MAPPING GUIDE

imprivata®

Mapping to the Sarbanes-Oxley Act (SOX)

Background

The Sarbanes-Oxley Act of 2002 (also known as the Public Company Accounting Reform and Investor Protection Act of 2002), is a United States federal law enacted on July 30, 2002 in response to many major corporate and accounting scandals. The Act is commonly called “SOX”.
As of 2006, all public companies are required to submit an annual assessment of the effectiveness of their internal financial auditing controls to the U.S. Securities and Exchange Commission (SEC). Additionally, each company’s external auditors are required to audit and report on the internal control reports of management, in addition to the company’s financial statements.

Who Needs To Comply to SOX

A YES TO ANY OF THESE QUESTIONS AND SOX AFFECTS YOUR COMPANY:

Is your company publicly traded?
The SOX legislation established new or enhanced standards for all U.S. public company boards, management, and public accounting firms. For compliance with Section 404 (explained later), public companies with a market capitalization over US $75 million needed to have their financial reporting frameworks operational for their first fiscal year-end report after November 15, 2006, then for all quarterly reports thereafter. For smaller companies, compliance is required for the first fiscal yearend financial report, then for all subsequent quarterly financial reports after July 15, 2006.

Is your company private, but planning an initial public offering (IPO)?
SOX does not apply to privately held companies, although those considering filing for an initial public offering (IPO) must demonstrate a SOX compliant framework.

Does your company provide financial services to either of the above?
Any account firm or other third party that provides financial services to publicly traded companies must comply with SOX.

Getting Started With SOX Compliance

The SOX legislation is compromised of eleven sections. The two most important sections for information security and compliance are sections 302 and 404 (https://www.sec.gov/rules/proposed/s74002/card941503.pdf)

SOX SECTION 302 - CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS

a) CEO and CFO must review all financial reports.
b) Financial report does not contain any misrepresentations.
c) Information in the financial report is “fairly presented”.
d) CEO and CFO are responsible for the internal controls.
e) CEO and CFO must report any deficiencies in internal accounting controls, or any fraud involving the management of the audit committee.
f) CEO and CFO must indicate any material changes in internal controls.

SOX SECTION 404: MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS

All annual financial reports must include an Internal Control Report stating that management is responsible for an “adequate” internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management’s assertion that internal accounting controls are in place, operational and effective.

Addressing SOX Requirements Through Use of COSO and COBIT Frameworks (and Imprivata FairWarning)

The SOX legislation does not mandate a control framework for use towards compliance. The legislation requires “management to base its evaluation of the effectiveness of the company’s ICFR on a suitable, recognized control framework”. (https://www.sec.gov/rules/final/33-8238.htm)

Although enterprises have flexibility in their choice of an internal control framework, in practice, most enterprises choose to adopt two. The COSO (Committee of Sponsoring Organizations) framework represents a joint effort between five accounting and auditing organizations and “is dedicated to providing through leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.” (https://www.coso.org/Pages/default.aspx)

However, COSO gives only very broad guidance on IT controls. Because of this lack of specificity in IT controls, COBIT (Control Objectives of Information and Related Technology) has been mapped to COSO to show how the two frameworks complement each other for purposes of SOX compliance.

Note that this document contains only a subsection of the COBIT controls that are:

- Pertinent to SOX compliance, and
- Supported by Imprivata FairWarning system capabilities.

Broadly, the COSO framework has five components:

COSO FRAMEWORK

- **Risk Assessment:** The processes and technologies used in identifying and understanding the areas of risk affecting the completeness and validity of financial reports and other important and sensitive information with impact to financial reporting.
- **Control Environment:** This is really the foundation of applying the COSO framework and achieving SOX compliance through it. It comprises the integrity and ethics of an organization end-to-end, management's philosophy and operating style, the way management assigns authority and responsibility, and organizes and develops its people as well as the attention and direction provided by the board of directors.
- **Control Activities:** This includes the approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.
- **Monitoring:** Auditing processes and schedules to address the high-risk areas within the IT organization. IT personnel should perform frequent internal audits.
- **Information and Communication:** IT management demonstrating to company management an understanding of what needs to be done to comply with Sarbanes-Oxley and how to get there.

COBIT FRAMEWORK

COBIT is used by many companies as a framework supporting IT specific efforts towards complying with SOX sections 302 and 404. However, there are certain aspects of COBIT that are outside the boundaries of SOX regulation. COBIT currently delineates five domains and thirty-seven processes. These processes are then further specified into practices. In this report of Imprivata FairWarning's applicability and support towards SOX compliance, we focus on the sixteen practices and activities pertinent to that.

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Align, Plan and Organize	Manage Human Resources	APO07.06	Manage contract staff	Conduct periodic reviews to ensure that contractors' roles and access rights are appropriate and in line with agreements.	Imprivata FairWarning will consistently monitor contractor access to ensure appropriateness and provide alerts (as built within the application).	Full	X	X		X	

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Align, Plan and Organize	Manage Suppliers	APO10.02	Select suppliers	In the specific case of acquisition of infrastructure, facilities and related services, include and enforce the rights and obligations of all parties in the contractual terms. These rights and obligations may include service levels, maintenance procedures, access controls, security, performance review, basis for payment and arbitration procedures.	FairWarning provides monitoring of access controls to monitor and/ or investigate supplier access to confidential data.	Partial	X	X	X	X	
	Manage Risk	APO12.03	Maintain a risk profile	Capture information on IT risk events that have materialized, for inclusion in the IT risk profile of the enterprise.	Imprivata FairWarning will capture incidents pertaining to inappropriate access. The customer can investigate and write up these incidents. Then, those incident reports can be outputted to a SIEM tool for a composite view of an organization's incidents and risks.	Partial	X	X		X	

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Align, Plan and Organize	Manage Security	APO13.02	Define and manage an information security risk treatment plan.	Maintain as part of the enterprise architecture an inventory of solution components that are in place to manage security-related risk.	Imprivata FairWarning is a solution to application level security issues dealing with data access. It can be part of a suite of components to manage security related risk.	Full	X	X	X	X	
		APO13.03	Monitor and review the ISMS.	Undertake regular reviews of the effectiveness of the ISMS (info security mgmt system) including meeting ISMS policy and objectives, and review of security practices. Take into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.	Imprivata FairWarning will assist in reviewing effectiveness of ISMS in terms of audit controls and access rights management.	Partial	X	X	X	X	

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Deliver, Service and Support	Manage Security Services	DSS05.04	Manage user identity and logical access	Maintain an audit trail of access to information classified as highly sensitive.	Imprivata FairWarning will assist in maintaining and reporting on audit data that shows user access to highly sensitive information. Customers can report on audit data themselves within the Imprivata FairWarning application or contract with Managed Privacy Services to assist with this activity.	Full		X	X	X	
	Manage Business Process Controls	DSS06.06	Secure information assets	Identify and implement processes, tools and techniques to reasonably verify compliance.	Imprivata FairWarning is a tool that can be used to verify compliance with various regulatory standards in terms of access rights management and audit controls.	Partial	X	X	X	X	

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Monitor, Evaluate and Assess	Monitor, Evaluate and Assess	MEA01.04	Analyze and report	Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports) and ensure that the cause and effect between goals and metrics are communicated in an understandable manner.	Imprivata FairWarning can be used to produce reports that track and summarize compliance activities for access rights management and audit controls.	Partial	X	X		X	
	Monitor, Evaluate and Assess the System of Internal Control	MEA02.01	Monitor internal controls	Identify the boundaries of the IT internal control system (e.g., consider how organizational IT internal controls take into account outsourced and/or offshore development or production activities).	Imprivata FairWarning's dynamic identity intelligence (DII) assists customers in identifying all users accessing monitored information. These users may represent outsourced and/or offshored accounts.	Partial	X	X		X	X

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Monitor, Evaluate and Assess	Monitor, Evaluate and Assess	MEA03.04	Obtain assurance of external compliance	Monitor and report on noncompliance issues and, where necessary, investigate the root cause.	Imprivata FairWarning will assist in monitoring user access that is non compliant with customer standards (built within the application).	Partial	X	X		X	X
Deliver, Service and Support	Manage Security Services	DSS05.04	Manage user identity and logical access	Maintain an audit trail of access to information classified as highly sensitive.	Imprivata FairWarning will assist in maintaining and reporting on audit data that shows user access to highly sensitive information. Customers can report on audit data themselves within the Imprivata FairWarning application or contract with Managed Privacy Services to assist with this activity.	Full		X	X	X	
	Manage Business Process Controls	DSS06.06	Secure information assets	Identify and implement processes, tools and techniques to reasonably verify compliance.	Imprivata FairWarning is a tool that can be used to verify compliance with various regulatory standards in terms of access rights management and audit controls.	Partial	X	X	X	X	

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Monitor, Evaluate and Assess	Monitor, Evaluate and Assess	MEA01.04	Analyze and report	Design process performance reports that are concise, easy to understand, and tailored to various management needs and audiences. Facilitate effective, timely decision making (e.g., scorecards, traffic light reports) and ensure that the cause and effect between goals and metrics are communicated in an understandable manner.	Imprivata FairWarning can be used to produce reports that track and summarize compliance activities for access rights management and audit controls.	Partial	X	X		X	
	Monitor, Evaluate and Assess the System of Internal Control	MEA02.01	Monitor internal controls	Identify the boundaries of the IT internal control system (e.g., consider how organizational IT internal controls take into account outsourced and/or offshore development or production activities).	Imprivata FairWarning's dynamic identity intelligence (DII) assists customers in identifying all users accessing monitored information. These users may represent outsourced and/or offshored accounts.	Partial	X	X		X	X

COBIT Domain	COBIT Process	COBIT Practice ID	COBIT Practice	Activity	Imprivata FairWarning Capability	Imprivata FairWarning Capability Level	Control Environment	Risk Assessment	Control Actions	Information and Communication	Monitoring Activities
Monitor, Evaluate and Assess	Monitor, Evaluate and Assess the System of Internal Control	MEA02.01	Monitor internal controls	Assess the status of external service providers' internal controls and confirm that service providers comply with legal and regulatory requirements and contractual obligations.	Imprivata FairWarning's dynamic identity intelligence (DII) assists customers in identifying all users accessing monitored information. These users may represent outsourced and/or offshored accounts.	Partial	X	X		X	X
	Monitor, Evaluate and Assess	MEA03.04	Obtain assurance of external compliance	Monitor and report on noncompliance issues and, where necessary, investigate the root cause.	Imprivata FairWarning will assist in monitoring user access that is non compliant with customer standards (built within the application).	Partial	X	X		X	X