



ArcSight Compliance Insight Package

Software Version: 1.0.0.1

Solutions Guide for ArcSight Compliance Insight Package

Document Release Date: October 2023

Software Release Date: February 2022

About this Compliance Pack

The **ArcSight Compliance Insight Package for SOX** is a package of reports and dashboards that assist you in complying with Section 404 (Management Assessment of Internal Controls) of the Sarbanes-Oxley Act (SOX). This compliance package leverages the litigation-quality, long-term repository of log and event data to facilitate better compliance audits, security forensics, and system maintenance using the reporting capability.

Section 404 of SOX states that a corporation must assess the effectiveness of its internal controls and report this assessment annually to the Securities and Exchange Commission. An outside auditing firm must also review and judge the assessment. The SOX Auditing Standard No. 2, published by the Public Company Accounting Oversight Board (PCAOB), further mandates that organizations and the parties who audit them assess “control risk” in order to determine the effectiveness of internal controls.

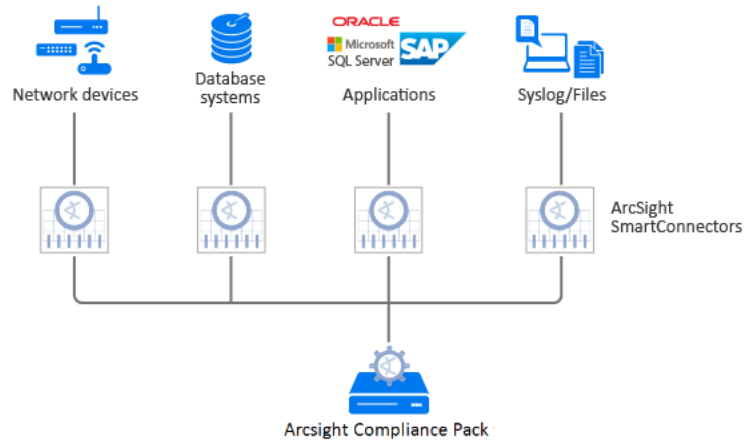
These regulations do not describe exactly how to demonstrate the effectiveness of internal controls. The ArcSight Compliance Insight Package for SOX is based on ISO27002:2013, which is the clearly-defined industry standard and accepted globally.

- ["How Events Flow to this Compliance Pack" below](#)
- ["Supported Devices" on the next page](#)

How Events Flow to this Compliance Pack

The dashboards and reports available with this ArcSight Compliance Pack operate on events in Common Event Format (CEF), which is an industry standard for the interoperability of event or log-generating devices. CEF events can come from a device that is already configured to post events in CEF. For devices in your network that are not already CEF-ready, the events must run through an ArcSight SmartConnector.

For more information about CEF events and how they are used, see the [Administrator's Guide for ArcSight Platform](#).



Supported Devices

This compliance pack can incorporate events generated by the following devices:

- Anti-virus solutions and EDR products
- Databases
- Content Security and Web Filtering systems
- Operating systems
- Physical security systems
- Host and network-based IDS
- Firewalls
- Wireless systems
- Vulnerability and assessment tools

Adding and Removing the Compliance Pack

This section describes how to download, add, and remove this compliance pack.


- ["Downloading this Pack" below](#)
- ["Installing this Pack" below](#)
- ["Uninstalling this Pack" below](#)

Downloading this Pack

To purchase this pack, please contact your account or sales representative.

After you purchase this pack, you can download the package from the [Software Licenses and Downloads \(SLD\) portal](#). Log in to the portal using your active service contract ID.

Installing this Pack

1. Select Reports > Content.
2. Click the Import Asset  icon.
3. Select the zip file for the compliance pack from the stored location.
4. Click Next.
5. Follow the prompt to import and continue with the installation.
6. To verify the installation is complete, locate the compliance pack folder under the Data Compliance Content folder.

Uninstalling this Pack


To uninstall this compliance pack, you must remove both the content (reports and dashboards) from the Reports repository and the worksheets that support the content.

- ["Removing Reports Content" on the next page](#)
- ["Removing Worksheets Content" on the next page](#)

Removing Reports Content



1. Select Reports > Portal.
2. Select Repository > Data Compliance Content.
3. Right-click the folder that you want to remove, then select Delete.
4. Click OK.

Removing Worksheets Content

1. Select Reports > Portal.
2. Click the Create  icon.
3. Click Data Worksheet.
4. In the *New Data Worksheet*, click Cancel.
5. In the navigation pane, select Data Worksheet > Data Compliance Content.
6. Right-click on the content, then select Remove.
7. Click OK.

Specifying Your SOX Assets

This section describes how to define assets using variables and case conditions.

1. Select Reports > Portal.
2. Click the Data  icon.
3. In the navigation pane, expand Data Source > Database > Events > Sarbanes Oxley.
4. In the **Logical Model** pane, expand Events.
5. Select the field that you want to define.
The  symbol indicates the fields that you can modify.
6. To add the case condition, modify the formula for the field.



By default, if the field values in the following table are equal to **No**, the reports and dashboards will be empty. If you want reports and dashboards to work against specific resource types, modify the values.

Examples

- Specific Resource Types

By default, the field values below are equal to **Yes**, which means reports and dashboards work against all environments. If you want reports and dashboards to work against specific resource types, modify the values from **Yes** to **No** for each specific resource type. Also, be sure the specific resource type expressions return **Yes** for your asset list.

Defines MAC Addresses	isSourceMacSOX
	isDestinationMacSOX
Defines IP Addresses	IsSourceAddressSOX
	IsDestinationAddressSOX
Defines SOX Host Names	isSourceHostNameSOX
	isDestinationHostNameSOX
Defines SOX Zones	IsSourceZoneSOX
	IsDestinationZoneSOX

For Example:

IP Address: 89.2.1.4,79.2.1.3,91.12.12.15,91.12.12.14,91.12.12.13

To define assets, modify these values:

Field	Old Value	New Value
isSourceMacSOX	Yes	No
IsSourceAddressSOX	Yes	CASE WHEN v6_ntoa(field['default_secops_adm.events.sourceAddressBin']) IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
IsSourceZoneSOX	Yes	No
isSourceHostNameSOX	Yes	No
isDestinationMacSOX	Yes	No
IsDestinationAddressSOX	Yes	CASE WHEN v6_ntoa(field['default_secops_adm.events.destinationAddressBin']) IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
IsDestinationZoneSOX	Yes	No
isDestinationHostNameSOX	Yes	No

For Example:

IP Address: 89.2.1.4,79.2.1.3,91.12.12.15,91.12.12.14,91.12.12.13

Zone: /All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)

To define assets, modify these values:

Field	Old Value	New Value
isSourceMacSOX	Yes	No
IsSourceAddressSOX	Yes	CASE WHEN v6_ntoa(field['default_secops_adm.events.sourceAddressBin']) IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
IsSourceZoneSOX	Yes	CASE WHEN default_secops_adm.events.sourceZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes' Else 'No' END
isSourceHostNameSOX	Yes	No
isDestinationMacSOX	Yes	No
IsDestinationAddressSOX	Yes	CASE WHEN v6_ntoa(field['default_secops_adm.events.destinationAddressBin']) IN ('89.2.1.4','79.2.1.3','91.12.12.15','91.12.12.14','91.12.12.13') THEN 'Yes' Else 'No' END
IsDestinationZoneSOX	Yes	CASE WHEN default_secops_adm.events.destinationZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes' Else 'No' END
isDestinationHostNameSOX	Yes	No

- Agent Zone Resource Type

By default, the field values below are equal to **No**. If you want to bring additional data from additional connectors, modify the values.

Defines Agent Zones	isAgentZoneSOX
	isAgentAddressSOX

For Example:

Zone: /All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)

To define assets, modify these values:

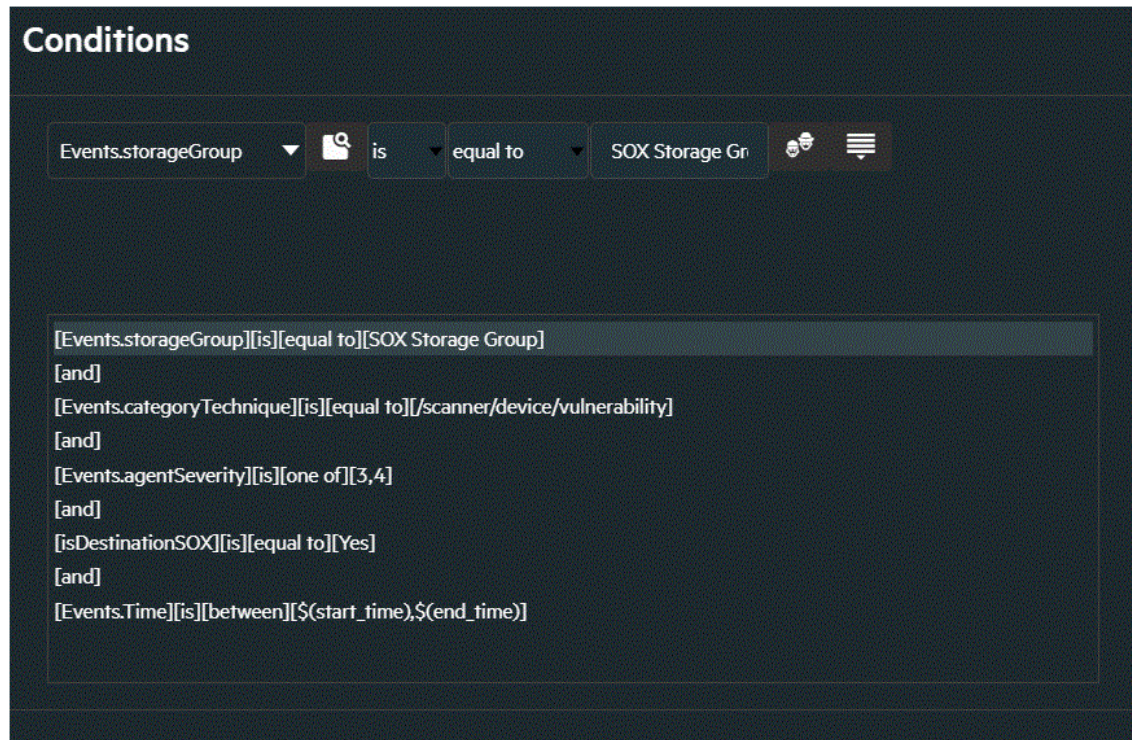
Field	Old Value	New Value
isAgentAddressSOX	No	No
isAgentZoneSOX	No	CASE WHEN default_secops_adm.events.agentZoneURI IN ('/All Zones/ArcSight System/Public Address Space Zones/ARIN/142.0.0.0-144.255.255.255 (ARIN)') THEN 'Yes 'Else 'No' END

- Adding Specific Storage Groups to Worksheets

If you want your reports and dashboards to work against a specific storage group, you can add it to the relevant worksheet.

For Example:

The image below displays a SOX worksheet working against a storage group named SOX Storage Group.



7. Click OK.
8. Save your changes.

Viewing Report and Dashboard Details

This compliance package provides a library of reports and dashboards to help you to address the following objectives.

Compliance Reporting	Supports the presentation of requirements to internal and external audit teams, as well as upper management.
Security Best Practices	Helps implement, monitor, and manage a best practices approach to information security management, as well as ensure that SOX security controls are in place and enforced.
Harmful User and Machine Monitoring	Tracks potentially harmful users and machines.
Visualizing Security Events	Displays security events graphically, which allows analysts to quickly analyze situations.
Vulnerabilities and Configuration Changes Monitoring	Tracks vulnerabilities and configuration changes on SOX systems.

For more information on the available dashboards and reports in this compliance pack, see the *Help* in ArcSight Recon or the [User's Guide for Recon in the ArcSight Platform](#).

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide for ArcSight Compliance Insight Package (Compliance Insight Package 1.0.0.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!

Additional Documentation

The ArcSight Platform documentation library includes the following resources.

- [Administrator's Guide for ArcSight Platform](#), which contains installation, user, and deployment guidance for the ArcSight software products and components that you deploy in the containerized platform.
- [User's Guide for Fusion 1.3 in the ArcSight Platform](#), which is embedded in the product to provide both context-sensitive Help and conceptual information.
- [Product Support Lifecycle Policy](#), which provides information on product support policies.

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2001 - 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.