SOC2

Summary

Regulation: Service Organization Control 2

Abbreviation: SOC2

Governs these parties: all technology service providers or SaaS companies that store or handle client data

Enforced by: the majority of global companies require their partners and vendors to meet these standards

Details

Service Organization Control (SOC) 2 is a set of compliance requirements and auditing processes targeted at third-party service providers. It was developed to help companies determine whether their business partners and vendors can securely manage data and protect the interests and privacy of their clients.

The rest of this document is designed to help our community understand SOC2 better by outlining the following information.

- **How it Relates to Cybersecurity**
- **How Coro Handles Compliance for You**

How it Relates to Cybersecurity

SOC2 is based on specific criteria for managing customer data correctly, which consists of five trust service categories: security, availability, processing integrity, confidentiality, and privacy.

These areas cover:

- Logical and physical access controls — how to restrict and manage logical and physical access, to prevent any unauthorized access
- System operations - how to manage system operations to detect and mitigate deviations from set procedures
- Change management - how to implement a controlled change management process and prevent unauthorized changes
- Risk mitigation - how to identify and develop risk mitigation activities when dealing with business disruptions and the use of any vendor services