To manage data in a UK retail bank, several systems and processes are typically used. For example, customer data is often managed through a CRM system, which enables the bank to track customer interactions and preferences. Transaction data is managed through core banking systems, which enable the bank to process transactions such as deposits, withdrawals, and transfers.

Data is typically stored in a data warehouse, which is designed to integrate data from multiple sources and provide a single source of truth. The data warehouse may also have data marts, which are designed to provide specific subsets of data for specific purposes, such as risk management or marketing.

To ensure data quality and governance, UK retail banks typically have a data governance framework in place. This framework includes policies, procedures, and controls for managing data, such as data quality checks, data access controls, and data retention policies.

1. ISO 27001: This is an internationally recognized standard for information security management systems. UK retail banks often use ISO 27001 as a framework for developing their own information security policies and procedures.
2. Data Classification: Data should be classified according to its sensitivity level. For example, personal customer data may be classified as highly sensitive, while transactional data may be classified as less sensitive. This classification enables the bank to apply appropriate security controls based on the sensitivity level of the data.
3. Data Access Controls: Access to data should be restricted based on the need-to-know principle. For example, only authorized personnel should have access to highly sensitive customer data.
4. Data Encryption: Data should be encrypted both at rest and in transit to protect it from unauthorized access.
5. Data Backup and Recovery: Data should be regularly backed up and tested to ensure that it can be recovered in the event of a disaster or system failure.
6. Incident Management: The bank should have an incident management process in place to respond to data security incidents, such as data breaches or system failures.
7. Security Awareness Training: All personnel should receive regular security awareness training to ensure that they are aware of their responsibilities and the risks associated with data management activities.
8. Third-Party Risk Management: The bank should have a process for managing the risks associated with third-party vendors and suppliers that have access to the bank's data.
9. Regulatory Compliance: The bank should comply with relevant data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) in the UK.