Grant Thornton | 90 in Bharat and beyond

#GTBharat SHAPING VIBRANT INDIA

Incident response management lifecycle for DPDPA

Incident management under the Digital Personal Data Protection Act (DPDPA), 2023[1] mandates a structured approach to detect, respond to and report personal data breaches. It emphasises timely incident identification, impact containment, and compliance with reporting obligations to safeguard personal data. Organisations implement robust security measures, maintain detailed logs, and ensure forensic readiness to meet strict breach notification timelines. This approach mitigates risks and reinforces accountability and trust in data handling.

Incident management under DPDPA ensures organisations uphold data protection principles, maintain trust, and avoid penalties. With strict timelines and comprehensive reporting obligations, it compels businesses to integrate governance, technical controls, and documentation into cybersecurity strategies. Robust incident management enables compliance with the 72-hour SLA, ensures timely reporting, regulatory adherence, and accelerates recovery for improved cyber resilience and incident response.

[1] https://www.meity.gov.in/static/uploads/2025/11/53d50e6e5dc0bfa85ebd78686cadad39.pdf

Why is an incident management framework needed?

Cyberattacks are becoming more frequent, complex, and unpredictable, forcing organisations to safeguard sensitive data, maintain operational continuity, and comply with strict regulations. Organisations must implement a proactive and well-structured incident management framework because it plays a critical role in modern cybersecurity strategy.

Future threats will grow more sophisticated, making a robust, updated, and compliant incident management framework essential for resilience and regulatory adherence. The framework delivers a structured, repeatable process to manage breaches efficiently, ensure legal compliance, and reduce penalties. By enabling rapid containment and recovery, it minimises financial loss, reputational damage, and operational disruption. It also ensures proper evidence collection, supports investigations, and drives continuous improvement through root cause analysis and post-incident reviews - strengthening security posture and future readiness.

Incident response under DPDPA: A legal imperative

The DPDPA, 2023 mandates a compliance-driven approach to incident response, making it a core element of organisational data protection strategies. Unlike traditional frameworks focused on technical containment, DPDPA enforces legal accountability, timely reporting, and transparency in managing personal data breaches.

Incident response under DPDPA is a legal obligation, not an option. Non-compliance leads to heavy penalties and reputational damage. Organisations must align Digital Forensics and Incident Response (DFIR) processes with DPDPA by:

1. Enabling rapid breach investigations within the mandated 72-hour timeframe.
2. Completing regulatory reporting within strict timelines.
3. Maintaining comprehensive documentation for audits.

Operationalising DPDPA: Key pillars for privacy and security

DPDPA sets the operational and legal foundation for data protection. It mandates incident management, breach reporting, governance, and documentation while defining obligations for Data Fiduciaries and rights for Data Principals to ensure privacy and security. The Act compels organisations to integrate privacy governance, incident management, and forensic readiness into operations. Compliance is mandatory - failure results in reputational damage and heavy penalties. To comply with DPDPA and strengthen data protection, organisations must implement these four critical pillars:

01 Prevention and security controls

- Implement security controls (encryption, access controls, firewalls).
- Conduct vulnerability assessments and penetration testing.
- Enable continuous monitoring and logging for incident detection.
- Perform Data Protection Impact Assessments (DPIA) for high-risk processing.
- Disable unused features/services and enforce centre for information security (CIS) benchmarks.

02 Detection and incident response

- Develop an incident response plan aligned with DPDPA.
- Define roles and responsibilities for handling incidents.
- Set up escalation procedures and maintain breach registers.
- Appoint Data Protection Officers for compliance, advisory, oversight, liaison, documentation and DPIAs.

03 Breach notification

- Notify Data Protection Board without delay and update findings within 72 hours.
- Share breach details with Data Principals, notify them 48 hours before processing.
- Document notifications and evidence, communicate via email.

04 Governance and documentation

- Retain breach-related logs for at least one year; erase personal data after retention period.
- Include breach clauses in vendor contracts.
- Prepare annual compliance reports for significant data fiduciaries.
- Document policies, timelines and escalation matrix.
- Maintain audit reports for internal/external audits and proof of DPDPA compliance.

Why compliance is critical

The Act imposes strict obligations on organisations for lawful processing, security safeguards, and breach reporting. Non-compliance triggers serious legal, financial, and reputational consequences:

- **Financial penalties:** Regulators can impose fines up to INR 250 crore for severe violations, including failure to report breaches or implement safeguards.
- **Regulatory action:** Authorities initiate investigations, mandate audits, and suspend data processing when breaches occur.
- **Legal risks:** Organisations face litigation and liability for damages caused by mishandling personal data.
- **Reputational damage:** Businesses lose customer trust, suffer negative publicity, and risk strained relationships.
- **Operational disruption:** Investigations lead to activity suspension, high remediation costs and resource strain.
- **Strategic impact:** Companies risk losing competitive advantage and market credibility, especially in BFSI and tech sectors.

5 | Incident management lifecycle for DPDPA

How Grant Thornton Bharat can assist clients

Assess DFIR readiness

- Evaluate current incident response capabilities against DPDPA mandates.
- Identify gaps in detection, containment, and reporting processes.
- Provide a maturity scorecard and roadmap for improvement.

Design incident response framework

- Develop customised SOPs and playbooks aligned with DPDPA requirements.
- Define roles, responsibilities, and escalation paths for breach handling.
- Integrate regulatory timelines and reporting templates.

Perform forensic investigation and evidence handling

- Acquire and analyse digital forensic evidence for compromised systems.
- Ensure chain of custody documentation for legal admissibility.
- Support root cause analysis and remediation planning.
- Provide validated evidence for regulatory investigations and legal proceedings.

Support breach notification and compliance

- Prepare breach reports for submission to the Data Protection Board.
- Draft communication templates for notifying affected individuals.
- Ensure compliance with DPDPA timelines and documentation standards.

Deliver governance and training

- Conduct incident management workshops for internal teams.
- Provide awareness sessions on regulatory obligations and forensic readiness.
- Establish governance structures for ongoing compliance.

Implement continuous monitoring and threat hunting

- Deploy proactive monitoring solutions for anomaly detection.
- Offer threat hunting services to identify potential breaches early.
- Integrate security information and event management (SIEM) and data loss prevention (DLP) tools for enhanced visibility.

Conclusion

Incident Management under DPDPA is vital for organisational resilience and trust. A structured approach to detecting, responding to, and reporting data breaches helps minimise harm, meet legal obligations, and maintain stakeholder confidence. Integrating DFIR strengthens this framework by enabling rapid detection, preserving evidence, analysing root causes, ensuring compliance, and driving continuous improvement. Together, DPDPA-compliant incident management and DFIR readiness ensure legal compliance, operational continuity and a robust security posture - positioning organisations to respond confidently and effectively to data breaches.

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

● Ahmedabad ● Bengaluru ● Chandigarh ● Chennai ● Dehradun
● Gandhinagar ● Goa ● Gurugram ● Hyderabad ● Indore ● Kochi
● Kolkata ● Mumbai ● New Delhi ● Noida ● Pune

Scan QR code to see our office addresses

www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP | @GrantThorntonBharat | @GrantThornton_Bharat
@GrantThorntonIN | @GrantThorntonBharatLLP | GTBharat@in.gt.com

Connect with our experts

Gaganpreet Singh Puri
Partner and Crisis & Resilience Leader
Grant Thornton Bharat
E: gagan.puri@in.gt.com

Akshay Garkel
Partner and Cyber Monitoring & Response Leader
Grant Thornton Bharat
E: akshay.garkel@in.gt.com

Jaspreet Singh
Partner and Cyber Assurance & Governance Leader
Grant Thornton Bharat
E: jaspreet.singh2@in.gt.com

Kush Wadhwa
Partner, Cyber Monitoring & Response
Grant Thornton Bharat
E: kush.wadhwa@in.gt.com

15361 | SS | RK