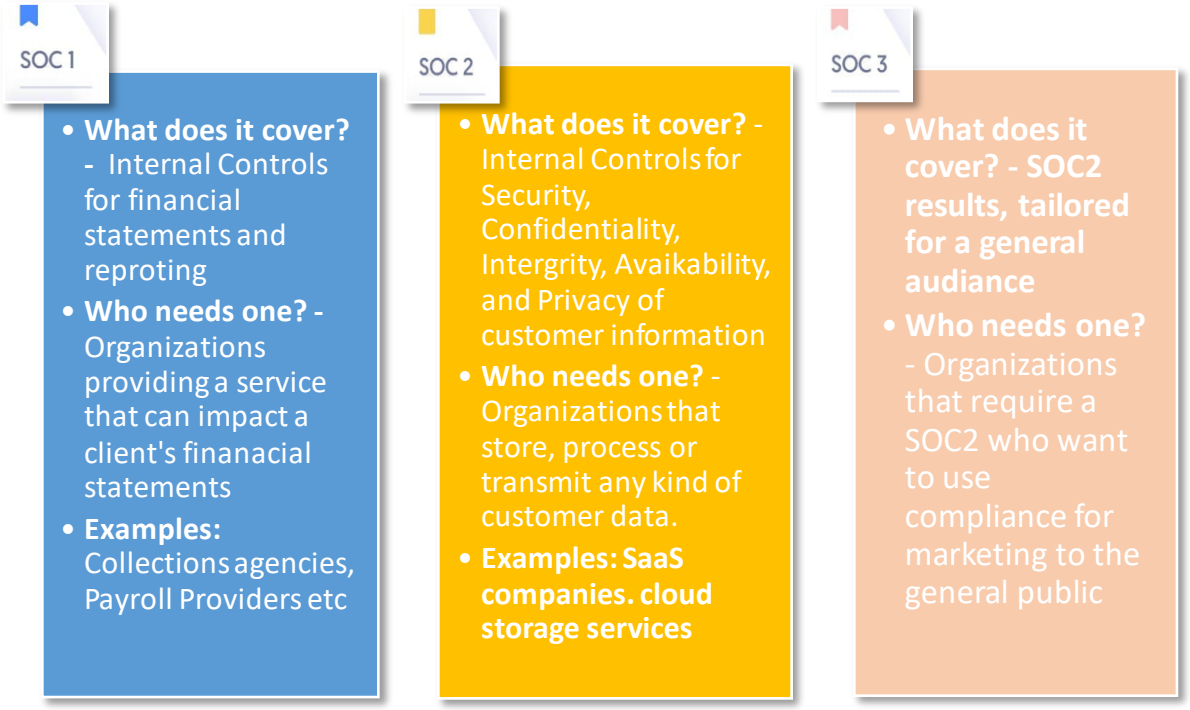
1. What is SOC?

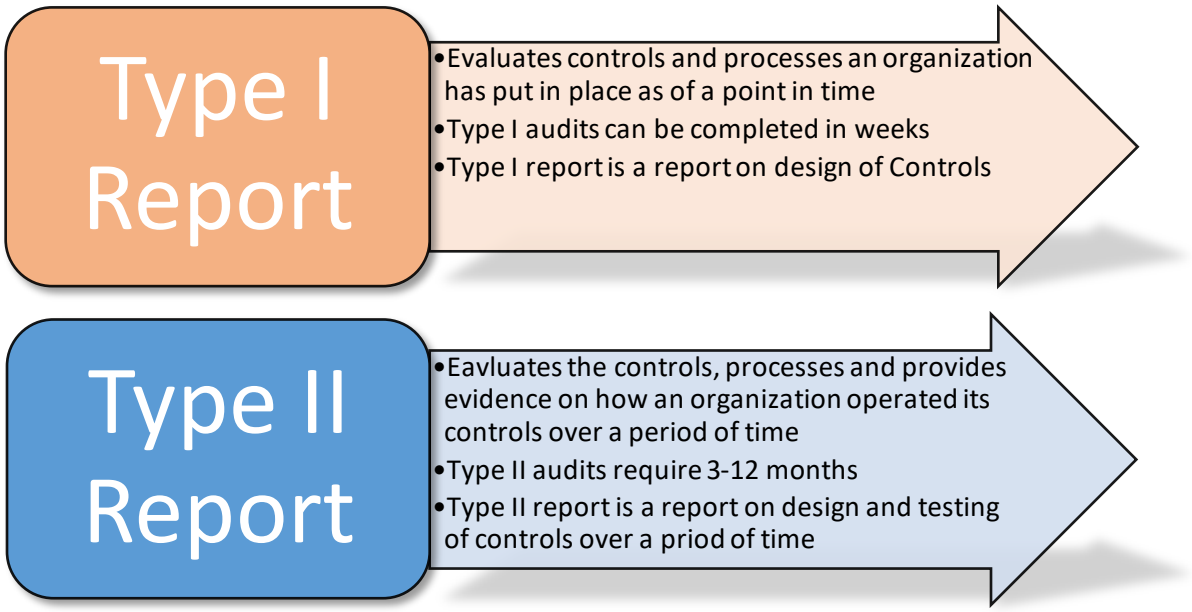
SOC (System and Organization Controls – formerly Service Organization Controls) audits are an independent assessment of the risks associated with using service organisations and other third parties.

The System and Organizations Control (SOC) framework's series of reports offer 3 types of reports:
SOC 1, SOC 2, and SOC 3



SOC 2 audits are divided into two types:

- **Type 1 –** An audit carried out on a specified date.
- **Type 2 –** An audit carried out over a specified period, usually a minimum of six months.



SOC 3 audits are always Type 2.

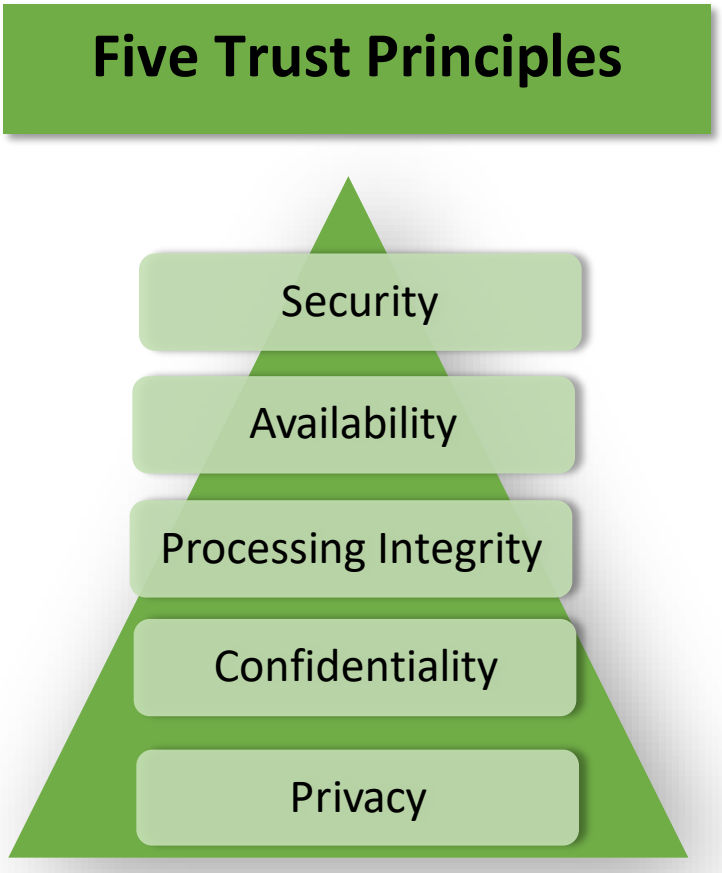
2. What is SOC2 Framework?

SOC 2, System and Organization Control Type 2, is a cyber-security compliance framework developed by the American Institute of Certified Public Accountants (AICPA).

SOC 2 ensures that third-party service providers stores and process client data in a secure manner.

The framework sets rules to make sure that data is super safe, and it does this by following five trust service principles.

1. Security
2. Privacy
3. Availability
4. Confidentiality
5. Processing integrity.



3. Five Trust Principles:

3.1 Security

The security principle involves safeguarding system resources from unauthorized entry. Access controls prevents possible misuse of the system, data theft, unauthorized data removal, improper use of software, and inappropriate changes or disclosures of information.

3.2 Availability

The Availability principle looks at how well a service organization can make sure its systems and services are up and running when they're supposed to be, as promised to its clients. Essentially, it checks how the organization plans to avoid and bounce back from anything that might disrupt its services.

3.3 Integrity

The Integrity Principle is all about making sure that a service organization's systems and the data they contain are trustworthy and correct. This principle guarantees that the

organization's data is whole, accurate, and shielded from any unauthorized changes or tampering.

3.4 Confidentiality

The Confidentiality Principle is all about checking how well a service organization keeps important information safe from people who shouldn't see it, and it makes sure that the organization keeps tight rules about who can access this confidential info.

3.5 Privacy

The Privacy Principle deals with how a system handles personal information, including gathering it, using it, keeping it, sharing it, and getting rid of it, following both the organization's privacy policy and the standards outlined in the AICPA's generally accepted privacy principles.

4. SOC2 Type II Report Scope

A SOC 2 Type II report is all about looking at how a service provider handles various aspects of data protection based on the American Institute of Certified Public Accountants (AICPA) Trust Service Criteria, which used to be called the Trust Service Principles. It checks the service provider's internal controls and systems to make sure they're secure, available, reliable, confidential, and respectful of privacy when it comes to data.

It focuses on the following areas:

- Infrastructure: The physical and hardware components (networks, facilities, and equipment) that support IT environment and help to deliver services.
- Software: The operating software and programs (utilities, applications, and systems) used to facilitate data and system processing.
- People: The personnel (managers, developers, users, and operators) involved in the management, security, governance, and operations to deliver services to customers.
- Data: The information (files, databases, transaction stream, and tables) used or processed within the service organization.
- Procedures: The manual or automated procedures that bind processes and keep service delivery ticking along.

5. Who needs a SOC 2 Type II report?

- SOC 2 Type II applies to any business handling sensitive customer information. It’s useful for cloud computing vendors, managed IT services providers, software-as-a-service (SaaS) providers, and data centres.
- A SOC 2 Type I report demonstrates the commitment to protecting sensitive data. However, it only represents a point-in-time snapshot, which may not be sufficient for enterprise clients.

- The SOC 2 Type II report breaks that ceiling, allowing businesses to scale to the next level and net contracts with larger enterprises that know their databases are prime targets for cybercriminals and want to avoid costly hacking incidents.
- Whether wooing start-ups or enterprise clients, customers want assurance that you've woven security controls into the organization's DNA. They also want to see that the organization have defined risk management, access controls, and change management in place, and that the organization monitor controls on an ongoing basis to make sure they are working optimally.

6. Steps Involved in the Audit Process for SOC2 Type2:

6.1 Planning and Scoping:

- The audit process begins with scoping and planning discussions between the service organization and the audit firm.
- The scope defines the systems, processes, and locations to be assessed.
- Audit objectives, timeline, and responsibilities are outlined.

6.2 Risk Assessment:

- The audit firm performs a risk assessment to identify the areas with the highest risk of control failures.
- This assessment guides the focus of the audit and helps tailor the testing procedures.

6.3 Control Identification and Documentation:

- The service organization documents its control activities related to the trust principles (security, availability, processing integrity, confidentiality, and privacy).
- The controls should be well-defined and mapped to the relevant principles.

6.4 Control Testing:

- The audit firm tests the effectiveness of the documented controls over a continuous period, typically six months or longer.
- This involves examining evidence, conducting interviews, and reviewing documentation to verify that the controls are operating as intended.

6.5 Sampling and Testing Procedures:

- The audit firm uses sampling to select a representative subset of transactions, data, or activities for testing.
- Testing procedures are applied to the selected samples to assess control effectiveness.

6.6 Issue Identification:

- During testing, the audit firm identifies any control deficiencies, deviations, or weaknesses.
- These issues are documented and categorized based on severity.

6.7 Management Response and Remediation:

- The service organization has an opportunity to review and respond to the identified issues.
- If deficiencies are found, the organization develops remediation plans to address them.

6.8 Report Preparation:

- The audit firm compiles the findings, testing results, management's responses, and any remediation plans into a formal SOC 2 Type 2 report.
- The report includes an opinion on the effectiveness of controls based on the audit procedures.

6.9 Opinion and Reporting:

- The SOC 2 Type 2 report includes an opinion section that states whether the controls were suitably designed and operating effectively during the assessment period.
- The report is issued to the service organization.

6.10 Distribution and Use of Report:

- The service organization shares the SOC 2 Type 2 report with clients, partners, stakeholders, and regulatory bodies to demonstrate its commitment to security and compliance.
- The report helps clients evaluate the organization's controls and make informed decisions about working with them.