Deloitte.

Data Protection

Private and confidential
February 2021

Data protection overview

With emerging threats to an enterprise's operational business environment, data confidentiality, integrity and availability is at significant risk and requires protection. Hence, it is imminent for an organisation to adopt robust data protection platforms and landscapes aligned to business operations and requirements

Key business challenges

Over the last three years, renowned organisations were imposed with financial penalties beyond 100 million. The cost to organisations comes at each stage of the incident response lifecycle; detection, notification, post response and the cost of business.

- 52% of data breaches reported were through theft and loss of information due to lack of sufficient data protection
- 50% of these data compromised due to breaches were Personally Identifiable Information (PII), and 38% credential data
- 30% of data breaches were through an insider leak and 25% through hacking and malware sources.

Extended organisation's blurred environment

Extended and blurred organisational environment that have hybrid cloud ecosystem or third-party vendor environment

Business As Usual (BAU) Isolated technology deployment

Sub optimal operation of business with technologies working in isolation

Emerging compliance regulatory requirements obligations

Regulatory requirements for data protection:

- **GDPR-** Articles 83 and 84
- **PDPB** Sections 57-61
- **CCPA-** Section 1798.155

Emerging potential threat landscape

Internal and external threats:

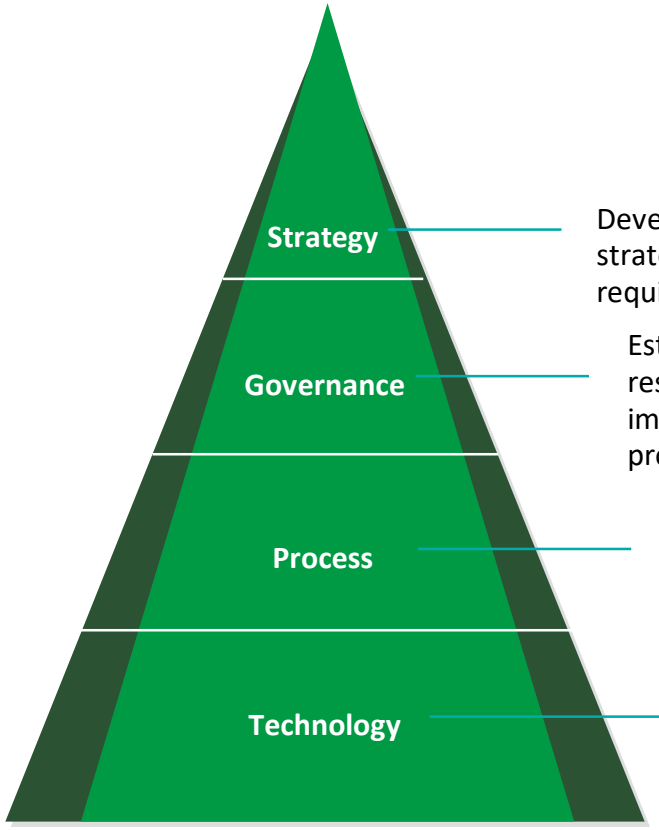
- Social engineering
- DDoS attacks
- Unauthorised data sharing outside organisation

Source: 1. https://www.marketsandmarkets.com/Market-Reports/data-protection-market-214254944.html
2. https://www.cisomag.com/6-times-data-regulators-churned-out-high-penalties-in-2019/
3-https://www.trendmicro.com/vinfo/us/security/definition/data-breach
4. https://cdn2.hubspot.net/hubfs/468115/Campaigns/2017-Ponemon-Report/2017-ponemon-report-key-findings.pdf

Data protection overview and key driving factors

Managing data protection involves establishing an organisation-wide programme, governance mechanisms, and implementing processes and technology for the protection of sensitive and confidential information

Managing data protection scope



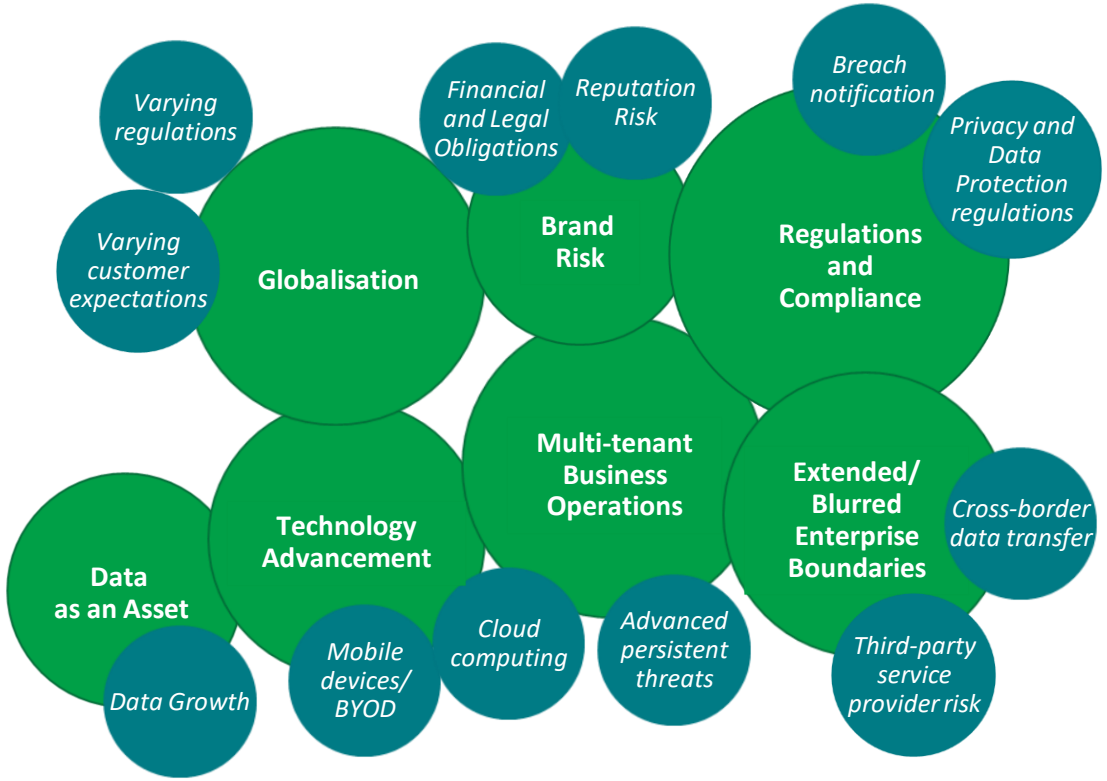
Develop a data protection programme strategy based on the business objectives and requirements.

Establish organisations structure, roles, responsibilities to govern and direct the implementation of the data protection programme.

Define and implement processes for data protection programme operations and sustenance.

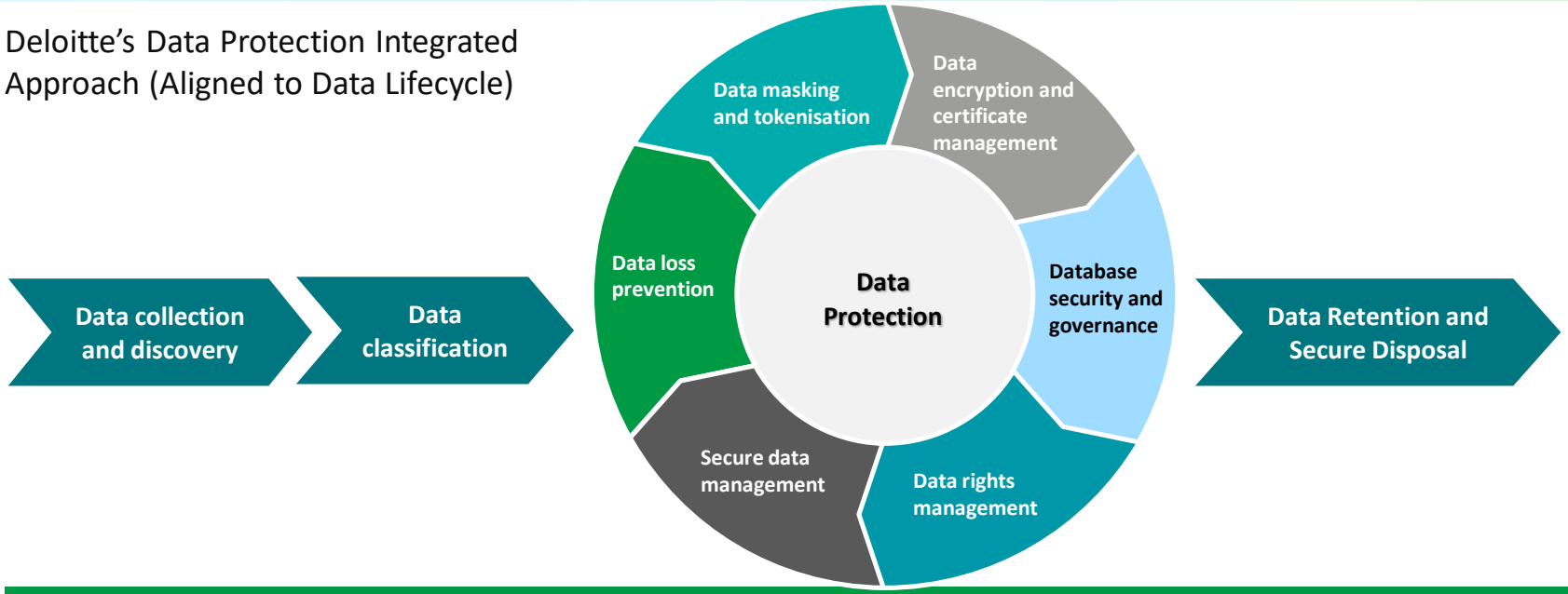
Implement data protection solutions and integrate it with the existing technology infrastructure.

Business drivers



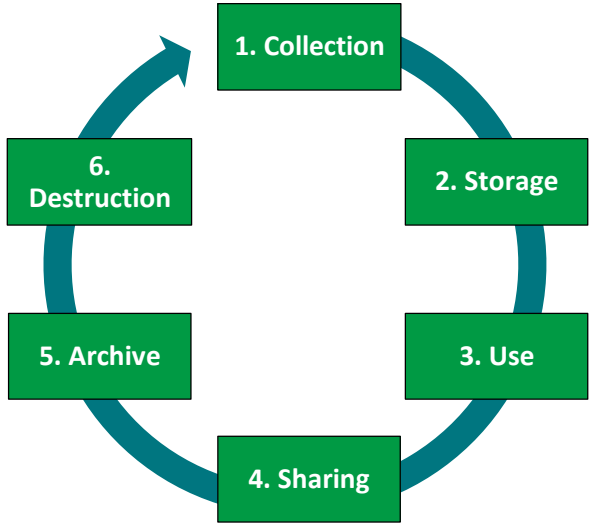
Deloitte's integrated data protection offering landscape

Deloitte's Data Protection Integrated Approach (Aligned to Data Lifecycle)



Our key-differentiator service offerings:

- Advisory Services
- Vendor Evaluation
- Conduct POC Session
- Current State Assessment
- Solution Implementation and Integration
- Optimisation and Enhancement
- End-to-end Managed Services

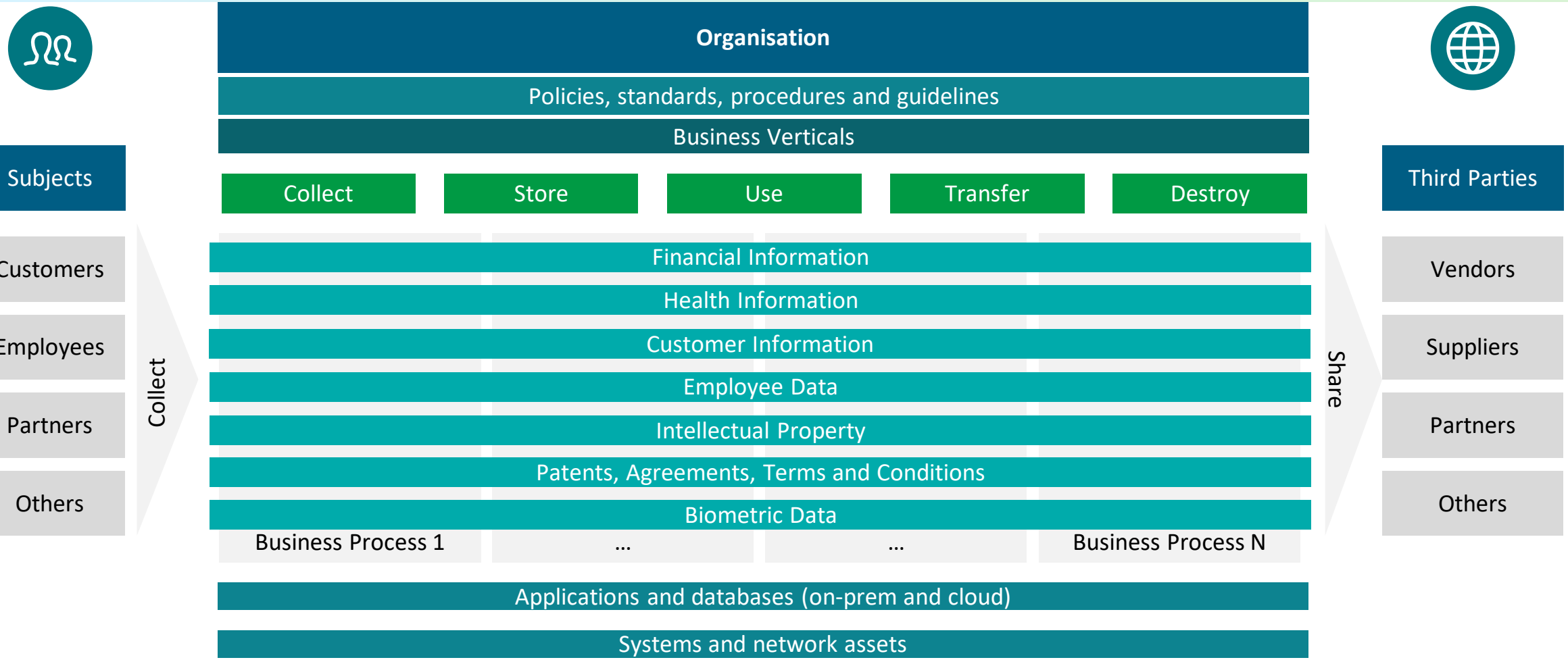


Functional Components

1. Collection: activities to analyse data collection methods, types of data being collected, and roles of those collecting data.
2. Storage: activities to analyse how and where data is being stored, who has access to the storage locations, and how and where copies of the data is being stored.
3. Use: activities to analyse the purpose of the data collection and how data is being processed.
4. Sharing: activities to analyse how and why data is being shared between one or more business processes or individuals.
5. Archive: activities to analyse when it is applicable to store outdated data and to resolve how and where this data is stored.
6. Destruction: activities to analyse how and when data is likely be destroyed.

Data protection scope

Sensitive and confidential information may include, but not limited to, financial, health, customer, employee and intellectual property information hosted in or processed across business processes. Managing data protection involves protection of this information across collection, storage, use, transfer and destruction stages of the data lifecycle



Data lifecycle

We, at Deloitte, identify the following technology platforms for different stages of data lifecycle as part of the enterprise's data protection landscape. Below we've identified

Data created	Identification / Classification User engagement	Control layer for data shared through endpoint, email and web channels or cloud	Data-at-rest and data-in-motion	Data shared with appropriate rights to ensure legitimate 3rd party handling
Structured / Unstructured data – Files, Email	Data discovery and classification	DLP / CASB	Encryption	IRM
Define critical data types and conduct data flow analysis	Define classification taxonomy and implement	Define monitor/block controls and implement	File level, database level, volume level encryption	Understanding critical business processes for 3rd party data handling policies and controls
Maintain and manage sensitive data inventory	Build user awareness, L&D material	Outsourcing operations/incident management	Certificate and key management	

Our capabilities

Establishing data governance framework	Compliance assessments and recommendations	Solution implementation, manage and optimisation

Deloitte's data discovery and classification programme

An effective data discovery and classification programme largely depends on identifying the "crown jewels" of an organisation. To do this, we recommend considering data discovery and classification across four main components:

Strategy, policy, and governance- Develop, review, refine and update the data discovery and classification programme's strategy, policy and governing documents

Comprehensive integration with data protection solutions- Integrate with other data protection solutions (such as DLP, CASB, Encryption etc.) to enhance overall data protection capabilities

Enablement through technology- Ensure compliance with data discovery and classification requirements through technological platforms

Data classification approach- Address requirements for data discovery and classification through user driven, automated or suggestive approach

Deloitte for DLP(Data Loss Prevention) / CASB (Cloud Access Security Broker) services

Below are the Deloitte's service offerings as per the key components of DLP/ CASB:

Key components

Data discovery is based on the policies defined in the discovery landscape/central management console

Central platform to define, deploy and implement enterprise policies across various DLP/CASB components

Discovery

Central servers

Network components

End-point agents

Monitor network communications to restrict the flow of data in motion as necessary

End-point agents reside within end user devices. Discover, collect data and enforce policies on the device

Secure data-at-rest, data-in-use, data-in-motion

Design and implementation

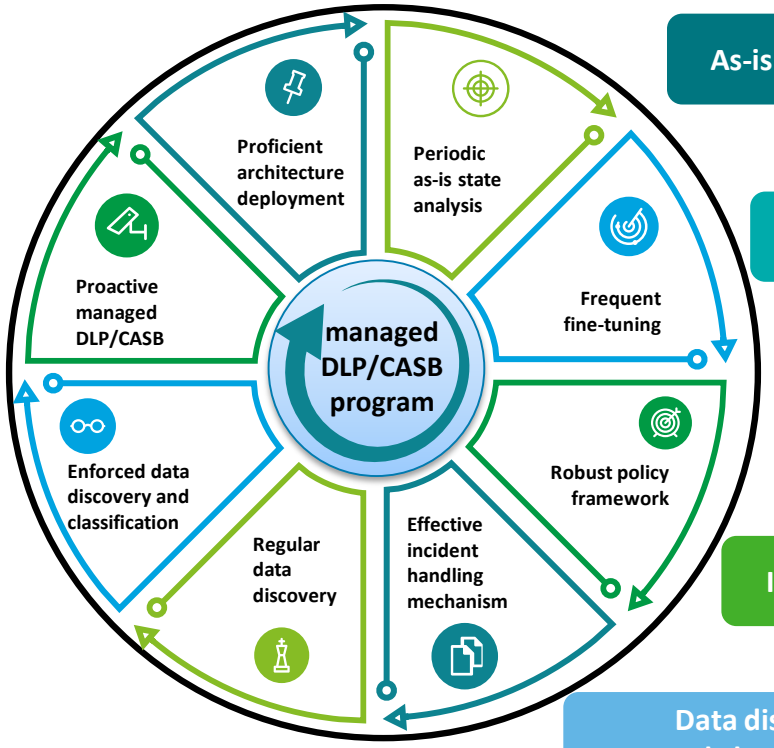
As-is state assessment

Fine tuning

Policy framework

Incident management

Data discovery and classification



Deloitte's services for data obfuscation

The below section outlines the driving factors for data masking and tokenisation as part of the data protection landscape

Deloitte's Capabilities

1. Assessment, strategy and roadmap
2. Proof of Concept (POC)/Vendor selection
3. Design, implementation and integration
4. CKMS operations

Data tokenisation

- 1. Compliance
- 2. Controlled Access
- 3. Ensure Privacy
- 4. Reduced Risks

Data masking

1. Data security (prod and non-prod environment)
2. Protection against insider threats
3. Compliance with regulatory requirements
4. Enhance productivity and automation

Our Resources

Core Data Protection Team

Deloitte has a network of experienced practitioners ranging from partners to consultants with skills not limited to Key and Certificate management but also encryption, test data management and data protection.

Managed Services through Deloitte Delivery Centres

Deloitte has multiple delivery centers globally, where skilled practitioners provide support for our cyber security managed services.

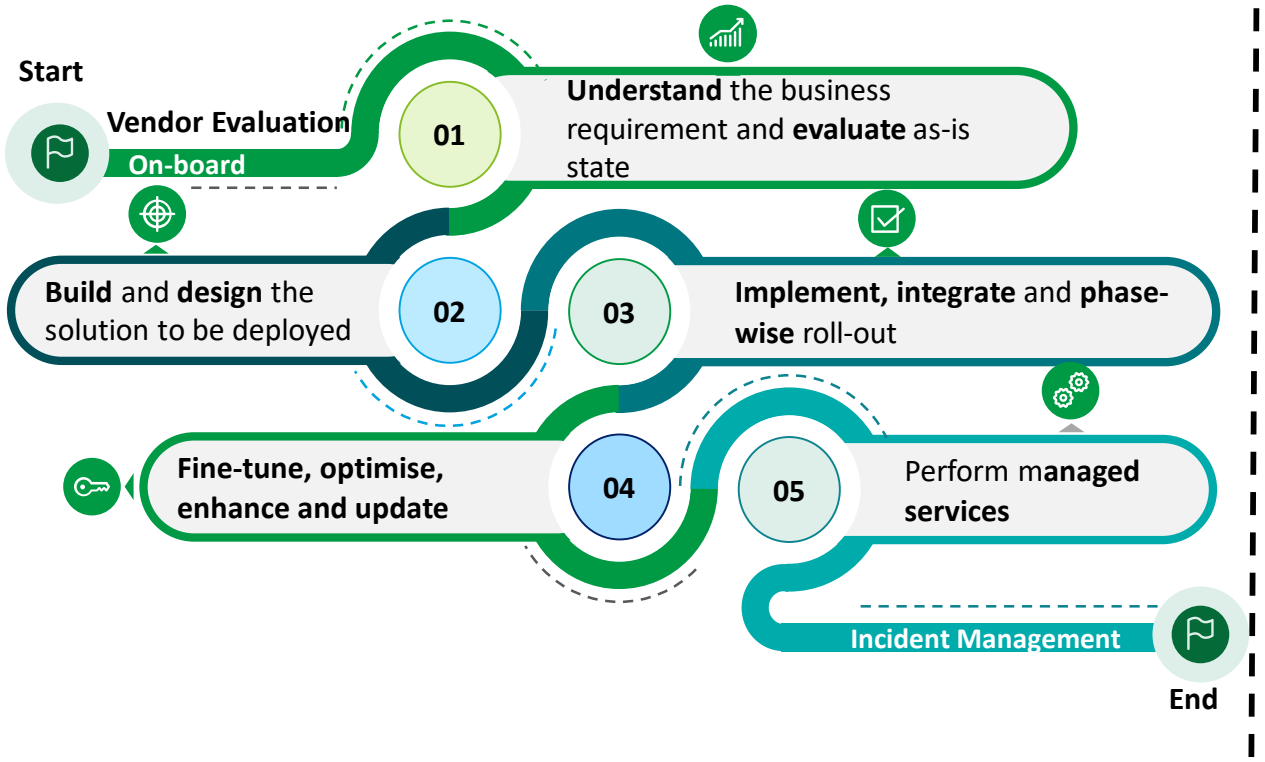
Vendor alliances

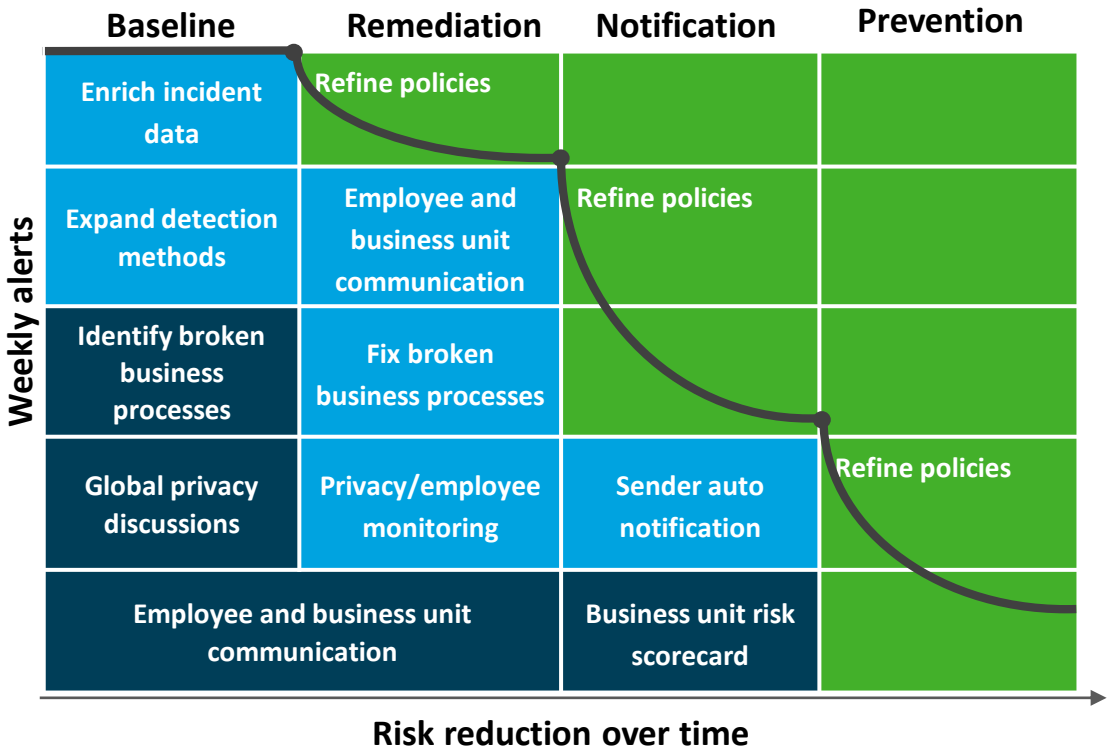
While Deloitte remains vendor independent, we have strong alliances with market leading vendors.

Deloitte's customised phase-wise approach

Aligned to our native Cyber Security framework, we have undertaken the following approach to deliver data-protection engagements across various industries and sectors

Process → **Outcome**





Our data protection team

Deloitte in India is one of the leading Data Protection and Privacy professional service provider with a rich heritage of serving the best-in-class clients in India, and in the global landscape.

Our team

Our team	**70+** professionals dedicated to Privacy and Data Protection
Certification	Data Protection team consists of professionals with: • CISA, CISSP, CIPP, CIPM and product specific certifications
Tools/Automation	• Use of chat-bot oriented Deloitte's indigenous Intelligent Risk Assistant (IRA) platform for Data Protection • Deloitte's native cyber-security framework • Deloitte's customised phase-wise approach

Footprints Across Verticals

- Consumer and Industrial Products
- Energy & resources
- Financial services
- Life sciences & healthcare
- Tech, media & telecom
- Public sector

Providing end-to-end managed services to ***10+*** clients across these sectors

Managed Service offerings include
SaaS offerings (***3+ clients***)
On-prem (***5+ clients***)
Remote services (***3+ clients***)

Contact us

National

Rohit Mahajan
President – Risk Advisory
Deloitte India
rmahajan@deloitte.com

Manish Sehgal
Partner, Risk Advisory
Deloitte India
masehgal@deloitte.com

Regional

West – Ashish Sharma
Partner, Risk Advisory
Deloitte India
sashish@deloitte.com

North – Gautam Kapoor
Partner, Risk Advisory
Deloitte India
gkapoor@deloitte.com

South – Gaurav Shukla
Partner, Risk Advisory
Deloitte India
shuklagaurav@deloitte.com

Deloitte.