement (NDA)
- Logical Access Control
- Physical Security
- Security Certifications
- Incident Management Process
- Business Continuity
- Patch Management
- Access Review
- Compliance with UIDAI Guidelines

6. Vendor Risk Assessment

Vendor 1 – Odisha State Data Centre (OSDC)

Particular	Details
Service	Hosting Infrastructure
Access to Aadhaar Application	Yes
Access to Aadhaar Data	Infrastructure Level Only
Risk Rating	Medium

Risks

- Infrastructure outage
- Hardware failure
- Unauthorized physical access
- Network disruption

Existing Controls

- Tier III Data Centre controls
- 24×7 monitoring
- Biometric access
- CCTV surveillance
- Fire suppression systems
- Redundant power
- Network redundancy

Recommendations

- Continue periodic infrastructure security reviews.
- Review access logs quarterly.
- Verify backup restoration periodically.

Residual Risk: **Low**

Vendor 2 – UIDAI

Particular	Details
Service	Aadhaar Authentication
Access to Aadhaar Application	API Integration
Access to Aadhaar Data	Authentication Services
Risk Rating	Low

Risks

- Authentication service outage
- API changes
- Certificate expiry

Existing Controls

- Secure API integration
- Digital certificates
- TLS encryption
- UIDAI-approved authentication mechanisms

Recommendations

- Monitor certificate validity.
- Track UIDAI advisories.
- Validate API compatibility after updates.

Residual Risk: **Low**

Vendor 3 – OCAC

Particular	**Details**
Service	MPLS VPN / OSWAN Connectivity
Access to Aadhaar Application	Network Connectivity
Access to Aadhaar Data	No
Risk Rating	Medium

Risks

- WAN connectivity failure
- Latency
- Network interruption

Existing Controls

- MPLS VPN
- Secure routing
- Network monitoring
- Incident response procedures

Recommendations

- Quarterly connectivity review.
- Maintain escalation procedures.
- Verify redundancy where available.

Residual Risk: **Low**

Vendor 4 – SMS Gateway Provider

Particular	**Details**
Service	OTP Delivery
Access to Aadhaar Application	Yes
Access to Aadhaar Data	No
Risk Rating	Medium

Risks

- SMS delivery failure
- OTP delay
- Service interruption

Existing Controls

- Secure API
- TLS encryption
- Monitoring
- SLA commitments

Recommendations

- Monitor SMS delivery reports.
- Conduct periodic SLA reviews.

Residual Risk: **Low**

Vendor 5 – Email Gateway Provider

Particular	**Details**
Service	Email Notifications
Access to Aadhaar Application	Limited
Access to Aadhaar Data	No
Risk Rating	Low

Risks

- Email delivery delays
- Unauthorized email relay

Existing Controls

- Secure SMTP
- TLS encryption
- SPF/DKIM/DMARC (if applicable)

Recommendations

- Periodically review email logs.
- Monitor service availability.

Residual Risk: **Low**

Vendor 6 – Payment Gateway

Particular	**Details**
Service	Online Payment
Access to Aadhaar Application	Integrated
Access to Aadhaar Data	No
Risk Rating	Medium

Risks

- Payment transaction failure
- Service downtime
- API failure

Existing Controls

- Secure payment APIs
- TLS encryption
- Transaction monitoring

Recommendations

- Review gateway logs.

- Validate payment reconciliation.

Residual Risk: **Low**

Vendor 7 – Cyber Security Audit Agency (Cybernerd)

Particular	**Details**
Service	Vulnerability Assessment & Security Audit
Access to Aadhaar Application	Temporary Authorized Access
Access to Aadhaar Data	Restricted
Risk Rating	Low

Risks

- Unauthorized disclosure of findings
- Misuse of temporary credentials

Existing Controls

- NDA executed
- Limited-time access
- Access approval process
- Access revoked after audit completion

Recommendations

- Verify credential removal after audit.
- Retain audit reports securely.

Residual Risk: **Low**

7. Vendor Risk Summary

Vendor	**Overall Risk**	**Residual Risk**
OSDC	Medium	Low
UIDAI	Low	Low
OCAC	Medium	Low
SMS Gateway	Medium	Low
Email Gateway	Low	Low
Payment Gateway	Medium	Low
Cyber Security Audit Agency	Low	Low

8. Risk Treatment Plan

The following controls are implemented for third-party risk management:

- Vendor Security Assessment before onboarding
- Non-Disclosure Agreements (NDA)
- Access approval process
- Least privilege access
- Annual security review
- Compliance verification
- SLA monitoring
- Incident reporting requirements
- Access revocation after contract completion
- Periodic security audit

9. Monitoring & Review

Third-party risks are monitored through:

- Annual vendor risk assessment
- Quarterly service review meetings
- Security audit observations
- SLA monitoring
- Incident management reviews
- Change management process
- Periodic access reviews

10. Conclusion

The assessment concludes that third-party vendors supporting the Odisha e-Registration System have been evaluated for information security risks based on the services provided and their level of access to the Aadhaar authentication ecosystem. Appropriate administrative, contractual, technical, and operational controls have been implemented to minimize risks associated with third-party involvement. The organization will continue to perform annual vendor risk assessments, monitor vendor performance, review access privileges, and ensure compliance with UIDAI Aadhaar Authentication Regulations and organizational information security policies.

11. APPROVAL

Prasanta Kumar Samal	Rashmi Mohanty	Sujay Kumar Pati	Debaranjan Mohanty
(TPOC)	**(Project Head)**	**(MPOC)**	**(CISO)**