S4 SOX Compliance

Without security, there can be no compliance. Security provides the necessary checks and balances to effectively implement compliance programs such as SOX.

Background

The Sarbanes-Oxley 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”.

S4, SOX, and the COBIT Framework

The two most important sections for information security and compliance in SOX are sections **302** and **404**. 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 S4’s applicability and support towards SOX compliance, we focus on the practices and activities pertinent to that.

COBIT ACTIVITY	S4 CAPABILITY
Conduct periodic reviews to ensure that contractors’ roles and access rights are appropriate and in line with agreements. (APO07.06)	✓ S4 identifies authorization bypass vulnerabilities which is an effective way to audit access rights.
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. (APO10.02)	✓ S4 identifies third-party integrations to Salesforce thus providing an effective way to audit data access and the associated security controls.
Capture information on IT risk events that have materialized, for inclusion in the IT risk profile of the enterprise. (APO12.03)	✓ S4 identifies risk associated with custom development and the output from S4 can be captured in a risk register.
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. (APO13.03)	✓ S4 is a full-spectrum application security platform which should be used on a regular basis to review the effectiveness of ISMS.

COBIT ACTIVITY	S4 CAPABILITY
Conduct internal ISMS audits at planned intervals. (APO13.03)	✓ S4 goes beyond regular intervals and is able to identify vulnerabilities on an on-going basis.
Maintain user access rights in accordance with business function and process requirements. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles. (DSS05.04)	✓ S4 identifies ineffective access control management settings that can lead to data breaches.
Administer all changes to access rights (creation, modifications and deletions) to take effect at the appropriate time based only on approved and documented transactions authorized by designated management individuals. (DSS05.04)	✓ S4 enables continuous review of every change related to configurations or code associated with a Salesforce environment.
Identify and implement processes, tools and techniques to reasonably verify compliance. (DSS06.06)	✓ S4 identifies security vulnerabilities that directly impact SOX compliance.
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). (MEA02.01)	✓ S4 identifies security vulnerabilities introduced by third-party outsourced development. This includes risk associated with third-party components installed or downloaded from AppExchange.
Monitor and report on non-compliance issues and, where necessary, investigate the root cause. (MEA03.04)	✓ S4 is a full-spectrum application security platform which should be used on a regular basis to review the non-compliance issues and help investigate root causes for vulnerabilities.