MOORE

DATA PRIVACY AND GOVERNANCE

Moore Hong Kong

WHY MOORE?

At Moore, it's not about us. It's all about you. When it comes to providing personalised and commercially astute audit, accounting, tax and business advisory services, it simply can't be anything else.

With over 30 directors and a team of over 300 staff, we offer a wide range of audit, assurance tax, and advisory services to our clients. Our global family of 30,000 professionals in more than 110 countries allows us to share expertise, knowledge, and best practices to ensure our clients receive the highest quality of service, no matter where their work takes them.

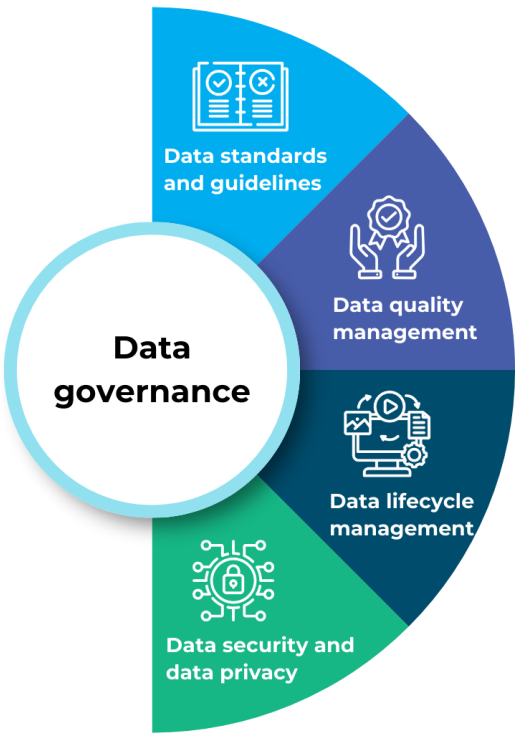
As your genuine professional partner, we will not only advise you but also challenge you to meet your goals and objectives for the future. With our team's personal qualities, skills, and experience, we are confident in our ability to support your group's development.

Data governance

Data governance is the overall management, control, and protection of an organisation's data assets

Data governance aims to define the roles and responsibilities of individuals and departments involved in data management, create data standards and guidelines, and enforce compliance with relevant regulations. It involves establishing a framework of policies, processes, and procedures to ensure data is accurate, consistent, secure, and used appropriately. It also encompasses data quality management, data lifecycle management, data security, and data privacy practices.

Effective data governance promotes data integrity, trustworthiness, and reliability, enabling organisations to make informed decisions based on reliable data. It helps organisations mitigate risk associated with data handling, improve operational efficiency, and maintain compliance with regulatory requirements. By implementing robust data governance practices, organisations can maximise the value of their data assets and leverage data as a strategic resource for achieving business objectives.



01 **Data standards and guidelines**
Ensuring data is handled in accordance with legal and regulatory requirements

02 **Data quality management**
Ensuring data accuracy, completeness, and consistency

03 **Data lifecycle management**
Addressing the entire lifecycle of data, from creation to archival or disposal

04 **Data security and data privacy**
Protect data from unauthorised access, breaches, and privacy violations

Data standards and guidelines

Data governance involves establishing data standards and guidelines. These standards define the rules and conventions for data collection, storage, processing, and usage. They help ensure consistency, accuracy, and understanding of data across different systems and departments within the organisation. Data standards may include data naming conventions, data formats, data classification schemes, and data integration practices.

Data quality management

Data quality management involves establishing processes and controls to ensure the accuracy, completeness, consistency, and timeliness of data. This may include data profiling to understand the characteristics of data, data cleansing to remove errors and inconsistencies, and data validation to ensure data meets predefined quality criteria. Data quality management activities help organisations make reliable decisions, enable effective reporting and analytics, and enhance overall operational efficiency.

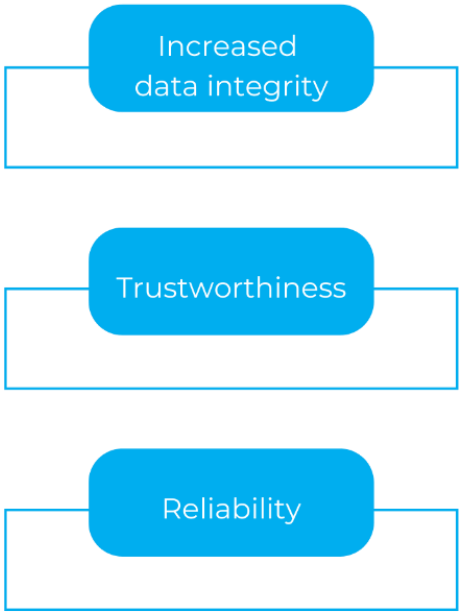
Data lifecycle management

Data lifecycle management encompasses the entire lifecycle of data, from its creation or acquisition to its archival or disposal. Data governance frameworks define policies and procedures for data retention, data storage, data backup and recovery, and data disposal. These measures help organisations manage data efficiently, optimise storage resources, and comply with legal and regulatory requirements regarding data retention and disposal.

Data security and data privacy

Data security and data privacy are paramount in data governance. Organisations employ various security measures, such as access controls, encryption, data masking, and data loss prevention techniques, to protect data from unauthorised access, breaches, or theft. Data governance frameworks also address privacy concerns by establishing policies and procedures for handling personally identifiable information and sensitive data. This includes obtaining appropriate consent for data collection and usage, implementing data anonymisation or pseudonymisation techniques, and ensuring compliance with privacy regulations.

By implementing robust data governance practices, organisations can achieve several benefits, including:



They enables stakeholders to make informed decisions based on accurate and trustworthy data. Effective data governance reduces the risk associated with data handling, such as data breaches, data loss, or data inconsistencies. It also improves operational efficiency by streamlining data processes, reducing data duplication, and optimising data storage and retrieval. Furthermore, data governance helps organisations maintain compliance with regulatory requirements, avoid penalties, and build a solid foundation for data-driven initiatives and strategic decision-making.

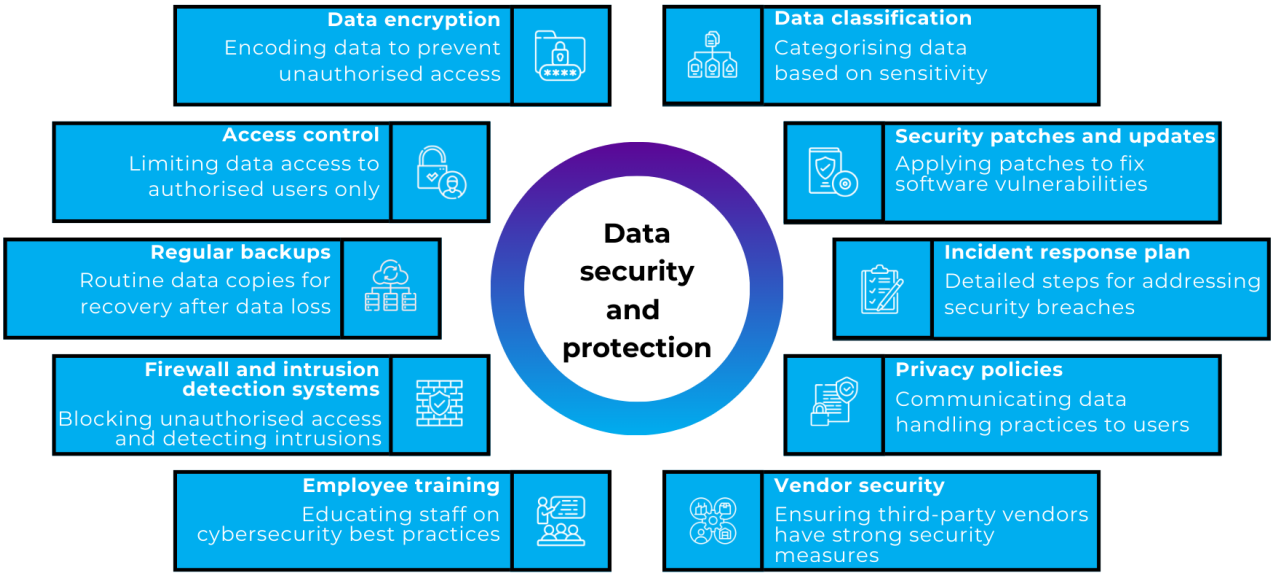
Data security and protection

Data security and protection are critical aspects of information technology and privacy

Data security and protection are measures and practices put in place to safeguard digital data from unauthorised access, corruption, theft, or other forms of compromise. It involves ensuring the confidentiality, integrity, and availability of data, whether it is stored, processed, or transmitted through various systems and networks.

Data security aims to prevent unauthorised individuals or entities from accessing sensitive information, while data protection involves strategies to ensure that data is not lost or compromised during storage, processing, or transmission. These practices are essential for maintaining the trust of customers, protecting business assets, complying with regulations, and mitigating the risks associated with cyber threats and data breaches.

Some key points to consider when addressing data security and protection:



Data encryption

Data encryption is the process of encoding information so that only authorised parties can access it. This is typically done using encryption algorithms and keys. Encryption can be applied to data at rest (stored data), data in transit (data being transmitted over networks), and data in use (data being processed). Strong encryption methods like AES (Advanced Encryption Standard) are commonly used to protect sensitive data.

Access control

Access control involves limiting access to data based on the principle of least privilege, which means users are granted the minimum level of access necessary to perform their tasks. Access control mechanisms include user authentication (verifying the identity of users), and audit trails (tracking who accessed what data and when).

Regular backups

Regular backups are essential for ensuring data availability and recoverability in case of data loss due to accidental deletion, hardware failure, cyberattacks, or natural disasters. Backups should be stored securely, preferably offsite or in the cloud, to prevent loss in the event of on-premises incidents.

Firewall and Intrusion Detection Systems (IDS)

Firewalls act as a barrier between a trusted internal network and untrusted external networks, controlling incoming and outgoing network traffic based on predetermined security rules. Intrusion Detection Systems (IDS) monitor network or system activities for malicious activities or policy violations and alert administrators to potential security incidents.

Employee training

Employee training is crucial for raising awareness about cybersecurity best practices and threats like phishing, social engineering, malware, and password security. Training should cover topics such as recognising suspicious emails, reporting security incidents, creating strong passwords, and following company security policies.

Data classification

Data classification involves categorising data based on its sensitivity or importance to the organisation. Common classifications include public, internal use, confidential, and restricted. Different levels of security controls are applied based on the data classification to ensure appropriate protection.

Security patches and updates

Security patches and updates are released by software vendors to fix known vulnerabilities and improve security. Regularly applying patches helps protect systems and software from exploitation by cybercriminals.

Incident response plan

An incident response plan outlines the steps to be taken in case of a security breach. It typically includes procedures for detecting, responding to, mitigating, and recovering from security breaches.

Privacy policies

Privacy policy specifies how an organisation collects, uses, stores, and protects personal data. They inform users about data handling practices and their rights regarding their personal information. Compliance with regulations like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) is essential for protecting user privacy.

Vendor security

Organisations must assess the security practices of third-party vendors who have access to their data. Vendor security assessments should verify that vendors have adequate security controls in place to protect data.

Our Services

HOW CAN MOORE HELP

Our highly trained security experts have years of experience with extensive knowledge and skills in cybersecurity helping global businesses from different industries achieving their cybersecurity goals. Our security experts hold top cybersecurity and risk management certifications including CISA, CISSP, CEH, CIA, CRISC, ISO20000(ITSM) and ISO27001(ISMS).

DIGITAL BUSINESS TRANSFORMATION

DATA PRIVACY AND GOVERNANCE

CYBERSECURITY RISK

SYSTEM DEPLOYMENT AND ADMINISTRATION

THREAT DETCETION PREVENTION AND RESPONSE

BUSINESS CONTINUITY

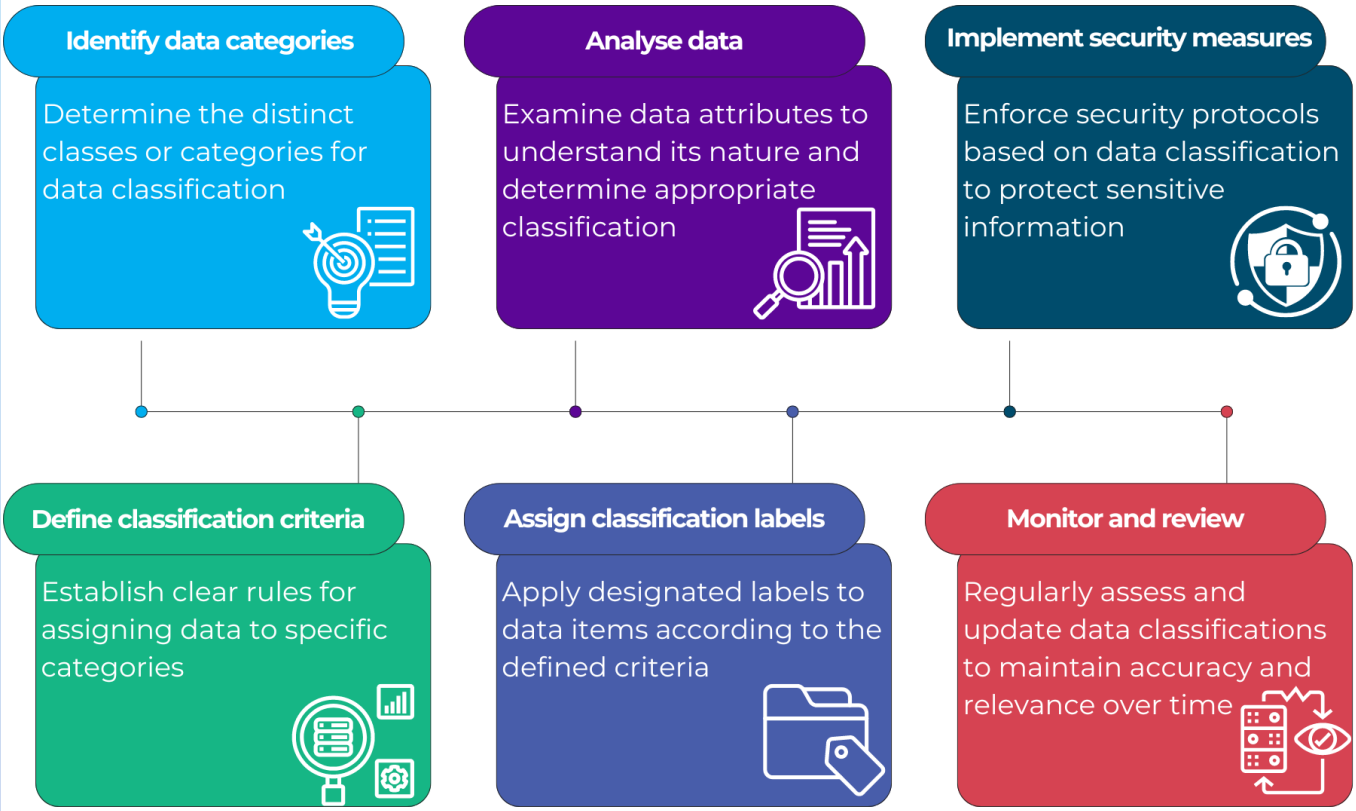
Data classification

Data classification is the process of categorising data based on its characteristics, properties, or attributes

Data classification involves organising data into different classes or groups to simplify its management, improve data security, and facilitate data retrieval and analysis.

Data classification helps in identifying the sensitivity, importance, and value of data, which enables organisations to apply appropriate security measures, access controls, and data handling procedures. It ensures that data is handled in compliance with relevant regulations and policies

Data classification works by following a systematic process that involves the following steps:



Step 1: Identify data categories

Determine the different categories or classes into which the data will be classified. This can be based on factors such as sensitivity, content, or ownership. The specific categories can vary based on the organisation's needs and goals. For example, common categories include public, internal, confidential, or highly sensitive. By identifying these categories, a framework for classifying data consistently across the organisation.

Step 2: Define classification criteria

Establish the criteria or rules for assigning data to specific categories. These criteria can be defined based on business requirements, regulatory guidelines, or organisational policies. For example, defining rules that classify data containing personally identifiable information as sensitive. The criteria should align with the organisation's data governance policies, regulatory requirements, and industry best practices.

Step 3: Analyse data

Assess the data to be classified and examine its characteristics or attributes. To understand the nature of data, factors like metadata (e.g., file name, creation date, author), content analysis (e.g., keyword scanning, pattern matching), or file types (e.g., pdf, excel) can be considered. This analysis provides insights into the data's sensitivity, context, or ownership, assisting in accurate classification.

Step 4: Assign classification labels

Apply classification labels or tags to the data based on the defined criteria. The labels can be alphanumeric codes, color-coded tags, or any form of identification that indicates the assigned classification. This can be done manually by trained data stewards or automated through software tools that use algorithms or machine learning models to classify data based on predefined rules.

Step 5: Implement security measures

Based on the assigned classification labels, implement appropriate security measures and access controls to protect the classified data. The security measures can include encryption, access restrictions, data loss prevention mechanisms, or other security practices based on the sensitivity of the data. For example, highly sensitive data may require stricter access controls and additional encryption layers, while public data may have more relaxed security measures.

Step 6: Monitor and review

Data classification is not a one-time activity. It requires periodic monitoring and review to ensure the accuracy and relevance of the assigned classifications. Data classification may change over time, so it is important to periodically reassess the classification of data as new information or requirements emerge. Regular monitoring helps identify any inconsistencies, misclassifications, or changes in data characteristics, enabling timely adjustments to the classification framework.

Data classification provides a structured approach to organise and manage data. Continuous improvement and refinement of the data classification process are crucial to maintaining data integrity, security, and compliance.

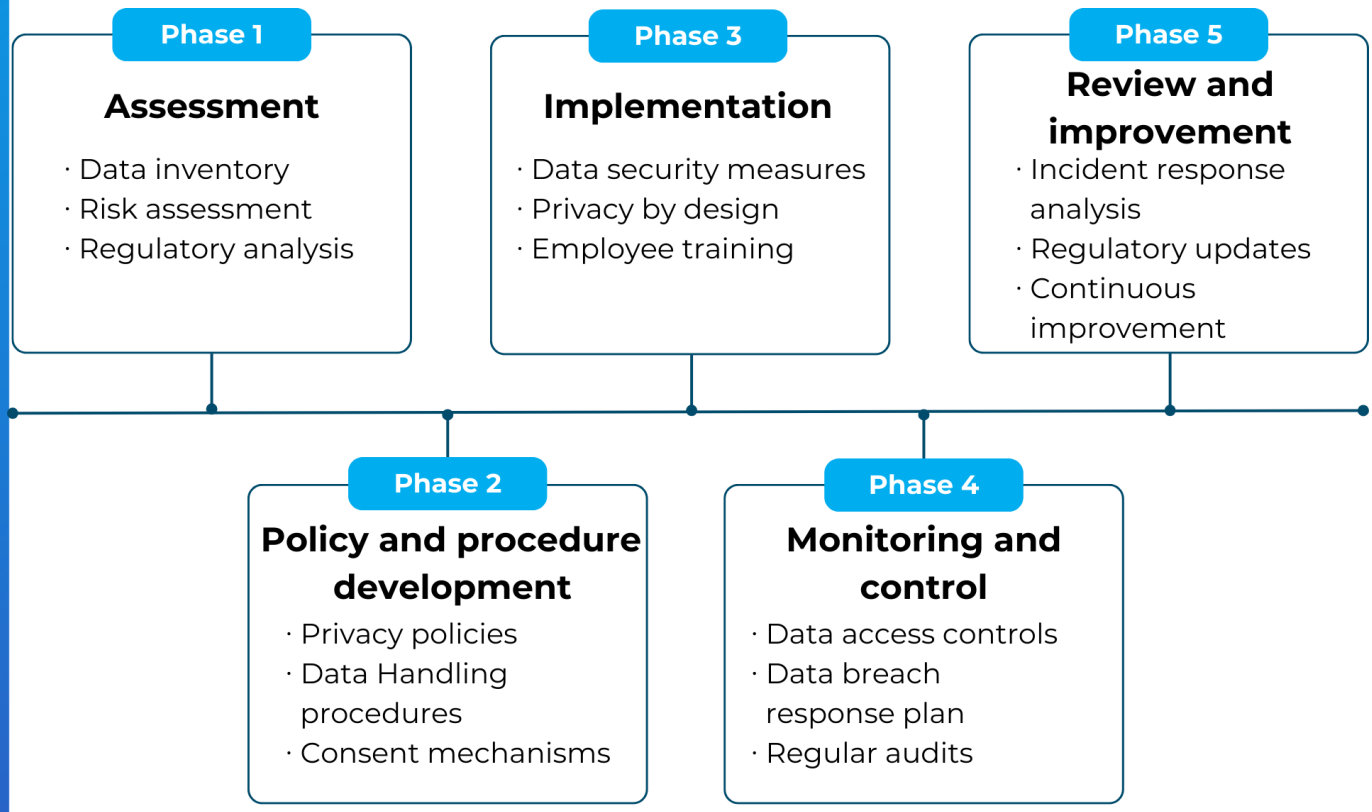
Organisations should establish clear guidelines, provide training to data stewards, and promote a culture of data awareness to ensure consistent and effective data classification practices throughout the organisation.

Data privacy compliance

Data privacy compliance refers to the adherence of organisations to regulations, standards, and best practices designed to protect user's private information

These regulations balance a company's need for collecting user data and an individual's right to control their personal information. Data privacy compliance also goes beyond simply complying with legal requirements. By pursuing compliances, organisations can foster a culture of responsibility towards users' trust while ensuring the ethical use of their personal data. Organisations can create positive consumer experience while fulfilling their obligation to secure valuable information.

Data privacy compliance includes five phases:



Phase 1: Assessment

Data inventory: Identify and document all personal data the organisation collects, stores, processes, and shares.

Risk assessment: Evaluate potential risks associated with data processing activities and data handling practices.

Regulatory analysis: Determine which data privacy regulations apply to the organisation and understand their requirements.

Phase 2: Policy and procedure development

Privacy policies: Develop and update privacy policies that clearly communicate how personal data is collected, used, and protected.

Data handling procedures: Establish procedures for data collection, storage, access, sharing, retention, and disposal.

Consent mechanisms: Implement mechanisms to obtain and manage consent for data processing activities.

Phase 3: Implementation

Data security measures: Implement technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, and destruction.

Privacy by design: Incorporate privacy considerations into the development of products, services, and systems.

Employee training: Provide training and awareness programmes to educate employees on data privacy best practices and compliance requirements.

Phase 4: Monitoring and control

Data access controls: Implement access controls to ensure that only authorised individuals can access personal data.

Data breach response plan: Develop and test a data breach response plan to detect, report, and respond to data breaches promptly and effectively.

Regular audits: Conduct regular audits and assessments to monitor compliance with data privacy policies and regulatory requirements.

Phase 5: Review and improvement

Incident response analysis: Analyse data breaches and privacy incidents to identify root causes and implement corrective actions.

Regulatory updates: Stay informed about changes in data privacy regulations and update policies and procedures accordingly.

Continuous improvement: Continuously review and improve data privacy practices based on lessons learned and emerging best practices.

The function of compliance programmes is to ensure that organisations meet the minimum standards of safety practices. The fact that full compliance does not mean you are doing enough to protect your data. Investing the necessary time and resources into compliance is important for avoiding penalties, and it puts organisations in an outstanding position to defend emerging threats.

Services we provide include:

Privacy impact assessments (PIA): To identify and mitigate privacy risks associated with new projects, systems, or processes, enabling proactive measures to protect sensitive information and uphold individual's privacy rights.

Privacy compliance assessment (PCA): To assess your organisation's current data privacy practices, highlighting areas of non-compliance and recommending corrective actions to align with regulatory requirements.

By leveraging PIA and PCA services, your organisation not only enhance data protection measures but also demonstrate your organisation's commitment to mainlining trust with customers, mitigating the risk of regulatory penalties, and safeguarding your organisation's reputation in an increasingly data-conscious world.

CONTACT US

Our IT and Cybersecurity practice offers a spectrum of services that help businesses to achieve a robust IT architecture and security framework through identifying vulnerabilities, threats, and areas for improvement.

For any enquiries, please contact our advisers directly.

PATRICK ROZARIO
Advisory Services Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
IT & Cybersecurity Principal

T +852 2738 4631
E kevinlau@moore.hk

At Moore, our purpose is to help people thrive – our clients, our people, and the communities they live and work in. We're a global accounting and advisory family with over 37,000 people in 558 offices across 114 countries, connecting and collaborating to take care of your needs – local, national and international.

MOORE