High-Level Personal Data Protection (PDP) Assessment

Helping Organizations Understand Their Current Readiness

November 2025

Our Approach: High-Level Free Assessment

Why Personal Data Protection "MATTERS"?

Organizations today face rising expectations from regulators, customers, and partners around how personal data is collected, stored, and used.

Failure to protect data leads not only to regulatory fines but also long-lasting reputational damage and loss of customer trust.

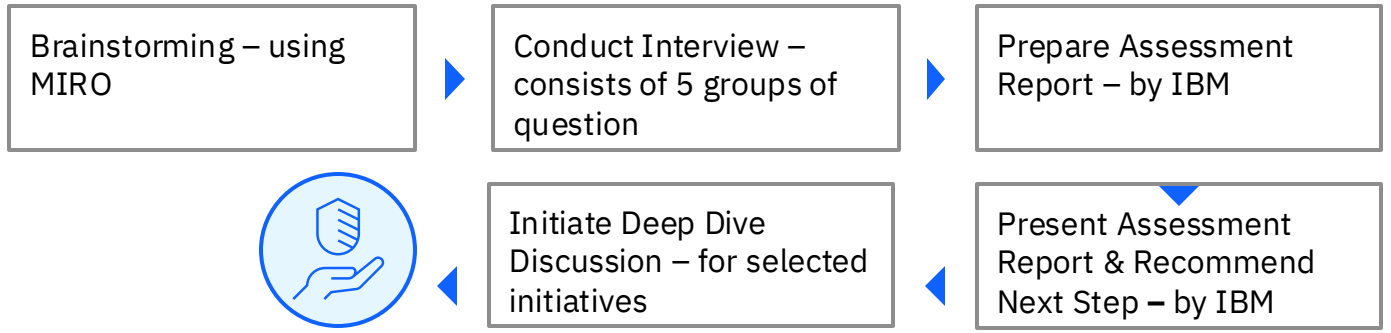
The financial impact of breaches is increasing due to more sophisticated cyberattacks, growing data volumes, and integration of AI systems that create new risks.

Data protection is not just about compliance — it enables innovation, secure data sharing, and building customer confidence as a competitive differentiator.

Our Complimentary High-Level PDP Assessment — WHAT & WHY

- **Purpose**: provide a quick, actionable snapshot of PDP readiness (high-level, non-invasive)
- **Duration**: typically 1 - 2 days workshops
- **Deliverable**: Findings report, maturity snapshot, prioritized technology recommendations

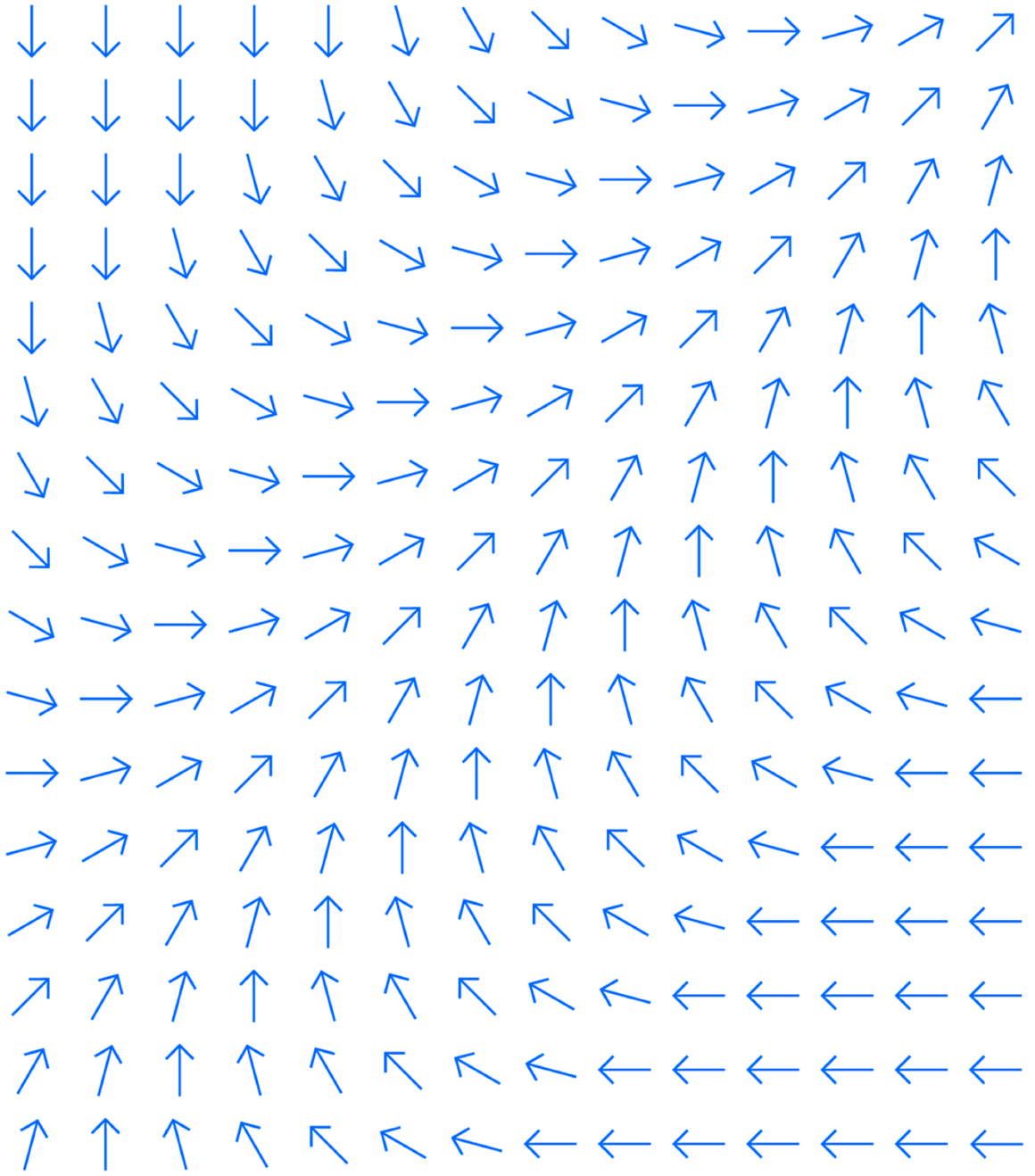
No-cost, limited-scope engagement intended to identify immediate risks and opportunities



7 Dimensions Covered (High-Level)

- Privacy Practices
- Data Processing
- Process & Risk Mgmt.
- Technology (**Focus**)
- Privacy Impact
- Data Governance
- People Readiness

IBM High-Level Privacy Assessment Report for Company A

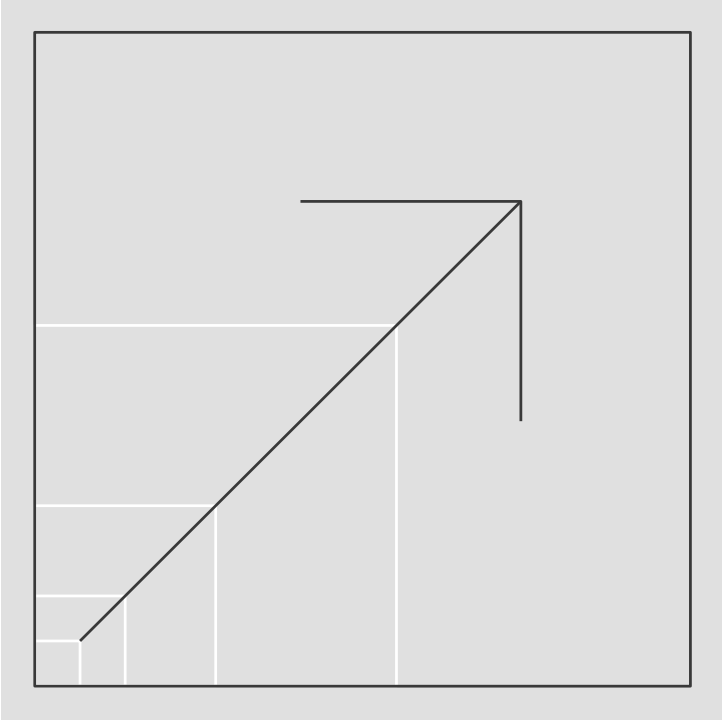


August 2025

IBM

Content

01. General Background
02. User Feedback
03. Assessment Result
04. Key Findings
05. Recommendations
06. Potential Solutions



Privacy compliance should be a practice as fundamental to the business as customer service. Privacy is an essential element of being a good business partner.

General Background

IBM conducted a privacy high-level assessment for Company A July 28, 2025

Participant

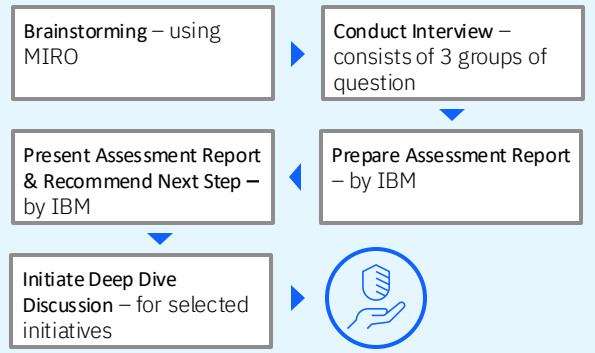
Company A :
- IT Development & Operation Team
- IT Strategy Partnership, Architecture, & Cybersecurity Governance

IBM:
- Client Engineering Team

Activities

- Privacy readiness survey of selected Business Unit representatives
- Interview in the area of privacy that is categorized into privacy impact, data governance, process management, people, and technology
- Gap analysis to compare subject responses with best practices from each subject
- Maturity scoring
- Propose recommendations and solutions

Process Flow

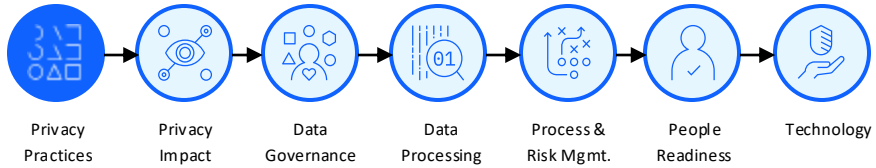


User Feedback

	☑ As-Is (In-Practice)	☒ To-be (Missing)
Tech.	**Data Loss Prevention (DLP):** End-point & email **Data Classification:** Manual Marking **Comply to ISO 270001** **Application Ownership:** Yearly list down of app. ownership **Antivirus:** Technicro **Logging & Monitoring:** Monitoring OS	**Data Flow Diagram** **Encryption** **Consent Management** **DPIA** **ROPA** **WebPrivacy** **Threat Intelligence** **Logging & Monitoring Application** **Data Masking**

Privacy Practices[1]

This section examines the organization's policies, procedures, and guidelines for handling personal data and protecting privacy.



Capability	Current State	Target State	Maturity	Recommendation
Identification of personal data collected within the organization	The organization has a clear understanding of the personal data it collects, processes, stores, or transmits, including details from core banking applications	Organization understands their personal data they collect, process, store or transmit	FC	
Availability of privacy policy	The organization has a privacy policy in place, and data is received with explicit consent, indicating full compliance.	Organization has detailed privacy policy that outlines privacy practice and data protection measures	FC	
Individual awareness of their rights under privacy law	Currently, users can submit data deletion requests, but full coverage of data subject rights across the data management lifecycle—such as data access, data transparency, or preference management offered automatically—is not yet in place. Therefore, the status is considered partially compliant with the principle of fulfilling data subject rights.	Individuals are aware of their rights under privacy laws, such as the right to access their personal data, request deletion, or opt-out of marketing communications	PC	The bank should establish a comprehensive and transparent consent management system tailored to each application and data processing activity involved.
Consent management	The organization obtains consent, including for sharing data with data processor (insurance), indicating full compliance.	Organization obtains explicit consent from individuals before collecting, processing, or sharing their personal data, and provide clear information about the purposes for which the data will be used	FC	

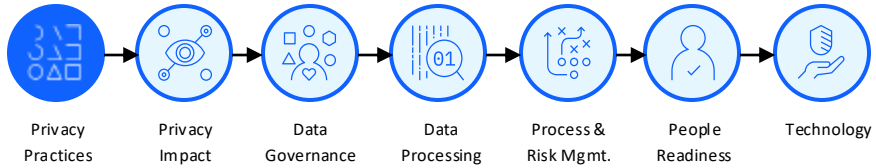
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Privacy Practices[2]

This section examines the organization's policies, procedures, and guidelines for handling personal data and protecting privacy.



Capability	Current State	Target State	Maturity	Recommendation
Privacy impact assessment	A Privacy Impact Assessment (PIA) has not yet been conducted, and consequently, associated risk assessments and mitigation measures for new projects, products, or services are not in place.	Organization has conducted a privacy impact assessment (PIA) to identify and mitigate privacy risks associated with new projects, products or services and assessed the risks associated with processing personal data, and implemented appropriate technical and organizational measures to mitigate those risks	NC	The bank should conduct Privacy Impact Assessments (PIA) to identify and mitigate privacy risks in new projects, products, or services, and implement appropriate technical and organizational safeguards.
Security measures to protect personal data	The bank currently utilizes user metrics and Active Directory (AD) to manage user access. However, this approach is not yet optimal and does not ensure comprehensive security controls over personal data.	Organization has implemented appropriate security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction	PC	Recommended that the bank implement end-to-end protections such as role-based access control (RBAC), complete audit trails, full encryption, and dynamic masking.
Procedures to handle data breach	The organization has established incident response procedures including monitoring and antivirus systems, a helpdesk, and specific BCP/escalation plans, indicating full functionality.	Organization has procedures in place to handle data breaches, including incident response plans, reporting requirements, and measures to mitigate the impact on affected individuals	FC	
Ensure personal data is processed by authorized personnel	Measures to ensure personal data is processed only by authorized personnel and relevant training for them are not yet in place.	Organization has implemented measures to ensure that personal data is only processed by authorized personnel, and have provided appropriate training to those personnel	NC	The bank should ensure that personal data is only processed by authorized personnel and that those personnel receive adequate training.

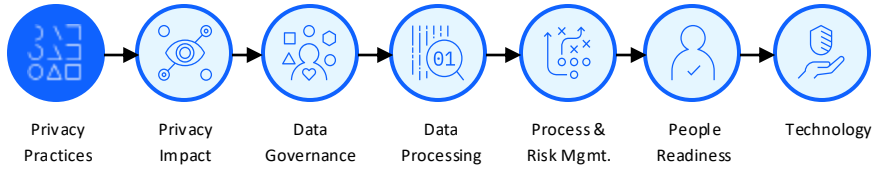
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Privacy Practices[4]

This section examines the organization's policies, procedures, and guidelines for handling personal data and protecting privacy.



Capability	Current State	Target State	Maturity	Recommendation
Process for handling personal data request by data subject	Currently, data changes are limited to specific menu functions and do not include the correction of critical data such as national identity numbers (KTP).	Organization has processes in place to handle requests for access, correction, deletion, or portability of personal data, and respond to these requests in a timely and transparent manner	PC	The system should be expanded to support secure correction requests for sensitive data, with layered authorization and complete audit logs.
Privacy governance structure availability	A formal DPO (Data Protection Officer) has not yet been appointed, indicating the privacy governance structure is still in its early stages of establishment.	Organization has established a privacy governance structure, including the appointment of a privacy officer, and do you conduct regular privacy reviews and audits	NC	The bank should establish a privacy governance structure, including the appointment of privacy personnel and implementation of regular privacy reviews and audits.
Appointed Data Protection Officer (DPO)	A formal DPO has not been appointed. Currently, no individual has been officially identified and made fully responsible for data protection compliance.	Organization has appointed a Data Protection Officer (DPO), or identified someone responsible for data protection compliance	NC	The bank should formally appoint a Data Protection Officer (DPO) who is fully responsible for ensuring data protection compliance.
Inventory all the personal data	An inventory of personal data collected and processed, including its types, purposes, and legal basis, does not yet exist.	Organization has conducted an inventory of all the personal data you collect and process, including the types of data, the purposes for processing, and the legal basis for processing	NC	The bank should conduct a thorough inventory of all personal data it collects and processes, including data types, processing purposes, and legal bases.
Procedure reporting data breaches	Procedures for reporting data incidents to the authorities and affected individuals, along with related risk assessments, are not yet in place.	Organization has procedures for reporting data breaches to the relevant supervisory authority and affected individuals, and have conducted a risk assessment to determine the level of risk to individuals	NC	The bank should have procedures in place for reporting data breaches to relevant authorities and affected individuals, along with risk assessments to evaluate potential impact.

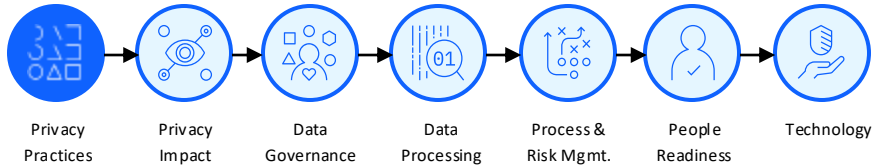
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Privacy Practices[5]

This section examines the organization's policies, procedures, and guidelines for handling personal data and protecting privacy.



Capability	Current State	Target State	Maturity	Recommendation
Compliance monitoring	Processes for monitoring PDP compliance, including regular audits, reviews, and updates to policies/procedures, are not yet established.	Organization has processes in place for monitoring compliance with PDP, including regular audits, reviews, and updates to policies and procedures.	NC	The bank should implement ongoing processes to monitor compliance with data protection regulations, including regular audits, reviews, and policy updates.
Vendor PDP compliance	An assessment of data protection practices and PDP compliance for vendors and third-party processors has not yet been conducted, and this information will only be mapped from the UU.	Organization has assessed the data protection practices and PDP compliance of your vendors and third-party processors.	NC	The bank should assess and monitor the data protection practices and compliance levels of its vendors and third-party processors.
Data processing agreement or contract with vendor	Data processing agreements or contracts meeting PDP requirements for engagement with third parties are not yet in place.	Organization has data processing agreements or contracts in place that meet the PDP requirements when engaging with third parties.	NC	The bank should ensure that data processing agreements with third parties meet the requirements set out in the Personal Data Protection (PDP) regulations.
PDP assurance for overseas data transfer	The organization currently complies with this requirement as no personal data is transferred outside of Indonesia; all data processing remains within the country.	Organization ensures that any data transfers to third countries outside Indonesia with PDP restrictions	FC	

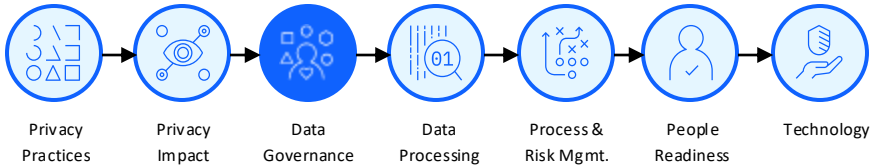
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Governance[1]

This section focuses on the framework and controls in place to ensure responsible data management, including data ownership, classification, and access controls.



Capability	Current State	Target State	Maturity	Recommendation
Data strategy and vision	The organization is drafting a data governance framework, including roles like data owners and stewards, but a clear data strategy and vision have yet to be established.	Organization has a clearly defined data strategy and vision	PC	Develop a clear data strategy and vision with defined objectives and key data areas. Get leadership approval and communicate it across the organization to ensure alignment and effective implementation.
Data governance priority	Data governance is not yet recognized as a strategic priority within the organization.	Data governance is considered a strategic priority within the organization	NC	Position data governance as a strategic priority by gaining executive support, integrating it into business planning, and allocating dedicated resources to drive implementation.
Data governance framework	The organization is in the process of developing a formal data governance framework.	Organization has a formal data governance framework in place	PC	Finalize and implement the formal data governance framework, ensuring it includes clear policies, roles, and processes to manage data effectively across the organization.
Data governance roles and responsibilities	Roles and responsibilities for data governance, including data stewards and data owners, are still being defined and have not yet been formalized.	There are defined roles and responsibilities for data governance, including data stewards and data owners	PC	Clearly define and formalize data governance roles and responsibilities, including data stewards and data owners, to ensure accountability and effective data management.

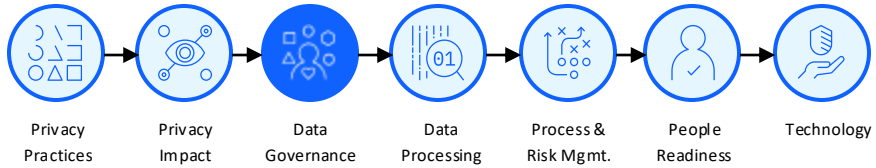
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Governance[2]

This section focuses on the framework and controls in place to ensure responsible data management, including data ownership, classification, and access controls.



Capability	Current State	Target State	Maturity	Recommendation
Documented data governance policy	A documented data governance policy is currently under development and has not yet been finalized or implemented.	There is a documented data governance policy that outlines the guiding principles and objectives	PC	Complete and implement the data governance policy, ensuring it clearly outlines guiding principles, objectives, and expectations for data management across the organization.
PDP policies and procedures	Policies and procedures to protect sensitive and personal data are in development but have not yet been established or implemented	Organization has robust policies and procedures in place to protect sensitive and personal data	PC	Establish and implement robust policies and procedures to protect sensitive and personal data, ensuring compliance with relevant regulations and reducing the risk of data breaches.
Compliance with PDP	Mechanisms to ensure compliance with applicable data protection regulations are still in the drafting stage and not yet operational.	There are mechanisms for ensuring compliance with applicable data protection regulations (e.g., PDP)	PC	Finalize and operationalize mechanisms to ensure compliance with applicable data protection regulations, such as PDP, including processes
Data privacy audit	Privacy and security practices are not yet established or subject to regular audits and assessments.	There are privacy and security practices regularly audited and assessed	NC	Establish privacy and security practices and implement regular audits and assessments
Managing metadata	There is no defined process in place for capturing and managing metadata.	There is a well-defined process for capturing and managing metadata	NC	Needs to establish privacy and security practices with regular audits and develop a defined process for capturing and managing metadata

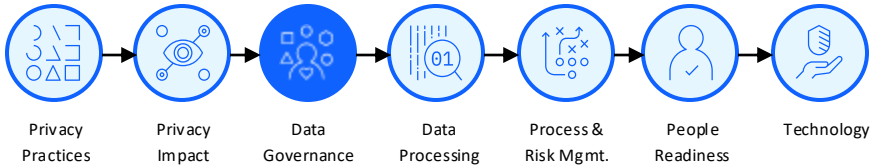
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Governance[3]

This section focuses on the framework and controls in place to ensure responsible data management, including data ownership, classification, and access controls.



Capability	Current State	Target State	Maturity	Recommendation
Standards and definition metadata	Standards and definitions are not yet established or consistently applied across the organization.	There are standards and definitions consistently applied across the organization	NC	Needs to establish and consistently apply data standards and definitions across all departments to ensure clarity, consistency, and data quality.
Accessing metadata	A centralized repository or catalog for storing and accessing metadata is not yet in place.	There is a centralized repository or catalog for storing and accessing metadata	NC	Implement a centralized metadata repository or catalog to improve data accessibility, consistency, and governance.
Data lifecycle	There is no defined process for managing the data lifecycle, from creation to archiving or deletion.	There is a defined process for managing the lifecycle of data, from creation to archiving or deletion	NC	Establish a clear data lifecycle management process
Data retention and disposal policy	Retention and disposal policies are in place, with core banking data retained and backed up without deletion, indicating partial implementation aligned with operational needs.	There is retention and disposal policies in place and followed	FC	
Data sensivity and criticality	Data classification is implemented, with categories such as highly protected, confidential use, internal use, and public, reflecting consideration of sensitivity and criticality.	Data is well classified based on its sensitivity and criticality	FC	

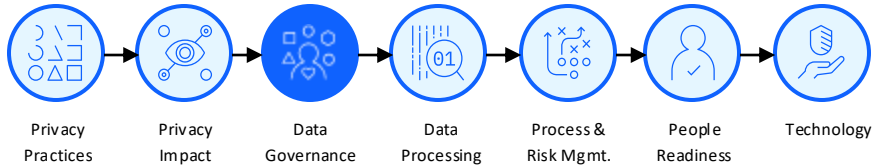
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Governance[4]

This section focuses on the framework and controls in place to ensure responsible data management, including data ownership, classification, and access controls.



Capability	Current State	Target State	Maturity	Recommendation
Data governance activities	Tools and technologies to support data governance activities, such as data lineage, profiling, or cataloging, are not yet in place.	There are tools and technologies in place to support data governance activities (e.g., data lineage, data profiling, data cataloging)	NC	Needs to adopt tools and technologies that support data governance activities, such as data lineage, profiling, and cataloging, to improve data visibility, quality, and control.
Data processor	There is no integration of data governance tools with existing systems and processes, as such tools are not yet implemented.	The tools are well integrated with existing systems and processes	NC	Implement data governance tools and ensure they are well integrated with existing systems and processes to enable seamless data management and operational efficiency.
Data governance	A roadmap for investing in or upgrading data governance tools exists, but clear direction and execution plans have not yet been established.	There are plans to invest in or upgrade data governance tools to improve capabilities	PC	Needs to translate the existing roadmap into a clear action plan

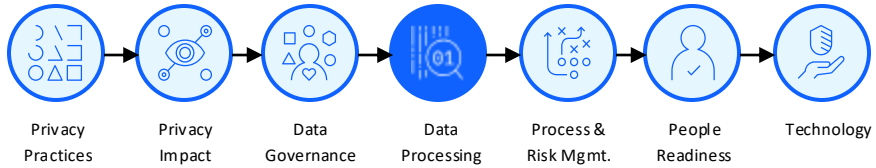
FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Processing[1]

This section outlines how personal data is collected, stored, processed, and transferred, ensuring compliance with relevant privacy regulations and guidelines.



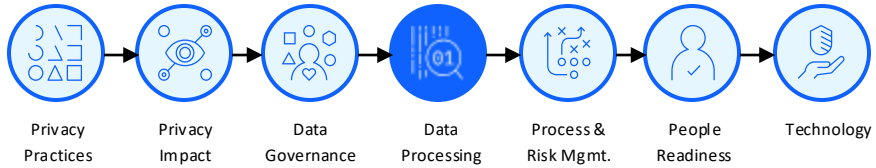
Capability	Current State	Target State	Maturity	Recommendation
Data fabric	The organization has implemented the ideal data process flow, where data from OLTP systems (e.g., core banking) is ingested, stored, and integrated into big data platforms, then consumed by various applications for reporting demonstrating a solid understanding from OLTP to data fabric.	Understands data process from OLTP to data fabric	FC	
Data processing	Data processing is handled internally	Understands if the data processing done by internal or 3rd party	FC	
Data fabric	The organization understands that private data, including personally identifiable information (PII) from customers, is loaded into the data fabric.	Understands if there is any private data loaded into the data fabric	FC	
Data collecting, storing, and processing	The organization collects, stores, and processes customer data as a primary data type.	Understands types of data does your organization collect, store, and process	FC	
Data protection	User consent for data processing is not currently obtained or managed through any established mechanism.	Ensures compliance with data protection and privacy regulations (e.g., PDP, CCPA) in data processing activities	NC	Needs to implement mechanisms to obtain and manage user consent, ensuring compliance with data protection and privacy regulations such as PDP and CCPA.

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Processing[2]



This section outlines how personal data is collected, stored, processed, and transferred, ensuring compliance with relevant privacy regulations and guidelines.

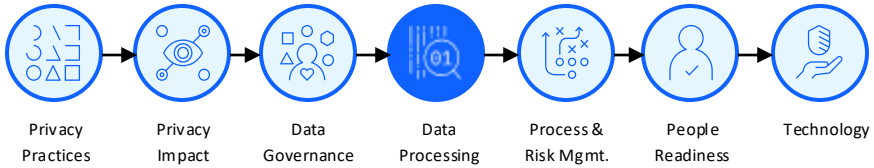
Capability	Current State	Target State	Maturity	Recommendation
Data security and protection	The organization has implemented data security measures, including Privileged Access Management (PAM), application-level metrics, and supervisor approval processes to help prevent unauthorized access and breaches.	Has measures in place to ensure data security and protect against unauthorized access or breaches	FC	
Data retention and disposal	Measures to ensure data security and protect against unauthorized access or breaches are in place within the organization.	Manage data retention and disposal in accordance with legal and regulatory requirements	FC	
Tracking data	Mechanisms or tools to track and manage data processing activities are not yet in place.	Has mechanisms or tools to track and manage data processing activities	NC	Implement tools or mechanisms to effectively track and manage data processing activities, ensuring transparency, accountability, and regulatory compliance.
User consent	There are no mechanisms in place to obtain or manage user consent for data processing.	Obtain and manage user consent for data processing	NC	Needs to establish mechanisms to obtain and manage user consent for data processing
Transparency Data Processing	Transparency in data processing is addressed through initial consent provided via forms, giving individuals basic information about how their data is used.	Ensure that data processing activities are transparent to individuals and provide them with sufficient information about how their data is used	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Data Processing[3]



This section outlines how personal data is collected, stored, processed, and transferred, ensuring compliance with relevant privacy regulations and guidelines.

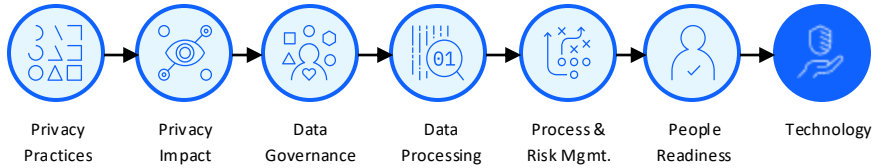
Capability	Current State	Target State	Maturity	Recommendation
Data transfers and sharing	The organization manages data transfers and sharing with third parties by sending raw data to regulators such as OJK and through API integrations with partners like insurance companies. These activities are governed by NDAs and formal agreements (PKS) to ensure data protection.	Manage data transfers and sharing with third parties or external organizations	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[1]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

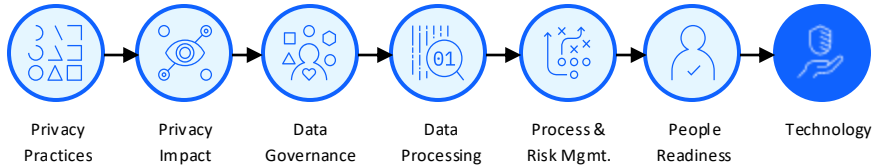
Capability	Current State	Target State	Maturity	Recommendation
Consent Management	Consent management is not currently in place, and there are no systems such as Consumer Identity & Access Management or dedicated consent management tools implemented.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Needs to implement a comprehensive consent management system along with consumer identity and access management tools to ensure proper handling of user permissions, improve data transparency, and comply with data protection regulations.
Single Sign-On	The organization uses Active Directory (LDAP) for access management, indicating a centralized approach, though it may not yet fully support Single Sign-On capabilities.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Database Encryption	Data encryption at the database level is not currently implemented.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Implement data encryption at the database level and across other relevant layers to protect sensitive information and ensure compliance with data security standards.
Network Encryption Standard	The organization implements network encryption using SSL for web-based communication and SFTP for file transfers, providing a foundational level of secure data transmission.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[2]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

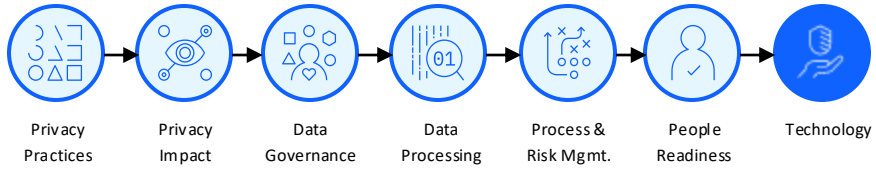
Capability	Current State	Target State	Maturity	Recommendation
Private Data Located	The organization has visibility into the location of private data, which resides in core banking systems (big data) and in hardcopy form at individual branch offices, reflecting basic data discovery and classification awareness.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Loss Prevention	The organization has implemented Data Loss Prevention (DLP) technology using Trellix, indicating efforts to protect data across various states, though specific deployment types (at rest, in motion, in use) are not detailed.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Loss Prevention Report	DLP reports are reviewed daily, with monthly summaries provided to management for reporting purposes, demonstrating a proactive approach to data loss monitoring and oversight.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Discovery	Data discovery tools to identify sensitive datasets are not currently in place.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Needs to implement data discovery and classification tools to identify, categorize,
Business Intelligence	The organization utilizes IBM Cognos, providing reporting capabilities to support business intelligence functions.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[3]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

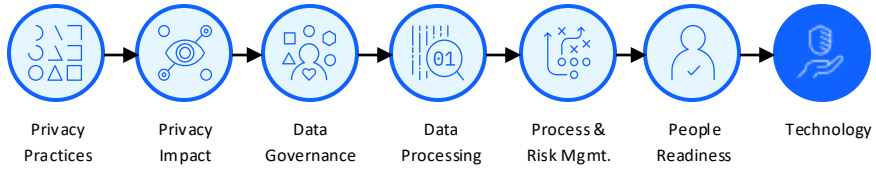
Capability	Current State	Target State	Maturity	Recommendation
Security Information and Event Management - Monitor & Detect Anomalies	Anomaly detection tools are not yet in place; current monitoring is limited to the operating system level without advanced Security Information and Event Management (SIEM) capabilities.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	PC	Needs to enhance its monitoring capabilities by implementing anomaly detection tools beyond the operating system level, ideally through a full-featured Security Information and Event Management (SIEM) solution to detect threats across the entire IT environment.
Security Information and Event Management - Log Sensitive Data	Security Information and Event Management (SIEM) capabilities are in place within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Database Firewall	Information protection is supported through network firewalls like Palo Alto, Checkpoint, Cisco, and Fortinet.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
- Disk Encryption - Network Encryption - File System Encryption - File Encryption	Encryption at various levels such as disk, network, file system, and individual files is not currently implemented within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Implement encryption at all levels disk, network, file system, and files to protect sensitive data and improve security.
Security Information and Event Management	The organization uses QRadar SIEM for monitoring and detecting security incidents.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[4]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

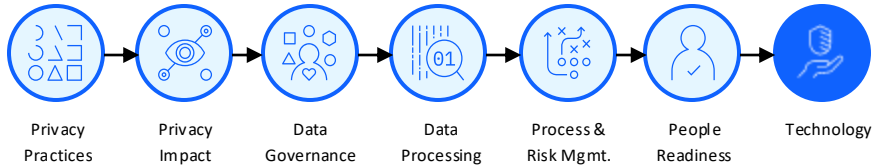
Capability	Current State	Target State	Maturity	Recommendation
Document Management	There are no technologies or formal methods currently in place to protect paper-based assets.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	
- Consumer Identity & Access Mgmt. - Consent Management	Tools to document or track notice, choice, and consent are not currently in place.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Implement tools to manage notice, choice, and consent, along with identity access systems, to ensure clear and compliant data processing.
Data Analytics	Analytics on notice, choice, and consent responses are not currently performed within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	The organization needs to deploy tools and analytics capabilities to effectively track, document, and analyze notice, choice, and consent responses, enabling data-driven insights and ensuring compliance with privacy regulations.
User Behavior Analytics	The organization uses QRadar, which supports analysis of user responses and behavior, enabling basic User Behavior Analytics capabilities.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Masking	The organization uses Thales for dynamic data masking of credit card (CC) data; however, implementation is not yet comprehensive across all classified data types.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	PC	The organization needs to extend the implementation of dynamic data masking across all relevant systems and classified data types to ensure consistent protection of sensitive information.

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[5]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

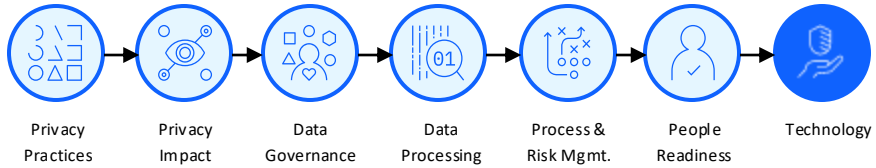
Capability	Current State	Target State	Maturity	Recommendation
Role Based Access Control	Role-based access control is implemented using LDAP, allowing data access to be limited based on specific user role groups.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Identity Governance and Administration	The organization uses firewalls and PAM to secure its network and control access.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
- Intrusion Detection System - Intrusion Prevention System	Firewalls and intrusion detection/prevention systems are in place, supporting the organization's network security and threat mitigation efforts.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
- Asset Management - Configuration Management Database	Network devices are regularly updated with security patches and firmware upgrades, reflecting adherence to asset and configuration management best practices.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
- Asset Management - Configuration Management Database	The organization uses vulnerability scans to keep systems and software up to date with security patches.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[6]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

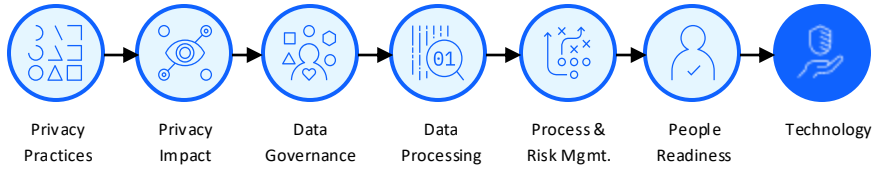
Capability	Current State	Target State	Maturity	Recommendation
Vulnerability Management	A vulnerability management process is in place, including regular vulnerability scanning to identify and address security risks proactively.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Privilege Account Management	Privileged accounts and access controls are managed using CyberArk	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
IAST, SAST, DAST	Secure coding practices are currently in progress and outlined in the roadmap, but have not yet been fully implemented	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	PC	Need to start to do secure coding practice in place
Data Activity Monitoring / Data Firewall	Sensitive data is protected in transit using SSL and SFTP, while data at rest is secured with password protection. However, advanced safeguards like Data Activity Monitoring or Data Firewalls are not yet in place.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Encryption	Data encryption mechanisms for sensitive information are not currently implemented.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	The organization needs to implement robust data encryption mechanisms for all sensitive information to protect data confidentiality and comply with security standards.

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[7]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

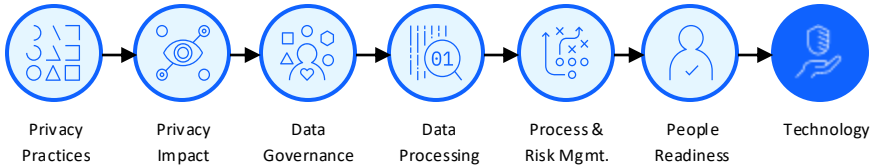
Capability	Current State	Target State	Maturity	Recommendation
Data Backup	Data backup and disaster recovery procedures are in place using Veritas, indicating established safeguards for data continuity, though encryption details were not specified.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Data Storage	Encrypted storage is not currently implemented within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Needs to implement encrypted storage solutions to ensure data at rest is securely protected against unauthorized access.
Identity Governance and Administration	User access to data is managed through Active Directory, supporting centralized control and basic enforcement of least privilege principles.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Security Information and Event Management - Monitoring and Detecting Security Incidents	Security incidents are monitored and detected using QRadar SIEM, providing centralized event logging and threat detection capabilities.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Security Information and Event Management – Logged Security Event	Security events and incidents are logged and analyzed through QRadar SIEM, enabling centralized analysis and response capabilities.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

Technology[8]



This section assesses the technical measures implemented to secure personal data, including encryption, access controls, data anonymization, and system monitoring.

Capability	Current State	Target State	Maturity	Recommendation
Security Orchestration, Automation and Response – Incident Response Team	An incident response plan and designated team to handle security incidents are not currently in place.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	The organization needs a clear incident response plan and a dedicated team to handle security incidents quickly and effectively.
Security Orchestration, Automation and Response	There is no established process for reporting or responding to security breaches or incidents.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	Set up clear processes and tools to quickly detect, report, and respond to security incidents.
Data Governance	Tools to govern and manage data are not currently in place within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	The organization needs data governance tools and frameworks to manage, control, and protect its data effectively.
Business Process Management	The organization uses K2 as a business process management platform, supporting workflow automation and process optimization efforts.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	FC	
Document Management	A document management system is not currently implemented within the organization.	Well implemented following best practice utilizing important features of the solution and covering majority of critical system.	NC	The organization needs to implement a robust document management system to efficiently store, organize, secure, and track both physical and digital documents, improving accessibility and compliance.

FC **Full Comply**
The organization has fully implemented the requirements of the standard or regulation

PC **Partially Comply**
The organization has implemented some of the requirements but not all of them

NC **Not Comply**
The organization has not implemented any of the requirements.

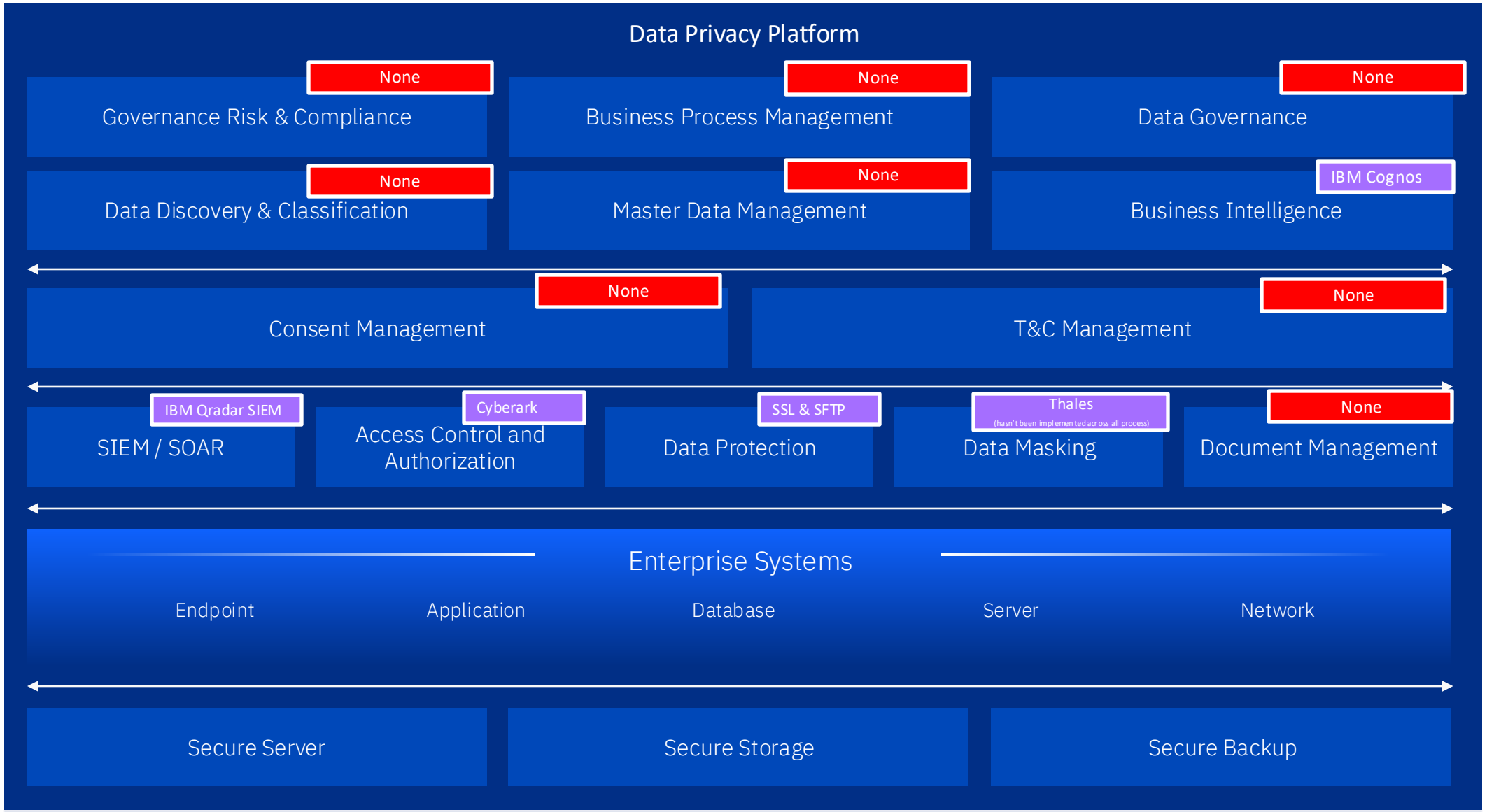
PDP Law compliance mapping to Company A Technology

Governance Lifecycle

Consent Management

Enterprise Security

Secure Infrastructure



Key Findings

38%

Privacy Practices

Company A demonstrates foundational compliance in its privacy practices. The organization has a clear grasp of personal data collection and consent, especially from its core banking systems. Explicit consent is obtained for data collection and sharing with third parties, and data deletion requests are supported.

However, full data subject rights—such as automated access requests or preference management—are not yet enabled, leading to only partial compliance in fulfilling data subject rights. A Privacy Impact Assessment (PIA) process has not been introduced, and there are no formal risk mitigation strategies for new initiatives. While incident monitoring and escalation procedures exist, access controls and training for personnel remain limited. The bank lacks a formal Data Protection Officer (DPO), and inventories of processed data or incident reporting procedures are still under development.

Overall, although foundational elements are in place, the governance and privacy accountability mechanisms are still maturing.

48%

Data Governance and Processing

Company A is in the early stages of implementing data governance. A framework is being drafted with roles like data stewards and owners in progress, but not yet formalized. Data governance is not currently treated as a strategic function. Metadata management, standardized definitions, and centralized data catalogs are absent, and lifecycle data management practices are not mature. While data classification is in place and the data pipeline from OLTP to data fabric is well understood, mechanisms to manage consent, audit data access, and monitor third-party data processing are lacking.

The organization shows readiness with its data process flow and understands the need for protecting PII; however, governance tools (such as for lineage, profiling, or cataloging) are not yet in place, and there is no operational monitoring of vendor PDP compliance.

Existing security controls (e.g., PAM and supervisor approvals) help mitigate unauthorized access, but consent and transparency processes remain limited.

62%

Technology

The organization has implemented several foundational technologies to safeguard data, such as SSL/SFTP for data in transit, Trellix DLP for loss prevention, QRadar for SIEM, and firewalls for network protection.

However, critical gaps exist in encryption (no data-at-rest encryption), consent management tools, data discovery, and anomaly detection capabilities. The use of LDAP for role-based access is a strength, but it does not extend to full CIAM or consent management functionalities. Paper-based asset protection is absent, and secure coding practices are still in the roadmap phase. While Veritas is used for backup and recovery, encrypted storage and comprehensive endpoint protection tools are not yet in place. Business process platforms like K2 exist, but there's no document management system to support PDP documentation requirements.

The current setup offers a solid foundation, but additional capabilities are needed to ensure compliance with PDP requirements.

Top recommended actions

Action Items:

1. **Deploy Data Protection**: For activity monitoring and policy enforcement across databases
2. **Implement Data Encryption**: Apply encryption at rest for structured and unstructured sensitive data, especially in core banking.
3. **Implement Security Discover & Classify**: To map and classify all personal and sensitive data, including at rest and in motion, across core banking, big data, and endpoints.
4. **Implement Data Governance Tooling:** Establish a centralized data catalog with governance rules, metadata management, and access policies to enforce enterprise-wide data governance
5. **Deploy Application Performance Monitoring**: Gain observability and detect anomalies in real time across data pipelines and applications—useful for data breach detection and ensuring availability & integrity.
6. **Formalize Consent Management Tooling**: Implement CIAM or similar solutions to automate consent capture, preference management, and consent lifecycle in compliance
7. **Introduce Governance Tooling**: Centralize privacy governance, incident tracking, and risk management aligned to PDP. While highly effective, it's more suitable as a longer-term governance enabler.

Closing the technology gap

Initiatives

1. Guardium Data Protection
2. Guardium Data Encryption
3. IBM Security Discover & Classify
4. IBM Knowledge Catalog (Data Governance)
5. Instana (Application Performance Monitoring)
6. IBM Verify (Consent Management)
7. IBM OpenPages (GRC)

Urgency

1. Enables monitoring and control of data access and usage, critical for security and auditability.
2. Encrypts sensitive personal data, ensuring secure data-at-rest in compliance with PDP Law.
3. Enables the organization to know where all personal data resides, essential for risk management and classification.
4. Establishes metadata governance, access rules, and glossary standards, enabling traceability and access control across the data lifecycle.
5. Monitors system health and detects anomalies in real time to proactively address breaches.
6. Captures and manages user consent, ensuring the organization respects and tracks data preferences.
7. Provides structured privacy governance, incident workflows, and regulatory compliance alignment.

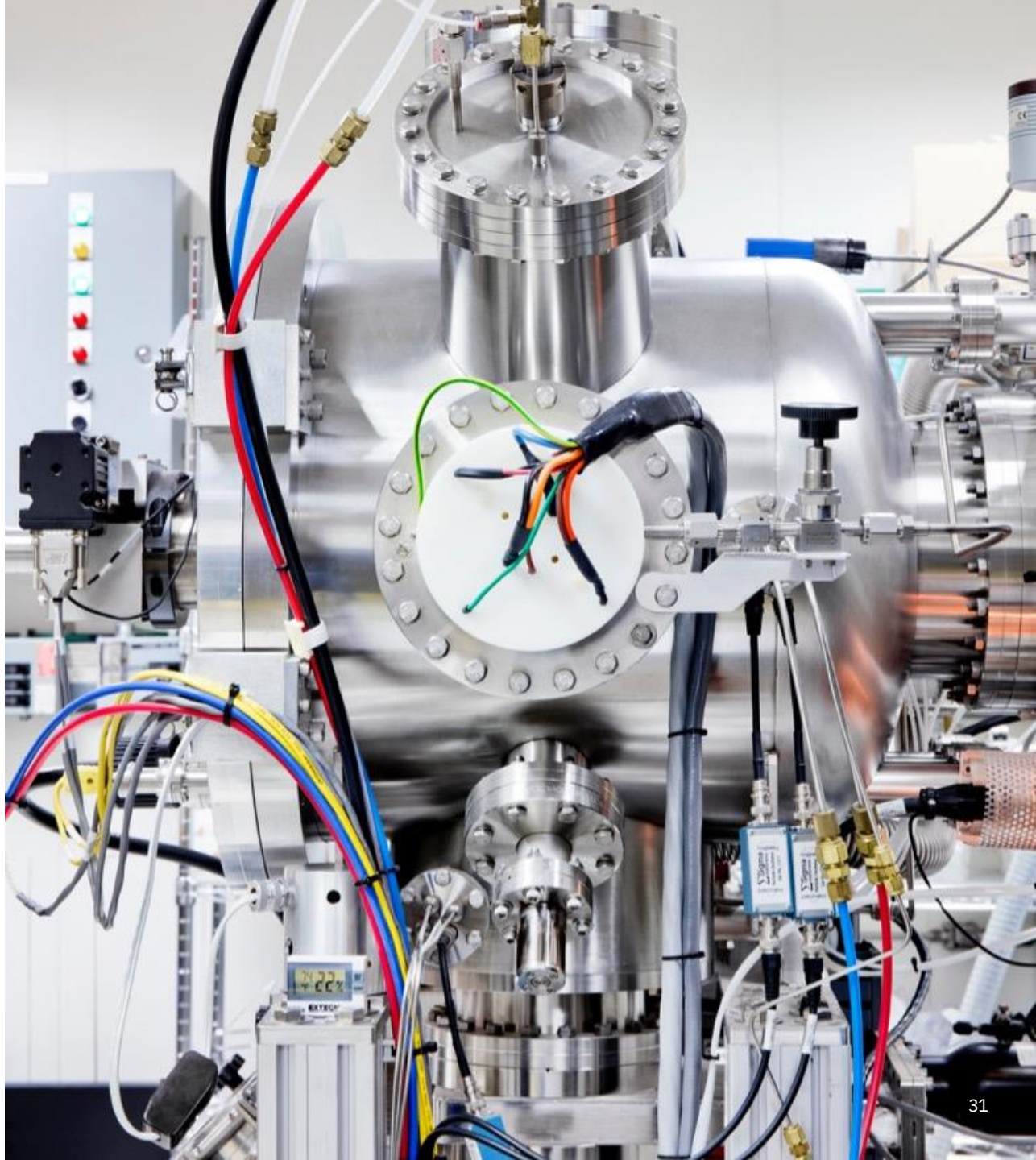
Next Steps

Selected technology deep-dive discussion

Discuss further with us to understand how specific technology within IBM can help you to comply with the PDP Law. See IBM's approach to the selected technology in action and get started with in-app guidance through common use cases.

Ask your rep to engage

More details about our solutions to support your privacy journey:
ibm.com/data-privacy



IBM PDP Law Compliance Quick-Start Package

Consent Management Quick Start

- **IBM Security Verify Access** – Access Management (Single Sign-On / Consumer Identity and Access Management / Adaptive Access) Use-Case
- **IBM Security Trusteer Pinpoint Detect** – Identity Risk Fraud Detection System (Known Users) Use-Case
- **IBM Security Verify Privilege Vault** – Privilege Access Management Use-Case

Endpoint Security Quick Start

- **IBM Security MaaS360 with Watson** – Unified Endpoint Management / BYOD Use-Case

Data Security Quick Start

- **IBM Security Verify Access** – Access Management (Single Sign-On / Consumer Identity and Access Management / Adaptive Access) Use-Case
- **IBM Security Trusteer Pinpoint Detect** – Identity Risk Fraud Detection System (Known Users) Use-Case
- **IBM Security Verify Privilege Vault** – Privilege Access Management Use-Case
- **IBM Security Discover and Classify** – Discover and Classify Use-Case
- **IBM Security Guardium Data Protection** – Data Protection / Firewall / Activity Monitoring Use-Case
- **IBM Security Guardium Data Encryption with Live Data Transformation** – Data Encryption Use-Case
- **IBM Security Guardium for Tokenization** – Data Tokenization part of Encryption Use-Case

Data Governance Quick Start

- **IBM Cloud Pak for Data Express Package** – end-to-end data governance to manage data categorization, data refinery, metadata management, catalog management, and data governance reporting

Compliance & Process Automation Quick Start

- **IBM Business Automation Workflow** for 25 concurrent users

Thank you

Feedback Form:
https://wkf.ms/4pCVyqT

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure, and no single product, service, or security measure can be completely effective in preventing improper use or access. IBM systems, products, and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures and may require other systems, products, or services to be most effective. IBM does not warrant that any systems, products, or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.