



Mapping the Lepide Data Security Platform to the **Sarbanes-Oxley Act (SOX)** using the **COBIT Framework**



SOX Compliance

The Sarbanes-Oxley Act of 2002 was passed by the United States Congress with the goal of providing security for consumers and the general public against corporations acting maliciously or carelessly. The general requirements of SOX compliance are geared towards ensuring that companies are transparent when it comes to financial reporting and that there are more official rules in place to prevent fraud.

Adhering to SOX compliance requirements is not only the law, it is also best practice for a more ethical and secure operation. Implementing SOX financial security controls, aside from being the right thing to do, also has the added benefit of helping to defend against data security threats and attacks.


SOX Requirements

SOX requires that all financial reports include an Internal Controls Report. This report should show that the company's financial data is accurate (a 5% variance is permitted) and that appropriate and adequate controls are in place to ensure that the data is secure.

Financial reports at the end of every year are also a requirement.

SOX audits are to be carried out by external auditors within which controls, policies and procedures are all to be reviewed during a Section 404 audit.





Section 404 audits will also involve looking into staff, potentially even conducting interviews, to ensure that job descriptions match duties, and that the required training on how to handle financial data has taken place.

SOX sections 302, 404 and 409 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.

SOX audits often require the use of frameworks like COBIT to audit internal controls and procedures. You must make sure that any log collection, auditing, and monitoring solutions are able to provide a complete audit trail of access to and interactions with sensitive data.

Mapping Lepide to SOX using the COBIT Framework

Key Activity	Control Text	Technology Alignment
Access Control	<p>APO07.06 Manage contract staff - Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.</p> <p>DSS05.04 Manage user identity and logical access - Ensure that all users have information access rights in accordance with their business requirements and coordinate with business units that manage their own access rights within business processes.</p> <p>DSS06.03 Manage roles, responsibilities, access privileges and levels of authority - Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.</p>	<p>Lepide Identify (Data Discovery and Classification)</p> <p>Lepide Trust (Access Governance)</p> <p>Lepide Insight (User and Entity Behavioural Analytics)</p>
Logging, Monitoring and Alerting	<p>DSS01.03 Monitor IT infrastructure - Monitor the IT infrastructure and related events. Store sufficient chronological information in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.</p> <p>DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events - Using intrusion detection tools, monitor the infrastructure for unauthorized access and ensure that any events are integrated with general event monitoring and incident management.</p>	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>

Key Activity	Control Text	Technology Alignment
Risk Analysis and Management	APO12.01 Collect data - Identify and collect relevant data to enable effective IT-related risk identification, analysis and reporting.	<p>Lepide Insight (User and Entity Behavioural Analytics)</p> <p>Lepide Detect (Threat Detection and Response)</p>
	APO12.02 Analyze risk - Develop useful information to support risk decisions that take into account the business relevance of risk factors.	
	APO12.06 Respond to risk - Respond in a timely manner with effective measures to limit the magnitude of loss from IT-related events.	
	APO13.01 Establish and maintain an ISMS - Establish and maintain an ISMS that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.	

Lepide Data Security Platform

Core Capabilities

Lepide Identify

(Data Discovery and Classification)

- Discover and classify data in real-time.
- Tag data.
- Data valuation.
- Identify data most at risk.

Lepide Trust

(Access Governance)

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Change permissions.

Lepide Insight

(User and Entity Behavior Analytics)

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

Lepide Detect

(Threat Detection and Response)

- Detect threats in real-time.
- Baseline/profile employee behaviour.
- Identify anomalous employee behaviour.
- Alert and respond to threats in real-time.



Start a free trial



Get a demo



Get a free risk
assessment