SOX

Summary

Regulation: Sarbanes–Oxley Act and accounting standards, COSO, COBIT®, SAS

Abbreviation: SOX

Governs these parties: all publicly traded companies in the USA, as well as any wholly-owned subsidiaries and foreign companies that are both publicly traded and do business with the USA. Any accounting firms that are auditing companies bound by SOX compliance are also, by proxy, obliged to comply

Enforced by: the Securities and Exchange Commission (SEC)

Details

SOX compliance lays out a set of requirements for annual audits to assess and protect shareholders in financial & IT public companies by securing their access controlling data management and preventing breaches and fraud. SOX describes a course of action to take in order to show evidence of accurate, secured financial reporting and it provides companies with a way of improving their data security whilst simultaneously helping to restore public confidence, reducing chances of falling victim to a data breach.

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

How it Relates to Cybersecurity

To comply with SOX, you will effectively have to model your security on the Data-Centric Audit and Protection model. This model requires you to understand where your sensitive data is, who has access to it, and what users are doing with it. SOX audits require that strict auditing, logging, and monitoring take place across all internal controls, network and database activity, login activity, account activity, user activity, and information access.

It includes all of the company's IT assets, such as computers, hardware, software, and all the other electronic devices that can access financial data.

Companies need to ensure that:

- they have a way to locate where sensitive data is, see who has access to it, and monitor user interactions with it