SALT

ISO/IEC 27001 & ISO/IEC 27017: Securing Cloud-Based APIs

ISO/IEC 27001 and ISO/IEC 27017 outline a framework for establishing an information security management system (ISMS) focused on cloud services. They promote a holistic approach to API security, urging organizations to implement measures that protect sensitive data. The standards address unique risks of cloud-based APIs, including data residency and shared responsibility, recommending technical controls like encryption and secure authentication. By following these standards, organizations enhance their commitment to information security and boost customer trust.

- Information Security Management:
  - Development and implementation of information security policies and procedures.
  - Regular review and update of security controls.
  - Employee training and awareness programs.
- Cloud Security:
  - Addressing data residency and compliance requirements.
  - Implementing secure data storage and transmission practices.
  - Managing shared responsibility for cloud security.
- Technical Controls:
  - Use of TLS 1.2+ encryption to protect data in transit.
  - Implementation of OAuth 2.0 and JWT for secure authentication.
  - Logging and monitoring of API activity for security incidents.

Why It Matters: ISO/IEC 27001 and 27017 are internationally recognized standards that demonstrate a strong commitment to information security, especially in cloud environments. Compliance builds confidence among customers and partners that sensitive data is handled responsibly, enhancing your organization's reputation and trust.

API Security Requirements:

- **Secure Transmission:** APIs must use TLS 1.2+ encryption for data-in-transit.
- **Access Management:** Enforce OAuth 2.0 and JWT-based authentication for APIs.

Relevant Sections Referencing APIs:

- **ISO/IEC 27017, Control 14.2.1:** APIs must be secured when exposed over public networks.

How Salt Security Helps: Salt Security supports ISO/IEC 27001 and 27017 compliance by providing comprehensive API discovery, identifying potential vulnerabilities, and detecting threats. Posture governance features offer continuous monitoring and reporting, enabling organizations to demonstrate the effectiveness of their security controls and maintain compliance. Salt Security's data security capabilities allow you to view sensitive data in motion through APIs, providing a deeper understanding of how data is accessed and processed in your cloud environments. Learn more about API Security and Compliance in our **White-paper.**