

DPDPA READINESS ASSESSMENT REPORT

Your Privacy, Our Priority.

PREPARED FOR

ABC Corporation

GENERATED BY

Verticz Intelligence Platform

POWERED BY

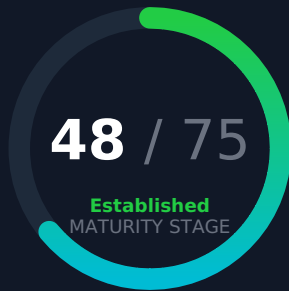
AZVIZORY

Advisory to Execution



02 EXECUTIVE SUMMARY

Overall DPDPA Readiness Score



DOMAINS ASSESSED
5



QUESTIONS COMPLETED
25 / 25



HIGH-RISK AREAS
4



COMPLIANCE READINESS
 • **Established**



ASSESSMENT DATE
July 14, 2026

“ Executive Insight

Your organisation demonstrates moderate DPDPA readiness with foundational governance and security controls established. Key improvements are recommended in consent management, data classification, and incident response governance. ”

03 OVERALL DPDPA READINESS SNAPSHOT

Domain Maturity Overview (Score out of 15)



Domain Score Summary

DOMAIN	SCORE (OUT OF 15)	PERCENTAGE	MATURITY STAGE	RISK LEVEL
1. Governance & Accountability	12 / 15	80%	Optimised	Medium
2. Data Inventory & Classification	8 / 15	53%	Established	High
3. Consent & Data Principal Rights	8 / 15	53%	Established	High
4. Security & Risk Management	12 / 15	80%	Optimised	Medium
5. Compliance, Audit & Inc. Response	8 / 15	53%	Established	High

04 MATURITY JOURNEY POSITIONING

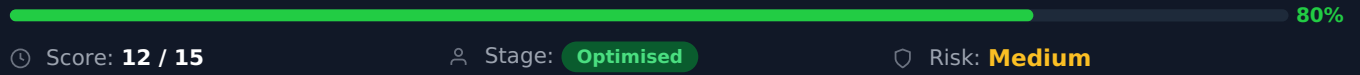


● You are currently at the **Established** stage.

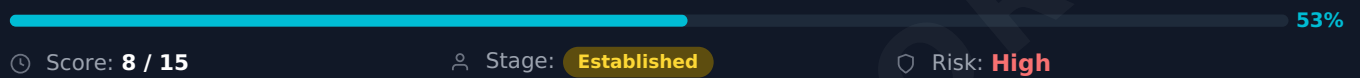
Defined frameworks and consistent execution.

05 DOMAIN-WISE ASSESSMENT SUMMARY

1. Governance & Accountability



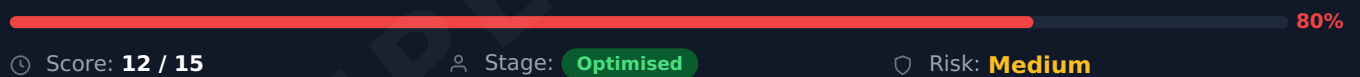
2. Data Inventory & Classification



3. Consent & Data Principal Rights



4. Security & Risk Management



5. Compliance, Audit & Inc. Response



06 DETAILED DOMAIN ANALYSIS

1. Governance & Accountability

Score: 12 / 15

Optimised

Medium Risk

Overview

Strong Governance & Accountability controls in place. Core frameworks are well-established.

Question-Level Summary

#	QUESTION	YOUR RESPONSE	SCORE	STATUS	OBSERVATION
1	Do you have a formally designated Data Protection Officer (DPO) or equivalent role?	Defined	2/3		Framework exists but needs enhancements.
2	Is there a documented data protection policy approved by leadership?	Mature	3/3		Strong implementation in place.
3	Are roles & responsibilities for personal data handling clearly defined across teams?	Defined	2/3		Framework exists but needs enhancements.
4	Does your leadership receive periodic updates on data privacy risks & compliance status?	Mature	3/3		Strong implementation in place.
5	Is there a defined escalation framework for data privacy incidents?	Defined	2/3		Framework exists but needs enhancements.

“ Domain Insight

Foundational controls are established and defined. Focus on consistent enforcement across all systems and formalizing undocumented exceptions.

06 DETAILED DOMAIN ANALYSIS

2. Data Inventory & Classification

Score: 8 / 15

Established

High Risk

Overview

Data Inventory & Classification is defined but inconsistent. Foundational elements exist but gaps remain.

Question-Level Summary

#	QUESTION	YOUR RESPONSE	SCORE	STATUS	OBSERVATION
1	Do you maintain an updated inventory of personal data processed across systems?	Defined	2/3		Framework exists but needs enhancements.
2	Is personal data classified based on sensitivity (e.g., personal vs sensitive personal data)?	Defined	2/3		Framework exists but needs enhancements.
3	Do you track data flow across third parties / vendors / systems?	Adhoc	1/3		Process is inconsistent and needs formalization.
4	Are data retention periods defined and enforced?	Defined	2/3		Framework exists but needs enhancements.
5	Can you quickly identify where a specific individual's data resides?	Adhoc	1/3		Process is inconsistent and needs formalization.

“ Domain Insight

Controls are implemented in an ad-hoc manner. Standardize processes, train staff, and implement consistent monitoring to reduce risk.

06 DETAILED DOMAIN ANALYSIS

+ 3. Consent & Data Principal Rights

Score: 8 / 15

Established

High Risk

Overview

Consent & Data Principal Rights is defined but inconsistent. Foundational elements exist but gaps remain.

Question-Level Summary

#	QUESTION	YOUR RESPONSE	SCORE	STATUS	OBSERVATION
1	Do you capture explicit and informed consent before collecting personal data?	Defined	2/3	●	Framework exists but needs enhancements.
2	Is there a mechanism to withdraw consent easily?	Defined	2/3	●	Framework exists but needs enhancements.
3	Can users access, correct, or erase their data upon request?	Defined	2/3	●	Framework exists but needs enhancements.
4	Do you track and respond to data principal requests within defined timelines?	Defined	2/3	●	Framework exists but needs enhancements.
5	Are consent notices clear, purpose-specific, and compliant with DPDPA language?	Not Initiated	0/3	●	Not yet initiated. Immediate attention needed.

“ Domain Insight

Controls are implemented in an ad-hoc manner. Standardize processes, train staff, and implement consistent monitoring to reduce risk.

06 DETAILED DOMAIN ANALYSIS

4. Security & Risk Management

Score: 12 / 15

Optimised

Medium Risk

Overview

Strong Security & Risk Management controls in place. Core frameworks are well-established.

Question-Level Summary

#	QUESTION	YOUR RESPONSE	SCORE	STATUS	OBSERVATION
1	Are technical safeguards (encryption, access control, logging) implemented?	Mature	3/3	●	Strong implementation in place.
2	Do you perform periodic VAPT / security assessments?	Defined	2/3	●	Framework exists but needs enhancements.
3	Is there a data breach detection and response mechanism?	Defined	2/3	●	Framework exists but needs enhancements.
4	Are employees trained on data privacy & cybersecurity awareness?	Mature	3/3	●	Strong implementation in place.
5	Do you conduct third-party/vendor risk assessments?	Defined	2/3	●	Framework exists but needs enhancements.

“ Domain Insight

Foundational controls are established and defined. Focus on consistent enforcement across all systems and formalizing undocumented exceptions.

06 DETAILED DOMAIN ANALYSIS

5. Compliance, Audit & Inc. Response

Score: 8 / 15

Established

High Risk

Overview

Compliance, Audit & Incident Response is defined but inconsistent. Foundational elements exist but gaps remain.

Question-Level Summary

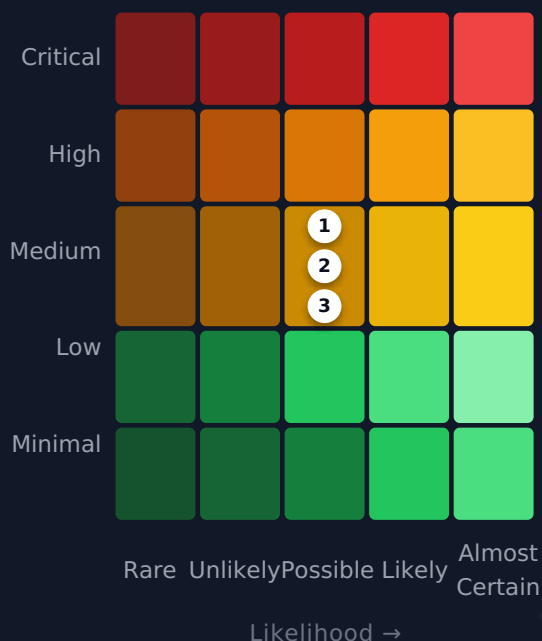
#	QUESTION	YOUR RESPONSE	SCORE	STATUS	OBSERVATION
1	Do you maintain audit logs and compliance documentation for DPDPA?	Defined	2/3	●	Framework exists but needs enhancements.
2	Is there a formal incident response plan for data breaches?	Defined	2/3	●	Framework exists but needs enhancements.
3	Can you notify authorities and affected individuals within regulatory timelines?	Defined	2/3	●	Framework exists but needs enhancements.
4	Do you conduct periodic internal audits or compliance reviews?	Defined	2/3	●	Framework exists but needs enhancements.
5	Have you mapped your processes against DPDPA obligations and gaps?	Not Initiated	0/3	●	Not yet initiated. Immediate attention needed.

“ Domain Insight

Controls are implemented in an ad-hoc manner. Standardize processes, train staff, and implement consistent monitoring to reduce risk.

07 RISK & GAP ANALYSIS

Risk Heatmap



Top Risks Identified

- Incomplete Data Inventory**
Severity **Medium**
Defined but inconsistent
- Missing Consent Lifecycle Management**
Severity **Medium**
Defined but inconsistent
- Incomplete Compliance Documentation**
Severity **Medium**
Defined but inconsistent

Risk Categories



Governance Risk



Operational Risk



Legal Risk



Technology Risk



Privacy Exposure

08 TOP GAPS & RECOMMENDATIONS

1 Do you capture explicit and informed consent before collecting personal data?

Implement explicit, informed, and purpose-specific consent mechanisms, ensuring clarity and transparency in user communication.

Impact: **High**

Priority:
Immediate

2 Is there a defined escalation framework for data privacy incidents?

Implement a formal escalation and incident management framework with contacts, triggers, and decision rights for data leakage incidents.

Impact: **High**

Priority:
Immediate

3 Do you maintain an updated inventory of personal data processed across systems?

Develop and maintain a centralized personal data inventory, capturing data types, systems, purposes, and ownership.

Impact: **High**

Priority:
Immediate

4 Do you track data flow across third parties / vendors / systems?

Perform end-to-end data flow mapping, including third-party transfers and integrations.

Impact: **Medium**

Priority:
Immediate

5 Do you have a formally designated Data Protection Officer (DPO) or equivalent role?

Formally designate a Data Protection Officer (DPO) or equivalent role with clearly defined responsibilities and a direct reporting line to senior management. Establish a dedicated email id for all communications.

Impact: **Medium**

Priority:
Immediate

09 GO BEYOND ASSESSMENT WITH AZVIZORY

End-to-end advisory and technology solutions for complete DPDPA compliance

1 Gap Assessment



- Deep-dive privacy maturity assessment
- Risk & gap identification
- Regulatory alignment
- Actionable roadmap

[Request Expert Assessment →](#)

2 Policy & Procedure Development / Revamp



- DPDPA-aligned policies and procedures
- Role-based SOPs and governance frameworks
- Templates, playbooks & guidelines
- Review and optimization

[Build Governance Framework →](#)

3 Tech-Enabled DPDPA Compliance Solution

Full-stack platform to operationalize privacy and ensure continuous compliance.



Data Discovery &
Classification



Consent &
Cookie
Management



Principal Rights
Management



Breach
Management



Deployment &
Integration

[Explore Azvizory Platform →](#)

10 ROADMAP TO COMPLIANCE



Phase 1 0 – 3 Months

Build the Foundation

- Strengthen governance and roles
- Develop / update policies
- Baseline risk assessment



Phase 2 3 – 6 Months

Gain Visibility

- Data inventory & classification
- Map data flows and systems
- Identify high-risk data



Phase 3 6 – 9 Months

Operationalize Controls

- Consent & rights management
- Incident response readiness
- Vendor and third-party oversight



Phase 4 9 – 12 Months

Automate & Monitor

- Deploy tech-enabled solutions
- Continuous monitoring & audit
- Drive continuous improvement

11 CONCLUSION & NEXT STEPS

Your Current DPDPA Readiness

48 / 75

Overall Score

Established

Maturity Stage

Compliance Readiness: **Established**

Suggested Next Actions



Improve consent management and lifecycle visibility



Strengthen data inventory and classification



Establish robust incident response and breach management



Implement continuous monitoring and audit mechanisms

Need Expert Guidance?

Azvizory experts can help you strengthen your privacy program and achieve full DPDPA compliance.



**Schedule
Consultation**



**Contact
Azvizory**



**Explore
Solutions**

13 DISCLAIMER & THANK YOU

This assessment is based on the information provided by your organization and reflects maturity levels as on the assessment date. It is intended for informational purposes only and should not be considered as legal advice. Organizations are responsible for ensuring their compliance with applicable laws and regulations.



Informational Purpose Only



Not Legal Advice



Based on Self-Assessment



Confidential & Proprietary

Thank You!

Together, let's build a privacy-first future.



Where insight leads



AZVIZORY

advisory to execution