**Data governance** refers to the structured management of an organization's data assets to guarantee their precision, accessibility, uniformity, compliance, and security.  
Successful data governance is built on a foundation of core principles that guide the proper handling and stewardship of data.  
These core principles include data precision, responsibility, uniformity, regulatory compliance, integrity, stewardship, and transparency.

**Data Precision**

A fundamental aspect of data governance is ensuring **data precision**, meaning data must accurately reflect the real-world subjects or situations it represents.  
Poorly maintained data can result in flawed decision-making, inefficiencies, and harm to the organization's reputation.  
High-accuracy data is vital for achieving positive business results—for instance, errors in customer records can disrupt communications, and mistakes in financial data can create compliance risks.  
To uphold data precision, companies should adopt practices such as continuous validation during data input and processing and leverage automated tools for cleansing data to detect and correct errors promptly.

**Data Accessibility**

**Data accessibility** pertains to how readily authorized personnel can obtain and utilize data when needed.  
However, ensuring accessibility must also consider data security and confidentiality.  
Organizations should make sure that appropriate users can access necessary data without delay.  
If access to data is restricted or cumbersome, it can lead to decisions based on partial information or inefficiencies from time lost searching for data.  
Best practices include implementing Role-Based Access Control (RBAC) to assign access permissions based on user roles, employing encryption to secure sensitive information, using data catalogs to enhance data discoverability, and providing self-service analytics platforms for independent data access and analysis.

**Data Uniformity**

Maintaining **data uniformity** means ensuring that data remains consistent across all systems and platforms within an organization.  
When data is inconsistent, it creates conflicting information that undermines the quality of reports, analytics, and strategic decisions.  
Uniform data is especially crucial when multiple systems share or exchange information.  
For example, a change in a customer's address that is updated in one system but not another can cause confusion and service issues.  
Organizations can enforce consistency by utilizing Master Data Management (MDM) systems to harmonize critical data elements and by integrating and aligning data across various departments and databases.

**Data Compliance**

**Data compliance** is the principle of following all applicable laws, regulations, and industry standards related to data privacy and security.  
Requirements like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) mandate strict adherence to data handling standards.  
Failure to comply can result in hefty fines, reputational damage, and a loss of customer trust.  
To ensure compliance, organizations should protect sensitive information, especially personally identifiable information (PII), manage data retention according to legal standards, and maintain detailed records and audit trails that demonstrate adherence to relevant laws.

**Data Integrity**

**Data integrity** focuses on ensuring that data remains accurate, consistent, and trustworthy throughout its existence.  
It safeguards data from unauthorized alterations and preserves its reliability for decision-making and reporting.  
To uphold integrity, organizations can use version control to monitor changes, validate data regularly to catch errors, and implement testing protocols to protect data from corruption or tampering.

**Data Stewardship**

**Data stewardship** refers to the responsibility of managing and overseeing data assets, typically carried out by designated data stewards.  
Data stewards ensure that data is properly handled, shared, and maintained in line with governance policies.  
They act as custodians who enforce data standards, ensure proper classification, and oversee compliance with organizational policies.  
Their roles include enforcing governance policies, enhancing data quality across systems, and fostering communication among departments to address data-related needs and challenges.

**Data Transparency**

The final principle is **data transparency**, which involves making the processes, ownership, and policies around data clearly visible to all relevant stakeholders.  
Transparency builds trust in the organization’s data practices and supports adherence to governance frameworks.  
To promote transparency, organizations should document **data lineage** (tracing data's path from its origin to its final form) and maintain openly available documentation regarding data definitions, usage guidelines, and governance responsibilities, helping all employees understand how data is managed and utilized.