

WHAT IS THE SOX ACT?

OVERVIEW

Sarbanes-Oxley, or SOX, is an Act passed by the USA in 2002 outlining regulations for financial reporting, information security, and auditing requirements. SOX aims to prevent corporate fraud.

SOX makes it illegal for any organisation to destroy or falsify financial records.

DO I HAVE TO COMPLY WITH SOX?

All publicly traded companies doing business in the USA or with US owned organisations must comply with SOX. This also includes any security analysts and accounting firms that audit these public companies.

REQUIREMENTS

There are three broad requirements for companies to comply with SOX:

1 - Filing Accurate Financial Reports

A company's CEO, CFO, or equivalent must sign off on every annual and quarterly financial report filed with the SEC. In doing this, they are affirming these reports are completely accurate.

An in-depth report on internal controls is also required, confirming their existence and that they have been validated within the last 90 days.

Cybersecurity incidents must also be reported if they have a material impact of financial status.

2 - Implementing Internal Controls

These controls are to prevent malicious actors from fraudulently altering or using financial data.

SOX does not explicitly state what these controls are, but they can include manual and automated measures such as staff training or implementing IT solutions to monitor business applications and data that fall into scope.

3 - Passing Regular Audits

Regular audits provide the signing executives the evidence to back up their affirmation of accuracy.

Audits continuously highlight gaps and weaknesses in the internal controls, allowing businesses to remedy their vulnerabilities.

*information courtesy of [IBM](#)



WHY IT MATTERS

By complying with SOX, businesses open their market to the US, inspire investor confidence, and protect themselves from cybersecurity threats and fraudulent activity.

SOX non-compliance risks criminal and civil charges for organisations and individuals.

Should a report be found to be inaccurate, the signatory risks fines up to \$1 million (USD).

HOW CAN RESPONSIV HELP?

Responsiv Cloud Data Compliance Service (RCDCS) automates data compliance monitoring and reporting for SOX, GDPR, PCI DSS, and more.

- Out the box policies
- Automated controls and reporting
- Active threat analytics and risk detection powered by ML
- No software installation required
- Managed cloud service

Our consultants are available to customise and optimise your solution as needed to streamline your compliance.

CONTACT US

sales@responsiv.co.uk