

Ensuring a Quality Data Governance

Data Governance is one of the strategic tasks that the CDO and his/her team must manage. The Standards obliges the CDOs to host their data in the cloud by collaborating with the partner in charge of data hosting and cloud for the Government.

However, apart from dealing with the National Data Center for hosting the data of the Ministries, the CDO has a strategic role to play in the data governance issue. Indeed, ensuring robust data governance involves establishing policies, processes, and practices to manage data effectively, securely, and in alignment with organisational goals. Here are key steps to achieve this:

- **Define Clear Objectives:** Establish clear data governance objectives aligned with the sector's overall Strategy. The various ICT laws (Data protection, security and cybersecurity, data privacy..) should be considered. Define what "good data governance" means for your specific context—whether it's data quality, security, compliance, or accessibility.
- **Leadership and Accountability:** Assign ownership of data governance to a dedicated team or team member. Ensure there's strong leadership support to drive data governance initiatives and establish accountability for data-related decisions.
- **Develop Policies and Standards:** Create comprehensive data governance policies, standards, and guidelines. These should cover data quality, security protocols, access controls, data lifecycle management, and compliance requirements.
- **Data Inventory and Classification:** Conduct a thorough inventory of all data assets, categorise them based on sensitivity and importance, and establish clear classification protocols. This ensures appropriate handling and protection of different types of data.
- **Data Quality Management:** Implement measures to maintain and improve data quality. Establish procedures for data cleansing, validation, and regular quality checks to ensure accuracy and reliability.
- **Data Security and Privacy:** Institute robust security measures to safeguard data from breaches or unauthorised access. Implement encryption, access controls, user authentication, and regular security audits. Ensure compliance with relevant data privacy regulations.
- **Data Lifecycle Management:** Define processes for data creation, storage, usage, archiving, and deletion. Establish clear guidelines for how long data should be retained based on legal, business, or regulatory requirements.
- **Data Governance Framework and Processes:** Develop a structured framework for decision-making, change management, and communication regarding data governance initiatives. Ensure that data-related processes are documented and communicated across the organisation.
- **Training and Awareness:** Conduct training programs (organising, or hosting trainings from institutions like MINICT, RISA) to educate employees on data governance policies, procedures, and best practices. Encourage a culture of data awareness and responsibility across the departments.
- **Continuous Monitoring and Improvement:** Regularly monitor compliance with data governance policies and standards. Gather feedback, conduct audits, and refine processes

to adapt to changing business needs and technological advancements.

Revision #1

Created 9 July 2025 21:45:08 by RISA

Updated 9 July 2025 21:45:26 by RISA