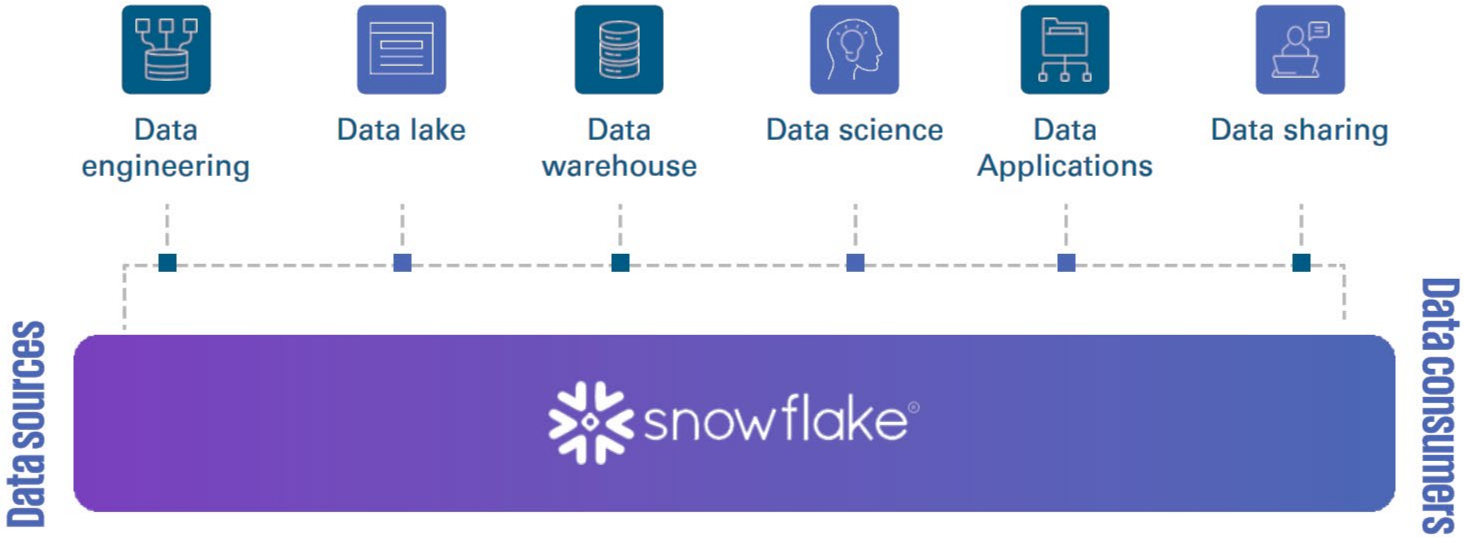
Avoiding an avalanche

Navigating Snowflake's data security risks and challenges

The 2023 KPMG Cloud Transformation survey highlights a surge in cloud-based information technology (IT) workload adoption, driven by the need for efficient data management and analytics. Snowflake stands out in this landscape as a fully managed, cloud-native data platform, offering exceptional storage, processing, and analysis capabilities for vast volumes of data. Due to its unique architecture, scalability, and compatibility with various data ecosystem tools, Snowflake is well-positioned as a choice solution for data-driven decision-making, ensuring secure and efficient infrastructure management.

Snowflake offers a unified platform for data warehousing, integration, and advanced analytics. It supports scalable architecture, enables seamless data sharing, and incorporates AI for analytics, optimizing data management and insight generation for organizations.



Frequently asked questions

Below are some of the questions that arise when organizations leverage Snowflake and its technology:

- I have key reports generated from Snowflake that support my business processes and controls. How do I know they are complete and accurate?
- How do we assess that data is secure and sensitive data is not exposed? In the context of using data from nonproduction schemas, what measures prevent unauthorized access to experimental or provisional datasets?
- How do we ensure that proper access and change management controls are in place?
- How are system IDs and secrets managed within Snowflake?
- How is Snowflake's integration with continuous integration and continuous delivery/deployment (CI/CD) tools and secrets management solutions managed to ensure operational security?
- What should be the shared responsibility model for the Snowflake environment's underlying data and how do you see it evolving?
- With the adoption of Snowflake's artificial intelligence (AI) capabilities, what are the implications for data privacy and protection, and how are AI-generated insights secured?

Risk and control considerations

Risk professionals play a key role in navigating the complexities of Snowflake, ensuring data security and governance are optimized to benefit the organization.

Risk professionals need to know how Snowflake is used by the company. This means knowing how data is ingested, stored, and secured in Snowflake, and how it is used for analysis. In-depth knowledge will help pinpoint where potential risks may lie and where controls should be put in place. The following steps will help you with this process:

- Gain a deep understanding of how data travels within Snowflake, from the moment it's ingested, through its processing, to final analysis.
- Conduct thorough walk-throughs of business processes to grasp the specific roles and uses of Snowflake within the organization.
- Identify potential risk scenarios (What Could Go Wrong) related to the use of Snowflake and map these scenarios to existing controls.
- Determine the key financial data elements within Snowflake and understand a clear path from their source to the reports they contribute to.
- Scope controls that focus and cover elements critical to a company's operations or compliance needs. You may consider the following specifics of Snowflake:
  - Consider how databases and schemas are configured to organize and control access to data according to their operational and compliance needs.
  - Inquire about the use of Secure Views and Secure UDFs to understand how management controls data access, protects sensitive information, and meets compliance during data access and processing.
- Ensure there is a clear understanding across a company on how to map the Complementary User Entity Controls called out in the Snowflake System and Organization Controls reports to the specific responsibilities in the company.

Specific ways to navigate data security with Snowflake

Deploying Snowflake introduces specific risk considerations that organizations must address to safeguard their data ecosystem. Below are listed some preventive measures for different aspects of securing Snowflake.

1 Snowflake combines data governance, information security, and change management for **data protection and compliant use.**

- Data governance and protection in Snowflake are enhanced through support for data cataloging and lineage, which facilitate classification, retention, and deletion. This is further complemented by the use of tags, custom classifiers, and the Time Travel feature to ensure data organization, compliance, and recovery.
- Snowflake's approach to information security includes end-to-end encryption for data both at rest and in transit, along with secure sharing mechanisms that guarantee privacy and prevent unauthorized access.

2 Foundational IT general controls

- Snowflake's security is bolstered by advanced access management, including role-based access control and row-level security, paired with multifactor authentication for authentication and robust data access monitoring.
- Efficient change management in Snowflake is achieved through strict version control and Zero-Copy Cloning for cost-effective testing, alongside CI/CD automation and monitoring tools to maintain data security and governance.

3 For controlling data access or integrating new datasets, features such as data sharing, secure views, data masking, anonymization, and data tokenization are vital. These capabilities ensure that **only approved users or accounts have access** to sensitive information, upholding data privacy and adherence to regulations. Snowflake offers comprehensive data masking, anonymization, and tokenization solutions to protect sensitive information effectively, while still allowing for its analysis and use in reporting.

4 Integrating Snowflake with your entity's data privacy processes and controls can help support compliance with applicable **privacy laws and regulations** including the General Data Protection Regulation and California Consumer Privacy Act. By leveraging Snowflake's continuous data protection features such as Time Travel or Deletion flags, organizations can fulfill data subject requests for access, correction, and deletion in timely and effective manner and enable data minimization.

5 By harnessing Snowflake's Snowpark and Data Science capabilities for analytics and machine learning directly on data, users can **proactively detect** anomalies, patterns, and trends to mitigate risks before they escalate.

Find out more about KPMG technology risk insights at the Centers of Excellence page KPMG Modern Technology Risk.

Contact us

Lavin Chainani
Managing Director,
Technology Risk
KPMG LLP
T: 410-949-8834
E: lchainani@kpmg.com

Chris Kypreos
Director,
Cyber Security Services
KPMG LLP
T: 415-963-5148
E: ckypreos@kpmg.com

Lena Buglak
Director,
Technology Risk
KPMG LLP
T: 248-895-7845
E: lbuglak@kpmg.com

Jack Baroudi
Senior Associate,
Technology Risk
KPMG LLP
T: 410-949-8500
E: jbaroudi@kpmg.com

Learn about us: in | **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.