SOC vs SOX

A Detailed Guide to Understanding the Difference Between SOC & SOX.

Definition & Purpose

SOC (System and Organization Controls): Ensures security, availability, processing integrity, confidentiality, and privacy of data handled by service organizations.

SOX (Sarbanes-Oxley Act): A U.S. federal law ensuring financial transparency and preventing corporate fraud.

Key Difference

SOC	SOX
It focuses on data security, privacy, and IT controls.	It focuses on financial transparency and fraud prevention.
Service providers are SaaS companies, cloud providers, and IT vendors.	Service providers are public companies, financial institutions etc.
Audit covers Trust Service Criteria (TSC) security, availability, confidentiality, etc.	Audit covers IT General Controls (ITGC), access controls, financial data security etc.

Compliance Scope & Applicability

Aspect	SOC	SOX
Control Frameworks	Based on TSC (Trust Services Criteria).	Uses COSO & COBIT frameworks.
Testing Approach	Controls-based testing.	Substantive & control testing.
Audit Frequency	Annual or as required.	Mandatory annual audits.
Key IT Systems Covered	Cloud, SaaS, IT service providers.	ERP, financial databases, ITGCs.
Penalties for Non-Compliance	Loss of trust, contract risks.	Fines, CEO/CFO liability, delisting.

Audit & Control Objectives

SOC AUDIT

SOC 1

Controls over financial reporting (Similar to SOX but voluntary).

SOC 2

Focuses on Security, Availability, Processing Integrity & Privacy.

Audit & Control Objectives

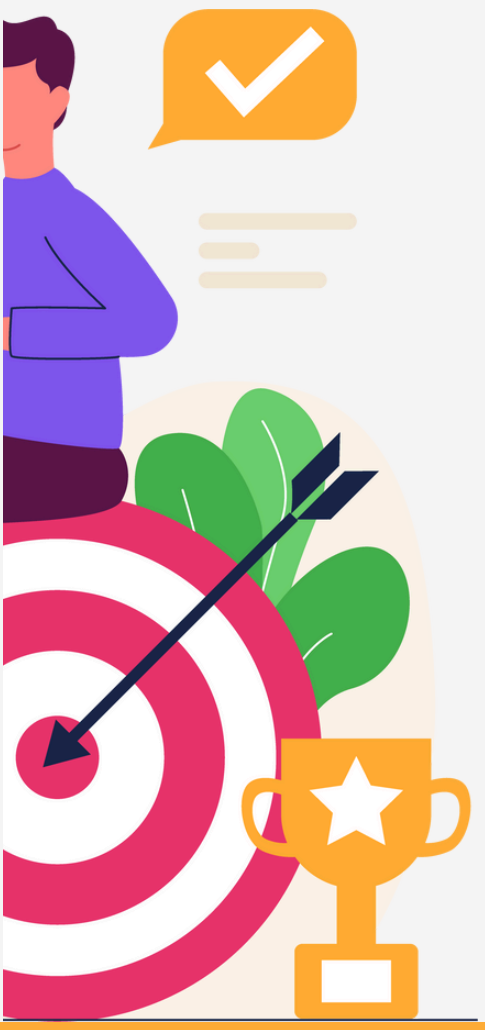
SOX AUDIT

SECTION 302

CEO/CFO must certify financial report accuracy.

SECTION 404

Internal controls must be assessed to prevent fraud.



Who Performs the Audits

Audit Type	Conducted By
SOC 1 & SOC 2 Reports	CPA firms (AICPA standards)
SOX Compliance	External auditors (PCAOB-regulated)
SOX IT Controls	Internal auditors + External SOX auditors
Regulatory Body	SOC: AICPA, SOX: SEC & PCAOB
Report Users	SOC: Clients, SOX: Regulators

Cost & Business Impact

Cost Comparison

- SOC Audit: ₹10-30 Lakhs (varies by scope & type).
- SOX Compliance: ₹50 Lakhs - ₹2 Crores (ongoing costs, stricter requirements).

Business Impact

- SOC: Enhances trust, attracts clients, and improves vendor risk management.
- SOX: Ensures financial integrity, prevents fraud, and avoids regulatory penalties

CONCLUSION

Both are critical for risk management, but their objectives differ.

✅ SOC = Data Trust | SOX = Financial Trust

02

SOX ensures financial integrity & regulatory compliance.

01

SOC focuses on data security & IT controls.

THANK YOU

Authored by: Khushi Malhotra