TIBCO LogLogic® Compliance Suite - Sarbanes-Oxley Edition Guide

Software Release 3.9.0
November 2017
Document Updated: April 2018

Two-Second Advantage®

Important Information

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This document contains excerpted portions of the Sarbanes-Oxley Act ("SOX") regulations (collectively, the "Regulatory Language"). The Regulatory Language is provided by TIBCO solely for your convenience and to provide context for certain functionality of the TIBCO LogLogic® products. The inclusion or omission by TIBCO of any Regulatory Language is in no way intended as legal advice regarding the SOX regulations and does not constitute any representation or warranty that any TIBCO products comply with the terms contained in such Regulatory Language. If you have additional questions about the SOX regulations, you should consult with an attorney for further legal guidance.

Contents

Figures

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO LogLogic® Compliance Suite - Sarbanes Oxley Edition Guide*
- *TIBCO LogLogic® Compliance Suite - Sarbanes Oxley Edition Readme*
- *TIBCO LogLogic® Compliance Suite - Sarbanes Oxley Edition Release Notes*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

Establishment IT Controls for Sarbanes-Oxley Compliance

Enacted in 2002 to restore investor confidence in the public markets and enhance corporate governance, the Sarbanes-Oxley (SOX) Act stipulates that companies establish and maintain internal control over financial reporting and assess the effectiveness of those controls annually. To carry out the mandates specified by SOX, Control Objectives for Information and Related Technology (COBIT) was established as a blueprint for IT risk management activities. COBIT maps IT processes to the components set forth by the Committee of the Sponsoring Organizations (COSO), the general framework recommended by the Public Company Accounting Oversight Board (PCAOB) to companies striving to achieve SOX compliance.

Basic best practices for implementing the COBIT framework include:

- Automating the Log Management and Intelligence (LMI) process
- Deploying LMI in a distributed environment
- Ensuring data integrity
- Establishing regular compliance reporting capabilities
- Performing ongoing user monitoring

It is the fiduciary responsibility of management to protect corporate assets against misuse, theft and downtime. Critical infrastructure data in the form of log files from corporate firewalls, VPN concentrators, web proxies, IDS systems, email servers, operating systems, enterprise applications and backup systems provide critical insight into the use of corporate assets, risks and IT performance. However, these logs are often not readily available or accessible when corporations need them most – during compliance audits or when responding to Legal, Human Resources and other business requests. Achieving compliance requires you to be able, in real-time, to access, search through and organize such data quickly and cost-effectively.

Today, tens of thousands of log data messages are produced by enterprise systems, applications and network devices every second. In most Fortune 1000 enterprises, these log messages add up to terabytes of data per month. At these rates, it is not humanly possible to extract from logs the necessary information using homegrown scripts. For example, to satisfy SOX auditors, you must not only ensure that appropriate IT controls are in place, you must also provide evidence of functioning controls and the documented results of testing procedures. This could take days using scripts – a luxury and expense that you can't afford.

The LogLogic® Compliance Suite - Sarbanes-Oxley Edition Overview

The LogLogic® Compliance Suite - Sarbanes-Oxley Edition delivers automated process validation, reporting and alerts based on infrastructure data to evidence and enforce business and IT policies related to compliance. By automating compliance reporting and alerting based on critical infrastructure data collected and stored by TIBCO LogLogic's appliances, the TIBCO LogLogic Compliance Suite reduces the complexity and resource requirements for implementing control frameworks like COBIT to successfully meet SOX and other regulations.

TIBCO LogLogic's Compliance Suite:

- Automates compliance activities and dramatically improves audit accuracy.
- Reduces the time to mitigate the risk factor.
- Allows organizations to use infrastructure data to provide evidence of and enforce IT controls.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting on COBIT for SOX compliance.
- Delivers approximately 520 out-of-the-box Compliance Reports and 170 out-of-the-box Alerts with executive-level views.

- Enables customization of any Compliance Report to map reports against your company's policies.
- Focuses on compliance with Section 404 of the SOX Act, which establishes the need for internal controls based on a recognized control framework.

To create the Compliance Suite, TIBCO identified a number of COBIT control objectives and mapped the general control principles with the functionality provided by TIBCO LogLogic reports and alerts. As a result, the Compliance Suite provides reports and alerts that are directly aligned with specific COBIT objectives.

> The SOX act of 2002 sets a standard for corporate accountability, requiring the definition and enforcement of internal IT controls and processes. It applies to all public companies. The Sarbanes-Oxley Act recommends companies regularly audit log files and keep a record of audit logs for up to seven years. SOX specifically requires companies to "audit unauthorized access, misuse and fraud, to ensure the accuracy of corporate financial and business information," and to "maintain financial records for seven years."

Sarbanes-Oxley Act Overview

The Sarbanes-Oxley Act is arguably the most well known of all recent regulatory changes impacting enterprises of all kinds. It was passed in July 2002 to restore investor confidence in the US public market after it was damaged by business scandals and lapses in corporate governance. As a result of SOX mandates, companies are taking measures to strengthen internal checks and balances and, ultimately, corporate accountability.

Several of the act's sections can be supported by IT controls and the TIBCO LogLogic Compliance Suite:

- Section 302 requires CFOs and CEOs to personally certify and attest to the accuracy of their companies' financial results.
- Section 404 establishes the need for internal controls based on a recognized control framework.
- Section 802 sets criminal penalties for destroying records connected with control audits.
- Section 409 defines requirements for real-time reporting of material events that could affect a company's financial performance.

Determining which and how many controls constitute an effective internal control environment is made and evaluated by management within a company, but must be agreed to by an external auditor.

Sarbanes-Oxley Section 404 Specifications

Section 404 requires senior management and business process owners to establish and maintain an adequate internal control structure. In addition, the specification requires senior management to assess the internal control's effectiveness on an annual basis. The following provides some specifics of Section 404:

- Management of public companies must assess the effectiveness of the organization's internal control over financial reporting.
- An annual review and assessment of the effectiveness of the internal controls must be completed.
- A company's independent auditor must attest to management's assessment of its internal control over financial reporting.
- A company must demonstrate the following internal controls:
  - Records are logged in reasonable details, accurate and reflect the transactions.
  - Transactions are being recorded.
  - Prevention or timely detection of unauthorized acquisition, use of disposition of the assets that could have a material effect on the financial statements.

  - The IT control environment must include the IT governance process, monitoring and reporting.
  - The IT governance process must include the information systems strategic plan, the IT risk management process, compliance and regulatory management, IT policies, procedures and standards.
  - Monitoring and reporting exists to ensure IT is aligned with business requirements.

An ineffective control environment can be a significant deficiency and a strong indicator that a material weakness in internal control over financial reporting exists.

Benefits of Building a Strong Internal Control Program within IT:

- Enhances overall IT governance.
- Enhances the understanding of IT among executives.
- Enables better business decisions with higher-quality and timely information.
- Aligns project initiatives with business requirements.
- Prevents loss of intellectual assets and the possibility of a system breach.
- Contributes to the compliance of other regulatory requirements, such as privacy.
- Provides a competitive advantage through more efficient and effective operations.
- Optimizes operations with an integrated approach to security, availability, and processing integrity.
- Enhances risk management competencies and prioritization of initiatives.

PCAOB Auditing Standard No. 5 Overview

The Public Company Accounting Oversight Board (PCAOB) was formed to protect the interests of investors and further the public interest in the preparation of informative, fair and independent audit reports. PCAOB was created under SOX as a private sector, non-profit corporation to oversee the auditors of public companies. It establishes auditing standards and provides direction to auditors.

The PCAOB adopted Auditing Standard No. 5, entitled “An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements” in May 2007. This standard supersedes the previous standard, Auditing Standard No. 2, and is effective for all audits of internal controls for fiscal years ending on or after November 15, 2007.

The four main goals of Auditing Standard No. 5 are to:

- Focus internal control audit on the most critical areas and areas of greatest risk. This includes focusing audit scope, improved audit planning, and providing guidance on alternatives for addressing lower risk areas.
- Eliminate unnecessary procedures. The PCAOB has removed the previous standard’s detailed requirements to evaluate management’s own evaluation process and removing the requirement to render an opinion on the adequacy of management’s process.
- Make the audit scalable. The updated standard provides details on how to scale the audit based on the organization’s size and complexity, allowing for an approach that is better tailored for smaller and less complex organizations.
- Simplify the standard. The new standard is shorter and more readable. This includes text reordering and reduction of duplication.

IT Controls to Consider

The following IT controls should be considered for compliance with PCAOB Auditing Standard No. 5:

- Access to Programs and Data

Controls provide reasonable assurance that all financially significant systems (that is networks, applications, and databases) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.

Risks of Non-compliance – Informal security administration and monitoring activities might result in unauthorized and/or inappropriate access to key financial systems, which might negatively impact the existence, accuracy and completeness of financial statements.

- Application Software Changes

  Controls provide reasonable assurance that all systems and system changes are appropriately requested, approved, tested, and validated by authorized personnel before the implementation to the production environment.

  Risks of Non-compliance – Informal change management activities might result in unauthorized changes and/or improper roll-out of new source code to key financial systems. This can negatively impact the existence, accuracy and completeness of financial statements.

- Computer Operations

  Controls provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated.

  Controls provide reasonable assurance that data recorded, processed, and reported remain complete, accurate and valid throughout the storage process.

  Controls provide reasonable assurance that problems and issues over the processing of business/IT transactions are addressed in a timely manner.

  Controls provide reasonable assurance that third party services are appropriately retained and monitored to ensure that activities are executed in accordance with Company standards.

- Risks of Non-Compliance

  Unauthorized program execution might result in inaccurate or untimely processing of key financial data.

  Informal and/or ineffective data management activities might result in loss of key financial data that can negatively impact the existence, accuracy and completeness of financial statements.

  Informal and/or ineffective problem management activities might result in unresolved system issues that might negatively impact the existence, accuracy and completeness of financial data.

  Informal third party services management might result in vendor activities that are inconsistent with company standards. This might lead to a negative impact on the accuracy and completeness of financial statements.

- Program Development

  Controls provide reasonable assurance that systems are developed and/or purchased in a manner that supports the accuracy and completeness of financial statements.

  Risks of Non-compliance – Informal system development activities might result in improper rollout of key financial systems.

Process Elements

The PCAOB standard requires auditors to evaluate all process elements that might be involved in period-end financial reporting: IT services, executive management and business processes. The following table identifies these process elements.

IT SERVICES	EXECUTIVE MANAGEMENT	BUSINESS PROCESSES
Shared services are those that are required by more than one department or process and are often delivered as a common service. From an IT perspective, services such as security, telecommunications and storage are necessary for any department or business unit and are often managed by a central IT function.	Executive management establishes and incorporates strategy into business activities. At the enterprise or entity level, business objectives are set, policies are established, and decisions are made on how to deploy and manage the resources of the organization. From an IT perspective, policies and other enterprise-wide guidelines are set and communicated throughout the organization.	Business processes are the organization's mechanism of creating and delivering value to its stakeholders. Inputs, processing and outputs are functions of business processes. Increasingly, business processes are being automated and integrated with complex and highly efficient IT systems.
General Controls Controls embedded in IT services form general controls, such as: Program development Program changes Computer operations Access to programs and data	Company-level Controls Company-level controls over the IT control environment set the tone for the organization. Examples include: Operating style Enterprise policies Governance Collaboration Information sharing	Application Controls Controls embedded in business process applications, such as large ERP systems and smaller best-of-breed systems, are commonly referred to as application controls. Examples include: Completeness Accuracy Validity Authorization Segregation of duties

COSO Overview

To fulfill the PCAOB auditing standard, SOX requires that organizations to select and implement a suitable internal control framework. The COSO framework (Internal Control—Integrated Framework) has become the most commonly adopted framework. Although other suitable frameworks have been published in other countries and can contain the same elements, PCAOB recommends that they carry all of COSO's general themes. Companies must be able to demonstrate how their IT controls support the COSO framework.

Based on the COSO framework, there are five essential components for effective internal control:

- Control environment: Control environment establishes the basis for effective internal control and creates the 'tone at the top' required for successful corporate governance.
- Risk assessment: Risk assessment includes the identification, analysis, and evaluation of risks that can impact the achievement of corporate objectives. The risk assessment component helps provide the basis for control design and related activities.
- Control activities: The policies and procedures that are implemented for the achievement of business objectives comprise the organization's control activities. These activities also include the various risk mitigation strategies that are put in to place based on the results of risk assessment.
- Information and communication: Information relevant to the business must be identified appropriately, and an organization's information systems must process and report on the data

effectively to support normal operations and control of the business. In addition, the organization must be appropriately structured to facilitate both internal and external communications.

- Monitoring: Monitoring must be in place to allow the organization to detect, measure, and assess the quality and performance of internal controls over time.

Primary Objectives

The COSO framework identifies three primary objectives of internal control:

- Efficiency and effectiveness of operations
- Financial reporting
- Compliance with laws and regulations

COBIT Version 4.1 Overview

The Committee of the Sponsoring Organizations (COSO) provides a high-level view of the components of an IT control framework necessary for meeting SOX compliance; however, it does not provide details on how to execute the framework. Additional details regarding IT control considerations can be found in COBIT, a control framework published by the IT Governance Institute. COBIT provides controls that address operational and compliance objectives related directly to financial reporting.

In addition to supporting the COSO framework, and hence Sarbanes-Oxley requirements, the COBIT framework addresses IT governance more broadly. IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extend the organization’s strategies and objectives. Furthermore, IT governance integrates and institutionalizes good practices to ensure that an enterprise’s IT organization supports business objectives. IT governance therefore enables an enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities, and gaining a competitive advantage.

COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

COBIT Version 4.1

COBIT released the fourth version of its control framework in December 2005. Version 4.1 of COBIT was released as an update in 2007. The framework approaches IT controls by looking at all of the information needed to support business requirements and the associated IT resources and processes. COBIT is intended for management, users, and auditors (mostly IT auditors).

Sarbanes-Oxley Section 404 is strictly focused on internal controls over financial reporting. All users of COBIT must first determine the relevance of a significant IT process or IT-dependent process by assessing its primary contributions to internal controls over financial reporting, rather than to the broad spectrum of IT control processes encompassed by COBIT. One way to ensure that IT is properly anchored to a significant account, business process, or major class of transaction is to critically question the role of IT in risk mitigation and in enhancing the integrity of financial reporting and financial-statement assertions. IT auditors have a new opportunity to add value by evaluating the design and operating effectiveness of automated application controls end-to-end in addressing fraud, yet this scope is not explicit in COBIT.

It is important that auditors select relevant IT Control Objectives from COBIT when defining their Sarbanes-Oxley scope. IT’s unique contribution centers around its ability to enhance the integrity, security, and availability of financial information within those identified business processes, as well as safeguarding assets – most notably information assets.

TIBCO LogLogic Compliance Suite Setup

Setting up the LogLogic® Compliance Suite - Sarbanes-Oxley Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

See Installing the Compliance Suite and Enabling Compliance Suite Alerts for more details.

Installing the Compliance Suite

Prerequisites

Before installing the LogLogic® Compliance Suite - Sarbanes-Oxley Edition, ensure that you have:

- LogLogic LX or MX or ST Appliance running LogLogic LMI Release 5.7.x or higher
- TIBCO LogLogic® Log Source Packages (LSP) 32.1 or 33 installed

The Compliance Suite includes one XML file containing SOX or COBIT search filters, custom reports, and alerts:

- `sox.xml` or `cobit.xml` – SOX and COBIT Reports, Search Filters, and Alerts

> ⚠ If you have previously imported any earlier versions of the Compliance Suite files, importing this version of the Compliance Suite will not overwrite the original files or any changes that have been made, unless you have saved the changes to the object using the default name.
>
> If you have made any changes to base Compliance Suite alerts, search filters, or custom reports, TIBCO recommends saving these items with non-default names. This will help ensure that the latest Compliance Suite updates can be installed without any compatibility issues or naming conflicts.

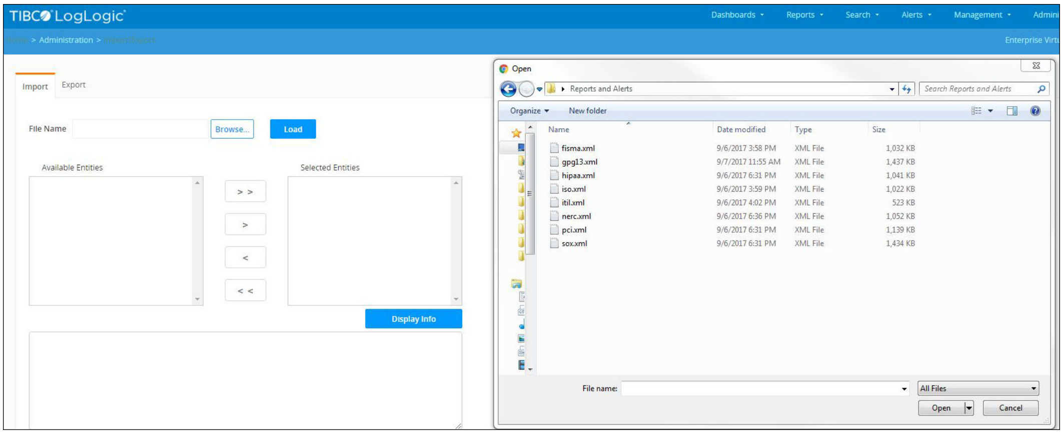
Procedure

1. Log in to your LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Administration** > **Import or Export** .

   The **Import** and **Export** tabs appear.
3. Load the Compliance Suite file by completing the following steps:
   a) In the **Import** tab, click **Browse**.
   b) In the **File Upload** window, select the appropriate XML file and then click **Open**.

   The following figure shows the **File Upload** window that appears after clicking **Browse** on the **Import** tab.

Loading a Compliance Suite File



Name	Date modified	Type	Size
fisma.xml	9/6/2017 3:58 PM	XML File	1,032 KB
gpg13.xml	9/7/2017 11:55 AM	XML File	1,437 KB
hipaa.xml	9/6/2017 6:31 PM	XML File	1,041 KB
iso.xml	9/6/2017 3:59 PM	XML File	1,022 KB
itil.xml	9/6/2017 4:02 PM	XML File	523 KB
nerc.xml	9/6/2017 6:36 PM	XML File	1,052 KB
pci.xml	9/6/2017 6:31 PM	XML File	1,139 KB
sox.xml	9/6/2017 6:31 PM	XML File	1,434 KB

c) Click **Load**.

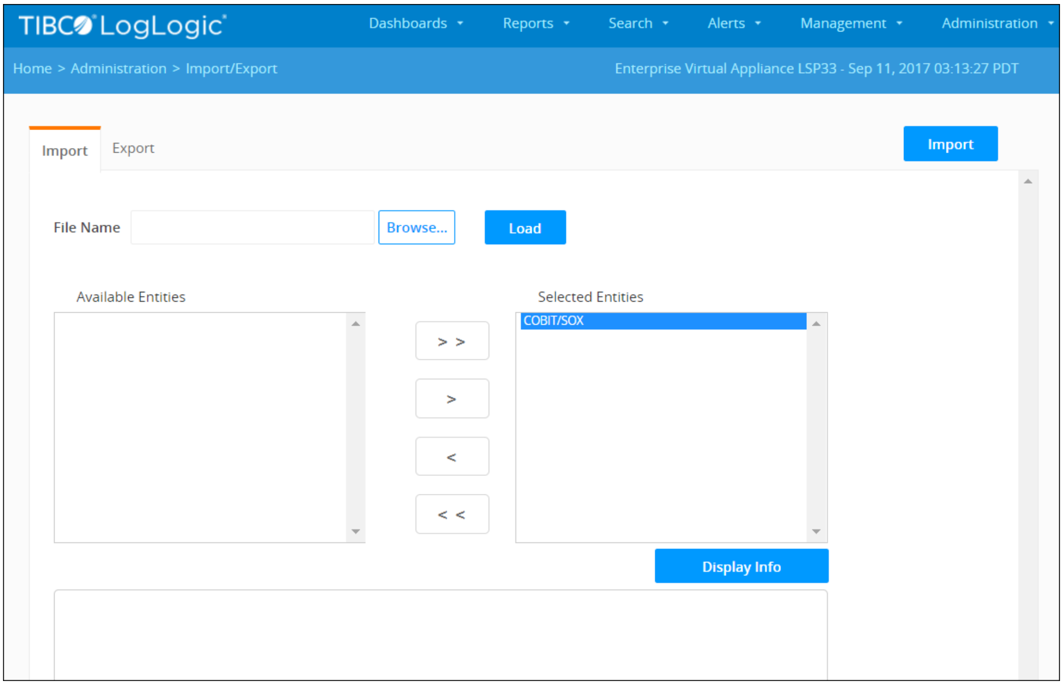
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

You can also select the specific COBIT or SOX entity from the **Available Entities** text block, and click **Add Selected Entities**.

The following figure shows all entities of the COBIT XML file that were selected by clicking **Add All Entities**.

Selected Entities to be Imported



Home > Administration > Import/Export

Enterprise Virtual Appliance LSP33 - Sep 11, 2017 03:13:27 PDT

Selected Entities: COBIT/SOX

4. Click **Import**.

An import successfully completed message appears above the **File Name** text field.

Installation is complete after the XML file is successfully imported.

The Compliance Suite Usage

After you have successfully installed the LogLogic® Compliance Suite - Sarbanes-Oxley Edition, you can begin using the custom reports and alerts.

The following sections help you view, test, and modify, the packaged custom reports and alerts. The custom reports and alerts were designed to run out-of-the box; however, LogLogic LMI enables you to perform further customization if necessary.

Compliance Suite Reports

All LogLogic® Compliance Suite - Sarbanes-Oxley Edition reports are designed to run out-of-the box as well as to be flexible if you must make modifications based on your business needs.

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for COBIT 4.1 and Sarbanes-Oxley.

Viewing Compliance Suite Reports and Output Data

By using TIBCO LogLogic LX or MX or ST Appliance, you can view all the Compliance Suite reports for the device and run them as well as view the output data.

Procedure

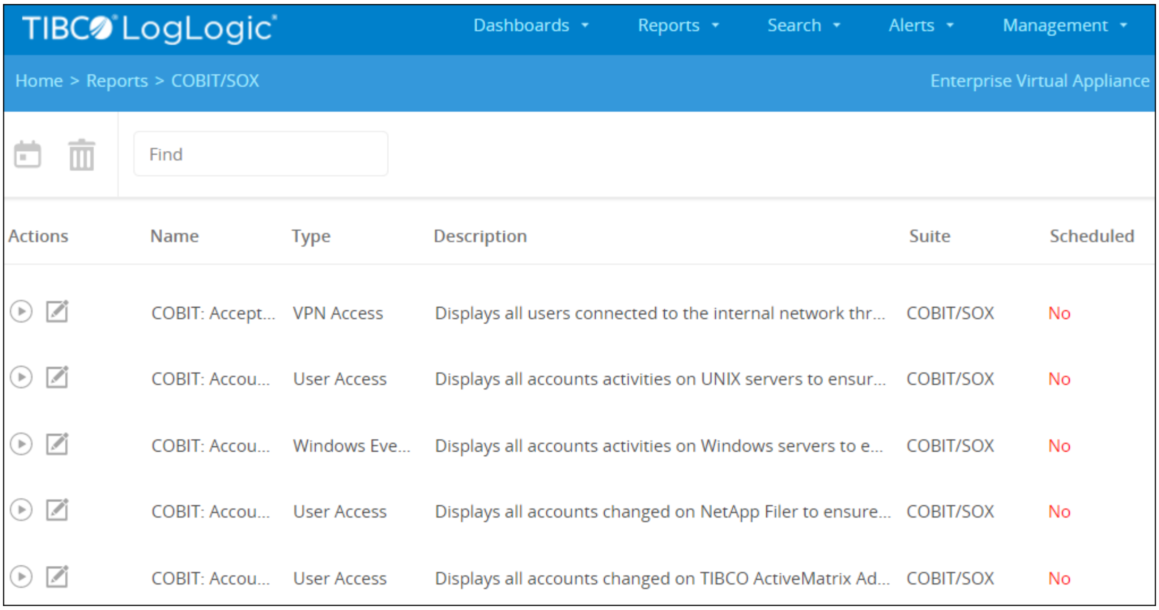
1. Log in to your LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Reports** > **COBIT/SOX** .

   You can also access all of your custom reports on the Appliance including the Compliance Suite reports you installed, by selecting **Reports** > **All Saved Reports** .
3. On the **Reports** page, you can see all of the custom reports you loaded during the installation process.

   You can navigate through all of the custom reports using the page navigation buttons at the top and bottom of the **Reports** page.

   The following figure shows a cropped list of the Compliance Suite reports loaded from the COBIT XML file.

   Compliance Suite Reports



Actions	Name	Type	Description	Suite	Scheduled
▷ ✎	COBIT: Accept...	VPN Access	Displays all users connected to the internal network thr...	COBIT/SOX	No
▷ ✎	COBIT: Accou...	User Access	Displays all accounts activities on UNIX servers to ensur...	COBIT/SOX	No
▷ ✎	COBIT: Accou...	Windows Eve...	Displays all accounts activities on Windows servers to e...	COBIT/SOX	No
▷ ✎	COBIT: Accou...	User Access	Displays all accounts changed on NetApp Filer to ensure...	COBIT/SOX	No
▷ ✎	COBIT: Accou...	User Access	Displays all accounts changed on TIBCO ActiveMatrix Ad...	COBIT/SOX	No

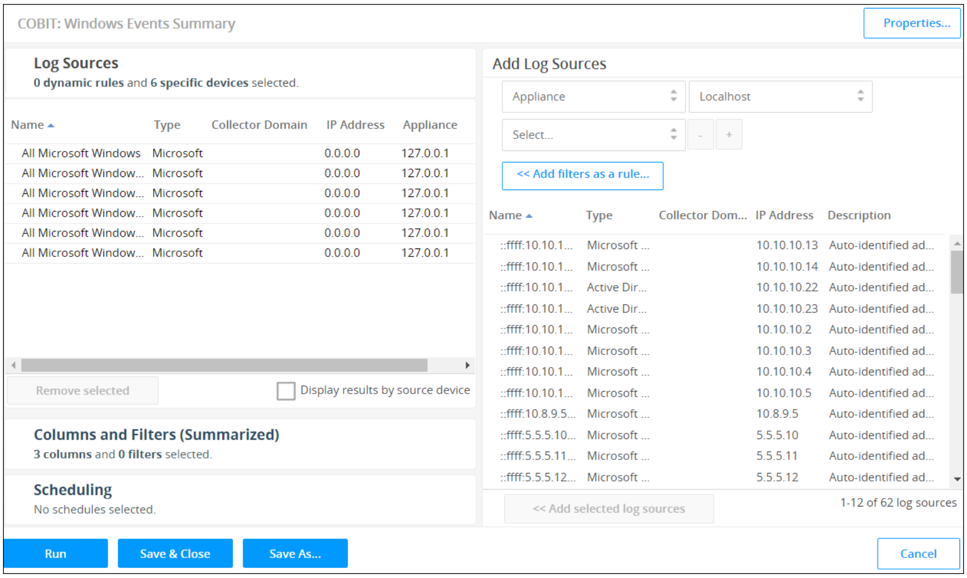
4. Click the **Edit** button of a report to see details such as, the appliance where the report runs, the associated device type, and when the report runs.

   a) To view the filter parameters, click **Columns and Filters**.

   b) To view details about a report such as the report name and description, click **Properties**.

   The following figure shows the details of the **COBIT: Windows Events Summary** report.

   Windows Events Summary Report Details


COBIT: Windows Events Summary
Properties...
Remove selected
<< Add filters as a rule...
<< Add selected log sources
Run
Save & Close
Save As...
Cancel

Log Sources

0 dynamic rules and **6 specific devices** selected.

Name ▲	Type	Collector Domain	IP Address	Appliance
All Microsoft Windows	Microsoft		0.0.0.0	127.0.0.1
All Microsoft Window...	Microsoft		0.0.0.0	127.0.0.1
All Microsoft Window...	Microsoft		0.0.0.0	127.0.0.1
All Microsoft Window...	Microsoft		0.0.0.0	127.0.0.1
All Microsoft Window...	Microsoft		0.0.0.0	127.0.0.1
All Microsoft Window...	Microsoft		0.0.0.0	127.0.0.1

□ Display results by source device

Columns and Filters (Summarized)

3 columns and **0 filters** selected.

Scheduling

No schedules selected.

Add Log Sources

Appliance: Localhost

Select...

Name ▲	Type	Collector Dom...	IP Address	Description
::ffff:10.10.1...	Microsoft ...		10.10.10.13	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.14	Auto-identified ad...
::ffff:10.10.1...	Active Dir...		10.10.10.22	Auto-identified ad...
::ffff:10.10.1...	Active Dir...		10.10.10.23	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.2	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.3	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.4	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.5	Auto-identified ad...
::ffff:10.8.9.5...	Microsoft ...		10.8.9.5	Auto-identified ad...
::ffff:5.5.5.10...	Microsoft ...		5.5.5.10	Auto-identified ad...
::ffff:5.5.5.11...	Microsoft ...		5.5.5.11	Auto-identified ad...
::ffff:5.5.5.12...	Microsoft ...		5.5.5.12	Auto-identified ad...

1-12 of 62 log sources

5. Run the report to view the report output data by completing the following steps:

   a) Click **Run**.

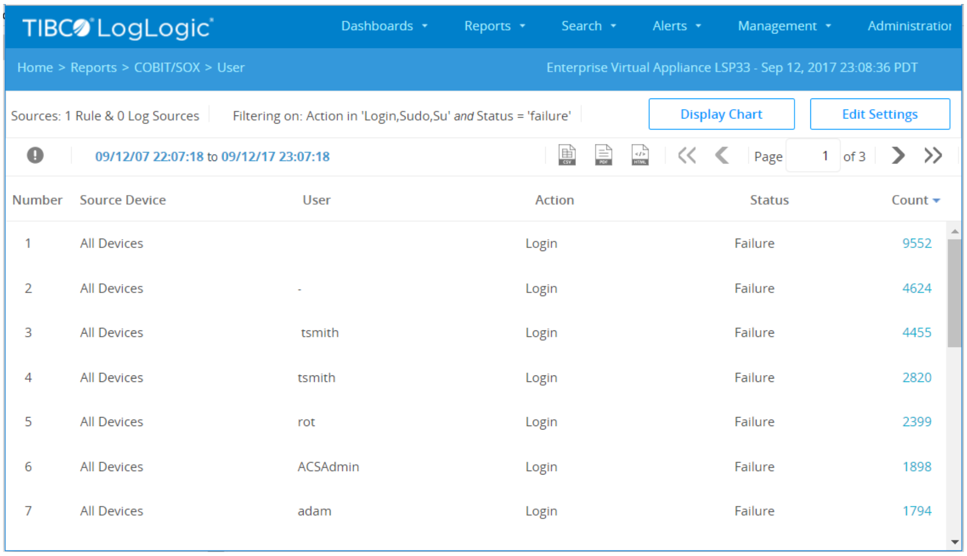
   The report runs and returns data based on the set parameters.

   b) To view detailed drill-down information, click the **Count** column link.

   You can use the **Back to summarized results** button to return to the main data output view.

   The following figure shows sample results from the **COBIT: Windows Events Summary** report.

   Windows Events Summary Results



Home > Reports > COBIT/SOX > User

Enterprise Virtual Appliance LSP33 - Sep 12, 2017 23:08:36 PDT

Sources: 1 Rule & 0 Log Sources

Filtering on: Action in 'Login,Sudo,Su' *and* Status = 'failure'

09/12/07 22:07:18 to 09/12/17 23:07:18

Page 1 of 3

Number	Source Device	User	Action	Status	Count
1	All Devices		Login	Failure	9552
2	All Devices	-	Login	Failure	4624
3	All Devices	tsmith	Login	Failure	4455
4	All Devices	tsmith	Login	Failure	2820
5	All Devices	rot	Login	Failure	2399
6	All Devices	ACSAdmin	Login	Failure	1898
7	All Devices	adam	Login	Failure	1794

If you want to modify the main data output view, you can modify the report parameters and then run the report again.

Customizing Compliance Suite Reports

The LogLogic® Compliance Suite - Sarbanes-Oxley Edition reports are designed to run out-of-the-box to meet specific compliance requirements. However, you might want to modify the reports to include additional information or devices depending on your business needs.

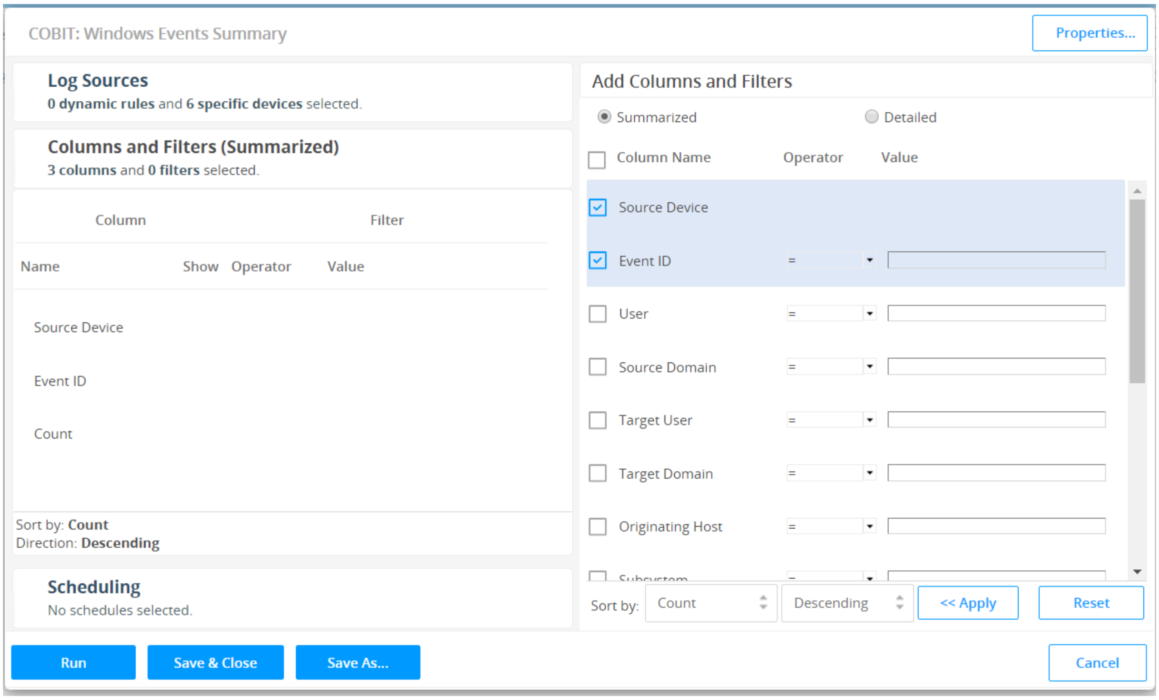
Procedure

1. Make sure that you are on the **Reports** page and click the **Edit** button of a report you want to modify.
2. Modify the report details (that is name, description, and so on.), filters, and parameters.

   LogLogic enables you to customize everything pertaining to the summarization and presentation of the reports. You can modify one of the devices on which the report runs, schedule when the report runs, and set specific report search filters.

   The following figure shows the report filters available under **Columns and Filters**.

   Advanced Options and Update Saved Custom Report Views



COBIT: Windows Events Summary

Log Sources
0 dynamic rules and 6 specific devices selected.

Columns and Filters (Summarized)
3 columns and 0 filters selected.

Column		Filter	
Name	Show	Operator	Value
Source Device			
Event ID			
Count			

Sort by: Count
Direction: Descending

Scheduling
No schedules selected.

Add Columns and Filters

● Summarized ○ Detailed

	Column Name	Operator	Value
☑	Source Device		
☑	Event ID	=	
□	User	=	
□	Source Domain	=	
□	Target User	=	
□	Target Domain	=	
□	Originating Host	=	
□	Subsystem	=	

Sort by: Count, Descending

> It is a good practice to test your modifications to ensure that the report meets your business needs.

3. To test the report, click **Run**.

   The report runs and returns data based on the set parameters. Verify that the returned data is what you want. Continue modifying and testing the report as needed.
4. Save the report by completing the following steps:

   a) Click **Save As**.

   Make any necessary modifications to the report details (that is **Report Name**, **Report Description**, and so on.).

   b) Click **Save & Close**.

   A report saved message appears. Your report is now modified. Consider testing the output of the report again to ensure you are returning all of the data you need from this report.

The Compliance Suite Alerts

The LogLogic® Compliance Suite - Sarbanes-Oxley Edition alerts enable you to manage activities and operations in conjunction with Sarbanes-Oxley compliance and COBIT 4.1 control objectives. Activities can include detecting unusual traffic on your network or detecting appliance system anomalies. By default, the Compliance Suite alerts are disabled so that you can configure your environment with only those alerts that are necessary.

For a description of all alerts in this Compliance Suite, see TIBCO LogLogic Alerts for COBIT 4.1 and Sarbanes-Oxley.

Accessing Available Compliance Suite Alerts

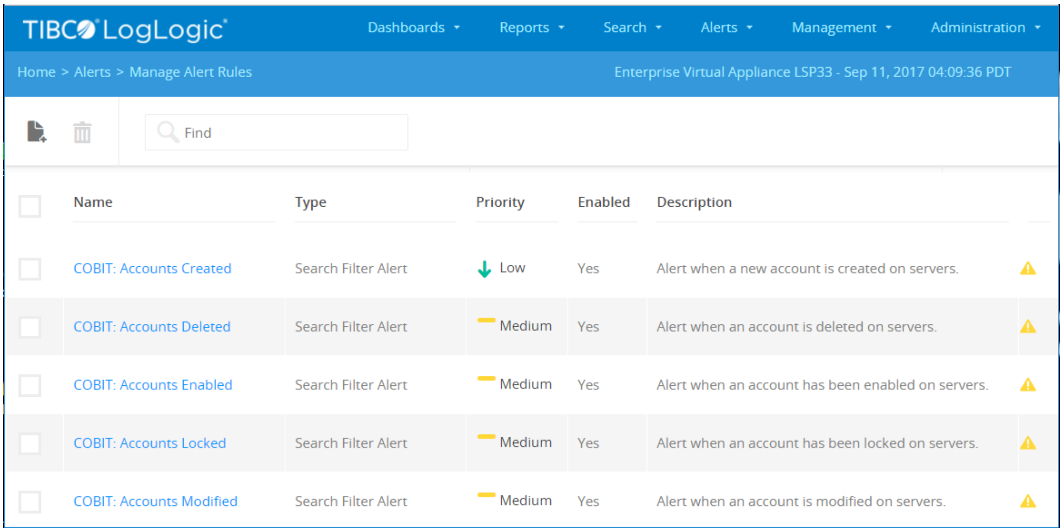
The Compliance Suite package contains a number of alerts that can be easily enabled and modified for your business needs.

Procedure

1. From the navigation menu, click **Alerts** > **Manage Alert Rules** .

   The following figure shows a cropped list of the Compliance Suite alerts loaded from the COBIT XML file.

   Compliance Suite Alerts


TIBCO LogLogic
Dashboards
Reports
Search
Alerts
Management
Administration
Home > Alerts > Manage Alert Rules
Enterprise Virtual Appliance LSP33 - Sep 11, 2017 04:09:36 PDT
Find

□	Name	Type	Priority	Enabled	Description	
□	COBIT: Accounts Created	Search Filter Alert	↓ Low	Yes	Alert when a new account is created on servers.	⚠
□	COBIT: Accounts Deleted	Search Filter Alert	— Medium	Yes	Alert when an account is deleted on servers.	⚠
□	COBIT: Accounts Enabled	Search Filter Alert	— Medium	Yes	Alert when an account has been enabled on servers.	⚠
□	COBIT: Accounts Locked	Search Filter Alert	— Medium	Yes	Alert when an account has been locked on servers.	⚠
□	COBIT: Accounts Modified	Search Filter Alert	— Medium	Yes	Alert when an account is modified on servers.	⚠

2. To view details of a specific alert, click the **Name** of the alert.

   The **General** tab is selected by default, but each tab on the page contains information required to enable an alert.

3. Click on each of the tabs to view the default entries.

Result

Make sure that you identify the default entries and areas that might have to be modified.

Enabling Compliance Suite Alerts

By default, the compliance suite alerts have pre-configured information to help you get started. In some instances, you can simply enable the alert because the default settings are aimed at capturing a broad range of alerts.

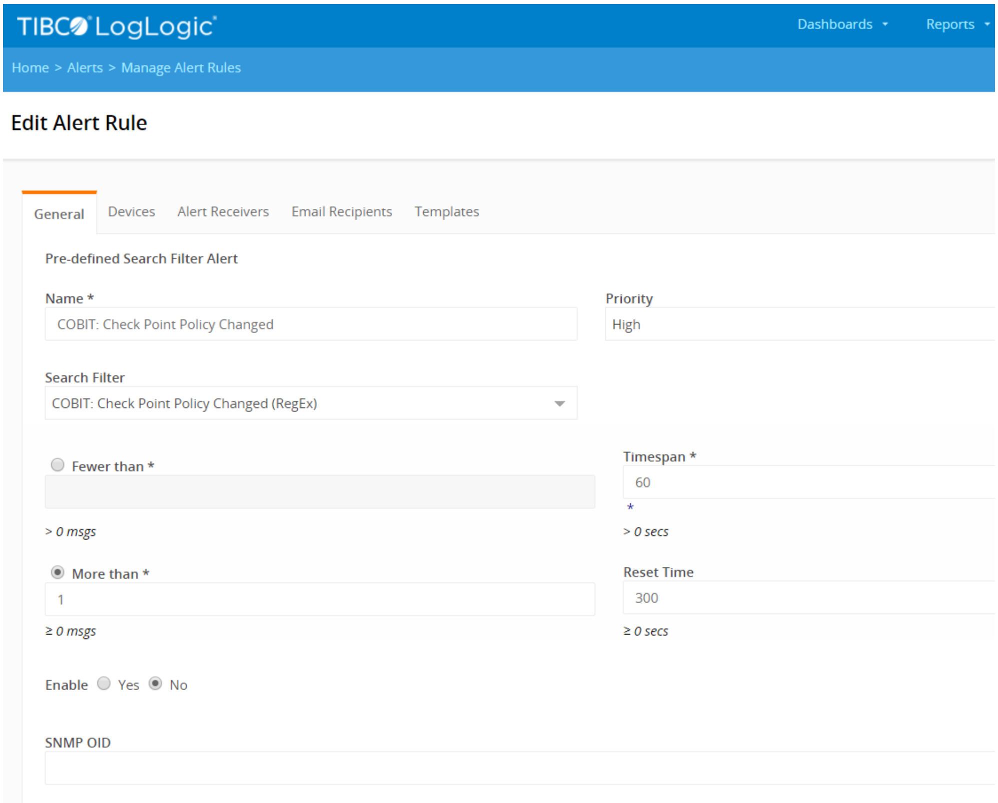
To enable alerts, you must set one of the devices to monitor, the SNMP trap receivers, as well as who receives an alert notification and how they receive it.

Procedure

1. From the navigation menu, select **Alerts** > **Manage Alert Rules** .
2. Click the **Name** of the alert.
3. On the **General** tab, for **Enable** select the **Yes** radio button.

   The following figure shows the **General** tab for the **COBIT: CheckPoint Policy Changed** alert.

   CheckPoint Policy Change Alert



Edit Alert Rule

Pre-defined Search Filter Alert

Name * COBIT: Check Point Policy Changed

Priority High

Search Filter COBIT: Check Point Policy Changed (RegEx)

○ Fewer than *

> 0 msgs

Timespan * 60

*

> 0 secs

● More than * 1

≥ 0 msgs

Reset Time 300

≥ 0 secs

Enable ○ Yes ● No

SNMP OID

4. Select one of the devices to be alerted on by completing the following steps:

   You can define alerts for all devices, a selection of devices, or a single device.

   a) Select the **Devices** tab.

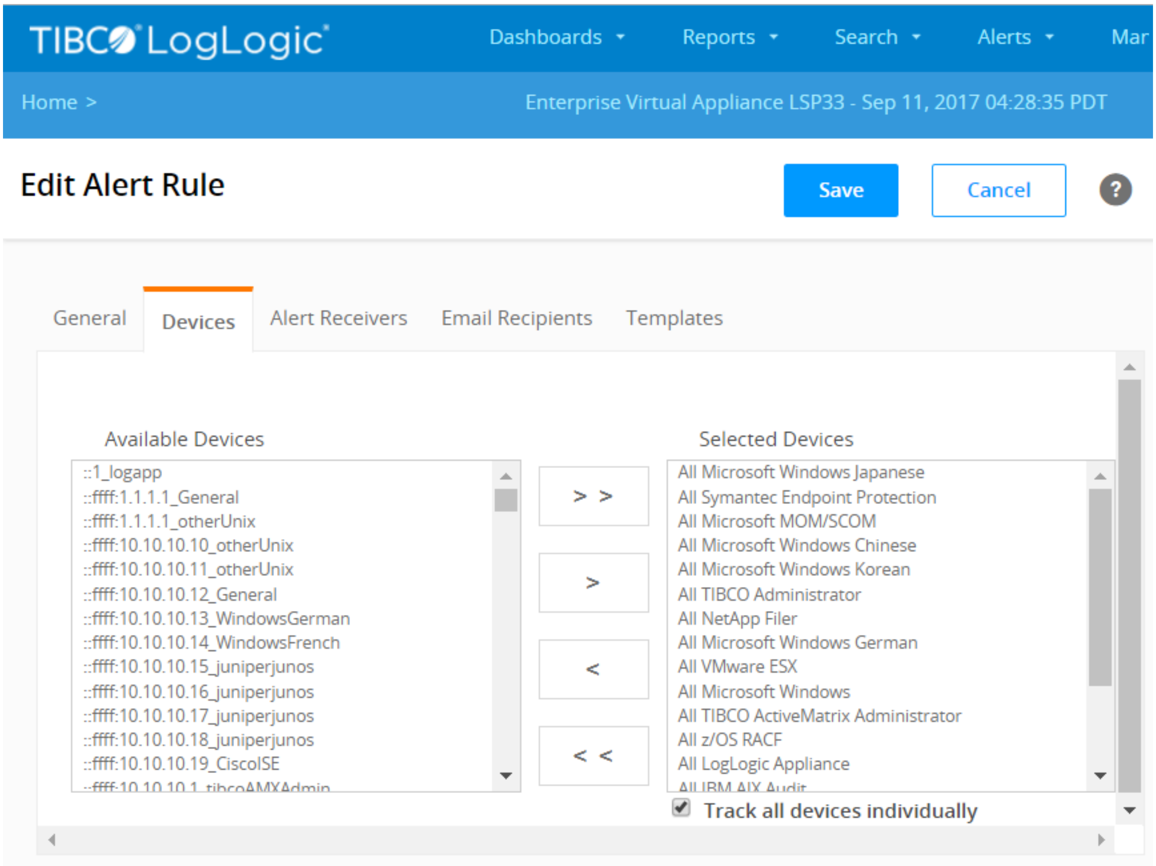
   b) In the **Available Devices** text block, select the appropriate log sources (that is devices) you want to monitor and be alerted on when an alert rule is triggered.

   > If the **Show Only Device Groups** setting is enabled on the Appliance, then the **Available Devices** text block lists only device groups. To enable or disable this feature, go to **Administration** > **System Settings** > **General** tab, scroll down to the **System** Performance Settings section and modify the **Optimize Device Selection List** option.

   c) Click **Add All** or **Add Selected Device(s)**.

   The following figure shows the **Devices** tab for the selected alert.

Available and Selected Devices



Available Devices

::1_logapp
::ffff:1.1.1.1_General
::ffff:1.1.1.1_otherUnix
::ffff:10.10.10.10_otherUnix
::ffff:10.10.10.11_otherUnix
::ffff:10.10.10.12_General
::ffff:10.10.10.13_WindowsGerman
::ffff:10.10.10.14_WindowsFrench
::ffff:10.10.10.15_juniperjunos
::ffff:10.10.10.16_juniperjunos
::ffff:10.10.10.17_juniperjunos
::ffff:10.10.10.18_juniperjunos
::ffff:10.10.10.19_CiscoISE
::ffff:10.10.10.1_tibcoAMXAdmin

Selected Devices

All Microsoft Windows Japanese
All Symantec Endpoint Protection
All Microsoft MOM/SCOM
All Microsoft Windows Chinese
All Microsoft Windows Korean
All TIBCO Administrator
All NetApp Filer
All Microsoft Windows German
All VMware ESX
All Microsoft Windows
All TIBCO ActiveMatrix Administrator
All z/OS RACF
All LogLogic Appliance
All IBM AIX Audit

☑ Track all devices individually

5. The Appliance has the ability to generate an SNMP trap that is sent to an SNMP trap receiver when an alert rule is triggered. Select the alert receivers available to your devices by completing the following steps:
   a) Select the **Alert Receivers** tab.
   b) In the **Available Alert Receivers** text block, select the appropriate alert receivers available for your devices.
   c) Click **Add All** or **Add Selected Receiver(s)**.
6. Select the email recipients to be alerted with a notification email when an alert rule is triggered by completing the following steps:
   a) Select the **Email Recipients** tab.
   b) In the **Available Users** text block, select the appropriate email recipients.

      The **Available Users** text block lists all of the user accounts on the Appliance.
   c) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

Viewing Compliance Suite Alert Results

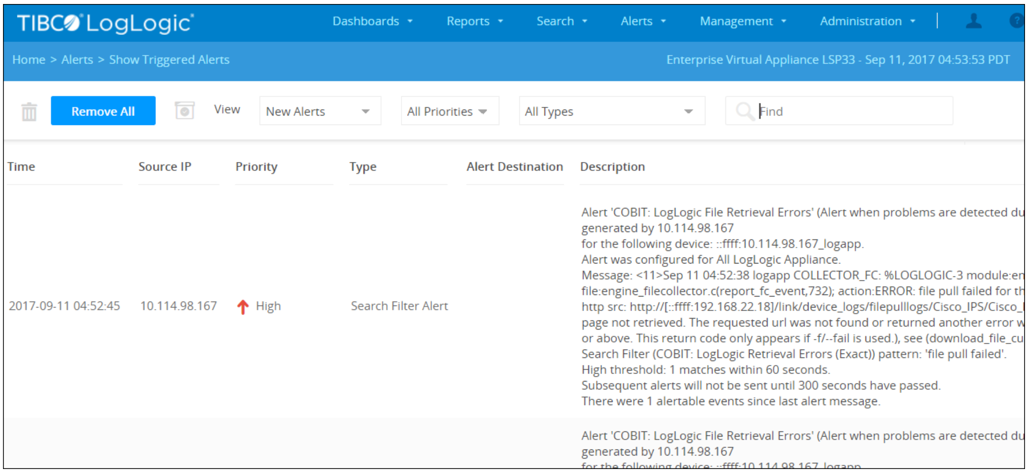
After you have enabled at least one alert, and that alert is triggered, you can view the results.

Procedure

1. In the navigation menu, select **Alerts** > **Show Triggered Alerts** .

   The following figure shows a cropped version of the **Show Triggered Alerts** page.

Aggregated Alert Log



Time	Source IP	Priority	Type	Alert Destination	Description
2017-09-11 04:52:45	10.114.98.167	↑ High	Search Filter Alert		Alert 'COBIT: LogLogic File Retrieval Errors' (Alert when problems are detected du generated by 10.114.98.167 for the following device: ::ffff:10.114.98.167_logapp. Alert was configured for All LogLogic Appliance. Message: <11>Sep 11 04:52:38 logapp COLLECTOR_FC: %LOGLOGIC-3 module:en file:engine_filecollector.c(report_fc_event,732); action:ERROR: file pull failed for th http src: http://[::ffff:192.168.22.18]/link/device_logs/filepulllogs/Cisco_IPS/Cisco_ page not retrieved. The requested url was not found or returned another error w or above. This return code only appears if -f/--fail is used.), see (download_file_cu Search Filter (COBIT: LogLogic Retrieval Errors (Exact)) pattern: 'file pull failed'. High threshold: 1 matches within 60 seconds. Subsequent alerts will not be sent until 300 seconds have passed. There were 1 alertable events since last alert message.
					Alert 'COBIT: LogLogic File Retrieval Errors' (Alert when problems are detected du generated by 10.114.98.167 for the following device: ::ffff:10.114.98.167_logapp

2. From the **Show** drop-down menu, select the desired alert and priority filters to show only those alerts you want to display. The defaults are **New Alerts** and **All Priorities**.
3. (Management Station Appliances Only) From the **From Appliance** drop-down menu, select the appliance from which you want to view the alerts.
4. View the results of your query. You can navigate through all of the data by using the page navigation buttons or page text field.
5. You can either acknowledge or remove an alert. Click the checkbox next to the alert name, then click either **Acknowledge**, **Remove**, or **Remove All**.

> Each alert was triggered based on your set alert parameters, so care must be taken when acknowledging or removing the alert.

COBIT 4.1 Control Objectives

By using TIBCO LogLogic Compliance Suite you can implement COBIT 4.1 control objectives.

Plan and Organize

The Plan and Organize Control Objectives addressed by the LogLogic® Compliance Suite - Sarbanes-Oxley Edition are:

PO2 Define the Information Architecture

- PO2.3 Data Classification Scheme (Maps to Process APO03.02 in COBIT 5)
- PO2.4 Integrity Management (Maps to Process APO01.06 in COBIT 5)

PO4 Define the IT Processes, Organization and Relationships

- PO4.11 Segregation of Duties (Maps to Process APO01.02 in COBIT 5)

PO7 Manage IT Human Resources

- PO7.8 Job Change and Termination (Maps to Process APO07.01 in COBIT 5)

PO2.3 Data Classification Scheme

Establish an enterprise-wide data classification scheme based on both business criticality and sensitivity requirements. Use this scheme as the basis for applying data-specific controls, such as encryption, access control, archive, and high availability.

Illustrative Controls and the TIBCO LogLogic Solution

An appropriate data classification scheme serves as the basis for applying, monitoring, and managing data-related IT security controls. The classification scheme provides the means for controlling data access, ensuring availability of critical data, and maintaining an audit trail for sensitive or critical data access.

To satisfy this objective, the organization must architect a classification scheme that accounts for all enterprise data. The scheme will take into account characteristics and issues such as sensitivity, criticality, and encryption and availability requirements. Implementing data access logging and monitoring helps ensure that the scheme is being applied in a suitable fashion and that data is being accessed by appropriate parties.

Reports and Alerts

Refer PO2.3 to see the PO2.3 reports and alerts.

PO2.4 Integrity Management

Develop and institute procedures to ensure electronic data integrity in all forms (that is files, databases, archives).

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must ensure that appropriate controls are in place to safeguard and preserve the integrity of electronic data. Maintaining data integrity provides assurances for the validity and accuracy of data and is a key component for financial reporting.

To satisfy this objective, administrators must ensure that controls are in place to detect and report on unauthorized (both accidental and malicious) data modifications. These controls should be applied on all relevant financial reporting systems. Additionally, strong change management controls and procedures help reduce the risk of data integrity violations caused by unauthorized or uncontrolled changes to system configurations.

Reports and Alerts

Refer PO2.4 to see the PO2.4 reports and alerts.

PO4.11 Segregation of Duties

Implement a division of roles and responsibilities that reduces the possibility for a single individual to subvert a critical process. Management also makes sure that personnel are performing only authorized duties relevant to their respective jobs and positions.

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must confirm that there is appropriate segregation of duties between the staff responsible for moving a program into production and the staff responsible for developing a program. In addition, organizations must consider whether or not a change to a program is performed in a segregated and controlled environment.

To satisfy this control objective, administrators must ensure that logins to financial reporting servers as well as permissions assigned to these users are appropriate for the tasks they are allowed to perform. Users with overlapping permission sets could indicate a compromise in the segregation of duties control consideration. Administrators must also review the process to request and grant access to systems and data and confirm that the same person does not perform these functions.

Demonstrate that only authorized users have access to sensitive data and applications.

Reports and Alerts

Refer PO4.11 to see the PO4.11 reports and alerts.

PO7.8 Job Change and Termination

Take expedient actions regarding job changes, especially job terminations. Knowledge transfer must be arranged, responsibilities reassigned, and access rights removed such that risks are minimized and continuity of the function is guaranteed.

Illustrative Controls and the TIBCO LogLogic Solution

When a person changes jobs or is terminated from a company, user access privileges must be modified according to the company’s business guidelines. To satisfy this control objective, administrators must periodically ensure that only current and authorized employees have access to financial reporting servers. Administrators must ensure that all terminated users have been disabled. In addition, Administrators must ensure that logins to financial reporting servers as well as permissions assigned to users who changed jobs are appropriate for the new role they are in. To ensure that the preceding requirements are met, Administrators must review reports of all user deletions and group member modifications. This ensures that the terminated users are removed and users who changed jobs have been removed from the appropriate groups.

Demonstrate that user access privileges are modified or revoked in a timely manner upon job change or termination. Review reports and alerts on account activities, accounts created or deleted, group members added or deleted, and successful logins to VPN concentrators and critical servers.

Reports and Alerts

Refer PO7.8 to see the PO7.8 reports and alerts.

Acquire and Implement

The Acquire and Implement Control Objectives addressed by the LogLogic® Compliance Suite - Sarbanes-Oxley Edition are:

AI2 Acquire and Maintain Application Software

- AI2.3 Application Control and Auditability (Maps to Process BAI03.05 in COBIT 5)
- AI2.4 Application Security and Availability (Maps to Processes BAI03.01, BAI03.02, BAI03.03, BAI03.05 in COBIT 5)

AI3 Acquire and Maintain Technology Infrastructure

- AI3.2 Infrastructure Resource Protection and Availability (Maps to Processes BAI03.03, DSS02.03 in COBIT 5)
- AI3.3 Infrastructure Maintenance (Maps to Process BAI03.10 in COBIT 5)

AI6 Manage Changes

- AI6.1 Change Standards and Procedures (Maps to Processes BAI06.01, BAI06.02, BAI06.03, BAI06.04 in COBIT 5)

AI2.3 Application Control and Auditability

Ensure that business controls are properly translated into application controls such that processing is accurate, complete, timely, authorized, and auditable. Issues to consider include authorization mechanisms, information integrity, access control, backup and design of audit trails.

Illustrative Controls and the TIBCO LogLogic Solution

Managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. You must maintain a complete and accurate audit trail for network devices, servers and applications. This enables you to address how your business identifies root causes of issues that can introduce inaccuracy in financial reporting. Also, your problem management system must provide for adequate audit trail facilities which allow tracing from incident to underlying cause.

To satisfy this control objective, administrators must ensure all financial reporting related network devices, servers, and applications are properly configured to log to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.

Verify that all critical applications and network devices are providing a complete audit trail in the form of log data by reviewing the log source status page.

Reports and Alerts

Refer AI2.3 to see the AI2.3 reports and alerts.

AI2.4 Application Security and Availability

Use identified areas of risk and organization-specific security architecture and data classification to address requirements for application availability and security.

Illustrative Controls and the TIBCO LogLogic Solution

Application security and availability controls help ensure the confidentiality, integrity, and availability of systems, applications, and data. These controls help implement the organization’s requirements for data classification, access control, and risk management.

To satisfy this objective, administrators must ensure that preventive and detective controls have been established to protect relevant applications and data. Monitoring availability-related events in application and system logs supports this control objective. Additionally, tracking and monitoring changes in authorization and access levels helps provide assurance that security controls are being implemented according to the policy.

Reports and Alerts

Refer AI2.4 to see the AI2.4 reports and alerts.

AI3.2 Infrastructure Resource Protection and Availability

Apply security and auditability measures during infrastructure and software implementation to ensure system integrity and availability and resource protection. Define roles and responsibilities for the operation of sensitive components and continually monitor and evaluate use.

Illustrative Controls and the TIBCO LogLogic Solution

Implementing controls during system integration and installation helps ensure that the integrity of systems and data.

To satisfy this objective, organizations should ensure the proper separation of responsibilities and environments for testing, development, and production operation. Implementation plans should include security and availability controls. Production deployment and change should be controlled through reviews, approvals, and accompanying rollback plans. Access to and maintenance of financial systems and supporting infrastructure must be monitored and logged.

Reports and Alerts

Refer AI3.2 to see the AI3.2 reports and alerts.

AI3.3 Infrastructure Maintenance

Develop a plan for maintenance of the environment. Ensure that change management procedures govern all changes. Include business requirements, patch management, upgrades, and security factors in the plan.

Illustrative Controls and the TIBCO LogLogic Solution

Unauthorized and unplanned changes to the environment present a significant risk to the infrastructure and associated data integrity and availability. To counter this risk, all changes to critical financial systems must be managed in a formal and controlled manner.

To satisfy this objective, the change management policy should include formal requests, implementation planning, approvals, testing, risk assessment, and contingency planning. System changes must be monitored to ensure that modifications occur only in conjunction with approved requests and plans.

Reports and Alerts

Refer AI3.3 Infrastructure Maintenance to see the AI3.3 reports and alerts.

AI6 Change Standards and Procedures

Set up formal change management procedures to handle all requests (including maintenance and patches) in a standardized manner.

Illustrative Controls and the TIBCO LogLogic Solution

Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area might significantly impact financial reporting. For example, changes to the programs that allocate financial data to accounts require appropriate approvals and testing before the change to ensure classification and reporting integrity.

Businesses must ensure that requests for program changes, system changes, and maintenance (including changes to system software) are standardized, documented, and subject to formal change management procedures.

To satisfy this control objective, administrators must review all changes to the production environment and compare the changes to documented approvals to ensure the approval process is followed. From the archived audit log data, obtain a sample of regular and emergency changes made to applications/ systems to determine whether they were adequately tested and approved before being placed into a production environment. Trace the sample of changes back to the change request log and supporting documentation.

Review all changes to the production environment and compare the changes to documented approvals utilizing alerts and reports on policy modifications, groups activities, escalated privilege activities, and permissions changed.

Reports and Alerts

Refer AI6 Change Standards and Procedures to see the AI6 reports and alerts.

Delivery and Support

The Deliver and Support Control Objectives addressed by the LogLogic® Compliance Suite - Sarbanes-Oxley Edition are:

DS1 Define and Manage Service Levels

- DS1.5 Monitoring and Reporting of Service Level Achievements (Maps to Process APO09.05 in COBIT 5)

DS2 Manage Third-Party Services

- DS2.4 Supplier Performance Monitoring (Maps to Process APO10.05 in COBIT 5)

DS3 Manage Performance and Capacity

- DS3.5 Monitoring and Reporting of Performance and Capacity (Maps to Process BAI04.04 in COBIT 5)

DS4 Ensure Continuous Service

- DS4.1 IT Continuity Framework (Maps to Processes DSS04.01, DSS04.02 in COBIT 5)
- DS4.5 Testing of the IT Continuity Plan (Maps to Process DSS04.05 in COBIT 5)

DS5 Ensure System Security

- DS5.2 IT Security Plan (Maps to Process APO13.02 in COBIT 5)
- DS5.3 Identity Management (1 of 4) (Maps to Process DSS05.04 in COBIT 5)
- DS5.3 Identity Management (2 of 4) (Maps to Process DSS05.04 in COBIT 5)
- DS5.3 Identity Management (3 of 4) (Maps to Process DSS05.04 in COBIT 5)
- DS5.3 Identity Management (4 of 4) (Maps to Process DSS05.04 in COBIT 5)
- DS5.4 User Account Management (Maps to Process DSS05.04 in COBIT 5)
- DS5.5 Security Testing, Surveillance, and Monitoring (Maps to Process DSS05.07 in COBIT 5)
- DS5.7 Protection of Security Technology (Maps to Process DSS05.05 in COBIT 5)
- DS5.8 Cryptographic Key Management (Maps to Process DSS05.03 in COBIT 5)
- DS5.10 Network Security (1 of 2) (Maps to Process DSS05.02 in COBIT 5)
- DS5.10 Network Security (2 of 2) (Maps to Process DSS05.02 in COBIT 5)

DS9 Manage the Configuration

- DS9.3 Configuration Integrity Review (Maps to Processes BAI10.04, BAI10.05, DSS02.05 in COBIT 5)

DS10 Manage Problems

- DS10.2 Problem Tracking and Resolution (Maps to Process DSS03.02 in COBIT 5)

DS11 Manage Data

- DS11.2 Storage and Retention Arrangements (Maps to Process DSS04.08, DSS06.04 in COBIT 5)
- DS11.5 Backup and Restoration (Maps to Process DSS04.08 in COBIT 5)
- DS11.6 Security Requirements for Data Management (Maps to Process DSS01.01, DSS05.08, DSS06.05 in COBIT 5)

DS13 Manage Operations

- DS 13.3 IT Infrastructure Monitoring (Maps to Process DSS01.03 in COBIT 5)

DS1.5 Monitoring and Reporting of Service Level Achievements

Continuously monitor specified service level performance criteria. Reports are provided in a format meaningful to the stakeholders on achievement of service levels. The monitoring statistics are analyzed and acted upon to identify negative and positive trends for individual services as well as for services overall.

Illustrative Controls and the TIBCO LogLogic Solution

The process of defining and managing service levels addresses how an organization meets the functional and operational expectations of its users and, ultimately, the objectives of the business. Deficiencies in this area could significantly impact financial reporting and disclosure of an entity. For example, if systems are poorly managed or system functionality is not delivered as required, financial information can not be processed as intended.

To satisfy this control objective, administrators must configure alerts to ensure all critical application failures, including firewalls, routers, switches, servers, and applications, are recognized immediately. Alerts must be reviewed periodically. In addition, administrators must perform independent reviews on the security, availability, and processing integrity of third-party service providers by continuously monitoring the service level agreements through adequate logging and reporting.

Continuously monitor the availability of the IT infrastructure using behavioral-based alerts. Administrators can configure alerts to monitor performance of firewalls, routers, switches, servers, applications, and operating systems so they can be notified immediately of the failures. Real-time reports and custom, regular-expression searches also enable administrators to quickly identify and determine the root cause of any problems. This further mitigates risk and minimizes interruptions to service availability.

Reports and Alerts

Refer DS1.5 to see the DS1.5 reports and alerts.

DS2.4 Supplier Performance Monitoring

It establishes a process to monitor service delivery to ensure the supplier is meeting current business requirements and is continuing to adhere to the contract agreements and service level agreements, and that performance is competitive with alternative suppliers and market conditions.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must configure proper alerts to monitor any anomalies related to system availability, capacity and performance.

Continuously monitor the availability of the IT infrastructure using behavioral-based alerts. Administrators can configure alerts to monitor performance of firewalls, routers, switches, servers, applications, and operating systems so they can be notified immediately if of failures. Real-time reports and custom, regular-expression searches also enable administrators to quickly identify and determine the root cause of any problems. This further mitigates risk and minimizes interruptions to service availability.

Reports and Alerts

Refer DS2.4 to see the DS2.4 reports and alerts.

DS3.5 Monitoring and Reporting of Performance and Capacity

Continuously monitor the performance and capacity of IT resources. Data gathered serve two purposes:

- To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans and resource acquisition
- To report delivered service availability to the business as required by the SLAs. Accompany all exception reports with recommendations for corrective action.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must configure proper alerts to monitor any anomalies related to system availability, capacity and performance.

Continuously monitor the availability of the IT infrastructure using behavioral-based alerts. Administrators can configure alerts to monitor performance of firewalls, routers, switches, servers, applications, and operating systems so they can be notified immediately of the failures. Real-time reports and custom, regular-expression searches also enable administrators to quickly identify and determine the root cause of any problems. This further mitigates risk and minimizes interruptions to service availability.

Reports and Alerts

Refer DS3.5 to see the DS3.5 reports and alerts.

DS4.1 IT Continuity Framework

Develop a framework for IT continuity to support enterprise-wide business continuity management with a consistent process. The objective of the framework is to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans.

The framework should address the organizational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers, and the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery.

Illustrative Controls and the TIBCO LogLogic Solution

Policies and procedures addressing backup and restoration activities must be documented, communicated, and updated to ensure guidance reflects current business conditions.

To satisfy this control objective, all policies and procedures must be accessed, reviewed, and updated periodically by appropriate users. Lack of access to these policies and procedures must indicate that they have not been regularly reviewed and updated.

Verify that IT Continuity Framework documents have been reviewed periodically by authorized personnel.

Reports and Alerts

Refer DS4.1 to see the DS4.1 reports and alerts.

DS4.5 Testing of the IT Continuity Plan

Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing.

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must have procedures in place to back up the data and programs based on IT and user requirements.

To satisfy this control objective, administrators must back up the data on a regular basis. In addition, administrators must review backup logs periodically to ensure backups are performed successfully. Backup logs must be reviewed periodically to ensure backup and restore are performed successfully on a regular basis.

Review backup logs periodically to ensure backup and restore are performed successfully on a regular basis.

Reports and Alerts

Refer DS4.5 to see the DS4.5 reports and alerts.

DS5.2 IT Security Plan

Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users.

Illustrative Controls and the TIBCO LogLogic Solution

Policies and procedures addressing backup and restoration activities must be documented, communicated, and updated to ensure guidance reflects current business conditions.

To satisfy this control objective, all policies and procedures must be accessed, reviewed, and updated periodically by appropriate users. Lack of access to these policies and procedures should indicate that they have not been regularly reviewed and updated.

Verify that IT Continuity and Security Plans have been reviewed periodically by authorized personnel.

Reports and Alerts

Refer DS5.2 IT Security Plan to see the DS5.2 reports and alerts.

DS5.3 Identity Management (1 of 4)

All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable.

Illustrative Controls and the TIBCO LogLogic Solution

Ensuring all users have uniquely identifiable IDs and that accurate and complete audit trails can be maintained. Deficiencies in this area can significantly impact accountability. For example, users logging in using shared IDs can modify financial records. This can prevent future audits to identify who have modified the data.

To satisfy this control objective, administrators must ensure all logins are not shared. Administrators must review the ID list to identify IDs that can be a generic ID and question who is using it and why it is there. Administrators must also validate that attempts to gain unauthorized access to financial reporting systems and subsystems are logged and are followed up on a timely basis. Monitor and verify all user access to programs and data. Review this access to ensure that there is segregation of duties as well as all access privileges are properly assigned and approved.

Reports and Alerts

Refer DS5.3 Identity Management (1 of 4) to see the DS5.3 reports and alerts.

DS5.3 Identity Management (2 of 4)

User access rights to systems and data should be in line with defined and documented business needs and job requirements.

Illustrative Controls and the TIBCO LogLogic Solution

Accurately managing user access rights addresses the issues of unintended or malicious modifications of financial data. Deficiencies in this area might allow unauthorized modifications that could lead to errors in financial reporting.

To satisfy this control objective, administrators must periodically review user access to files and programs to ensure the users have not accessed items outside of their role. Administrators should select a sample of users who have logged in to financial reporting servers and review their access for appropriateness based upon their job functions.

Monitor and verify that all user access to programs and data. Review this access to ensure there is segregation of duties as well as all access privileges are properly assigned and approved.

Reports and Alerts

Use the following link/reference to see the DS5.3 reports and alerts: DS5.3 Identity Management (2 of 4)

DS5.3 Identity Management (3 of 4)

User access rights are requested by user management, approved by the system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository.

Illustrative Controls and the TIBCO LogLogic Solution

Ensure that user access rights are properly requested, approved, and implemented. A control process must exist and followed to periodically review and confirm access rights.

To satisfy this control objective, administrators must periodically review all privileged user access to servers and applications that are related to the financial reporting process. Also, Administrators must ensure that new users or users assigned to new groups have the appropriate level of access. Administrators can select a sample of new users created and permissions modified recently and determine if management approved their access and the access granted agrees with the access privileges that were approved.

Monitor and verify that all user access to programs and data. Review access levels to ensure there is segregation of duties as well as all access privileges are properly assigned and approved.

Reports and Alerts

Use the following link/reference to see the DS5.3 reports and alerts: DS5.3 (3/4).

DS5.3 Identity Management (4 of 4)

Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.

Illustrative Controls and the TIBCO LogLogic Solution

All logins to network devices, operating systems, platforms, databases and applications must be reviewed to ensure only authorized and appropriate personnel have access.

To satisfy this control objective, administrators must assess the authentication mechanisms used to validate user credentials (new and existing) for financial reporting systems to support the validity of transactions. Server and application activities must be monitored for locked-out accounts as they can represent malicious activities.

Monitor and verify all user access to programs and data. Review access to ensure there is segregation of duties as well as all access privileges are properly assigned and approved.

Reports and Alerts

Use the following link/reference to see the DS5.3 reports and alerts: DS5.3 (4/4).

DS5.4 User Account Management

Ensure that requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges are tasks that are appropriately addressed by user account management policies and procedures.

An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users.

Perform regular management review of all accounts and related privileges.

Illustrative Controls and the TIBCO LogLogic Solution

Demonstrate that procedures exist for the registration, change, and deletion of users from financial reporting systems and subsystems on a timely basis and confirm that the procedures are followed. Procedures must exist and be followed to ensure timely action relating to requesting, establishing, issuing, suspending, and closing user accounts.

To satisfy this control objective, administrators must ensure that permissions have been granted to the appropriate users. Permissions incorrectly assigned to users can indicate failure to meet this control objective. Also, Administrators must ensure that all network and application access requests are adequately documented and approved by appropriate Management personnel. As proof, Administrators can select a sample of terminated employees and to ensure the accounts for these employees have been terminated in a timely manner.

Administrators must ensure the policies on all servers and applications are set appropriately to ensure passwords are changed. Server and application logs must be reviewed to ensure passwords are changed periodically.

Monitor any account management activities such as user or group addition, deletion, and modification to ensure all user access privileges are appropriate and approved. Set up real-time alerts to detect any unauthorized or unapproved changes to users or groups.

Reports and Alerts

Use the following link/reference to see the DS5.4 reports and alerts: DS5.4.

DS5.5 Security Testing, Surveillance, and Monitoring

Ensure that IT security is tested and monitored proactively. IT security should be reaccredited periodically to ensure the approved security level is maintained.

A logging and monitoring function enables the early detection of unusual or abnormal activities that must be addressed.

Access to the logging information is in line with business requirements in terms of access rights and retention requirements.

Illustrative Controls and the TIBCO LogLogic Solution

IT security administration must monitor and log security activity, and identify security violations to report to senior management. This control directly addresses the issues of timely detection and correction of financial data modification.

To satisfy this control, administrators must review the user access logs on a regular basis on a weekly basis for any access violations or unusual activity. Administrators must periodically, such as daily or weekly, review reports that show user access to servers related to financial reporting process. Review of these reports must be shown to auditors to satisfy this requirement.

Monitor and log all user activities on servers and applications. Detect any unusual behavior using real-time alerts. Identify security violations to report to senior management.

Reports and Alerts

Use the following link/reference to see the DS5.5 reports and alerts: DS5.5.

DS5.7 Protection of Security Technology

Make security and related technology tamper-resistant. Do not unnecessarily disclose or distribute security documentation.

Illustrative Controls and the TIBCO LogLogic Solution

Because of their criticality, security technologies must be protected from unauthorized tampering and modification. Documentation and information about security design and infrastructure should be protected appropriately.

To satisfy this objective, the organization should implement and monitor available tamper controls for deployed security technologies. System operations and related events that might signal tampering should be logged and monitored closely. Access to security-related documentation must be strictly controlled and monitored to detect inappropriate access.

Reports and Alerts

Use the following link/reference to see the DS5.7 reports and alerts: DS5.7.

DS5.8 Cryptographic Key Management

Design and implement policies and procedures to govern cryptographic key management. These policies and procedures must include topics such as key generation, revocation, distribution, use, and escrow.

Illustrative Controls and the TIBCO LogLogic Solution

Since encryption is typically employed for an organization’s most valuable systems and data, the secure management of these encryption keys is critical to maintaining the confidentiality, integrity, and availability of this data.

To satisfy this control objective, the organization must ensure that key management policies and procedures are appropriate for the sensitivity of the data being encrypted. Logging and monitoring of key management activities should be implemented to help ensure the security and integrity of the key management process.

Reports and Alerts

Use the following link/reference to see the DS5.8 reports and alerts: DS5.8.

DS5.10 Network Security (1 of 2)

Ensure that security techniques and related management procedures are used to authorize access and control information flows from and to networks.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must periodically review IDS logs to ensure the IDS tools are fully utilized.

Review all remote access to the IT infrastructure through VPN or through firewalls. Detect any anomalies such as excessive IDS attacks or firewall traffic using behavioral-based alerts.

Reports and Alerts

Use the following link/reference to see the DS5.10 reports and alerts: DS5.10.

DS5.10 Network Security (2 of 2)

Ensure that security techniques and related management procedures are used to authorize access and regulate information flows from and to networks with controls such as firewalls and network segmentation.

Illustrative Controls and the TIBCO LogLogic Solution

Administrators must periodically review all firewall rules to ensure accurate access control list. In addition, Administrators must review network traffic correlated with the firewall policy to ensure appropriate rules are used to protect the company.

Review all remote access to the IT infrastructure using VPN or through firewalls. Detect any anomalies such as excessive IDS attacks or firewall traffic using behavioral-based alerts.

Reports and Alerts

Use the following link/reference to see the DS5.10 reports and alerts: DS5.10.

DS9.3 Configuration Integrity Review

Review and verify on a regular basis, using, where necessary, appropriate tools, the status of configuration items to confirm the integrity of the current and historical configuration data and to compare against the actual situation. Review periodically against the policy for software usage the existence of any personal or unlicensed software or any software instances in excess of current license agreements. Errors and deviations must be reported, acted on and corrected.

Illustrative Controls and the TIBCO LogLogic Solution

Configuration management ensures that security, availability, and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security and availability exposures that can permit unauthorized access to systems and data and impact financial reporting.

To satisfy this control objective, administrators must ensure that only authorized software is permitted for use by employees using company IT assets. System infrastructure, including firewalls, routers, switches, network operating systems, servers and other related devices, is properly configured to prevent unauthorized access. Application software and data storage systems must be properly configured to provision access based on the individual’s demonstrated must view, add, change or delete data.

Real-time reports and alerts enable administrators to review and monitor any configuration changes made to critical IT infrastructure. Administrators can take immediate action to mitigate the risks introduced by inappropriate configuration modifications.

Reports and Alerts

Refer DS9.3 to see the DS9.3 reports and alerts.

DS10.2 Problem Tracking and Resolution

The problem management system should provide for adequate audit trail facilities that allow tracking, analyzing, and determining the root cause of all reported problems considering:

- All associated configuration items
- Outstanding problems and incidents
- Known and suspected errors

Illustrative Controls and the TIBCO LogLogic Solution

Managing problems and incidents addresses how an organization identifies, documents and responds to events that fall outside of normal operations. You must maintain a complete and accurate audit trail for network devices, servers, and applications. This enables you to address how your business identifies root causes of issues that can introduce inaccuracy in financial reporting. Also, your problem management system must provide for adequate audit trail facilities which allow tracing from incident to underlying cause.

To satisfy this control objective, administrators must ensure all financial reporting related network devices, servers, and applications are properly configured to log to a centralized server. Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.

By alerting on any failures that occur, administrators can respond rapidly to potential problems and incidents that might affect availability, security, or performance. Real-time data monitoring and reporting capabilities reduce time to repair after incidents, reducing costs, and improving application availability.

Reports and Alerts

Use the following link/reference to see the DS10.2 reports and alerts: DS10.2.

DS11.2 Storage and Retention Arrangements

Implement procedures to govern data storage and retention. Ensure that business and security objectives as well as regulatory requirements are reflected in the procedures.

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must have sound and comprehensive policies and procedures to govern the storage, retention, and archive of enterprise data. All relevant regulatory influences must be accounted for, and the data classification scheme should provide direct input to the implementation of associated access control and data handling procedures.

To satisfy this objective, organizations should ensure that an enterprise-wide data storage, retention, and handling policy has been documented and implemented, and that financial reporting systems are covered appropriately. Backup and restore operations should be proactively monitored to help ensure compliance with organizational policies, and hardware and storage errors should be acted upon immediately to facilitate the organization’s availability, storage, and retention requirements.

Reports and Alerts

Use the following link/reference to see the DS11.2 reports and alerts: DS11.2.

DS11.5 Backup and Restoration

Define and implement procedures for backup and restoration of systems, data and documentation in line with business requirements and the continuity plan. Verify compliance with the backup procedures, and verify the ability to and time required for successful and complete restoration. Test backup media and the restoration process.

Illustrative Controls and the TIBCO LogLogic Solution

Organizations must have procedures in place to back up data and programs based on IT and user requirements.

To satisfy this control objective, administrators must back up data on a regular basis. In addition, administrators must review backup logs periodically to ensure backups are performed successfully. Backup logs must be reviewed periodically to ensure backup and restore are performed successfully on a regular basis.

Review backup logs periodically to ensure backup and restore are performed successfully on a regular basis.

Reports and Alerts

Use the following link/reference to see the DS11.5 reports and alerts: DS11.5.

DS11.6 Security Requirements for Data Management

Establish arrangements to identify and apply security requirements applicable to the receipt, processing, physical storage and output of data and sensitive messages. This includes physical records, data transmissions and any data stored offsite.

Illustrative Controls and the TIBCO LogLogic Solution

Changes to data structures are authorized, made in accordance with design specifications and implemented in a timely manner.

To satisfy this control objective, verify that data structure changes adhere to the design specifications and that they are implemented in the time-frame required. Administrators can review data structure changes data such as alerts and reports.

Monitor and review all changes to data structures such as data using alerts and reports.

Reports and Alerts

Use the following link/reference to see the DS11.6 reports and alerts: DS11.6.

DS13.3 IT Infrastructure Monitoring

Define and implement procedures to monitor the IT infrastructure and related events. Ensure sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of operations and the other activities surrounding or supporting operations.

Illustrative Controls and the TIBCO LogLogic Solution

Managing operations addresses how an organization maintains reliable application systems in support of the business to initiate, record, process and report financial information. Deficiencies in this area could significantly impact an entity’s financial reporting. For instance, lapses in the continuity of application systems might prevent an organization from recording financial transactions and thereby undermine its integrity.

System event data must be sufficiently retained to provide chronological information and logs to enable the review, examination and reconstruction of system and data processing.

System event data can also be used to provide reasonable assurance as to the completeness and timeliness of system and data processing.

To satisfy this control objective, administrators must ensure all financial reporting related network devices, servers, and applications are properly configured to log to a centralized server.

Administrators must also periodically review logging status to ensure these devices, servers and applications are logging correctly.

Review of these reports must be shown to auditors to satisfy this requirement.

Continuously monitor the availability of the IT infrastructure using behavioral-based alerts. Configure alerts to monitor performance of firewalls, routers, switches, servers, and applications and operating systems to be notified immediately if there’s a failure.

Reports and Alerts

Use the following link/reference to see the DS13.3 reports and alerts: DS13.3.

TIBCO LogLogic Reports and Alerts for Sarbanes-Oxley and COBIT 4.1

TIBCO LogLogic Reports for Sarbanes-Oxley and COBIT 4.1

The following table lists the reports included in the LogLogic® Compliance Suite - Sarbanes-Oxley Edition and COBIT 4.1.

Serial Number	TIBCO LogLogic Report	Description
1	COBIT: Accepted VPN Connections - RADIUS	Displays all users connected to the internal network through the RADIUS VPN.
2	COBIT: Account Activities on UNIX Servers	Displays all accounts activities on UNIX servers to ensure authorized and appropriate access.
3	COBIT: Account Activities on Windows Servers	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
4	COBIT: Accounts Changed on NetApp Filer	Displays all accounts changed on NetApp Filer to ensure authorized and appropriate access.
5	COBIT: Accounts Changed on Sidewinder	Displays all accounts changed on Sidewinder to ensure authorized and appropriate access.
6	COBIT: Accounts Changed on TIBCO ActiveMatrix Administrator	Displays all accounts changed on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
7	COBIT: Accounts Changed on TIBCO Administrator	Displays all accounts changed on TIBCO Administrator to ensure authorized and appropriate access.
8	COBIT: Accounts Changed on UNIX Servers	Displays all accounts changed on UNIX servers to ensure authorized and appropriate access.
9	COBIT: Accounts Changed on Windows Servers	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
10	COBIT: Accounts Created on NetApp Filer	Displays all accounts created on NetApp Filer to ensure authorized and appropriate access.
11	COBIT: Accounts Created on NetApp Filer Audit	Displays all accounts created on NetApp Filer Audit to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
12	COBIT: Accounts Created on Sidewinder	Displays all accounts created on Sidewinder to ensure authorized and appropriate access.
13	COBIT: Accounts Created on Symantec Endpoint Protection	Displays all accounts created on Symantec Endpoint Protection to ensure authorized and appropriate access.
14	COBIT: Accounts Created on TIBCO ActiveMatrix Administrator	Displays all accounts created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
15	COBIT: Accounts Created on TIBCO Administrator	Displays all accounts created on TIBCO Administrator to ensure authorized and appropriate access.
16	COBIT: Accounts Created on UNIX Servers	Displays all accounts created on UNIX servers to ensure authorized and appropriate access.
17	COBIT: Accounts Created on Windows Servers	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
18	COBIT: Accounts Deleted on NetApp Filer	Displays all accounts deleted on NetApp Filer to ensure authorized and appropriate access.
19	COBIT: Accounts Deleted on NetApp Filer Audit	Displays all accounts deleted on NetApp Filer Audit to ensure authorized and appropriate access.
20	COBIT: Accounts Deleted on Sidewinder	Displays all accounts deleted on Sidewinder to ensure authorized and appropriate access.
21	COBIT: Accounts Deleted on Symantec Endpoint Protection	Displays all accounts deleted on Symantec Endpoint Protection to ensure authorized and appropriate access.
22	COBIT: Accounts Deleted on TIBCO ActiveMatrix Administrator	Displays all accounts deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
23	COBIT: Accounts Deleted on TIBCO Administrator	Displays all accounts deleted on TIBCO Administrator to ensure authorized and appropriate access.
24	COBIT: Accounts Deleted on UNIX Servers	Displays all accounts deleted on UNIX servers to ensure authorized and appropriate access.
25	COBIT: Accounts Deleted on Windows Servers	Displays all accounts deleted on Windows servers to ensure authorized and appropriate access.
26	COBIT: Active Connections for Cisco ASA	Displays all currently active firewall connections for Cisco ASA.

Serial Number	TIBCO LogLogic Report	Description
27	COBIT: Active Connections for Cisco FWSM	Displays all currently active firewall connections for Cisco FWSM.
28	COBIT: Active Connections for Cisco PIX	Displays all currently active firewall connections for Cisco PIX.
29	COBIT: Active Directory Syste m Changes	Displays changes made within Active Directory.
30	COBIT: Active VPN Connections for Cisco VPN Concentrators	Displays all currently active VPN connections for Cisco VPN Concentrators.
31	COBIT: Active VPN Connections for Nortel ivity	Displays all currently active VPN connections for Nortel Contivity VPN devices.
32	COBIT: Active VPN Connectio ns for RADIUS	Displays all currently active VPN connections for RADIUS Acct Client.
33	COBIT: Administrator Logins on Windows Servers	Displays all logins with the administrator account on Windows servers.
34	COBIT: Allowed URLs by Source IPs	Displays successful access to URLs by source IP addresses.
35	COBIT: Allowed URLs by Source IPs - F5 BIG-IP TMOS	Displays successful access to URLs by source IP addresses on F5 BIG-IP TMOS.
36	COBIT: Allowed URLs by Sour ce IPs - Microsoft IIS	Displays successful access to URLs by source IP addresses on Microsoft IIS.
37	COBIT: Allowed URLs by Source Users	Displays successful access to URLs by source users.
38	COBIT: Allowed URLs by Source Users - F5 BIG-IP TMOS	Displays successful access to URLs by source users on F5 BIG-IP TMOS.
39	COBIT: Allowed URLs by Sour ce Users - Microsoft IIS	Displays successful access to URLs by source users on Microsoft IIS.
40	COBIT: Applications Under Attack	Displays all applications under attack as well as the attack signatures.
41	COBIT: Applications Under Attack - Cisco IOS	Displays all applications under attack as well as the attack signatures by Cisco IOS.
42	COBIT: Applications Under Attack - FireEye MPS	Displays all applications under attack as well as the attack signatures by FireEye MPS.

Serial Number	TIBCO LogLogic Report	Description
43	COBIT: Applications Under Attack - ISS SiteProtector	Displays all applications under attack as well as the attack signatures by ISS SiteProtector.
44	COBIT: Applications Under Attack - SiteProtector	Displays all applications under attack as well as the attack signatures by SiteProtector.
45	COBIT: Applications Under Attack - Sourcefire Defense Center	Displays all applications under attack as well as the attack signatures by Sourcefire Defense Center.
46	COBIT: Attackers by Service	Displays all attack source IP address and service ports.
47	COBIT: Attackers by Service - Cisco IOS	Displays all attack source IP address and service ports by Cisco IOS.
48	COBIT: Attackers by Service - ISS SiteProtector	Displays all attack source IP address and service ports by ISS SiteProtector.
49	COBIT: Attackers by Service - FireEye MPS	Displays all attack source IP address and service ports by FireEye MPS.
50	COBIT: Attackers by Service - SiteProtector	Displays all attack source IP address and service ports by SiteProtector.
51	COBIT: Attackers by Service - Sourcefire Defense Center	Displays all attack source IP address and service ports by Sourcefire Defense Center.
52	COBIT: Attackers by Signature	Displays all attack source IP address and signatures.
53	COBIT: Attackers by Signature - Cisco IOS	Displays all attack source IP address and signatures by Cisco IOS.
54	COBIT: Attackers by Signature - FireEye MPS	Displays all attack source IP address and signatures by FireEye MPS.
55	COBIT: Attackers by Signature - ISS SiteProtector	Displays all attack source IP address and signatures by ISS SiteProtector.
56	COBIT: Attackers by Signature - SiteProtector	Displays all attack source IP address and signatures by SiteProtector.
57	COBIT: Attackers by Signature - Sourcefire Defense Center	Displays all attack source IP address and signatures by Sourcefire Defense Center.
58	COBIT: Attacks Detected	Displays all IDS attacks detected against servers and applications.
59	COBIT: Attacks Detected - Cisco IOS	Displays all IDS attacks detected against servers and applications by Cisco IOS.

Serial Number	TIBCO LogLogic Report	Description
60	COBIT: Attacks Detected - HIPS	Displays all IPS attacks detected against servers and applications.
61	COBIT: Attacks Detected - ISS SiteProtector	Displays all IDS attacks detected against servers and applications by ISS SiteProtector.
62	COBIT: Attacks Detected - SiteProtector	Displays all IDS attacks detected against servers and applications by SiteProtector.
63	COBIT: Attacks Detected - Sourcefire Defense Center	Displays all IDS attacks detected against servers and applications by Sourcefire Defense Center.
64	COBIT: Bandwidth Usage by User	Displays users who are using the most bandwidth.
65	COBIT: Blocked URLs by Source IPs	Displays URLs that have been blocked by source IP addresses.
66	COBIT: Blocked URLs by Source IPs - F5 BIG-IP TMOS	Displays URLs that have been blocked by source IP addresses on F5 BIG-IP TMOS.
67	COBIT: Blocked URLs by Sourc e IPs - Microsoft IIS	Displays URLs that have been blocked by source IP addresses on Microsoft IIS.
68	COBIT: Blocked URLs by Source Users	Displays URLs that have been blocked by source users.
69	COBIT: Blocked URLs by Source Users - F5 BIG-IP TMOS	Displays URLs that have been blocked by source users on F5 BIG-IP TMOS.
70	COBIT: Blocked URLs by Sourc e Users - Microsoft IIS	Displays URLs that have been blocked by source users on Microsoft IIS.
71	COBIT: Check Point Configuration Changes	Displays all Check Point audit events related to configuration changes.
72	COBIT: Check Point Management Station Login	Displays all login events to the Check Point management station.
73	COBIT: Check Point Objects Created	Displays all Check Point audit events related to object creation in policies.
74	COBIT: Check Point Objects Deleted	Displays all Check Point audit events related to policy objects deleted.
75	COBIT: Check Point Objects Modified	Displays all Check Point audit events related to policy objects modified.
76	COBIT: Check Point SIC Revoked	Displays all Check Point audit events related to the security certificate being revoked.

Serial Number	TIBCO LogLogic Report	Description
77	COBIT: Cisco ESA: Attacks by Event ID	Displays Cisco ESA attacks by Event ID.
78	COBIT: Cisco ESA: Attacks Detected	Displays attacks detected by Cisco ESA.
79	COBIT: Cisco ESA: Attacks by Threat Name	Displays Cisco ESA attacks by threat name.
80	COBIT: Cisco ESA: Scans	Displays scans using Cisco ESA.
81	COBIT: Cisco ESA: Updated	Displays updates to Cisco ESA.
82	COBIT: Cisco ISE, ACS Accounts Created	Displays all accounts created on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
83	COBIT: Cisco ISE, ACS Accounts Removed	Displays all accounts removed on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
84	COBIT: Cisco ISE, ACS Configuration Changes	Displays Cisco ISE and Cisco SecureACS configuration changes.
85	COBIT: Cisco ISE, ACS Password Changes	Displays all password change activities on Cisco ISE and Cisco SecureACS to ensure authorized and appropriate access.
86	COBIT: Cisco Line Protocol Status Changes	Displays all Cisco line protocol up and down events.
87	COBIT: Cisco Link Status Changes	Displays all Cisco link up and down events.
88	COBIT: Cisco Peer Reset/ Reload	Displays all Cisco Peer reset and reload events.
89	COBIT: Cisco Peer Supervisor Status Changes	Displays all Cisco Peer Supervisor status changes.
90	COBIT: Cisco PIX, ASA, FWSM Failover Disabled	Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability.
91	COBIT: Cisco PIX, ASA, FWSM Failover Performed	Displays all logs related to performing a Cisco PIX, ASA, and FWSM failover.
92	COBIT: Cisco PIX, ASA, FWSM Policy Changed	Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices.
93	COBIT: Cisco Routers and Switches Restart	Displays all Cisco routers and switches restart activities to detect unusual activities.

Serial Number	TIBCO LogLogic Report	Description
94	COBIT: Cisco Switch Policy Changes	Displays all configuration changes to the Cisco router and switch policies.
95	COBIT: Creation and Deletion of System Level Objects: AIX Audit	Displays AIX audit events related to creation and deletion of system-level objects.
96	COBIT: Creation and Deletion of System Level Objects: DB2 Database	Displays DB2 database events related to creation and deletion of system-level objects.
97	COBIT: Creation and Deletion of System Level Objects: HP-UX Audit	Displays HP-UX audit events related to creation and deletion of system-level objects.
98	COBIT: Creation and Deletion of System Level Objects: Windows	Displays all Windows events related to creation and deletion of system-level objects.
99	COBIT: Creation and Deletion of System Level Objects: Oracle	Displays Oracle database events related to creation and deletion of system-level objects.
100	COBIT: Creation and Deletion of System Level Objects: Solaris BSM	Displays Solaris BSM events related to creation and deletion of system-level objects.
101	COBIT: Creation and Deletion of System Level Objects: SQL Server	Displays Microsoft SQL Server events related to creation and deletion of system-level objects.
102	COBIT: DB2 Database Backup Failed	Displays all IBM DB2 Database Server backup failures.
103	COBIT: DB2 Database Configuration Changes	Displays DB2 database configuration changes.
104	COBIT: DB2 Database Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
105	COBIT: DB2 Database Successful Logins	Displays successful DB2 database logins.
106	COBIT: DB2 Database Restore Failed	Displays all IBM DB2 Database restore failure events.
107	COBIT: DB2 Database Stop and Start Events	Displays DB2 database events related to starting and stopping the database.
108	COBIT: DB2 Database User Additions and Deletions	Displays IBM DB2 Database events related to creation and deletion of database users.

Serial Number	TIBCO LogLogic Report	Description
109	COBIT: Decru DataFort Cryptographic Key Events	Displays events related to cryptographic key handling.
110	COBIT: Decru DataFort Zeroization Events	Displays events related to Decru DataFort zeroization.
111	COBIT: Denied Connections by IP Addresses - Check Point	Displays remote IP addresses with the most denied connections from Check Point.
112	COBIT: Denied Connections by IP Addresses - Cisco ASA	Displays remote IP addresses with the most denied connections from Cisco ASA.
113	COBIT: Denied Connections by IP Addresses - Cisco FWSM	Displays remote IP addresses with the most denied connections from Cisco FWSM.
114	COBIT: Denied Connections by IP Addresses - Cisco PIX	Displays remote IP addresses with the most denied connections from Cisco PIX.
115	COBIT: Denied Connections by IP Addresses - Nortel	Displays remote IP addresses with the most denied connections from Nortel.
116	COBIT: Denied Connections - Cisco IOS	Displays all connections that have been denied by the Cisco IOS devices.
117	COBIT: Denied Connections - Cisco NXOS	Displays all connections that have been denied by the Cisco NXOS devices.
118	COBIT: Denied Connections - Cisco Router	Displays all connections that have been denied by the Cisco Router devices.
119	COBIT: Denied Connections - VMware vShield	Displays all connections that have been denied by the VMware vShield devices.
120	COBIT: Denied Connections - Sidewinder	Displays all connections that have been denied by the Sidewinder devices.
121	COBIT: Denied Inbound Conne ctions - Cisco ASA	Displays all inbound connections that have been denied by the Cisco ASA devices.
122	COBIT: Denied Inbound Connections - Cisco FWSM	Displays all inbound connections that have been denied by the Cisco FWSM devices.
123	COBIT: Denied Inbound Connections - Cisco PIX	Displays all inbound connections that have been denied by the Cisco PIX devices.
124	COBIT: Denied Inbound Connections - Check Point	Displays all inbound connections that have been denied by the Check Point devices.
125	COBIT: Denied Inbound Connections - Juniper Firewall	Displays all inbound connections that have been denied by the Juniper Firewalls.

Serial Number	TIBCO LogLogic Report	Description
126	COBIT: Denied Outbound Connections - Cisco ASA	Displays all outbound connections that have been denied by the Cisco ASA.
127	COBIT: Denied Outbound Connections - Cisco FWSM	Displays all outbound connections that have been denied by the Cisco FWSM.
128	COBIT: Denied Outbound Connections - Check Point	Displays all outbound connections that have been denied by the Check Point.
129	COBIT: Denied Outbound Con nections - Cisco PIX	Displays all outbound connections that have been denied by the Cisco PIX.
130	COBIT: Denied Connections - F5 BIG-IP TMOS	Displays all connections that have been denied by the F5 BIG-IP TMOS devices.
131	COBIT: Denied Outbound Connections - Juniper Firewall	Displays all outbound connections that have been denied by the Juniper Firewall.
132	COBIT: Denied VPN Connections - RADIUS	Displays all users denied access to the internal network by the RADIUS VPN.
133	COBIT: Domain activities on Symantec Endpoint Protection	Displays all domain activities on Symantec Endpoint Protection.
134	COBIT: DHCP Granted/ Renewed Activities on Microsoft DHCP	Displays all DHCP Granted/Renewed activities on Microsoft DHCP Server.
135	COBIT: DHCP Granted/ Renewed Activities on VMware vShield	Displays all DHCP Granted/Renewed activities on VMware vShield Edge.
136	COBIT: DNS Server Error	Displays all events when DNS Server has errors.
137	COBIT: Domains Sending the Most Email - Exchange 2000/2003	Displays the top domains sending email.
138	COBIT: Email Recipients Receiving the Most Emails by Count - Exchange 2000/2003	Displays the email recipients who receiving the most emails by count.
139	COBIT: Email Recipients Receiving the Most Emails by Count - Exchange 2007/10	Displays the email recipients who receiving the most emails by count.
140	COBIT: Email Recipients Receiving the Most Emails by Size - Exchange 2000/2003	Displays the email recipients who received the most emails by mail size.

Serial Number	TIBCO LogLogic Report	Description
141	COBIT: Email Senders Sending the Most Emails by Count - Exchange 2000/2003	Displays the email senders who sent the most emails by count.
142	COBIT: Email Senders Sending the Most Emails by Count - Exchange 2007/10	Displays the email senders who sent the most emails by count.
143	COBIT: Email Senders Sending the Most Emails by Size - Exchange 2000/2003	Displays the email senders who sent the most emails by mail size.
144	COBIT: Email Senders Sending the Most Emails by Size - Exchange 2007/10	Displays the email senders who sent the most emails by mail size.
145	COBIT: Email Source IP Sending To Most Recipients	Displays IP addresses that are sending to the most recipients using Exchange 2007/10.
146	COBIT: Escalated Privilege Activities on Servers	Displays all privilege escalation activities performed on servers to ensure appropriate access.
147	COBIT: ESX Accounts Activities	Displays all accounts activities on VMware ESX servers to ensure authorized and appropriate access.
148	COBIT: ESX Accounts Created	Displays all accounts created on VMware ESX servers to ensure authorized and appropriate access.
149	COBIT: ESX Accounts Deleted	Displays all accounts deleted on VMware ESX servers to ensure authorized and appropriate access.
150	COBIT: ESX Failed Logins	Failed VMware ESX logins for known user.
151	COBIT: ESX Group Activities	Displays all group activities on VMware ESX servers to ensure authorized and appropriate access.
152	COBIT: ESX Kernel log daemon terminating	Displays all VMware ESX Kernel log daemon terminating.
153	COBIT: ESX Kernel logging Stop	Displays all VMware ESX Kernel logging stops.
154	COBIT: ESX Logins Failed Unknown User	Failed VMware ESX logins for unknown user.
155	COBIT: ESX Logins Succeeded	Displays successful logins to VMware ESX to ensure only authorized personnel have access.
156	COBIT: ESX Syslogd Restart	Displays all VMware ESX syslogd restarts.

Serial Number	TIBCO LogLogic Report	Description
157	COBIT: F5 BIG-IP TMOS Login Failed	Displays all F5 BIG-IP TMOS login events which have failed.
158	COBIT: F5 BIG-IP TMOS Login Successful	Displays all F5 BIG-IP TMOS login events which have succeeded.
159	COBIT: F5 BIG-IP TMOS Password Changes	Displays all password change activities on F5 BIG-IP TMOS to ensure authorized and appropriate access.
160	COBIT: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS has been restarted.
161	COBIT: Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
162	COBIT: Failed Windows Events Summary	Displays summary of all failed access-related Windows events.
163	COBIT: Files Accessed on NetApp Filer Audit	Displays all files accessed on NetApp Filer Audit to ensure appropriate access.
164	COBIT: Files Accessed on Servers	Displays all files accessed on servers to ensure appropriate access.
165	COBIT: Files Accessed through Juniper SSL VPN (Secure Access)	Displays all files accessed through Juniper SSL VPN (Secure Access).
166	COBIT: Files Accessed through PANOS	Displays all files accessed through Palo Alto Networks.
167	COBIT: Files Downloaded via Proxy	Displays all proxy-based downloads ensure authorized and appropriate access.
168	COBIT: Files Downloaded via Proxy - Cisco WSA	Displays all proxy-based downloads to ensure authorized and appropriate access on Cisco WSA.
169	COBIT: Files Downloaded via Proxy - Blue Coat Proxy	Displays all proxy-based downloads to ensure authorized and appropriate access on Blue Coat Proxy.
170	COBIT: Files Downloaded via Proxy - Microsoft IIS	Displays all proxy-based downloads to ensure authorized and appropriate access on Microsoft IIS.
171	COBIT: Files Downloaded via the Web	Displays all web-based downloads ensure authorized and appropriate access.
172	COBIT: Files Downloaded via t he Web - F5 BIG-IP TMOS	Displays all web-based downloads ensure authorized and appropriate access on F5 BIG-IP TMOS.

Serial Number	TIBCO LogLogic Report	Description
173	COBIT: Files Downloaded via t he Web - Microsoft IIS	Displays all web-based downloads ensure authorized and appropriate access on Microsoft IIS.
174	COBIT: Files Uploaded via Proxy	Displays all proxy-based uploads to ensure only authorized data can be uploaded.
175	COBIT: Files Uploaded via Proxy - Blue Coat Proxy	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Blue Coat Proxy.
176	COBIT: Files Uploaded via Proxy - Cisco WSA	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Cisco WSA.
177	COBIT: Files Uploaded via Proxy - Microsoft IIS	Displays all proxy-based uploads to ensure only authorized data can be uploaded on Microsoft IIS.
178	COBIT: Files Uploaded via the Web	Displays all web-based uploads to ensure only authorized data can be uploaded.
179	COBIT: Files Uploaded via the Web - F5 BIG-IP TMOS	Displays all web-based uploads to ensure only authorized data can be uploaded on F5 BIG-IP TMOS.
180	COBIT: Files Uploaded via the Web - Microsoft IIS	Displays all web-based uploads to ensure only authorized data can be uploaded on Microsoft IIS.
181	COBIT: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.
182	COBIT: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
183	COBIT: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
184	COBIT: FortiOS: Attacks by Event ID	Displays FortiOS attacks by Event ID.
185	COBIT: FortiOS: Attacks by Threat Name	Displays FortiOS attacks by threat name.
186	COBIT: FortiOS: Attacks Detected	Displays attacks detected by FortiOS.
187	COBIT: FortiOS DLP Attacks Detected	Displays all DLP attacks detected by FortiOS.
188	COBIT: Group Activities on NetApp Filer Audit	Displays all group activities on NetApp Filer Audit to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
189	COBIT: Group Activities on Symantec Endpoint Protection	Displays all group activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
190	COBIT: Group Activities on TIBCO ActiveMatrix Administrator	Displays all group activities on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
191	COBIT: Group Activities on UNIX Servers	Displays all group activities on UNIX servers to ensure authorized and appropriate access.
192	COBIT: Group Activities on Windows Servers	Displays all group activities on Windows servers to ensure authorized and appropriate access.
193	COBIT: Groups Created on NetApp Filer Audit	Displays all groups created on NetApp Filer Audit to ensure authorized and appropriate access.
194	COBIT: Groups Created on TIBCO ActiveMatrix Administrator	Displays all groups created on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
195	COBIT: Groups Created on UNIX Servers	Displays all groups created on UNIX servers to ensure authorized and appropriate access.
196	COBIT: Groups Created on Windows Servers	Displays all groups created on Windows servers to ensure authorized and appropriate access.
197	COBIT: Groups Deleted on NetApp Filer Audit	Displays all groups deleted on NetApp Filer Audit to ensure authorized and appropriate access.
198	COBIT: Groups Deleted on TIBCO ActiveMatrix Administrator	Displays all groups deleted on TIBCO ActiveMatrix Administrator to ensure authorized and appropriate access.
199	COBIT: Groups Deleted on UNIX Servers	Displays all groups deleted on UNIX servers to ensure authorized and appropriate access.
200	COBIT: Groups Deleted on Windows Servers	Displays all groups deleted on Windows servers to ensure authorized and appropriate access.
201	COBIT: Guardium SQL Guard Audit Configuration Changes	Displays all configuration changes on the Guardium SQL Guard Audit database.
202	COBIT: Guardium SQL Guard Audit Data Access	Displays all select statements made on Guardium SQL Audit Server.
203	COBIT: Guardium SQL Guard Audit Logins	Displays all login attempts to the Guardium SQL Server Audit database.
204	COBIT: Guardium SQL Guard Audit Startup or Shutdown	Displays all startup and shutdown events on Guardium SQL Audit Server.

Serial Number	TIBCO LogLogic Report	Description
205	COBIT: Guardium SQL Guard Configuration Changes	Displays all configuration changes on the Guardium SQL Guard database.
206	COBIT: Guardium SQL Guard Data Access	Displays all select statements made on Guardium SQL Server.
207	COBIT: Guardium SQL Guard Logins	Displays all login attempts to the Guardium SQL Server database.
208	COBIT: Guardium SQL Guard Startup or Shutdown	Displays all startup and shutdown events on Guardium SQL Server.
209	COBIT: HP NonStop Audit Configuration Changes	Displays all audit configuration changes on HP NonStop.
210	COBIT: HP NonStop Audit Login Failed	Displays all HP NonStop Audit login events which have failed.
211	COBIT: HP NonStop Audit Login Successful	Displays all HP NonStop Audit login events which have succeeded.
212	COBIT: HP NonStop Audit Object Access	Displays HP NonStop Audit events related to object access.
213	COBIT: HP NonStop Audit Object Changes	Displays HP NonStop Audit events related to object changes.
214	COBIT: HP NonStop Audit Permissions Changed	Displays all permission modification activities on HP NonStop Audit to ensure authorized access.
215	COBIT: Files Accessed through Pulse Connect Secure	Displays all files accessed through Pulse Connect Secure.
216	COBIT: i5/OS Access Control List Modifications	Displays i5/OS events related to access control list modification.
217	COBIT: i5/OS Audit Configuration Changes	Displays all audit configuration changes on i5/OS.
218	COBIT: i5/OS DST Password Reset	Displays i5/OS events related to the reset of the DST (Dedicated Service Tools) password.
219	COBIT: i5/OS Internet Security Management Events	Displays i5/OS events related to Internet Security Management (IPSec/VPN).
220	COBIT: i5/OS Key Ring File Events	Displays i5/OS key ring file events (cryptographic key management).
221	COBIT: i5/OS Network Authentication Events	Displays i5/OS network authentication events.

Serial Number	TIBCO LogLogic Report	Description
222	COBIT: i5/OS Object Access	Displays i5/OS events related to object access.
223	COBIT: i5/OS Object Creation and Deletion	Displays i5/OS events related to object creation and deletion.
224	COBIT: i5/OS Restore Events	Displays i5/OS events related to object, program, and profile restoration.
225	COBIT: i5/OS Server Security User Information Actions	Displays i5/OS events related to server security user information actions.
226	COBIT: i5/OS System Management Changes	Displays i5/OS events related to system management changes.
227	COBIT: i5/OS User Profile Creation, Modification, or Restoration	Displays i5/OS events related to user profile creation, modification, or restoration.
228	COBIT: Juniper Firewall Escalated Privilege	Displays events related to users having escalated privileges in the Juniper Firewall.
229	COBIT: Juniper Firewall Policy Changed	Displays all configuration changes to the Juniper Firewall policies.
230	COBIT: Juniper Firewall Reset Accepted	Displays events that indicate the Juniper Firewall has been reset to its factory default state.
231	COBIT: Juniper Firewall Reset Imminent	Displays events that indicate the Juniper Firewall will be reset to its factory default state.
232	COBIT: Juniper Firewall Restart ed	Displays all Juniper Firewall restart events.
233	COBIT: Juniper Firewall VPN Tunnel Status Change	Displays events when the Juniper Firewall VPN Tunnel is setup or taken down.
234	COBIT: Juniper SSL VPN Successful Logins	Displays successful connections through the Juniper SSL VPN.
235	COBIT: Juniper SSL VPN (Secure Access) Policy Changed	Displays all configuration changes to the Juniper SSL VPN (Secure Access) policies.
236	COBIT: Juniper SSL VPN (Secure Access) Successful Logins	Displays all successfull logins through the Juniper SSL VPN (Secure Access).
237	COBIT: Last Activities Performed by Administrators	Displays the latest activities performed by administrators and root users to ensure appropriate access.

Serial Number	TIBCO LogLogic Report	Description
238	COBIT: Last Activities Performed by All Users	Displays the latest activities performed by all users to ensure appropriate access.
239	COBIT: Logins by Authentication Type	Displays all logins categorized by the authentication type.
240	COBIT: LogLogic DSM Configuration Changes	Displays all configuration changes on the LogLogic DSM database.
241	COBIT: LogLogic DSM Data Access	Displays all select statements made on LogLogic DSM database.
242	COBIT: LogLogic DSM Logins	Displays all login attempts to the LogLogic DSM database.
243	COBIT: LogLogic DSM Startup or Shutdown	Displays all startup and shutdown events on LogLogic DSM database.
244	COBIT: LogLogic File Retrieval Errors	Displays all errors while retrieving log files from devices, servers and applications.
245	COBIT: LogLogic Management Center Account Activities	Displays all accounts activities on LogLogic management center to ensure authorized and appropriate access.
246	COBIT: LogLogic Management Center Backup Activities	Displays all backup activities on LogLogic management center.
247	COBIT: LogLogic Management Center Login	Displays all login events to the LogLogic management center.
248	COBIT: LogLogic Management Center Password Changes	Displays all password change activities on LogLogic management center to ensure authorized and appropriate access.
249	COBIT: LogLogic Management Center Restore Activities	Displays all restore activities on LogLogic management center.
250	COBIT: LogLogic Management Center Upgrade Success	Displays all successful events related to the system's upgrade.
251	COBIT: LogLogic Message Routing Errors	Displays all log forwarding errors on the LogLogic appliance to ensure all logs are archived properly.
252	COBIT: LogLogic Universal Collector Configuration Changes	Displays LogLogic universal collector configuration changes.
253	COBIT: McAfee AntiVirus: Atta cks by Event ID	Displays McAfee AntiVirus attacks by Event ID.

Serial Number	TIBCO LogLogic Report	Description
254	COBIT: McAfee AntiVirus: Atta cks by Threat Name	Displays McAfee AntiVirus attacks by threat name.
255	COBIT: McAfee AntiVirus: Atta cks Detected	Displays attacks detected by McAfee AntiVirus.
256	COBIT: Microsoft Operations Manager - Failed Windows Events	Displays summary of all failed access-related Windows events.
257	COBIT: Microsoft Operations Manager - Windows Accounts Activities	Displays all accounts activities on Windows servers to ensure authorized and appropriate access.
258	COBIT: Microsoft Operations Manager - Windows Accounts Changed	Displays all accounts changed on Windows servers to ensure authorized and appropriate access.
259	COBIT: Microsoft Operations Manager - Windows Accounts Created	Displays all accounts created on Windows servers to ensure authorized and appropriate access.
260	COBIT: Microsoft Operations Manager - Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
261	COBIT: Microsoft Operations Manager - Windows Events by Users	Displays a summary of access-related Windows events by source and target users.
262	COBIT: Microsoft Operations Manager - Windows Events Summary	Displays a summary of access-related Windows events by count.
263	COBIT: Microsoft Operations Manager - Windows Password Changes	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
264	COBIT: Microsoft Operations Manager - Windows Permissions Modified	Displays all permission modification activities on Windows servers to ensure authorized access.
265	COBIT: Microsoft Operations Manager - Windows Policies Modified	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
266	COBIT: Microsoft Operations Manager - Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.

Serial Number	TIBCO LogLogic Report	Description
267	COBIT: Microsoft Sharepoint Content Deleted	Displays all events when content has been deleted from Microsoft Sharepoint.
268	COBIT: Microsoft Sharepoint Content Updates	Displays all events when content is updated within Microsoft Sharepoint.
269	COBIT: Microsoft Sharepoint Permissions Changed	Displays all user/group permission events to Microsoft Sharepoint.
270	COBIT: Microsoft Sharepoint Policy Add, Remove, or Modify	Displays all events when a Microsoft Sharepoint policy is added, removed, or modified.
271	COBIT: Microsoft SQL Server Backup Failed	Displays all Microsoft SQL Server backup failures.
272	COBIT: Microsoft SQL Server Configuration Changes	Displays Microsoft SQL database configuration changes.
273	COBIT: Microsoft SQL Server Data Access	Displays data access events on Microsoft SQL Server databases.
274	COBIT: Microsoft SQL Server Database Failed Logins	Displays failed Microsoft SQL Server database logins.
275	COBIT: Microsoft SQL Server Database Successful Logins	Displays successful Microsoft SQL Server database logins.
276	COBIT: Microsoft SQL Server Database Permission Events	Displays events related to Microsoft SQL Server database permission modifications.
277	COBIT: Microsoft SQL Server Database User Additions and Deletions	Displays Microsoft SQL Server events related to creation and deletion of database users.
278	COBIT: Microsoft SQL Server Password Changes	Displays password changes for Microsoft SQL Server database accounts.
279	COBIT: Microsoft SQL Server Restore Failed	Displays all Microsoft SQL Server restore failure events.
280	COBIT: Microsoft SQL Server Schema Corruption	Displays all schema corruption events on Microsoft SQL Server databases.
281	COBIT: Microsoft SQL Server Shutdown by Reason	Displays all Microsoft SQL Server shutdown events by reason.
282	COBIT: Most Active Email Sen ders - Exchange 2000/2003	Displays the most active email senders based on activity.
283	COBIT: Most Active Ports Through Firewall - Check Point	Displays the most active ports used through the Check Point firewall.

Serial Number	TIBCO LogLogic Report	Description
284	COBIT: Most Active Ports Through Firewall - Cisco ASA	Displays the most active ports used through the Cisco ASA firewall.
285	COBIT: Most Active Ports Through Firewall - Cisco FWSM	Displays the most active ports used through the Cisco FWSM firewall.
286	COBIT: Most Active Ports Through Firewall - Cisco PIX	Displays the most active ports used through the Cisco PIX firewall.
287	COBIT: Most Active Ports Through Firewall - Fortinet	Displays the most active ports used through the Fortinet firewall.
288	COBIT: Most Active Ports Through Firewall - Juniper Firewall	Displays the most active ports used through the Juniper firewall.
289	COBIT: Most Active Ports Through Firewall - Nortel	Displays the most active ports used through the Nortel firewall.
290	COBIT: Most Used Mail Commands - Exchange 2000/2003	Displays the most used email protocol commands on Microsoft Exchange servers.
291	COBIT: NetApp Filer Audit Accounts Enabled	Displays all accounts enabled on NetApp Filer Audit to ensure authorized and appropriate access.
292	COBIT: NetApp Filer Audit Group Members Added	Displays all accounts added to groups on the NetApp Filer Audit to ensure appropriate access.
293	COBIT: NetApp Filer Audit Group Members Deleted	Displays all accounts removed from groups on the NetApp Filer Audit to ensure appropriate access.
294	COBIT: NetApp Filer Audit Logs Cleared	Displays all audit logs clearing activities on NetApp Filer Audit to detect access violations or unusual activity.
295	COBIT: NetApp Filer Audit Login Failed	Displays all NetApp Filer Audit Login events which have failed.
296	COBIT: NetApp Filer Audit Login Successful	Displays all NetApp Filer Audit Login events which have succeeded.
297	COBIT: NetApp Filer Audit Policies Modified	Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access.
298	COBIT: NetApp Filer Snapshot Error	Displays events that indicate backup on the NetApp Filer has failed.

Serial Number	TIBCO LogLogic Report	Description
299	COBIT: NetApp Filer File Activity	Displays all file activities on NetApp Filer.
300	COBIT: NetApp Filer Login Failed	Displays all NetApp Filer Login events which have failed.
301	COBIT: NetApp Filer Login Successful	Displays all NetApp Filer Login events which have succeeded.
302	COBIT: NetApp Filer Password Changes	Displays all password change activities on NetApp Filer to ensure authorized and appropriate access.
303	COBIT: Network Traffic per Rule - Check Point	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
304	COBIT: Network Traffic per Rule - Juniper Firewall	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
305	COBIT: Network Traffic per Rule - Nortel	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
306	COBIT: Oracle Database Configuration Changes	Displays Oracle database configuration changes.
307	COBIT: Oracle Database Data Access	Displays data access events on Oracle databases.
308	COBIT: Oracle Database Failed Logins	Displays all failed login attempts to the Oracle database.
309	COBIT: Oracle Database Successful Logins	Displays successful Oracle database logins.
310	COBIT: Oracle Database Permission Events	Displays events related to Oracle Server database role and privilege management.
311	COBIT: Oracle Database Shutdown	Displays Oracle database events related to shutting down the server.
312	COBIT: Oracle Database User Additions and Deletions	Displays Oracle database events related to creation and deletion of database users.
313	COBIT: PANOS: Attacks by Event ID	Displays Palo Alto Networks attacks by Event ID.
314	COBIT: PANOS: Attacks by Threat Name	Displays Palo Alto Networks attacks by threat name.
315	COBIT: PANOS: Attacks Detected	Displays attacks detected by Palo Alto Networks.

Serial Number	TIBCO LogLogic Report	Description
316	COBIT: Password Changes on Windows Servers	Displays all password change activities on Windows servers to ensure authorized and appropriate access.
317	COBIT: Peer Servers and Status	Displays all web servers providing data for cache servers and the status of requests.
318	COBIT: Peer Servers and Status - Cisco WSA	Displays all web servers providing data for cache servers and the status of requests on Cisco WSA.
319	COBIT: Peer Servers and Status - Blue Coat Proxy	Displays all web servers providing data for cache servers and the status of requests on Blue Coat Proxy.
320	COBIT: Peer Servers and Status - Microsoft IIS	Displays all web servers providing data for cache servers and the status of requests on Microsoft IIS.
321	COBIT: Periodic Review of Log Reports	Displays all review activities performed by administrators to ensure review for any access violations.
322	COBIT: Periodic Review of User Access Logs	Displays all review activities performed by administrators to ensure review for any access violations.
323	COBIT: Permissions Modified on Windows Servers	Displays all permission modification activities on Windows Servers to ensure authorized access.
324	COBIT: Policies Modified on Windows Servers	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
325	COBIT: Ports Allowed Access - Check Point	Displays all connections passed through the Check Point by port.
326	COBIT: Ports Allowed Access - Cisco ASA	Displays all connections passed through the Cisco ASA by port.
327	COBIT: Ports Allowed Access - Cisco IOS	Displays all connections passed through the Cisco IOS by port.
328	COBIT: Ports Allowed Access - Cisco FWSM	Displays all connections passed through the Cisco FWSM by port.
329	COBIT: Ports Allowed Access - Cisco Netflow	Displays all connections passed through the Cisco Netflow by port.
330	COBIT: Ports Allowed Access - Cisco PIX	Displays all connections passed through the Cisco PIX by port.
331	COBIT: Ports Allowed Access - F5 BIG-IP TMOS	Displays all connections passed through the F5 BIG-IP TMOS by port.

Serial Number	TIBCO LogLogic Report	Description
332	COBIT: Ports Allowed Access - Fortinet	Displays all connections passed through the Fortinet by port.
333	COBIT: Ports Allowed Access - Juniper Firewall	Displays all connections passed through the Juniper Firewall by port.
334	COBIT: Ports Allowed Access - Juniper JunOS	Displays all connections passed through the Juniper JunOS by port.
335	COBIT: Ports Allowed Access - Juniper RT Flow	Displays all connections passed through the Juniper RT Flow by port.
336	COBIT: Ports Allowed Access - Nortel	Displays all connections passed through the Nortel by port.
337	COBIT: Ports Allowed Access - PANOS	Displays all connections passed through the Palo Alto Networks by port.
338	COBIT: Ports Allowed Access - Sidewinder	Displays all connections passed through the Sidewinder by port.
339	COBIT: Ports Allowed Access - VMware vShield	Displays all connections passed through the VMware vShield by port.
340	COBIT: Ports Denied Access - Check Point	Displays the applications that have been denied access the most by the Check Point.
341	COBIT: Ports Denied Access - Cisco ASA	Displays the applications that have been denied access the most by the Cisco ASA.
342	COBIT: Ports Denied Access - Cisco FWSM	Displays the applications that have been denied access the most by the Cisco FWSM.
343	COBIT: Ports Denied Access - Cisco IOS	Displays the applications that have been denied access the most by the Cisco IOS.
344	COBIT: Ports Denied Access - Cisco PIX	Displays the applications that have been denied access the most by the Cisco PIX.
345	COBIT: Ports Denied Access - Cisco Router	Displays the applications that have been denied access the most by the Cisco Router.
346	COBIT: Ports Denied Access - F5 BIG-IP TMOS	Displays the applications that have been denied access the most by the F5 BIG-IP TMOS.
347	COBIT: Ports Denied Access - Fortinet	Displays the applications that have been denied access the most by the Fortinet.
348	COBIT: Ports Denied Access - Juniper Firewall	Displays the applications that have been denied access the most by the Juniper Firewall.

Serial Number	TIBCO LogLogic Report	Description
349	COBIT: Ports Denied Access - Juniper JunOS	Displays the applications that have been denied access the most by the Juniper JunOS.
350	COBIT: Ports Denied Access - Juniper RT Flow	Displays the applications that have been denied access the most by the Juniper RT Flow.
351	COBIT: Ports Denied Access - Nortel	Displays the applications that have been denied access the most by the Nortel.
352	COBIT: Ports Denied Access - PANOS	Displays the applications that have been denied access the most by the Palo Alto Networks.
353	COBIT: Ports Denied Access - Sidewinder	Displays the applications that have been denied access the most by the Sidewinder.
354	COBIT: Ports Denied Access - VMware vShield	Displays the applications that have been denied access the most by the VMware vShield Edge.
355	COBIT: Pulse Connect Secure Policy Changed	Displays all configuration changes to the Pulse Connect Secure policies.
356	COBIT: Pulse Connect Secure Successful Logins	Displays all successful logins through the Pulse Connect Secure.
357	COBIT: RACF Accounts Created	Displays all accounts created on RACF servers to ensure authorized and appropriate access.
358	COBIT: RACF Accounts Deleted	Displays all accounts deleted on RACF servers to ensure authorized and appropriate access.
359	COBIT: RACF Accounts Modified	Displays all events when a network user profile has been modified.
360	COBIT: RACF Failed Logins	Displays all failed login attempts to review any access violations or unusual activity.
361	COBIT: RACF Files Accessed	Displays all files accessed on RACF servers to ensure appropriate access.
362	COBIT: RACF Password Changed	Displays all password change activities on RACF servers to ensure authorized and appropriate access.
363	COBIT: RACF Permissions Changed	Displays all permission modification activities on RACF to ensure authorized access.
364	COBIT: RACF Process Started	Displays all processes started on the RACF servers.
365	COBIT: RACF Successful Logins	Displays successful logins to ensure only authorized personnel have access.

Serial Number	TIBCO LogLogic Report	Description
366	COBIT: Recipient Domains Experiencing Delay - Exchange 2000/2003	Displays the recipient domains that have experienced the most delivery delays.
367	COBIT: Root Logins	Displays root logins.
368	COBIT: Sender and Recipients Exchanging the Most Emails - Exchange 2000/2003	Displays the top email sender and recipient combinations.
369	COBIT: Sensors Generating Alerts	Displays the IDS sensors that generated the most alerts.
370	COBIT: Sensors Generating Ale rts - Cisco IOS	Displays the IDS sensors that generated the most alerts by Cisco IOS.
371	COBIT: Sensors Generating Alerts - FireEye MPS	Displays the IDS sensors that generated the most alerts by FireEye MPS.
372	COBIT: Sensors Generating Ale rts - SiteProtector	Displays the IDS sensors that generated the most alerts by SiteProtector.
373	COBIT: Sensors Generating Ale rts - Sourcefire Defense Center	Displays the IDS sensors that generated the most alerts by Sourcefire Defense Center.
374	COBIT: Servers Under Attack	Displays all servers under attack.
375	COBIT: Servers Under Attack - Cisco IOS	Displays all servers under attack by Cisco IOS.
376	COBIT: Servers Under Attack - HIPS	Displays all servers under attack.
377	COBIT: Servers Under Attack - FireEye MPS	Displays all servers under attack by FireEye MPS.
378	COBIT: Servers Under Attack - ISS SiteProtector	Displays all servers under attack by ISS SiteProtector.
379	COBIT: Servers Under Attack - SiteProtector	Displays all servers under attack by SiteProtector.
380	COBIT: Servers Under Attack - Sourcefire Defense Center	Displays all servers under attack by Sourcefire Defense Center.
381	COBIT: Sidewinder Configuration Changes	Displays Sidewinder configuration changes.
382	COBIT: Source IP Sending To Most Recipients - Exchange 2000/2003	Displays IP addresses that are sending to the most recipients.

Serial Number	TIBCO LogLogic Report	Description
383	COBIT: Source of Attacks	Displays the sources that have initiated the most attacks.
384	COBIT: Source of Attacks - Cisco IOS	Displays the sources that have initiated the most attacks by Cisco IOS.
385	COBIT: Source of Attacks - HIPS	Displays the sources that have initiated the most attacks.
386	COBIT: Source of Attacks - ISS SiteProtector	Displays the sources that have initiated the most attacks by ISS SiteProtector.
387	COBIT: Source of Attacks - FireEye MPS	Displays the sources that have initiated the most attacks by FireEye MPS.
388	COBIT: Source of Attacks - SiteProtector	Displays the sources that have initiated the most attacks by SiteProtector.
389	COBIT: Source of Attacks - Sourcefire Defense Center	Displays the sources that have initiated the most attacks by Sourcefire Defense Center.
390	COBIT: Successful Logins	Displays successful logins to ensure only authorized personnel have access.
391	COBIT: Sybase ASE Database Backup and Restoration	Displays Sybase ASE DUMP and LOAD events.
392	COBIT: Sybase ASE Database Configuration Changes	Displays configuration changes to the Sybase database.
393	COBIT: Sybase ASE Database Create Events	Displays Sybase ASE events involving the CREATE statement.
394	COBIT: Sybase ASE Database Data Access	Displays Sybase ASE events involving the SELECT statement.
395	COBIT: Sybase ASE Database Drop Events	Displays Sybase ASE events involving the DROP statement.
396	COBIT: Sybase ASE Database Startup or Shutdown	Displays all startup and shutdown events for the Sybase database.
397	COBIT: Sybase ASE Database User Additions and Deletions	Displays Sybase database events related to creation and deletion of database users.
398	COBIT: Sybase ASE Failed Logins	Displays failed Sybase ASE database logins.
399	COBIT: Sybase ASE Successful Logins	Displays successful Sybase ASE database logins.

Serial Number	TIBCO LogLogic Report	Description
400	COBIT: Symantec AntiVirus: At tacks by Threat Name	Displays Symantec AntiVirus attacks by threat name.
401	COBIT: Symantec AntiVirus: At tacks Detected	Displays attacks detected by Symantec AntiVirus.
402	COBIT: Symantec AntiVirus: Sc ans	Displays scans using Symantec AntiVirus.
403	COBIT: Symantec AntiVirus: U pdated	Displays updates to Symantec AntiVirus.
404	COBIT: Symantec Endpoint Protection: Attacks by Threat Name	Displays Symantec Endpoint Protection attacks by threat name.
405	COBIT: Symantec Endpoint Protection: Attacks Detected	Displays attacks detected by Symantec Endpoint Protection.
406	COBIT: Symantec Endpoint Protection Configuration Changes	Displays Symantec Endpoint Protection configuration changes.
407	COBIT: Symantec Endpoint Protection Password Changes	Displays all password change activities on Symantec Endpoint Protection to ensure authorized and appropriate access.
408	COBIT: Symantec Endpoint Protection Policy Add, Remove, or Modify	Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified.
409	COBIT: Symantec Endpoint Protection: Scans	Displays scans using Symantec Endpoint Protection.
410	COBIT: Symantec Endpoint Protection: Updated	Displays updates to Symantec Endpoint Protection.
411	COBIT: TIBCO ActiveMatrix Administrator Failed Logins	Displays all TIBCO ActiveMatrix Administrator login events which have failed.
412	COBIT: TIBCO ActiveMatrix Administrator Permission Changes	Displays events related to TIBCO ActiveMatrix Administrator permission modifications.
413	COBIT: TIBCO ActiveMatrix Administrator Successful Logins	Displays successful logins to TIBCO ActiveMatrix Administrator to ensure only authorized personnel have access.

Serial Number	TIBCO LogLogic Report	Description
414	COBIT: TIBCO Administrator Password Changes	Displays all password change activities on TIBCO Administrator to ensure authorized and appropriate access.
415	COBIT: TIBCO Administrator Permission Changes	Displays events related to TIBCO Administrator permission modifications.
416	COBIT: TrendMicro Control Manager: Attacks Detected	Displays attacks detected by TrendMicro Control Manager.
417	COBIT: TrendMicro Control Manager: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro Control Manager by threat name.
418	COBIT: TrendMicro OfficeScan: Attacks Detected	Displays attacks detected by TrendMicro OfficeScan.
419	COBIT: TrendMicro OfficeScan: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro OfficeScan by threat name.
420	COBIT: Tripwire Modifications, Additions, and Deletions	Displays system modifications, additions, and deletions detected by Tripwire.
421	COBIT: Trusted Domain Created on Windows Servers	Displays all trusted domains created on Windows servers to ensure authorized and appropriate access.
422	COBIT: Trusted Domain Deleted on Windows Servers	Displays all trusted domains deleted on Windows servers to ensure authorized and appropriate access.
423	COBIT: Unauthorized Logins	Displays all logins from unauthorized users to ensure appropriate access to data.
424	COBIT: Unencrypted Logins	Displays all unencrypted logins to ensure secure access to data.
425	COBIT: Unencrypted Network Services - Check Point	Displays Check Point firewall traffic containing unencrypted network services.
426	COBIT: Unencrypted Network Services - Cisco ASA	Displays Cisco ASA firewall traffic containing unencrypted network services.
427	COBIT: Unencrypted Network Services - Cisco FWSM	Displays Cisco FWSM firewall traffic containing unencrypted network services.
428	COBIT: Unencrypted Network Services - Cisco IOS	Displays Cisco IOS firewall traffic containing unencrypted network services.
429	COBIT: Unencrypted Network Services - Cisco Netflow	Displays Cisco Netflow traffic containing unencrypted network services.

Serial Number	TIBCO LogLogic Report	Description
430	COBIT: Unencrypted Network Services - Cisco PIX	Displays Cisco PIX firewall traffic containing unencrypted network services.
431	COBIT: Unencrypted Network Services - F5 BIG-IP TMOS	Displays F5 BIG-IP TMOS firewall traffic containing unencrypted network services.
432	COBIT: Unencrypted Network Services - Fortinet	Displays Fortinet firewall traffic containing unencrypted network services.
433	COBIT: Unencrypted Network Services - Juniper Firewall	Displays Juniper firewall traffic containing unencrypted network services.
434	COBIT: Unencrypted Network Services - Juniper JunOS	Displays Juniper JunOS firewall traffic containing unencrypted network services.
435	COBIT: Unencrypted Network Services - Juniper RT Flow	Displays Juniper RT Flow firewall traffic containing unencrypted network services.
436	COBIT: Unencrypted Network Services - Nortel	Displays Nortel firewall traffic containing unencrypted network services.
437	COBIT: Unencrypted Network Services - PANOS	Displays Palo Alto Networks firewall traffic containing unencrypted network services.
438	COBIT: Unencrypted Network Services - Sidewinder	Displays Sidewinder firewall traffic containing unencrypted network services.
439	COBIT: Unencrypted Network Services - VMware vShield	Displays VMware vShield firewall traffic containing unencrypted network services.
440	COBIT: UNIX Failed Logins	Displays failed UNIX logins for known and unknown users.
441	COBIT: Users Created on Servers	Displays all users created on servers to ensure authorized and appropriate access.
442	COBIT: Users Removed from Servers	Displays all users removed from servers to ensure timely removal of terminated users.
443	COBIT: Users Using the Proxies	Displays users who have been surfing the web through the proxy servers.
444	COBIT: Users Using the Proxies - Cisco WSA	Displays users who have been surfing the web through the proxy servers on Cisco WSA.
445	COBIT: Users Using the Proxies - Blue Coat Proxy	Displays users who have been surfing the web through the proxy servers on Blue Coat Proxy.
446	COBIT: Users Using the Proxies - Microsoft IIS	Displays users who have been surfing the web through the proxy servers on Microsoft IIS.

Serial Number	TIBCO LogLogic Report	Description
447	COBIT: vCenter Change Attributes	Modification of VMware vCenter and VMware ESX properties.
448	COBIT: vCenter Data Move	Entity has been moved within the VMware vCenter Infrastructure.
449	COBIT: vCenter Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter.
450	COBIT: vCenter Failed Logins	Failed logins to the VMware vCenter console.
451	COBIT: vCenter Modify Firewall Policy	Displays changes to the VMware ESX allowed services firewall policy.
452	COBIT: vCenter Orchestrator Change Attributes	Modification of VMware vCenter Orchestrator properties.
453	COBIT: vCenter Orchestrator Datastore Events	Displays create, modify, and delete datastore events on VMware vCenter Orchestrator.
454	COBIT: vCenter Orchestrator Data Move	Entity has been moved within the VMware vCenter Orchestrator Infrastructure.
455	COBIT: vCenter Orchestrator Failed Logins	Displays all failed logins for VMware vCenter Orchestrator.
456	COBIT: vCenter Orchestrator Virtual Machine Created	Virtual machine has been created from VMware vCenter Orchestrator.
457	COBIT: vCenter Orchestrator Virtual Machine Deleted	Virtual machine has been deleted from VMware vCenter Orchestrator.
458	COBIT: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
459	COBIT: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
460	COBIT: vCenter Orchestrator vSwitch Added, Changed or Removed	vSwitch has been added, modified or removed from VMware vCenter Orchestrator console.
461	COBIT: vCenter Resource Usage Change	Resources have changed on VMware vCenter.
462	COBIT: vCenter Restart ESX Services	VMware vCenter restarted services running on VMware ESX Server.
463	COBIT: vCenter Shutdown or Restart of ESX Server	VMware ESX Server is shutdown or restarted from VMware vCenter console.

Serial Number	TIBCO LogLogic Report	Description
464	COBIT: vCenter Successful Logins	Successful logins to the VMware vCenter console.
465	COBIT: vCenter User Permission Change	A permission role has been added, changed, removed, or applied to a user on VMware vCenter server.
466	COBIT: vCenter Virtual Machine Created	Virtual machine has been created from VMware vCenter console.
467	COBIT: vCenter Virtual Machine Deleted	Virtual machine has been deleted or removed from VMware vCenter console.
468	COBIT: vCenter Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter console.
469	COBIT: vCenter Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter console.
470	COBIT: vCenter vSwitch Added, Changed or Removed	vSwitch on VMware ESX server has been added, modified or removed from the VMware vCenter console.
471	COBIT: vCloud Failed Logins	Failed logins to the VMware vCloud Director console.
472	COBIT: vCloud Organization Created	VMware vCloud Director Organization created events.
473	COBIT: vCloud Organization Deleted	VMware vCloud Director Organization deleted events.
474	COBIT: vCloud Organization Modified	VMware vCloud Director Organization modified events.
475	COBIT: vCloud Successful Logins	Successful logins to the VMware vCloud Director console.
476	COBIT: vCloud User Created	VMware vCloud Director User created events.
477	COBIT: vCloud User Deleted or Removed	VMware vCloud Director users have been deleted or removed from the system.
478	COBIT: vCloud vApp Created, Modified, or Deleted	VMware vCloud Director vApp created, deleted, and modified events.
479	COBIT: vCloud vDC Created, Modified, or Deleted	VMware vCloud Director virtual datacenter created, modified, or deleted events.
480	COBIT: VPN Connection Average Bandwidth	Displays the average bandwidth for VPN connections.

Serial Number	TIBCO LogLogic Report	Description
481	COBIT: VPN Connection Average Duration	Displays the average duration of VPN connections.
482	COBIT: VPN Connections by Users	Displays users who are made the most connections.
483	COBIT: VPN Denied Connections by Users	Displays users with the most denied connections.
484	COBIT: VPN Connection Disconnect Reasons	Displays the disconnect reasons for VPN connections.
485	COBIT: VPN Sessions by Destination IPs	Displays all VPN sessions categorized by destination IP addresses.
486	COBIT: VPN Sessions by Source IPs	Displays all VPN sessions categorized by source IP addresses.
487	COBIT: VPN Sessions by Users	Displays all VPN sessions categorized by authenticated users.
488	COBIT: VPN Users Accessing Corporate Network	Displays all users logging into the corporate network via Virtual Private Network to ensure appropriate access.
489	COBIT: vShield Edge Configuration Changes	Displays changes to VMware vShield Edge policies.
490	COBIT: Web Access from All Users	Displays all web-based access by all users for regular reviews and updates.
491	COBIT: Web Access from All U sers - F5 BIG-IP TMOS	Displays all web-based access by all users for regular reviews and updates on F5 BIG-IP TMOS.
492	COBIT: Web Access from All Users - Fortinet	Displays all web-based access by all users for regular reviews and updates on Fortinet.
493	COBIT: Web Access from All Users - PANOS	Displays all web-based access by all users for regular reviews and updates on Palo Alto Networks.
494	COBIT: Web Access from All U sers - Microsoft IIS	Displays all web-based access by all users for regular reviews and updates on Microsoft IIS.
495	COBIT: Web Access to Applications	Displays all web-based access to applications to ensure appropriate and authorized access.
496	COBIT: Web Access to Applications - F5 BIG-IP TMOS	Displays all web-based access to applications to ensure appropriate and authorized access on F5 BIG-IP TMOS.

Serial Number	TIBCO LogLogic Report	Description
497	COBIT: Web Access to Applications - Fortinet	Displays all web-based access to applications to ensure appropriate and authorized access on Fortinet.
498	COBIT: Web Access to Applications - PANOS	Displays all web-based access to applications to ensure appropriate and authorized access on Palo Alto Networks.
499	COBIT: Web Access to Applications - Microsoft IIS	Displays all web-based access to applications to ensure appropriate and authorized access on Microsoft IIS.
500	COBIT: Web URLs Visited	Displays URLs that have been visited.
501	COBIT: Web URLs Visited - F5 BIG-IP TMOS	Displays URLs that have been visited on F5 BIG-IP TMOS.
502	COBIT: Web URLs Visited - Fortinet	Displays URLs that have been visited on Fortinet.
503	COBIT: Web URLs Visited - Microsoft IIS	Displays URLs that have been visited on Microsoft IIS.
504	COBIT: Web URLs Visited - PANOS	Displays URLs that have been visited on Palo Alto Networks.
505	COBIT: Web URLs Visited via Proxy	Displays URLs that have been visited via a proxy server.
506	COBIT: Web URLs Visited via Proxy - Blue Coat Proxy	Displays URLs that have been visited via a proxy server on Blue Coat Proxy.
507	COBIT: Web URLs Visited via Proxy - Cisco WSA	Displays URLs that have been visited via a proxy server on Cisco WSA.
508	COBIT: Web URLs Visited via Proxy - Microsoft IIS	Displays URLs that have been visited via a proxy server on Microsoft IIS.
509	COBIT: Windows Accounts Enabled	Displays all accounts enabled on Windows servers to ensure authorized and appropriate access.
510	COBIT: Windows Audit Logs Cleared	Displays all audit logs clearing activities on Windows servers to detect access violations or unusual activity.
511	COBIT: Windows Events by Users	Displays a summary of access-related Windows events by source and target users.
512	COBIT: Windows Events Summary	Displays a summary of access-related Windows events by count.

Serial Number	TIBCO LogLogic Report	Description
513	COBIT: Windows Group Members Added	Displays all accounts added to groups on the Windows servers to ensure appropriate access.
514	COBIT: Windows Group Members Deleted	Displays all accounts removed from groups on the Windows servers to ensure appropriate access.
515	COBIT: Windows New Services Installed	Displays a list of new services installed on Windows servers to ensure authorized access.
516	COBIT: Windows Programs Accessed	Displays all programs started and stopped on servers to ensure appropriate access.
517	COBIT: Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.
518	COBIT: Windows Software Update Activities	Displays all events related to the system's software or patch update.
519	COBIT: Windows Software Update Failures	Displays all failed events related to the system’s software or patch update.
520	COBIT: Windows Software Update Successes	Displays all successful events related to the system's software or patch update.

TIBCO LogLogic Alerts for Sarbanes-Oxley and COBIT 4.1

The following table lists the alerts included in the LogLogic® Compliance Suite - Sarbanes-Oxley Edition and COBIT 4.1.

Serial Number	TIBCO LogLogic Alert	Description
1	COBIT: Accounts Created	Alerts when a new account is created on servers.
2	COBIT: Accounts Deleted	Alerts when an account is deleted on servers.
3	COBIT: Accounts Enabled	Alerts when an account has been enabled on servers.
4	COBIT: Accounts Locked	Alerts when an account has been locked on servers.
5	COBIT: Accounts Modified	Alerts when an account is modified on servers.
6	COBIT: Active Directory Changes	Alerts when changes are made within Active Directory.
7	COBIT: Allowed Connections	Allowed firewall connections.
8	COBIT: Check Point Policy Changed	Alerts when a Check Point firewall's policy has been modified.

Serial Number	TIBCO LogLogic Alert	Description
9	COBIT: Cisco ISE, ACS Configuration Changed	Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS.
10	COBIT: Cisco ISE, ACS Passwords Changed	Alerts when a user changes their password via Cisco ISE or Cisco SecureACS.
11	COBIT: Cisco PIX, ASA, FWSM Commands Executed	Alerts when a Cisco PIX, ASA, or FWSM commands are executed.
12	COBIT: Cisco PIX, ASA, FWSM Failover Disabled	Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled.
13	COBIT: Cisco PIX, ASA, FWSM Failover Errors	Alerts when an error has occurred during PIX, ASA, or FWSM failover.
14	COBIT: Cisco PIX, ASA, FWSM Failover Performed	Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices.
15	COBIT: Cisco PIX, ASA, FWSM Fragment Database Limit	The fragment database count has been reached on Cisco PIX, ASA, or FWSM devices.
16	COBIT: Cisco PIX, ASA, FWSM Logon Failure	Login failure attempts to the Cisco PIX, ASA, or FWSM devices.
17	COBIT: Cisco PIX, ASA, FWSM Logon Success	Successful login attempts to the Cisco PIX, ASA, or FWSM Firewall.
18	COBIT: Cisco PIX, ASA, FWSM NAT Failure	Failures in Network Address Translation (NAT) on the Cisco PIX, ASA, or FWSM.
19	COBIT: Cisco PIX, ASA, FWSM Policy Changed	Alerts when a Cisco PIX, ASA, or FWSM firewall policy has been modified.
20	COBIT: Cisco PIX, ASA, FWSM Protocol Failure	Alerts when possible network protocol failures on the Cisco PIX, ASA, or FWSM devices.
21	COBIT: System Restarted	Alerts when system has been restarted
22	COBIT: Cisco PIX, ASA, FWSM Routing Failure	Alerts when routing failure occurred in the Cisco PIX, ASA, or FWSM devices.
23	COBIT: Cisco PIX, ASA, FWSM Shun Added	Alerts when a shun rule has been added to the PIX, ASA, or FWSM configuration.
24	COBIT: Cisco PIX, ASA, FWSM Shun Deleted	Alerts when a shun rule has been removed from the PIX, ASA, or FWSM configuration.
25	COBIT: Cisco PIX, ASA, FWSM VPN Tunnel Creation	A VPN tunnel has been created on the Cisco PIX, ASA, or FWSM devices.

Serial Number	TIBCO LogLogic Alert	Description
26	COBIT: Cisco PIX, ASA, FWSM VPN Tunnel Teardown	Alerts when a VPN tunnel has been removed on the Cisco PIX, ASA, or FWSM devices.
27	COBIT: Cisco Switch Card Insert	Alerts when a card module is inserted into a switch.
28	COBIT: Cisco Switch Device Reload	Alerts when a command to reload a Cisco switch has been executed.
29	COBIT: Cisco Switch Device Restart	Alerts when a router or switch has been rebooted.
30	COBIT: Cisco Switch HA Failure (ver)	Alerts when a HA setup has version incompatibility issues.
31	COBIT: Cisco Switch Interface Change	Alerts when network interfaces are going up or down.
32	COBIT: Cisco Switch Interface Down	Alerts when Cisco switch interface is going down.
33	COBIT: Cisco Switch Interface Up	Alerts when the Cisco switch interface is back up.
34	COBIT: Cisco Switch Policy Changed	Alerts when Cisco router or switch configuration has been modified.
35	COBIT: DB2 Database Backup Failed	Alerts when a DB2 database backup fails.
36	COBIT: DB2 Database Configuration Change	Alerts when a configuration is changed on a DB2 database.
37	COBIT: DB2 Database Restore Failed	Alerts when a database restore fails on a DB2 database.
38	COBIT: DB2 Database Started or Stopped	Alerts when a DB2 database is started or stopped.
39	COBIT: DB2 Database User Added or Dropped	Alerts when a user is added or dropped from a DB2 database.
40	COBIT: Disallowed Services	Disallowed firewall services.
41	COBIT: DNS Server Shutdown	Alerts when DNS Server has been shutdown.
42	COBIT: DNS Server Started	Alerts when DNS Server has been started.
43	COBIT: Excessive IDS Attack	IDS anomalies using message volume threshold alerts.

Serial Number	TIBCO LogLogic Alert	Description
44	COBIT: Group Members Added	Alerts when new members are added to user groups.
45	COBIT: Group Members Deleted	Alerts when members are removed from user groups.
46	COBIT: Groups Created	Alerts when new user groups are created.
47	COBIT: Groups Deleted	Alerts when a user group is deleted.
48	COBIT: Groups Modified	Alerts when a user group has been modified.
49	COBIT: Guardium SQL Guard Config Changes	Alerts when a configuration is changed on Guardium SQL Database.
50	COBIT: Guardium SQL Guard Data Access	Alerts when a select statement is made on Guardium SQL Database.
51	COBIT: Guardium SQL Guard Logins	Alerts when a user logs into the Guardium SQL Database.
52	COBIT: Guardium SQL Guard Startup or Shutdown	Alerts when the Guardium SQL Database is started or stopped.
53	COBIT: HP NonStop Audit Configuration Changed	Alerts when configuration changes are made to the HP NonStop Audit.
54	COBIT: HP NonStop Audit Permission Changed	Alerts on HP NonStop Audit permission changed events.
55	COBIT: i5/OS Network Profile Changes	Alerts when any changes are made to an i5/OS network profile.
56	COBIT: i5/OS Permission or Policy Change	Alerts when policies or permissions are changed on the i5/OS.
57	COBIT: i5/OS Server or Service Status Change	Alerts when the i5/OS is restarted or a service stops or starts.
58	COBIT: i5/OS Software Updates	Alerts when events related to the i5/OS software updates.
59	COBIT: i5/OS User Profile Changes	Alerts when a user profile is changed on the i5/OS.
60	COBIT: IBM AIX Password Changed	Alerts when an account password is changed on IBM AIX servers.
61	COBIT: Juniper Firewall HA State Change	Alerts when Juniper Firewall has changed its failover state.

Serial Number	TIBCO LogLogic Alert	Description
62	COBIT: Juniper Firewall Logon Failure	Login failure attempts to the Juniper Firewall.
63	COBIT: Juniper Firewall Logon Success	Successful login attempts to the Juniper Firewall.
64	COBIT: Juniper Firewall Peer Missing	Alerts when a Juniper Firewall HA peer is missing.
65	COBIT: Juniper Firewall Policy Changes	Alerts when Juniper Firewall configuration is changed.
66	COBIT: Juniper Firewall Policy Out of Sync	Alerts when the Juniper Firewall's policy is out of sync.
67	COBIT: Juniper Firewall System Reset	Alerts when the Juniper Firewall has been reset to system default.
68	COBIT: Juniper VPN Policy Change	Alerts when Juniper VPN policy or configuration change.
69	COBIT: Logins Failed	Alerts when login failures are over the defined threshold.
70	COBIT: Logins Succeeded	Alerts when successful logins are over the defined threshold.
71	COBIT: LogLogic Disk Full	Alerts when the LogLogic appliance’s disk is near full.
72	COBIT: LogLogic DSM Configuration Changes	Alerts when a configuration is changed on LogLogic DSM database.
73	COBIT: LogLogic DSM Data Access	Alerts when a select statement is made on LogLogic DSM database.
74	COBIT: LogLogic DSM Logins	Alerts when a user logs into the LogLogic DSM database.
75	COBIT: LogLogic DSM Startup or Shutdown	Alerts when the LogLogic DSM database is started or stopped.
76	COBIT: LogLogic File Retrieval Errors	Alerts when problems are detected during log file retrieval.
77	COBIT: LogLogic Management Center Backed Up or Restored	Alerts on backup and restore events to the LogLogic management center.
78	COBIT: LogLogic Management Center Passwords Changed	Alerts when users have changed their passwords.

Serial Number	TIBCO LogLogic Alert	Description
79	COBIT: LogLogic Management Center Upgrade Succeeded	Alerts for successful events related to the system's upgrade.
80	COBIT: LogLogic Message Routing Errors	Alerts when problems are detected during message forwarding.
81	COBIT: LogLogic Universal Collector Configuration Changed	Alerts when configuration changes are made to the LogLogic universal collector.
82	COBIT: Microsoft Operations Manager - Permissions Changed	Alerts when user or group permissions have been changed.
83	COBIT: Microsoft Operations Manager - Windows Passwords Changed	Alerts when users have changed their passwords.
84	COBIT: Microsoft Operations Manager - Windows Policies Changed	Alerts when Windows policies changed.
85	COBIT: Microsoft Operations Manager- Windows Server Restarted	Alerts when a Windows server has been restarted.
86	COBIT: Microsoft Sharepoint Content Deleted	Alerts on Microsoft Sharepoint content deleted events.
87	COBIT: Microsoft Sharepoint Content Updated	Alerts on Microsoft Sharepoint content updated events.
88	COBIT: Microsoft Sharepoint Permission Changed	Alerts on Microsoft Sharepoint permission changed events.
89	COBIT: Microsoft Sharepoint Policies Added, Removed, Modified	Alerts on Microsoft Sharepoint policy additions, deletions, and modifications.
90	COBIT: Microsoft SQL Server Backup Failed	Alerts when Microsoft SQL Server backup process has failed.
91	COBIT: Microsoft SQL Server Restore Failed	Alerts when Microsoft SQL Server restore process failed.
92	COBIT: Microsoft SQL Server Shutdown	Alerts when Microsoft SQL Server has been shutdown.
93	COBIT: Neoteris Files Accessed	Identifies all files being accessed through the Juniper SSL VPN.

Serial Number	TIBCO LogLogic Alert	Description
94	COBIT: NetApp Authentication Failure	Alerts when NetApp authentication failure events occur.
95	COBIT: NetApp Bad File Handle	Alerts when a bad file handle is detected on a NetApp device.
96	COBIT: NetApp Bootblock Update	Alerts when the bootblock has been updated on a NetApp Filer.
97	COBIT: NetApp Filer Audit Policies Changed	Alerts when NetApp Filer Audit policies changed.
98	COBIT: NetApp Filer Disk Failure	Alerts when a disk fails on a NetApp Filer.
99	COBIT: NetApp Filer Disk Inserted	Alerts when a disk is inserted into the NetApp Filer.
100	COBIT: NetApp Filer Disk Missing	Alerts when a disk is missing on the NetApp Filer device.
101	COBIT: NetApp Filer Disk Pulled	Alerts when a RAID disk has been pulled from the Filer device.
102	COBIT: NetApp Filer Disk Scrub Suspended	Alerts when the disk scrubbing process has been suspended.
103	COBIT: NetApp Filer File System Full	Alerts when the file system is full on the NetApp Filer device.
104	COBIT: NetApp Filer NIS Group Update	Alerts when the NIS group has been updated on the Filer device.
105	COBIT: NetApp Filer Snapshot Error	Alerts when an error has been detected during a NetApp Filer snapshot.
106	COBIT: NetApp Filer Unauthorized Mounting	Alerts when an unauthorized mount event occurs.
107	COBIT: Oracle Database Configuration Change	Alerts when a ALTER or UPDATE command is executed on Oracle DB’s.
108	COBIT: Oracle Database Data Access	Alerts when Oracle tables are accessed.
109	COBIT: Oracle Database Permissions Changed	Alerts when permissions are changed on Oracle databases.
110	COBIT: Oracle Database Shutdown	Alerts when an Oracle database is shutdown.

Serial Number	TIBCO LogLogic Alert	Description
111	COBIT: Oracle Database User Added or Deleted	Alerts when a user is added or deleted from an Oracle database.
112	COBIT: Policy Violation	Firewall policy violations.
113	COBIT: Pulse Connect Secure Policy Change	Alerts when Pulse Connect Secure Policy or configuration changes.
114	COBIT: RACF Files Accessed	Alerts when files are accessed on the RACF servers.
115	COBIT: RACF Passwords Changed	Alerts when users have changed their passwords.
116	COBIT: RACF Permissions Changed	Alerts when user or group permissions have been changed.
117	COBIT: RACF Process Started	Alerts whenever a process is run on a RACF server.
118	COBIT: Sidewinder Configuration Changed	Alerts when configuration changes are made to the Sidewinder.
119	COBIT: Sybase ASE Database Backed Up or Restored	Alerts on backup and restore events to the Sybase ASE Database.
120	COBIT: Sybase ASE Database Config Changes	Alerts on Sybase ASE Database configuration change events.
121	COBIT: Sybase ASE Database Data Access	Alerts on Sybase ASE Database data access events.
122	COBIT: Sybase ASE Database Started	Alerts on Sybase ASE Database start events.
123	COBIT: Sybase ASE Database Stopped	Alerts on Sybase ASE Database stop events.
124	COBIT: Symantec Endpoint Protection Configuration Changed	Alerts when configuration changes are made to the Symantec Endpoint Protection.
125	COBIT: Symantec Endpoint Protection Policy Add, Delete, Modify	Alerts on Symantec Endpoint Protection additions, deletions, and modifications.
126	COBIT: System Anomalies	Detects and alerts any anomalies based on past log patterns.
127	COBIT: System Restarted	Alerts when systems such as routers and switches have restarted.

Serial Number	TIBCO LogLogic Alert	Description
128	COBIT: TIBCO ActiveMatrix Administrator Permission Changed	Alerts on TIBCO ActiveMatrix Administrator permission changed events.
129	COBIT: UNIX Groups Added	Alerts when a new group has been added to the UNIX/Linux servers.
130	COBIT: UNIX Groups Deleted	Alerts when a user group is deleted on UNIX/Linux servers.
131	COBIT: UNIX Groups Modified	Alerts when a user group has been modified on UNIX/Linux servers.
132	COBIT: UNIX Privilege Escalated	Alerts when a user has escalated privileges using commands such as su/sudo.
133	COBIT: vCenter Create Virtual Machine	Alerts when virtual machine has been created from VMware vCenter console.
134	COBIT: vCenter Data Move	Alerts when entity has been moved within the VMware vCenter infrastructure.
135	COBIT: vCenter Datastore Event	Alerts on create, modify, and delete datastore events on VMware vCenter.
136	COBIT: vCenter Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter console.
137	COBIT: vCenter Firewall Policy Change	Alerts when changes to the VMware ESX allowed services firewall policy.
138	COBIT: vCenter Orchestrator Create Virtual Machine	Virtual machine has been created from VMware vCenter Orchestrator console.
139	COBIT: vCenter Orchestrator Data Move	Entity has been moved within the VMware vCenter Orchestrator infrastructure.
140	COBIT: vCenter Orchestrator Datastore Events	Alerts on create, modify, and delete datastore events on VMware vCenter Orchestrator.
141	COBIT: vCenter Orchestrator Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter Orchestrator console.
142	COBIT: vCenter Orchestrator Login Failed	Failed logins to the VMware vCenter Orchestrator console.
143	COBIT: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.

Serial Number	TIBCO LogLogic Alert	Description
144	COBIT: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
145	COBIT: vCenter Orchestrator vSwitch Add, Modify or Delete	vSwitch on VMware ESX server has been added, modified or removed from vCenter Orchestrator.
146	COBIT: vCenter Permission Change	Alerts when a permission role has been added, changed, removed, or applied on VMware vCenter.
147	COBIT: vCenter Restart ESX Services	Alerts when VMware vCenter restarted services running on VMware ESX Server.
148	COBIT: vCenter Shutdown or Restart ESX	Alerts when VMware ESX Server is shutdown from vCenter console.
149	COBIT: vCenter User Login Failed	Alerts on failed logins to the VMware vCenter console.
150	COBIT: vCenter User Login Successful	Alerts on successful logins to the VMware vCenter console.
151	COBIT: vCenter Virtual Machine Shutdown	Alerts when virtual machine has been shutdown or paused from VMware vCenter console.
152	COBIT: vCenter Virtual Machine Started	Alerts when virtual machine has been started or resumed from VMware vCenter console.
153	COBIT: vCenter vSwitch Add, Modify or Delete	Alerts when vSwitch on VMware ESX server has been added, modified or removed from vCenter.
154	COBIT: vCloud Director Login Failed	Alerts on failed logins to the VMware vCloud Director console.
155	COBIT: vCloud Director Login Success	Alerts on successful logins to the VMware vCloud Director console.
156	COBIT: vCloud Organization Created	Alerts when organization successfully created on VMware vCloud Director.
157	COBIT: vCloud Organization Deleted	Alerts when organization successfully deleted on VMware vCloud Director.
158	COBIT: vCloud Organization Modified	Alerts when organization successfully modified on VMware vCloud director.
159	COBIT: vCloud User Created	Alerts when a user successfully created on VMware vCloud Director.
160	COBIT: vCloud User, Group, or Role Modified	Alerts when VMware vCloud Director user, group, or role has been modified.

Serial Number	TIBCO LogLogic Alert	Description
161	COBIT: vCloud vApp Created, Deleted, or Modified	Alerts when VMware vCloud Director vApp has been created, deleted, or modified.
162	COBIT: vCloud vDC Created, Modified, or Deleted	Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified.
163	COBIT: vShield Edge Configuration Change	Alerts when configuration changes to VMware vShield Edge policies.
164	COBIT: Windows Audit Log Cleared	Alerts when audit logs on Windows servers have been cleared.
165	COBIT: Windows Files Accessed	Show files accessed on the Windows servers.
166	COBIT: Windows Group Members Added	Alerts when new members are added to user groups on Windows servers.
167	COBIT: Windows Group Members Deleted	Alerts when members are removed from user groups on Windows servers.
168	COBIT: Windows Groups Created	Alerts when new user groups are created on Windows servers.
169	COBIT: Windows Groups Deleted	Alerts when a user group is deleted on Windows servers.
170	COBIT: Windows Groups Modified	Alerts when a user group has been modified on Windows servers.
171	COBIT: Windows Passwords Changed	Alerts when users have changed their passwords.
172	COBIT: Windows Permissions Changed	Alerts when user or group permissions have been changed.
173	COBIT: Windows Policies Changed	Alerts when Windows policies changed.
174	COBIT: Windows Privileges Escalated	Alerts when a user or program has escalated the privileges.
175	COBIT: Windows Programs Accessed	Alerts when a program is accessed on a Windows server.
176	COBIT: System Restarted	Alerts when system has been restarted.
177	COBIT: Windows Software Updates	Alerts when events related to the Windows' software updates.

Serial Number	TIBCO LogLogic Alert	Description
178	COBIT: Windows Software Updates Failed	Alerts when failed events related to the software updates.
179	COBIT: Windows Software Updates Succeeded	Alerts for successful events related to the software updates.

TIBCO LogLogic Reports and Alerts Quick Reference

The following table describes the reports and alerts included in the LogLogic® Compliance Suite - Sarbanes-Oxley Edition and COBIT 4.1.

Control Objective	Description	Compliance Suite Reports and Alerts
PO2 Define the Information Architecture		
PO2.3	Data Classification Scheme	**Compliance Suite Reports** COBIT: Guardium SQL Guard Audit Data Access COBIT: Guardium SQL Guard Data Access COBIT: HP NonStop Audit Object Access COBIT: LogLogic DSM Data Access COBIT: Microsoft Sharepoint Content Deleted COBIT: Microsoft Sharepoint Content Updates COBIT: Microsoft SQL Server Data Access COBIT: Microsoft SQL Server Schema Corruption COBIT: Oracle Database Data Access COBIT: Sybase ASE Database Data Access COBIT: i5/OS Object Access **Compliance Suite Alerts** COBIT: Guardium SQL Guard Data Access COBIT: LogLogic DSM Data Access COBIT: Microsoft Sharepoint Content Deleted COBIT: Microsoft Sharepoint Content Updated COBIT: Oracle Database Data Access COBIT: Sybase ASE Database Data Access

Control Objective	Description	Compliance Suite Reports and Alerts
PO2.4	Integrity Management	**Compliance Suite Report** COBIT: Microsoft Sharepoint Content Deleted COBIT: Microsoft Sharepoint Content Updates COBIT: Microsoft SQL Server Schema Corruption COBIT: Tripwire Modifications, Additions, and Deletions **Compliance Suite Alerts** COBIT: Microsoft Sharepoint Content Deleted COBIT: Microsoft Sharepoint Content Updated
PO4 Define the IT Processes, Organization and Relationships		

Control Objective	Description	Compliance Suite Reports and Alerts
PO4.11	Segregation of Duties	**Compliance Suite Reports** COBIT: Pulse Connect Secure successful Logins COBIT: Accepted VPN Connections - RADIUS COBIT: Account Activities on UNIX Servers COBIT: Account Activities on Windows Servers COBIT: Accounts Created on NetApp Filer Audit COBIT: Accounts Created on NetApp Filer COBIT: Accounts Created on Sidewinder COBIT: Accounts Created on Symantec Endpoint Protection COBIT: Accounts Created on TIBCO ActiveMatrix Administrator COBIT: Accounts Created on TIBCO Administrator COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Active Directory System Changes COBIT: Administrator Logins on Windows Servers COBIT: Check Point Management Station Login COBIT: Cisco ISE, ACS Accounts Created COBIT: DB2 Database Successful Logins COBIT: ESX Accounts Activities COBIT: ESX Accounts Created COBIT: ESX Group Activities COBIT: ESX Logins Succeeded COBIT: F5 BIG-IP TMOS Login Successful COBIT: Group Activities on NetApp Filer Audit COBIT: Group Activities on Symantec Endpoint Protection COBIT: Group Activities on TIBCO ActiveMatrix Administrator COBIT: Group Activities on UNIX Servers COBIT: Group Activities on Windows Servers COBIT: Groups Created on NetApp Filer Audit COBIT: Groups Created on TIBCO ActiveMatrix Administrator COBIT: Groups Created on UNIX Servers COBIT: Groups Created on Windows Servers

Control Objective	Description	Compliance Suite Reports and Alerts
PO4.11	Segregation of Duties	**Compliance Suite Reports** (*Cont.*) COBIT: Groups Deleted on NetApp Filer Audit COBIT: Groups Deleted on TIBCO ActiveMatrix Administrator COBIT: Groups Deleted on UNIX Servers COBIT: Groups Deleted on Windows Servers COBIT: Guardium SQL Guard Audit Logins COBIT: Guardium SQL Guard Logins COBIT: HP NonStop Audit Login Successful COBIT: HP NonStop Audit Permissions Changed COBIT: i5/OS Access Control List Modifications COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Last Activities Performed by Administrators COBIT: Last Activities Performed by All Users COBIT: Logins by Authentication Type COBIT: LogLogic DSM Logins COBIT: LogLogic Management Center Account Activities COBIT: LogLogic Management Center Login COBIT: Microsoft Operations Manager - Windows Accounts Activities COBIT: Microsoft Operations Manager - Windows Accounts Created COBIT: Microsoft Operations Manager - Windows Permissions Modified COBIT: Microsoft Sharepoint Permissions Changed COBIT: Microsoft Sharepoint Policy Add, Remove, or Modify COBIT: Microsoft SQL Server Database Permission Events COBIT: Microsoft SQL Server Database Successful Logins COBIT: NetApp Filer Audit Login Successful COBIT: NetApp Filer Login Successful COBIT: Oracle Database Permission Events COBIT: Oracle Database Successful Logins

Control Objective	Description	Compliance Suite Reports and Alerts
PO4.11	Segregation of Duties	**Compliance Suite Reports** (*Cont.*) COBIT: Permissions Modified on Windows Servers COBIT: RACF Accounts Created COBIT: RACF Permissions Changed COBIT: RACF Successful Logins COBIT: Root Logins COBIT: Successful Logins COBIT: Sybase ASE Successful Logins COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TIBCO ActiveMatrix Administrator Successful Logins COBIT: TIBCO Administrator Permission Changes COBIT: Unauthorized Logins COBIT: Unencrypted Logins COBIT: vCenter Orchestrator Virtual Machine Created COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter Successful Logins COBIT: vCenter User Permission Change COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud Successful Logins COBIT: vCloud User Created COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted

Control Objective	Description	Compliance Suite Reports and Alerts
PO4.11	Segregation of Duties	**Compliance Suite Alerts** COBIT: Accounts Created COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: DB2 Database User Added or Dropped COBIT: Groups Created COBIT: Groups Deleted COBIT: Group Members Added COBIT: Guardium SQL Guard Logins COBIT: HP NonStop Audit Permission Changed COBIT: i5/OS Permission or Policy Change COBIT: Juniper Firewall Logon Success COBIT: Logins Succeeded COBIT: LogLogic DSM Logins COBIT: Microsoft Operations Manager - Permissions Changed COBIT: Microsoft Sharepoint Permission Changed COBIT: Microsoft Sharepoint Policies Added, Removed, Modified COBIT: Oracle Database Permissions Changed COBIT: RACF Permissions Changed COBIT: Symantec Endpoint Protection Policy Add, Delete, Modify COBIT: TIBCO ActiveMatrix Administrator Permission Changed COBIT: UNIX Groups Added COBIT: UNIX Groups Deleted COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCenter Permission Change COBIT: vCenter User Login Successful COBIT: vCloud Director Login Success COBIT: vCloud Organization Created

Control Objective	Description	Compliance Suite Reports and Alerts
PO4.11	Segregation of Duties	**Compliance Suite Alerts** (*Cont.*) COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud User Created COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: Windows Group Members Added COBIT: Windows Groups Created COBIT: Windows Groups Deleted COBIT: Windows Permissions Changed
PO7 Manage IT Human Resources		

Control Objective	Description	Compliance Suite Reports and Alerts
PO7.8	Job Change and Termination	**Compliance Suite Reports** COBIT: Pulse Connect Secure Successful Logins COBIT: Accepted VPN Connections - RADIUS COBIT: Account Activities on UNIX Servers COBIT: Account Activities on Windows Servers COBIT: Accounts Changed on NetApp Filer COBIT: Accounts Changed on TIBCO Administrator COBIT: Accounts Created on NetApp Filer COBIT: Accounts Created on NetApp Filer Audit COBIT: Accounts Created on Sidewinder COBIT: Accounts Created on Symantec Endpoint Protection COBIT: Accounts Created on TIBCO ActiveMatrix Administrator COBIT: Accounts Created on TIBCO Administrator COBIT: Accounts Changed on UNIX Servers COBIT: Accounts Changed on Windows Servers COBIT: Accounts Changed on Sidewinder COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Accounts Deleted on NetApp Filer COBIT: Accounts Deleted on NetApp Filer Audit COBIT: Accounts Deleted on Sidewinder COBIT: Accounts Deleted on Symantec Endpoint Protection

Control Objective	Description	Compliance Suite Reports and Alerts
PO7.8	Job Change and Termination	**Compliance Suite Reports** (*Cont.*) COBIT: Accounts Deleted on TIBCO ActiveMatrix Administrator COBIT: Accounts Deleted on TIBCO Administrator COBIT: Accounts Deleted on UNIX Servers COBIT: Accounts Deleted on Windows Servers COBIT: Active VPN Connections for Cisco VPN Conc entrators COBIT: Active VPN Connections for Nortel Contivity COBIT: Active VPN Connections for RADIUS COBIT: Check Point Management Station Login COBIT: Cisco ISE, ACS Accounts Created COBIT: Cisco ISE, ACS Accounts Removed COBIT: DB2 Database Failed Logins COBIT: DB2 Database Successful Logins COBIT: ESX Accounts Activities COBIT: ESX Accounts Created COBIT: ESX Accounts Deleted COBIT: ESX Failed Logins COBIT: ESX Group Activities COBIT: ESX Logins Failed Unknown User COBIT: ESX Logins Succeeded COBIT: F5 BIG-IP TMOS Login Failed COBIT: F5 BIG-IP TMOS Login Successful COBIT: Failed Logins COBIT: Group Activities on NetApp Filer Audit COBIT: Group Activities on Symantec Endpoint Protection COBIT: Group Activities on TIBCO ActiveMatrix Administrator COBIT: Group Activities on UNIX Servers COBIT: Group Activities on Windows Servers COBIT: Guardium SQL Guard Audit Logins COBIT: Guardium SQL Guard Logins COBIT: HP NonStop Audit Login Failed COBIT: HP NonStop Audit Login Successful

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: HP NonStop Audit Permissions Changed

Control Objective	Description	Compliance Suite Reports and Alerts
PO7.8	Job Change and Termination	**Compliance Suite Reports** (*Cont.*) COBIT: Last Activities Performed by All Users COBIT: i5/OS Access Control List Modifications COBIT: i5/OS Network Authentication Events COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Last Activities Performed by Administrators COBIT: Logins by Authentication Type COBIT: LogLogic DSM Logins COBIT: LogLogic Management Center Account Activities COBIT: LogLogic Management Center Login COBIT: Microsoft Operations Manager - Windows Accounts Activities COBIT: Microsoft Operations Manager - Windows Accounts Changed COBIT: Microsoft Operations Manager - Windows Accounts Created COBIT: Microsoft Operations Manager - Windows Accounts Enabled COBIT: Microsoft Operations Manager - Windows Permissions Modified COBIT: Microsoft SQL Server Database Failed Logins COBIT: Microsoft SQL Server Database Successful Logins COBIT: NetApp Filer Audit Group Members Deleted COBIT: NetApp Filer Audit Login Failed COBIT: NetApp Filer Audit Login Successful COBIT: NetApp Filer Login Failed COBIT: NetApp Filer Login Successful COBIT: Oracle Database Failed Logins COBIT: Oracle Database Successful Logins COBIT: Permissions Modified on Windows Servers COBIT: RACF Accounts Created COBIT: RACF Accounts Deleted COBIT: RACF Accounts Modified COBIT: RACF Failed Logins

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: RACF Permissions Changed COBIT: RACF Successful Logins

Control Objective	Description	Compliance Suite Reports and Alerts
PO7.8	Job Change and Termination	**Compliance Suite Reports** (*Cont.*) COBIT: Successful Logins COBIT: Sybase ASE Failed Logins COBIT: Sybase ASE Successful Logins COBIT: TIBCO ActiveMatrix Administrator Failed Logins COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TIBCO ActiveMatrix Administrator Successful Logins COBIT: TIBCO Administrator Permission Changes COBIT: Unencrypted Logins COBIT: UNIX Failed Logins COBIT: Users Removed from Servers COBIT: vCenter Failed Logins COBIT: vCenter Orchestrator Failed Logins COBIT: vCenter Successful Logins COBIT: vCloud Failed Logins COBIT: vCloud Successful Logins COBIT: vCloud User Created COBIT: vCloud User Deleted or Removed COBIT: Windows Group Members Deleted **Compliance Suite Alerts** COBIT: Accounts Created COBIT: Accounts Deleted COBIT: Accounts Modified COBIT: Cisco PIX, ASA, FWSM Logon Failure COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: DB2 Database User Added or Dropped COBIT: Guardium SQL Guard Logins COBIT: Groups Deleted COBIT: Group Members Added COBIT: Group Members Deleted COBIT: Groups Modified COBIT: HP NonStop Audit Permission Changed COBIT: i5/OS Network Profile Changes

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: i5/OS User Profile Changes
PO7.8	Job Change and Termination	**Compliance Suite Alerts** (*Cont.*) COBIT: Juniper Firewall Logon Failure COBIT: Juniper Firewall Logon Success COBIT: Logins Failed COBIT: Logins Succeeded COBIT: LogLogic DSM Logins COBIT: NetApp Filer NIS Group Update COBIT: UNIX Groups Deleted COBIT: UNIX Groups Modified COBIT: vCenter Orchestrator Login Failed COBIT: vCenter User Login Failed COBIT: vCenter User Login Successful COBIT: vCloud Director Login Failed COBIT: vCloud Director Login Success COBIT: vCloud User Created COBIT: vCloud User, Group, or Role Modified COBIT: Windows Group Members Added COBIT: Windows Group Members Deleted COBIT: Windows Groups Deleted COBIT: Windows Groups Modified
AI2 Acquire and Maintain Application Software		
AI2.3	Application Control and Auditability	**Compliance Suite Reports** COBIT: ESX Kernel log daemon terminating COBIT: ESX Kernel logging Stop COBIT: ESX Syslogd Restart COBIT: LogLogic File Retrieval Errors COBIT: LogLogic Message Routing Errors COBIT: RACF Process Started COBIT: vCenter Orchestrator Virtual Machine Created COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter Restart ESX Services

Control Objective	Description	Compliance Suite Reports and Alerts
AI2.3	Application Control and Auditability	**Compliance Suite Reports** (*Cont.*) COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted COBIT: Windows New Services Installed
AI2.3	Application Control and Auditability	**Compliance Suite Alerts** COBIT: LogLogic Message Routing Errors COBIT: LogLogic File Retrieval Errors COBIT: RACF Process Started COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Restart ESX Services COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: Windows Programs Accessed

Control Objective	Description	Compliance Suite Reports and Alerts
AI2.4	Application Security and Availability	**Compliance Suite Reports** COBIT: Active Directory System Changes COBIT: HP NonStop Audit Permissions Changed COBIT: i5/OS Access Control List Modifications COBIT: Microsoft Operations Manager - Windows Permissions Modified COBIT: Microsoft Sharepoint Permissions Changed COBIT: Microsoft Sharepoint Policy Add, Remove, or Modify COBIT: Microsoft SQL Server Database Permission Events COBIT: Oracle Database Permission Events COBIT: Permissions Modified on Windows Servers COBIT: RACF Permissions Changed COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TIBCO Administrator Permission Changes COBIT: vCenter Orchestrator Virtual Machine Created COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter User Permission Change COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted **Compliance Suite Alerts** COBIT: HP NonStop Audit Permission Changed COBIT: i5/OS Permission or Policy Change COBIT: Microsoft Sharepoint Permission Changed COBIT: Microsoft Sharepoint Policies Added, Removed, Modified COBIT: Oracle Database Permissions Changed COBIT: RACF Permissions Changed

Control Objective	Description	Compliance Suite Reports and Alerts
AI2.4	Application Security and Availability	**Compliance Suite Reports** (*Cont.*) COBIT: Symantec Endpoint Protection Policy Add, Delete, Modify COBIT: TIBCO ActiveMatrix Administrator Permission Changed COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCenter Permission Change COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: Windows Permissions Changed
AI3 Acquire and Maintain Technology Infrastructure		
AI3.2	Infrastructure Resource Protection and Availability	**Compliance Suite Reports** COBIT: Active Directory System Changes COBIT: Check Point Objects Created COBIT: Check Point Objects Deleted COBIT: Creation and Deletion of System Level Objects: AIX Audit COBIT: Creation and Deletion of System Level Objects: DB2 Database COBIT: Creation and Deletion of System Level Objects: HP-UX Audit COBIT: Creation and Deletion of System Level Objects: Windows COBIT: Creation and Deletion of System Level Objects: Oracle COBIT: Creation and Deletion of System Level Objects: SQL Server COBIT: Creation and Deletion of System Level Objects: Solaris BSM

Control Objective	Description	Compliance Suite Reports and Alerts
AI3.2	Infrastructure Resource Protection and Availability	**Compliance Suite Reports** (*Cont.*) COBIT: Domain activities on Symantec Endpoint Protection COBIT: i5/OS Object Creation and Deletion COBIT: Microsoft SQL Server Schema Corruption COBIT: Sybase ASE Database Create Events COBIT: Sybase ASE Database Drop Events COBIT: Tripwire Modifications, Additions, and Deletions COBIT: Trusted Domain Created on Windows Servers COBIT: Trusted Domain Deleted on Windows Servers COBIT: vCenter Orchestrator Virtual Machine Created COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted
AI3.2	Infrastructure Resource Protection and Availability	**Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM NAT Failure COBIT: Cisco PIX, ASA, FWSM Protocol Failure COBIT: Cisco PIX, ASA, FWSM Routing Failure COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted

Control Objective	Description	Compliance Suite Reports and Alerts
AI3.3	Infrastructure Maintenance	**Compliance Suite Reports** COBIT: Active Directory System Changes COBIT: Check Point Configuration Changes COBIT: Cisco ISE, ACS Configuration Changes COBIT: Cisco Peer Reset/Reload COBIT: Cisco Peer Supervisor Status Changes COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco Routers and Switches Restart COBIT: DB2 Database Configuration Changes COBIT: DB2 Database Stop and Start Events COBIT: Cisco ESA: Updated COBIT: F5 BIG-IP TMOS Restarted COBIT: Guardium SQL Guard Audit Configuration Changes COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Configuration Changes COBIT: Guardium SQL Guard Startup or Shutdown COBIT: HP NonStop Audit Configuration Changes COBIT: i5/OS System Management Changes COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Juniper Firewall Restarted COBIT: LogLogic DSM Configuration Changes COBIT: LogLogic DSM Startup or Shutdown COBIT: LogLogic Management Center Upgrade Success COBIT: LogLogic Universal Collector Configuration Changes COBIT: Microsoft Operations Manager - Windows Servers Restarted COBIT: Microsoft SQL Server Configuration Changes COBIT: Microsoft SQL Server Shutdown by Reason COBIT: Oracle Database Configuration Changes COBIT: Oracle Database Shutdown

Control Objective	Description	Compliance Suite Reports and Alerts
AI3.3	Infrastructure Maintenance	**Compliance Suite Reports** (*Cont.*) COBIT: Peer Servers and Status COBIT: Peer Servers and Status - Blue Coat Proxy COBIT: Peer Servers and Status - Cisco WSA COBIT: Peer Servers and Status - Microsoft IIS COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: RACF Process Started COBIT: Sidewinder Configuration Changes COBIT: Sybase ASE Database Configuration Changes COBIT: Sybase ASE Database Startup or Shutdown COBIT: Symantec AntiVirus: Updated COBIT: Symantec Endpoint Protection Configuration Changes COBIT: Symantec Endpoint Protection: Updated COBIT: vCenter Orchestrator Virtual Machine Created COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart of ESX Server COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted COBIT: Windows New Services Installed COBIT: Windows Servers Restarted COBIT: Windows Software Update Activities COBIT: Windows Software Update Failures COBIT: Windows Software Update Successes

Control Objective	Description	Compliance Suite Reports and Alerts
AI3.3	Infrastructure Maintenance	**Compliance Suite Alerts** COBIT: Check Point Policy Changed COBIT: Microsoft Operations Manager - Windows Server Restarted COBIT: Cisco ISE, ACS Configuration Changed COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Errors COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: System Restarted COBIT: Cisco Switch Card Insert COBIT: Cisco Switch Device Reload COBIT: Cisco Switch Device Restart COBIT: Cisco Switch HA Failure (ver) COBIT: DB2 Database Configuration Change COBIT: DB2 Database Started or Stopped COBIT: DNS Server Shutdown COBIT: DNS Server Started COBIT: Guardium SQL Guard Config Changes COBIT: Guardium SQL Guard Startup or Shutdown COBIT: HP NonStop Audit Configuration Changed COBIT: i5/OS Server or Service Status Change COBIT: i5/OS Software Updates COBIT: Juniper Firewall HA State Change COBIT: Juniper Firewall Peer Missing COBIT: Juniper Firewall System Reset COBIT: LogLogic Disk Full COBIT: LogLogic DSM Configuration Changes COBIT: LogLogic DSM Startup or Shutdown COBIT: LogLogic Management Center Upgrade Succeeded COBIT: LogLogic Universal Collector Configuration Changed COBIT: Microsoft SQL Server Shutdown COBIT: NetApp Bad File Handle COBIT: NetApp Filer Disk Failure COBIT: NetApp Filer Disk Missing

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: NetApp Filer File System Full COBIT: NetApp Filer Disk Inserted COBIT: NetApp Filer Disk Pulled
AI3.3	Infrastructure Maintenance	**Compliance Suite Alerts** (*Cont.*) COBIT: Oracle Database Configuration Change COBIT: Oracle Database Shutdown COBIT: RACF Process Started COBIT: Sidewinder Configuration Changed COBIT: Sybase ASE Database Config Changes COBIT: Sybase ASE Database Started COBIT: Sybase ASE Database Stopped COBIT: Symantec Endpoint Protection Configuration Changed COBIT: System Anomalies COBIT: System Restarted COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart ESX COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: System Restarted COBIT: Windows Software Updates COBIT: Windows Software Updates Failed COBIT: Windows Software Updates Succeeded
AI6 Manage Changes		

Control Objective	Description	Compliance Suite Reports and Alerts
AI6	Change Standards and Procedures	**Compliance Suite Reports** COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: vCenter Orchestrator Virtual Machine Created

Control Objective	Description	Compliance Suite Reports and Alerts
AI6	Change Standards and Procedures	**Compliance Suite Reports** (*Cont.*)
		COBIT: vCenter Orchestrator Virtual Machine Deleted
		COBIT: vCenter Orchestrator Virtual Machine Shutdown
		COBIT: vCenter Orchestrator Virtual Machine Started
		COBIT: vCenter Shutdown or Restart of ESX Server
		COBIT: vCenter Virtual Machine Created
		COBIT: vCenter Virtual Machine Deleted
		COBIT: vCenter Virtual Machine Shutdown
		COBIT: vCenter Virtual Machine Started
		COBIT: vCloud Organization Created
		COBIT: vCloud Organization Deleted
		COBIT: vCloud Organization Modified
		COBIT: vCloud vApp Created, Modified, or Deleted
		COBIT: vCloud vDC Created, Modified, or Deleted
		Compliance Suite Alerts
		COBIT: Cisco PIX, ASA, FWSM Failover Disabled
		COBIT: Cisco PIX, ASA, FWSM Failover Errors
		COBIT: Cisco PIX, ASA, FWSM Failover Performed
		COBIT: System Restarted
		COBIT: Cisco Switch Device Reload
		COBIT: Cisco Switch Device Restart
		COBIT: Cisco Switch HA Failure (ver)
		COBIT: DB2 Database Configuration Change
		COBIT: DB2 Database Started or Stopped
		COBIT: DNS Server Shutdown
		COBIT: DNS Server Started
		COBIT: i5/OS Server or Service Status Change
		COBIT: Juniper Firewall HA State Change
		COBIT: Juniper Firewall Peer Missing
		COBIT: Juniper Firewall System Reset
		COBIT: Microsoft SQL Server Shutdown
		COBIT: Microsoft Operations Manager - Windows Server Restarted
		COBIT: NetApp Filer File System Full
		COBIT: Oracle Database Configuration Change

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Oracle Database Shutdown
AI6	Change Standards and Procedures	**Compliance Suite Alerts** (*Cont.*) COBIT: System Anomalies COBIT: System Restarted COBIT: vCenter Create Virtual Machine COBIT: vCenter Delete Virtual Machine COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart ESX COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: System Restarted
AI6.1	Change Standards and Procedures	**Compliance Suite Reports** COBIT: Active Directory System Changes COBIT: Check Point Configuration Changes COBIT: Check Point Objects Modified COBIT: Cisco ESA: Updated COBIT: Cisco ISE, ACS Configuration Changes COBIT: Cisco Peer Reset/Reload COBIT: Cisco Peer Supervisor Status Changes COBIT: Cisco Routers and Switches Restart COBIT: DB2 Database Configuration Changes COBIT: DB2 Database Stop and Start Events COBIT: Domain activities on Symantec Endpoint Protection COBIT: F5 BIG-IP TMOS Restarted

Control Objective	Description	Compliance Suite Reports and Alerts
AI6.1	Change Standards and Procedures	**Compliance Suite Reports** (*Cont.*) COBIT: Guardium SQL Guard Audit Configuration Changes COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Configuration Changes COBIT: Guardium SQL Guard Startup or Shutdown COBIT: HP NonStop Audit Configuration Changes COBIT: i5/OS Audit Configuration Changes COBIT: i5/OS System Management Changes COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Juniper Firewall Restarted COBIT: LogLogic DSM Configuration Changes COBIT: LogLogic DSM Startup or Shutdown COBIT: LogLogic Management Center Upgrade Success COBIT: LogLogic Universal Collector Configuration Changes COBIT: Microsoft Operations Manager - Windows Servers Restarted COBIT: Microsoft SQL Server Configuration Changes COBIT: Microsoft SQL Server Shutdown by Reason COBIT: Oracle Database Configuration Changes COBIT: Oracle Database Shutdown COBIT: Peer Servers and Status COBIT: Peer Servers and Status - Blue Coat Proxy COBIT: Peer Servers and Status - Cisco WSA COBIT: Peer Servers and Status - Microsoft IIS COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: RACF Process Started COBIT: Sidewinder Configuration Changes COBIT: Sybase ASE Database Configuration Changes COBIT: Sybase ASE Database Startup or Shutdown COBIT: Symantec AntiVirus: Updated

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Symantec Endpoint Protection Configuration Changes COBIT: Symantec Endpoint Protection: Updated
AI6.1	Change Standards and Procedures	**Compliance Suite Reports** (*Cont.*) COBIT: Trusted Domain Created on Windows Servers COBIT: Trusted Domain Deleted on Windows Servers COBIT: Windows New Services Installed COBIT: Windows Servers Restarted COBIT: Windows Software Update Activities COBIT: Windows Software Update Failures COBIT: Windows Software Update Successes **Compliance Suite Alerts** COBIT: Check Point Policy Changed COBIT: Cisco ISE, ACS Configuration Changed COBIT: Guardium SQL Guard Config Changes COBIT: Guardium SQL Guard Startup or Shutdown COBIT: HP NonStop Audit Configuration Changed COBIT: i5/OS Software Updates COBIT: LogLogic DSM Configuration Changes COBIT: LogLogic DSM Startup or Shutdown COBIT: LogLogic Management Center Upgrade Succeeded COBIT: LogLogic Universal Collector Configuration Changed COBIT: RACF Process Started COBIT: Sidewinder Configuration Changed COBIT: Sybase ASE Database Config Changes COBIT: Sybase ASE Database Started COBIT: Sybase ASE Database Stopped COBIT: Symantec Endpoint Protection Configuration Changed COBIT: Windows Software Updates COBIT: Windows Software Updates Failed COBIT: Windows Software Updates Succeeded
DS1 Define and Manage Service Levels		

Control Objective	Description	Compliance Suite Reports and Alerts
DS1.5	Monitoring and Reporting of Service Level Achievements	**Compliance Suite Reports** COBIT: Cisco Line Protocol Status Changes COBIT: Cisco Link Status Changes COBIT: Cisco Peer Reset/Reload COBIT: Cisco Peer Supervisor Status Changes

Control Objective	Description	Compliance Suite Reports and Alerts
DS1.5	Monitoring and Reporting of Service Level Achievements	**Compliance Suite Reports** (*Cont.*) COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco Routers and Switches Restart COBIT: DB2 Database Stop and Start Events COBIT: DHCP Granted/Renewed Activities on Microsoft DHCP COBIT: DHCP Granted/Renewed Activities on VMware vShield COBIT: DNS Server Error COBIT: F5 BIG-IP TMOS Restarted COBIT: Failed Windows Events Summary COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Startup or Shutdown COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Juniper Firewall Restarted COBIT: LogLogic DSM Startup or Shutdown COBIT: Microsoft Operations Manager - Failed Windows Events COBIT: Microsoft Operations Manager - Windows Events Summary COBIT: Microsoft Operations Manager - Windows Servers Restarted COBIT: Microsoft SQL Server Shutdown by Reason COBIT: Oracle Database Shutdown COBIT: Peer Servers and Status COBIT: Peer Servers and Status - Blue Coat Proxy COBIT: Peer Servers and Status - Cisco WSA COBIT: Peer Servers and Status - Microsoft IIS COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: Sybase ASE Database Startup or Shutdown COBIT: vCenter Orchestrator Virtual Machine Shutdown

Control Objective	Description	Compliance Suite Reports and Alerts
DS1.5	Monitoring and Reporting of Service Level Achievements	**Compliance Suite Reports** (*Cont.*) COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart of ESX Server COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: Windows Events Summary COBIT: Windows Servers Restarted **Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Errors COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco PIX, ASA, FWSM NAT Failure COBIT: Cisco PIX, ASA, FWSM Protocol Failure COBIT: System Restarted COBIT: Cisco PIX, ASA, FWSM Routing Failure COBIT: Cisco Switch Device Reload COBIT: Cisco Switch Device Restart COBIT: Cisco Switch HA Failure (ver) COBIT: Cisco Switch Interface Change COBIT: Cisco Switch Interface Down COBIT: Cisco Switch Interface Up COBIT: DB2 Database Started or Stopped COBIT: DNS Server Shutdown COBIT: DNS Server Started COBIT: Guardium SQL Guard Startup or Shutdown COBIT: i5/OS Server or Service Status Change COBIT: Juniper Firewall HA State Change COBIT: Juniper Firewall Peer Missing COBIT: Juniper Firewall System Reset COBIT: LogLogic Disk Full COBIT: LogLogic DSM Startup or Shutdown COBIT: Microsoft Operations Manager - Windows Server Restarted COBIT: Microsoft SQL Server Shutdown COBIT: NetApp Bad File Handle COBIT: NetApp Filer Disk Failure

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: NetApp Filer Disk Missing
DS1.5	Monitoring and Reporting of Service Level Achievements	**Compliance Suite Alerts** (*Cont.*) COBIT: NetApp Filer File System Full COBIT: Oracle Database Shutdown COBIT: Sybase ASE Database Started COBIT: Sybase ASE Database Stopped COBIT: System Anomalies COBIT: System Restarted COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart ESX COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: System Restarted
DS2 Manage Third-Party Services		

Control Objective	Description	Compliance Suite Reports and Alerts
DS2.4	Supplier Performance Monitoring	**Compliance Suite Reports** COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco Routers and Switches Restart COBIT: DB2 Database Stop and Start Events COBIT: DNS Server Error COBIT: F5 BIG-IP TMOS Restarted COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Startup or Shutdown COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Startup or Shutdown COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Juniper Firewall Restarted COBIT: Juniper Firewall VPN Tunnel Status Change COBIT: LogLogic DSM Startup or Shutdown

Control Objective	Description	Compliance Suite Reports and Alerts
DS2.4	Supplier Performance Monitoring	**Compliance Suite Reports** (*Cont.*) COBIT: Microsoft Operations Manager - Windows Servers Restarted COBIT: Microsoft SQL Server Shutdown by Reason COBIT: Oracle Database Shutdown COBIT: Peer Servers and Status COBIT: Peer Servers and Status - Blue Coat Proxy COBIT: Peer Servers and Status - Cisco WSA COBIT: Peer Servers and Status - Microsoft IIS COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: Sybase ASE Database Startup or Shutdown COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart of ESX Server COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: Windows Servers Restarted **Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Errors COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: System Restarted COBIT: Cisco PIX, ASA, FWSM VPN Tunnel Creation COBIT: Cisco PIX, ASA, FWSM VPN Tunnel Teardown COBIT: Cisco Switch Device Reload COBIT: Cisco Switch Device Restart COBIT: Cisco Switch HA Failure (ver) COBIT: DB2 Database Started or Stopped COBIT: DNS Server Shutdown COBIT: DNS Server Started COBIT: Guardium SQL Guard Startup or Shutdown COBIT: i5/OS Server or Service Status Change COBIT: Juniper Firewall HA State Change

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Juniper Firewall System Reset
DS2.4	Supplier Performance Monitoring	**Compliance Suite Alerts** (*Cont.*) COBIT: LogLogic DSM Startup or Shutdown COBIT: Microsoft SQL Server Shutdown COBIT: Microsoft Operations Manager - Windows Server Restarted COBIT: NetApp Filer File System Full COBIT: Oracle Database Shutdown COBIT: Sybase ASE Database Started COBIT: Sybase ASE Database Stopped COBIT: System Anomalies COBIT: System Restarted COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart ESX COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: System Restarted
DS3 Manage Performance and Capacity		

Control Objective	Description	Compliance Suite Reports and Alerts
DS3.5	Monitoring and Reporting of Performance and Capacity	**Compliance Suite Reports** COBIT: Bandwidth Usage by User COBIT: Cisco Line Protocol Status Changes COBIT: Cisco Link Status Changes COBIT: Cisco Peer Reset/Reload COBIT: Cisco Peer Supervisor Status Changes COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco Routers and Switches Restart COBIT: DB2 Database Stop and Start Events COBIT: DNS Server Error COBIT: F5 BIG-IP TMOS Restarted COBIT: Failed Windows Events Summary COBIT: Guardium SQL Guard Audit Startup or Shutdown COBIT: Guardium SQL Guard Startup or Shutdown COBIT: Juniper Firewall Reset Accepted COBIT: Juniper Firewall Reset Imminent COBIT: Juniper Firewall Restarted

Control Objective	Description	Compliance Suite Reports and Alerts
DS3.5	Monitoring and Reporting of Performance and Capacity	**Compliance Suite Reports** (*Cont.*) COBIT: LogLogic DSM Startup or Shutdown COBIT: Microsoft Operations Manager - Failed Windows Events COBIT: Microsoft Operations Manager - Windows Events Summary COBIT: Microsoft Operations Manager - Windows Servers Restarted COBIT: Microsoft SQL Server Shutdown by Reason COBIT: Oracle Database Shutdown COBIT: Peer Servers and Status COBIT: Peer Servers and Status - Blue Coat Proxy COBIT: Peer Servers and Status - Cisco WSA COBIT: Peer Servers and Status - Microsoft IIS COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: Sybase ASE Database Startup or Shutdown COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart of ESX Server COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: VPN Connection Average Bandwidth COBIT: VPN Connection Average Duration COBIT: VPN Connection Disconnect Reasons COBIT: Windows Events Summary COBIT: Windows Servers Restarted **Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM Failover Disabled COBIT: Cisco PIX, ASA, FWSM Failover Errors COBIT: Cisco PIX, ASA, FWSM Failover Performed COBIT: Cisco PIX, ASA, FWSM NAT Failure COBIT: Cisco PIX, ASA, FWSM Protocol Failure COBIT: System Restarted COBIT: Cisco PIX, ASA, FWSM Routing Failure

Control Objective	Description	Compliance Suite Reports and Alerts
DS3.5	Monitoring and Reporting of Performance and Capacity	**Compliance Suite Alerts** (*Cont.*) COBIT: Cisco Switch Device Reload COBIT: Cisco Switch HA Failure (ver) COBIT: Cisco Switch Device Restart COBIT: Cisco Switch Interface Change COBIT: Cisco Switch Interface Down COBIT: Cisco Switch Interface Up COBIT: DB2 Database Started or Stopped COBIT: DNS Server Shutdown COBIT: DNS Server Started COBIT: Guardium SQL Guard Startup or Shutdown COBIT: i5/OS Server or Service Status Change COBIT: Juniper Firewall HA State Change COBIT: Juniper Firewall Peer Missing COBIT: Juniper Firewall System Reset COBIT: LogLogic Disk Full COBIT: LogLogic DSM Startup or Shutdown COBIT: Microsoft SQL Server Shutdown COBIT: Microsoft Operations Manager - Windows Server Restarted COBIT: NetApp Bad File Handle COBIT: NetApp Filer Disk Failure COBIT: NetApp Filer Disk Missing COBIT: NetApp Filer File System Full COBIT: Oracle Database Shutdown COBIT: Sybase ASE Database Started COBIT: Sybase ASE Database Stopped COBIT: System Anomalies COBIT: System Restarted COBIT: vCenter Orchestrator Virtual Machine Shutdown COBIT: vCenter Orchestrator Virtual Machine Started COBIT: vCenter Shutdown or Restart ESX COBIT: vCenter Virtual Machine Shutdown COBIT: vCenter Virtual Machine Started COBIT: System Restarted

Control Objective	Description	Compliance Suite Reports and Alerts
DS4 Ensure Continuous Service		

Control Objective	Description	Compliance Suite Reports and Alerts
DS4.1	IT Continuity Framework	**Compliance Suite Reports** COBIT: Files Accessed through Pulse Connect Secure COBIT: Files Accessed on NetApp Filer Audit COBIT: Files Accessed on Servers COBIT: Files Accessed through Juniper SSL VPN (Secure Access) COBIT: Files Accessed through PANOS COBIT: Files Downloaded via Proxy COBIT: Files Downloaded via Proxy - Blue Coat Proxy COBIT: Files Downloaded via Proxy - Cisco WSA COBIT: Files Downloaded via Proxy - Microsoft IIS COBIT: Files Downloaded via the Web COBIT: Files Downloaded via the Web - F5 BIG-IP TMOS COBIT: Files Downloaded via the Web - Microsoft IIS COBIT: Files Uploaded via Proxy COBIT: Files Uploaded via Proxy - Blue Coat Proxy COBIT: Files Uploaded via Proxy - Cisco WSA COBIT: Files Uploaded via Proxy - Microsoft IIS COBIT: Files Uploaded via the Web COBIT: Files Uploaded via the Web - F5 BIG-IP TMOS COBIT: Files Uploaded via the Web - Microsoft IIS COBIT: NetApp Filer Snapshot Error COBIT: NetApp Filer File Activity COBIT: RACF Files Accessed COBIT: vCenter Datastore Events COBIT: vCenter Data Move COBIT: vCenter Orchestrator Datastore Events COBIT: vCenter Orchestrator Data Move **Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM NAT Failure COBIT: Cisco PIX, ASA, FWSM Protocol Failure COBIT: Cisco PIX, ASA, FWSM Routing Failure COBIT: Neoteris Files Accessed COBIT: NetApp Filer Snapshot Error

Control Objective	Description	Compliance Suite Reports and Alerts
DS4.1	IT Continuity Framework	**Compliance Suite Alerts** (*Cont.*) COBIT: NetApp Filer Unauthorized Mounting COBIT: RACF Files Accessed COBIT: vCenter Datastore Event COBIT: vCenter Data Move COBIT: vCenter Orchestrator Data Move COBIT: vCenter Orchestrator Datastore Events COBIT: Windows Files Accessed
DS4.5	Testing of the IT Continuity Plan	**Compliance Suite Reports** COBIT: DB2 Database Backup Failed COBIT: LogLogic Management Center Backup Activities COBIT: LogLogic Management Center Restore Activities COBIT: Microsoft SQL Server Backup Failed COBIT: NetApp Filer Snapshot Error COBIT: Sybase ASE Database Backup and Restoration Compliance Suite Alert COBIT: DB2 Database Backup Failed COBIT: LogLogic Management Center Backed Up or Restored COBIT: Microsoft SQL Server Backup Failed COBIT: Sybase ASE Database Backed Up or Restored
DS5 Ensure System Security		

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.2	IT Security Plan	**Compliance Suite Reports** COBIT: Files Accessed through Pulse Connect Secure COBIT: Files Accessed on NetApp Filer Audit COBIT: Files Accessed on Servers COBIT: Files Accessed through Juniper SSL VPN (Secure Access) COBIT: Files Accessed through PANOS COBIT: Files Downloaded via Proxy COBIT: Files Downloaded via Proxy - Blue Coat Proxy COBIT: Files Downloaded via Proxy - Cisco WSA COBIT: Files Downloaded via Proxy - Microsoft IIS COBIT: Files Downloaded via the Web COBIT: Files Downloaded via the Web - F5 BIG-IP TMOS COBIT: Files Downloaded via the Web - Microsoft IIS

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.2	IT Security Plan	**Compliance Suite Reports** (*Cont.*) COBIT: Files Uploaded via Proxy COBIT: Files Uploaded via Proxy - Blue Coat Proxy COBIT: Files Uploaded via Proxy - Cisco WSA COBIT: Files Uploaded via Proxy - Microsoft IIS COBIT: Files Uploaded via the Web COBIT: Files Uploaded via the Web - F5 BIG-IP TMOS COBIT: Files Uploaded via the Web - Microsoft IIS COBIT: NetApp Filer File Activity COBIT: RACF Files Accessed COBIT: vCenter Datastore Events COBIT: vCenter Data Move COBIT: vCenter Orchestrator Datastore Events COBIT: vCenter Orchestrator Data Move **Compliance Suite Alerts** COBIT: Neoteris Files Accessed COBIT: NetApp Filer Unauthorized Mounting COBIT: RACF Files Accessed COBIT: vCenter Datastore Event COBIT: vCenter Data Move COBIT: vCenter Orchestrator Data Move COBIT: vCenter Orchestrator Datastore Events COBIT: Windows Files Accessed
DS5.3	Identity Management (1/4)	**Compliance Suite Reports** COBIT: Files Accessed Through Pulse Connect Secure COBIT: Pulse Connect Secure Successful Logins COBIT: Accepted VPN Connections - RADIUS COBIT: Account Activities on Windows Servers COBIT: Accounts Changed on NetApp Filer COBIT: Accounts Changed on Sidewinder COBIT: Accounts Changed on TIBCO Administrator COBIT: Accounts Changed on UNIX Servers COBIT: Accounts Changed on Windows Servers COBIT: Accounts Created on NetApp Filer

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3	Identity Management (1/4)	**Compliance Suite Reports** (*Cont.*) COBIT: Accounts Created on NetApp Filer Audit COBIT: Accounts Created on Sidewinder COBIT: Accounts Created on Symantec Endpoint Protection COBIT: Accounts Created on TIBCO ActiveMatrix Administrator COBIT: Accounts Created on TIBCO Administrator COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Check Point Management Station Login COBIT: Cisco ISE, ACS Accounts Created COBIT: DB2 Database Failed Logins COBIT: DB2 Database Successful Logins COBIT: DB2 Database User Additions and Deletions COBIT: Denied VPN Connections - RADIUS COBIT: ESX Accounts Activities COBIT: ESX Accounts Created COBIT: ESX Failed Logins COBIT: ESX Group Activities COBIT: ESX Logins Failed Unknown User COBIT: ESX Logins Succeeded COBIT: F5 BIG-IP TMOS Login Failed COBIT: F5 BIG-IP TMOS Login Successful COBIT: Failed Logins COBIT: Files Accessed on NetApp Filer Audit COBIT: Files Accessed through Juniper SSL VPN (Secure Access) COBIT: Groups Deleted on UNIX Servers COBIT: Groups Deleted on Windows Servers COBIT: Guardium SQL Guard Audit Logins COBIT: Guardium SQL Guard Logins COBIT: Group Activities on NetApp Filer Audit COBIT: Group Activities on Symantec Endpoint Protection COBIT: Group Activities on TIBCO ActiveMatrix Administrator

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3	Identity Management (1/4)	**Compliance Suite Reports** (*Cont.*) COBIT: HP NonStop Audit Login Failed COBIT: HP NonStop Audit Login Successful COBIT: HP NonStop Audit Object Changes COBIT: HP NonStop Audit Permissions Changed COBIT: i5/OS Network Authentication Events COBIT: i5/OS User Profile Creation, Modification, or Restoration COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Logins by Authentication Type COBIT: LogLogic DSM Logins COBIT: LogLogic Management Center Account Activities COBIT: LogLogic Management Center Login COBIT: Microsoft Operations Manager - Windows Accounts Activities COBIT: Microsoft Operations Manager - Windows Accounts Changed COBIT: Microsoft Operations Manager - Windows Accounts Created COBIT: Microsoft Operations Manager - Windows Events by Users COBIT: Microsoft Operations Manager - Windows Permissions Modified COBIT: Microsoft Operations Manager - Windows Policies Modified COBIT: Microsoft Sharepoint Permissions Changed COBIT: Microsoft Sharepoint Policy Add, Remove, or Modify COBIT: Microsoft SQL Server Database Failed Logins COBIT: Microsoft SQL Server Database Successful Logins COBIT: NetApp Filer Audit Login Failed COBIT: NetApp Filer Audit Login Successful COBIT: NetApp Filer File Activity COBIT: NetApp Filer Login Failed COBIT: NetApp Filer Login Successful

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3	Identity Management (1/4)	**Compliance Suite Reports** (*Cont.*) COBIT: Oracle Database Failed Logins COBIT: Oracle Database Successful Logins COBIT: Oracle Database User Additions and Deletions COBIT: RACF Accounts Created COBIT: RACF Accounts Modified COBIT: RACF Failed Logins COBIT: RACF Files Accessed COBIT: RACF Permissions Changed COBIT: RACF Successful Logins COBIT: Successful Logins COBIT: Sybase ASE Database User Additions and Deletions COBIT: Sybase ASE Successful Logins COBIT: Sybase ASE Failed Logins COBIT: TIBCO ActiveMatrix Administrator Failed Logins COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TIBCO ActiveMatrix Administrator Successful Logins COBIT: TIBCO Administrator Permission Changes COBIT: Unauthorized Logins COBIT: Unencrypted Logins COBIT: UNIX Failed Logins COBIT: Users Created on Servers COBIT: vCenter Datastore Events COBIT: vCenter Data Move COBIT: vCenter Failed Logins COBIT: vCenter Orchestrator Datastore Events COBIT: vCenter Orchestrator Data Move COBIT: vCenter Orchestrator Failed Logins COBIT: vCenter Successful Logins COBIT: vCenter User Permission Change

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3	Identity Management (1/4)	**Compliance Suite Reports** (*Cont.*) COBIT: vCloud Failed Logins COBIT: vCloud Successful Logins COBIT: vCloud User Created COBIT: VPN Users Accessing Corporate Network COBIT: Windows Accounts Enabled **Compliance Suite Alerts** COBIT: Accounts Created COBIT: Accounts Enabled COBIT: Accounts Modified COBIT: Cisco PIX, ASA, FWSM Logon Failure COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: DB2 Database User Added or Dropped COBIT: Guardium SQL Guard Logins COBIT: Groups Created COBIT: Group Members Added COBIT: HP NonStop Audit Permission Changed COBIT: i5/OS Network Profile Changes COBIT: i5/OS Permission or Policy Change COBIT: i5/OS User Profile Changes COBIT: Juniper Firewall Logon Failure COBIT: Juniper Firewall Logon Success COBIT: Logins Succeeded COBIT: Logins Failed COBIT: LogLogic DSM Logins COBIT: Microsoft Operations Manager - Permissions Changed COBIT: Microsoft Operations Manager - Windows Policies Changed COBIT: Microsoft Sharepoint Permission Changed COBIT: Microsoft Sharepoint Policies Added, Removed, Modified COBIT: NetApp Filer Audit Policies Changed COBIT: NetApp Authentication Failure COBIT: NetApp Filer NIS Group Update

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3	Identity Management (1/4)	**Compliance Suite Alerts** (*Cont.*) COBIT: Oracle Database User Added or Deleted COBIT: RACF Files Accessed COBIT: RACF Permissions Changed COBIT: Symantec Endpoint Protection Policy Add, Delete, Modify COBIT: TIBCO ActiveMatrix Administrator Permission Changed COBIT: UNIX Groups Added COBIT: UNIX Groups Deleted COBIT: UNIX Groups Modified COBIT: vCenter Datastore Event COBIT: vCenter Data Move COBIT: vCenter Orchestrator Data Move COBIT: vCenter Orchestrator Datastore Events COBIT: vCenter Orchestrator Login Failed COBIT: vCenter Permission Change COBIT: vCenter User Login Successful COBIT: vCloud Director Login Success COBIT: vCloud User Created COBIT: vCenter User Login Failed COBIT: vCloud Director Login Failed COBIT: Windows Group Members Added COBIT: Windows Groups Created

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3 (2/4)	Identity Management (2/4)	**Compliance Suite Reports** COBIT: Account Activities on UNIX Servers COBIT: Account Activities on Windows Servers COBIT: Check Point Management Station Login COBIT: DB2 Database Successful Logins COBIT: Escalated Privilege Activities on Servers COBIT: Files Accessed on Servers COBIT: Group Activities on UNIX Servers COBIT: Group Activities on Windows Servers COBIT: Groups Deleted on TIBCO ActiveMatrix Administrator COBIT: i5/OS Access Control List Modifications COBIT: i5/OS Network Authentication Events COBIT: Juniper Firewall Escalated Privilege COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Logins by Authentication Type COBIT: Microsoft SQL Server Database Successful Logins COBIT: Oracle Database Successful Logins COBIT: Permissions Modified on Windows Servers COBIT: Policies Modified on Windows Servers COBIT: Successful Logins COBIT: Sybase ASE Successful Logins COBIT: Unauthorized Logins COBIT: Unencrypted Logins COBIT: VPN Users Accessing Corporate Network COBIT: Windows Events by Users COBIT: Windows Programs Accessed

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3 (2/4)	Identity Management (2/4)	**Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: Juniper Firewall Logon Success COBIT: Neoteris Files Accessed COBIT: NetApp Filer Unauthorized Mounting COBIT: Logins Succeeded COBIT: UNIX Groups Added COBIT: UNIX Groups Deleted COBIT: UNIX Groups Modified COBIT: UNIX Privilege Escalated COBIT: Windows Files Accessed COBIT: Windows Permissions Changed COBIT: Windows Policies Changed COBIT: Windows Privileges Escalated
DS5.3 (3/4)	Identity Management (3/4)	**Compliance Suite Reports** COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Groups Deleted on UNIX Servers COBIT: Groups Deleted on Windows Servers COBIT: i5/OS Access Control List Modifications COBIT: i5/OS User Profile Creation, Modification, or Restoration COBIT: Microsoft SQL Server Database User Additions and Deletions COBIT: Permissions Modified on Windows Servers COBIT: Policies Modified on Windows Servers COBIT: Users Created on Servers COBIT: Windows Accounts Enabled COBIT: Windows Group Members Added

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3 (3/4)	Identity Management (3/4)	**Compliance Suite Alerts** COBIT: Accounts Enabled COBIT: UNIX Groups Added COBIT: UNIX Groups Deleted COBIT: UNIX Groups Modified COBIT: Windows Groups Created COBIT: Windows Group Members Added COBIT: Windows Policies Changed COBIT: Windows Permissions Changed
DS5.3 (4/4)	Identity Management (4/4)	**Compliance Suite Reports** COBIT: Account Activities on UNIX Servers COBIT: Account Activities on Windows Servers COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Check Point Management Station Login COBIT: DB2 Database Successful Logins COBIT: Escalated Privilege Activities on Servers COBIT: Failed Logins COBIT: Files Accessed on Servers COBIT: Files Accessed through PANOS COBIT: Group Activities on UNIX Servers COBIT: Group Activities on Windows Servers COBIT: Groups Deleted on NetApp Filer Audit COBIT: Groups Deleted on UNIX Servers COBIT: Groups Deleted on Windows Servers COBIT: i5/OS Access Control List Modifications COBIT: i5/OS Network Authentication Events COBIT: i5/OS User Profile Creation, Modification, or Restoration COBIT: Juniper Firewall Escalated Privilege COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3 (4/4)	Identity Management (4/4)	**Compliance Suite Reports** (*Cont.*) COBIT: Logins by Authentication Type COBIT: Microsoft SQL Server Database Failed Logins COBIT: Microsoft SQL Server Database Successful Logins COBIT: NetApp Filer Audit Accounts Enabled COBIT: NetApp Filer Audit Group Members Added COBIT: Oracle Database Successful Logins COBIT: Permissions Modified on Windows Servers COBIT: Policies Modified on Windows Servers COBIT: Successful Logins COBIT: Sybase ASE Failed Logins COBIT: Sybase ASE Successful Logins COBIT: Unauthorized Logins COBIT: Unencrypted Logins COBIT: UNIX Failed Logins COBIT: Users Created on Servers COBIT: VPN Users Accessing Corporate Network COBIT: Windows Accounts Enabled COBIT: Windows Events by Users COBIT: Windows Group Members Added COBIT: Windows Programs Accessed **Compliance Suite Alerts** COBIT: Accounts Enabled COBIT: Cisco PIX, ASA, FWSM Logon Failure COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: Juniper Firewall Logon Failure COBIT: Juniper Firewall Logon Success COBIT: Logins Failed COBIT: Logins Succeeded COBIT: Neoteris Files Accessed COBIT: NetApp Authentication Failure COBIT: NetApp Filer NIS Group Update COBIT: NetApp Filer Unauthorized Mounting

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.3 (4/4)	Identity Management (4/4)	**Compliance Suite Alerts** (*Cont.*) COBIT: UNIX Groups Added COBIT: UNIX Groups Deleted COBIT: UNIX Groups Modified COBIT: UNIX Privilege Escalated COBIT: Windows Files Accessed COBIT: Windows Groups Created COBIT: Windows Group Members Added COBIT: Windows Permissions Changed COBIT: Windows Policies Changed COBIT: Windows Privileges Escalated
DS5.4	User Account Management	**Compliance Suite Reports** COBIT: Account Activities on UNIX Servers COBIT: Account Activities on Windows Servers COBIT: Accounts Created on NetApp Filer COBIT: Accounts Created on NetApp Filer Audit COBIT: Accounts Created on Sidewinder COBIT: Accounts Created on Symantec Endpoint Protection COBIT: Accounts Created on TIBCO ActiveMatrix Administrator COBIT: Accounts Created on TIBCO Administrator COBIT: Accounts Created on UNIX Servers COBIT: Accounts Created on Windows Servers COBIT: Accounts Deleted on NetApp Filer COBIT: Accounts Deleted on NetApp Filer Audit COBIT: Accounts Deleted on Sidewinder COBIT: Accounts Deleted on Symantec Endpoint Protection COBIT: Accounts Deleted on TIBCO ActiveMatrix Administrator COBIT: Accounts Deleted on TIBCO Administrator COBIT: Accounts Deleted on UNIX Servers COBIT: Accounts Deleted on Windows Servers COBIT: Cisco ISE, ACS Accounts Created COBIT: Cisco ISE, ACS Accounts Removed

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.4	User Account Management	**Compliance Suite Reports** (*Cont.*) COBIT: Cisco ISE, ACS Password Changes COBIT: DB2 Database User Additions and Deletions COBIT: ESX Accounts Activities COBIT: ESX Accounts Created COBIT: ESX Accounts Deleted COBIT: ESX Group Activities COBIT: F5 BIG-IP TMOS Password Changes COBIT: Group Activities on NetApp Filer Audit COBIT: Group Activities on Symantec Endpoint Protection COBIT: Group Activities on TIBCO ActiveMatrix Administrator COBIT: Group Activities on UNIX Servers COBIT: Group Activities on Windows Servers COBIT: Groups Created on NetApp Filer Audit COBIT: Groups Created on TIBCO ActiveMatrix Administrator COBIT: Groups Created on UNIX Servers COBIT: Groups Created on Windows Servers COBIT: Groups Deleted on NetApp Filer Audit COBIT: Groups Deleted on TIBCO ActiveMatrix Administrator COBIT: Groups Deleted on UNIX Servers COBIT: Groups Deleted on Windows Servers COBIT: HP NonStop Audit Object Changes COBIT: HP NonStop Audit Permissions Changed COBIT: i5/OS Access Control List Modifications COBIT: i5/OS Audit Configuration Changes COBIT: i5/OS DST Password Reset COBIT: i5/OS Server Security User Information Actions COBIT: i5/OS User Profile Creation, Modification, or Restoration COBIT: LogLogic Management Center Account Activities COBIT: LogLogic Management Center Password Changes

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.4	User Account Management	COBIT: Microsoft Operations Manager - Windows Accounts Activities COBIT: Microsoft Operations Manager - Windows Accounts Created COBIT: Microsoft Operations Manager - Windows Password Changes COBIT: Microsoft Operations Manager - Windows Permissions Modified COBIT: Microsoft Sharepoint Permissions Changed COBIT: Microsoft Sharepoint Policy Add, Remove, or Modify COBIT: Microsoft SQL Server Database User Additions and Deletions COBIT: Microsoft SQL Server Password Changes COBIT: NetApp Filer Audit Group Members Deleted COBIT: NetApp Filer Password Changes COBIT: Oracle Database User Additions and Deletions COBIT: Password Changes on Windows Servers COBIT: Permissions Modified on Windows Servers COBIT: RACF Accounts Created COBIT: RACF Accounts Deleted COBIT: RACF Password Changed COBIT: RACF Permissions Changed COBIT: Sybase ASE Database User Additions and Deletions COBIT: Symantec Endpoint Protection Password Changes COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TIBCO ActiveMatrix Administrator Permission Changed COBIT: TIBCO Administrator Password Changes COBIT: TIBCO Administrator Permission Changes COBIT: Users Removed from Servers COBIT: vCenter User Permission Change COBIT: vCloud User Created COBIT: vCloud User Deleted or Removed COBIT: Windows Group Members Deleted

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.4	User Account Management	**Compliance Suite Alerts** COBIT: Accounts Created COBIT: Accounts Deleted COBIT: Accounts Locked COBIT: Cisco ISE, ACS Passwords Changed COBIT: DB2 Database User Added or Dropped COBIT: Groups Created COBIT: Group Members Added COBIT: HP NonStop Audit Permission Changed COBIT: i5/OS Permission or Policy Change COBIT: IBM AIX Password Changed COBIT: LogLogic Management Center Passwords Changed COBIT: Microsoft Operations Manager - Permissions Changed COBIT: Microsoft Operations Manager - Windows Passwords Changed COBIT: Microsoft Sharepoint Permission Changed COBIT: Microsoft Sharepoint Policies Added, Removed, Modified COBIT: Oracle Database User Added or Deleted COBIT: RACF Passwords Changed COBIT: RACF Permissions Changed COBIT: Symantec Endpoint Protection Policy Add, Delete, Modify COBIT: UNIX Groups Added COBIT: vCenter Permission Change COBIT: vCloud User Created COBIT: Windows Groups Created COBIT: Windows Group Members Added COBIT: Windows Passwords Changed COBIT: Windows Permissions Changed
DS5.5	Security Testing, Surveillance, and Monitoring	**Compliance Suite Reports** COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.7	Protection of Security Technology	**Compliance Suite Reports** COBIT: Decru DataFort Zeroization Events COBIT: Tripwire Modifications, Additions, and Deletions
DS5.8	Cryptographic Key Management	**Compliance Suite Reports** COBIT: Check Point SIC Revoked COBIT: Decru DataFort Cryptographic Key Events COBIT: Decru DataFort Zeroization Events COBIT: i5/OS Key Ring File Events

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (1/2)	**Compliance Suite Reports** COBIT: Applications Under Attack - FireEye MPS COBIT: Attackers by Service - FireEye MPS COBIT: Attackers by Signature - FireEye MPS COBIT: FireEye MPS - Attackers by Event ID COBIT: FireEye MPS - Attackers by Threat Name COBIT: FireEye MPS - Attacks Detected COBIT: Pulse Connect Secure Successful Logins COBIT: Servers Under Attacks - FireEye MPS COBIT: Source of Attack - FireEye MPS COBIT: Accepted VPN Connections - RADIUS COBIT: Active Connections for Cisco ASA COBIT: Active Connections for Cisco FWSM COBIT: Active Connections for Cisco PIX COBIT: Allowed URLs by Source IPs COBIT: Allowed URLs by Source IPs - F5 BIG-IP TMOS COBIT: Allowed URLs by Source IPs - Microsoft IIS COBIT: Allowed URLs by Source Users COBIT: Allowed URLs by Source Users - F5 BIG-IP TMOS COBIT: Allowed URLs by Source Users - Microsoft IIS COBIT: Applications Under Attack COBIT: Applications Under Attack - Cisco IOS COBIT: Applications Under Attack - ISS SiteProtector COBIT: Applications Under Attack - SiteProtector COBIT: Applications Under Attack - Sourcefire Defense Center COBIT: Attackers by Service COBIT: Attackers by Service - Cisco IOS COBIT: Attackers by Service - ISS SiteProtector COBIT: Attackers by Service - SiteProtector COBIT: Attackers by Service - Sourcefire Defense Center COBIT: Attackers by Signature COBIT: Attackers by Signature - Cisco IOS

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Attackers by Signature - ISS SiteProtector

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (1/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Attackers by Signature - SiteProtector COBIT: Attackers by Signature - Sourcefire Defense Center COBIT: Attacks Detected COBIT: Attacks Detected - Cisco IOS COBIT: Attacks Detected - HIPS COBIT: Attacks Detected - ISS SiteProtector COBIT: Attacks Detected - Sourcefire Defense Center COBIT: Attacks Detected - SiteProtector COBIT: Blocked URLs by Source IPs COBIT: Blocked URLs by Source IPs - F5 BIG-IP TMOS COBIT: Blocked URLs by Source IPs - Microsoft IIS COBIT: Blocked URLs by Source Users COBIT: Blocked URLs by Source Users - F5 BIG-IP TMOS COBIT: Blocked URLs by Source Users - Microsoft IIS COBIT: Check Point Management Station Login COBIT: Cisco ESA: Attacks by Event ID COBIT: Cisco ESA: Attacks Detected COBIT: Cisco ESA: Attacks by Threat Name COBIT: Cisco ESA: Scans COBIT: DB2 Database Successful Logins COBIT: Denied Connections by IP Addresses - Check Point COBIT: Denied Connections by IP Addresses - Cisco ASA COBIT: Denied Connections by IP Addresses - Cisco FWSM COBIT: Denied Connections by IP Addresses - Cisco PIX COBIT: Denied Connections by IP Addresses - Nortel COBIT: Denied Connections - Cisco IOS COBIT: Denied Connections - Cisco NXOS COBIT: Denied Connections - Cisco Router COBIT: Denied Connections - F5 BIG-IP TMOS COBIT: Denied Connections - Sidewinder

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Denied Connections - VMware vShield COBIT: Denied Inbound Connections - Cisco ASA COBIT: Denied Inbound Connections - Cisco FWSM
DS5.10	Network Security (1/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Denied Inbound Connections - Cisco PIX COBIT: Denied Inbound Connections - Check Point

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (2/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Denied Inbound Connections - Juniper Firewall COBIT: Denied Outbound Connections - Check Point COBIT: Denied Outbound Connections - Cisco ASA COBIT: Denied Outbound Connections - Cisco FWSM COBIT: Denied Outbound Connections - Cisco PIX COBIT: Denied Outbound Connections - Juniper Firewall COBIT: ESX Logins Succeeded COBIT: F5 BIG-IP TMOS Login Successful COBIT: FortiOS: Attacks by Event ID COBIT: FortiOS: Attacks by Threat Name COBIT: FortiOS: Attacks Detected COBIT: FortiOS DLP Attacks Detected COBIT: Guardium SQL Guard Audit Logins COBIT: Guardium SQL Guard Logins COBIT: HP NonStop Audit Login Successful COBIT: i5/OS Internet Security Management Events COBIT: Juniper SSL VPN Successful Logins COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Logins by Authentication Type COBIT: LogLogic DSM Logins COBIT: LogLogic Management Center Login COBIT: McAfee AntiVirus: Attacks by Event ID COBIT: McAfee AntiVirus: Attacks by Threat Name COBIT: McAfee AntiVirus: Attacks Detected COBIT: Microsoft SQL Server Database Successful Logins COBIT: Most Active Ports Through Firewall - Check Point COBIT: Most Active Ports Through Firewall - Cisco ASA COBIT: Most Active Ports Through Firewall - Cisco FWSM COBIT: Most Active Ports Through Firewall - Cisco PIX

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Most Active Ports Through Firewall - Fortinet

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (2/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Most Active Ports Through Firewall - Juniper Firewall COBIT: Most Active Ports Through Firewall - Nortel COBIT: NetApp Filer Audit Login Successful COBIT: NetApp Filer Login Successful COBIT: Network Traffic per Rule - Check Point COBIT: Network Traffic per Rule - Juniper Firewall COBIT: Network Traffic per Rule - Nortel COBIT: Oracle Database Successful Logins COBIT: PANOS: Attacks by Event ID COBIT: PANOS: Attacks by Threat Name COBIT: PANOS: Attacks Detected COBIT: Ports Allowed Access - Check Point COBIT: Ports Allowed Access - Cisco ASA COBIT: Ports Allowed Access - Cisco IOS COBIT: Ports Allowed Access - Cisco FWSM COBIT: Ports Allowed Access - Cisco Netflow COBIT: Ports Allowed Access - Cisco PIX COBIT: Ports Allowed Access - F5 BIG-IP TMOS COBIT: Ports Allowed Access - Fortinet COBIT: Ports Allowed Access - Juniper JunOS COBIT: Ports Allowed Access - Juniper Firewall COBIT: Ports Allowed Access - Juniper RT Flow COBIT: Ports Allowed Access - Nortel COBIT: Ports Allowed Access - PANOS COBIT: Ports Allowed Access - Sidewinder COBIT: Ports Allowed Access - VMware vShield COBIT: Ports Denied Access - Check Point COBIT: Ports Denied Access - Cisco ASA COBIT: Ports Denied Access - Cisco FWSM COBIT: Ports Denied Access - Cisco IOS COBIT: Ports Denied Access - Cisco PIX COBIT: Ports Denied Access - Cisco Router COBIT: Ports Denied Access - F5 BIG-IP TMOS

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Ports Denied Access - Fortinet

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (2/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Ports Denied Access - Juniper JunOS COBIT: Ports Denied Access - Juniper Firewall COBIT: Ports Denied Access - Juniper RT Flow COBIT: Ports Denied Access - Nortel COBIT: Ports Denied Access - PANOS COBIT: Ports Denied Access - Sidewinder COBIT: Ports Denied Access - VMware vShield COBIT: RACF Successful Logins COBIT: Servers Under Attack COBIT: Servers Under Attack - Cisco IOS COBIT: Servers Under Attack - HIPS COBIT: Servers Under Attack - ISS SiteProtector COBIT: Servers Under Attack - SiteProtector COBIT: Servers Under Attack - Sourcefire Defense Center COBIT: Source of Attacks COBIT: Source of Attacks - Cisco IOS COBIT: Source of Attacks - HIPS COBIT: Source of Attacks - ISS SiteProtector COBIT: Source of Attacks - SiteProtector COBIT: Source of Attacks - Sourcefire Defense Center COBIT: Sybase ASE Successful Logins COBIT: Symantec AntiVirus: Attacks by Threat Name COBIT: Symantec AntiVirus: Attacks Detected COBIT: Symantec AntiVirus: Scans COBIT: Symantec Endpoint Protection: Attacks Detected COBIT: Symantec Endpoint Protection: Attacks by Threat Name COBIT: Symantec Endpoint Protection: Scans COBIT: Successful Logins COBIT: TIBCO ActiveMatrix Administrator Permission Changes COBIT: TrendMicro Control Manager: Attacks Detected

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: TrendMicro Control Manager: Attacks Detected by Threat Name

Control Objective	Description	Compliance Suite Reports and Alerts
DS5.10	Network Security (2/2)	**Compliance Suite Reports** (*Cont.*) COBIT: TrendMicro OfficeScan: Attacks Detected COBIT: TrendMicro OfficeScan: Attacks Detected by Threat Name COBIT: Unencrypted Logins COBIT: Unencrypted Network Services - Check Point COBIT: Unencrypted Network Services - Cisco ASA COBIT: Unencrypted Network Services - Cisco FWSM COBIT: Unencrypted Network Services - Cisco IOS COBIT: Unencrypted Network Services - Cisco Netflow COBIT: Unencrypted Network Services - Cisco PIX COBIT: Unencrypted Network Services - F5 BIG-IP TMOS COBIT: Unencrypted Network Services - Fortinet COBIT: Unencrypted Network Services - Juniper Firewall COBIT: Unencrypted Network Services - Juniper JunOS COBIT: Unencrypted Network Services - Juniper RT Flow COBIT: Unencrypted Network Services - Nortel COBIT: Unencrypted Network Services - PANOS COBIT: Unencrypted Network Services - Sidewinder COBIT: Unencrypted Network Services - VMware vShield COBIT: Users Using the Proxies COBIT: Users Using the Proxies - Blue Coat Proxy COBIT: Users Using the Proxies - Cisco WSA COBIT: Users Using the Proxies - Microsoft IIS COBIT: vCenter Successful Logins COBIT: vCloud Successful Logins COBIT: VPN Connections by Users COBIT: VPN Sessions by Destination IPs COBIT: VPN Sessions by Source IPs COBIT: VPN Sessions by Users COBIT: VPN Denied Connections by Users COBIT: Web Access from All Users

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Web Access from All Users - Fortinet COBIT: Web Access from All Users - PANOS COBIT: Web Access to Applications
DS5.10	Network Security (2/2)	**Compliance Suite Reports** (*Cont.*) COBIT: Web Access to Applications - F5 BIG-IP TMOS COBIT: Web Access to Applications - Microsoft IIS COBIT: Web Access to Applications - Fortinet COBIT: Web Access to Applications - PANOS COBIT: Web Access from All Users - F5 BIG-IP TMOS COBIT: Web Access from All Users - Microsoft IIS COBIT: Web URLs Visited COBIT: Web URLs Visited - F5 BIG-IP TMOS COBIT: Web URLs Visited - Fortinet COBIT: Web URLs Visited - Microsoft IIS COBIT: Web URLs Visited - PANOS COBIT: Web URLs Visited via Proxy COBIT: Web URLs Visited via Proxy - Blue Coat Proxy COBIT: Web URLs Visited via Proxy - Cisco WSA COBIT: Web URLs Visited via Proxy - Microsoft IIS **Compliance Suite Alerts** COBIT: Active Directory Changes COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: Disallowed Services COBIT: Guardium SQL Guard Logins COBIT: Juniper Firewall Logon Success COBIT: Logins Succeeded
DS5.10	Network Security (2/2)	**Compliance Suite Alerts** (*Cont.*) COBIT: LogLogic DSM Logins COBIT: Excessive IDS Attack COBIT: vCenter User Login Successful COBIT: vCloud Director Login Success
DS9 Manage the Configuration		

Control Objective	Description	Compliance Suite Reports and Alerts
DS9.3	Configuration Integrity Review	**Compliance Suite Reports** COBIT: Check Point Management Station Login COBIT: Cisco PIX, ASA, FWSM Policy Changed COBIT: Cisco Switch Policy Changes COBIT: Pulse Connect Secure Policy Changed COBIT: Pulse Connect Secure Successful Logins

Control Objective	Description	Compliance Suite Reports and Alerts
DS9.3	Configuration Integrity Review	**Compliance Suite Reports** (*Cont.*) COBIT: DB2 Database Successful Logins COBIT: ESX Kernel log daemon terminating COBIT: ESX Kernel logging Stop COBIT: ESX Logins Succeeded COBIT: ESX Syslogd Restart COBIT: F5 BIG-IP TMOS Login Successful COBIT: Guardium SQL Guard Audit Logins COBIT: Guardium SQL Guard Logins COBIT: HP NonStop Audit Login Successful COBIT: Juniper Firewall Policy Changed COBIT: Juniper SSL VPN (Secure Access) Policy Changed COBIT: Juniper SSL VPN (Secure Access) Successful Logins COBIT: Juniper SSL VPN Successful Logins COBIT: Logins by Authentication Type COBIT: LogLogic DSM Logins COBIT: LogLogic Management Center Login COBIT: Microsoft SQL Server Database Successful Logins COBIT: Microsoft SQL Server Schema Corruption COBIT: NetApp Filer Audit Login Successful COBIT: NetApp Filer Audit Policies Modified COBIT: NetApp Filer Login Successful COBIT: Oracle Database Successful Logins COBIT: RACF Successful Logins COBIT: Successful Logins COBIT: Sybase ASE Successful Logins COBIT: Symantec Endpoint Protection Policy Add, Remove, or Modify COBIT: TIBCO ActiveMatrix Administrator Successful Logins COBIT: Tripwire Modifications, Additions, and Deletions COBIT: Unencrypted Logins COBIT: vCenter Change Attributes

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: vCenter Orchestrator Change Attributes COBIT: vCenter Orchestrator Virtual Machine Created

Control Objective	Description	Compliance Suite Reports and Alerts
DS9.3	Configuration Integrity Review	**Compliance Suite Reports** (*Cont.*) COBIT: vCenter Orchestrator Virtual Machine Deleted COBIT: vCenter Modify Firewall Policy COBIT: vCenter Orchestrator vSwitch Added, Changed or Removed COBIT: vCenter Resource Usage Change COBIT: vCenter Restart ESX Services COBIT: vCenter Successful Logins COBIT: vCenter Virtual Machine Created COBIT: vCenter Virtual Machine Deleted COBIT: vCenter vSwitch Added, Changed or Removed COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud Successful Logins COBIT: vCloud vApp Created, Modified, or Deleted COBIT: vCloud vDC Created, Modified, or Deleted COBIT: vShield Edge Configuration Changes COBIT: Windows Programs Accessed **Compliance Suite Alerts** COBIT: Cisco PIX, ASA, FWSM Logon Success COBIT: Cisco PIX, ASA, FWSM Policy Changed COBIT: Cisco Switch Policy Changed COBIT: Guardium SQL Guard Logins COBIT: Juniper Firewall Policy Changes COBIT: Juniper Firewall Logon Success COBIT: Juniper Firewall Policy Out of Sync COBIT: Juniper VPN Policy Change COBIT: Logins Succeeded COBIT: LogLogic DSM Logins COBIT: Microsoft Operations Manager - Windows Policies Changed COBIT: Pulse Connect Secure Policy Change COBIT: NetApp Filer Audit Policies Changed COBIT: vCenter Create Virtual Machine

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: vCenter Delete Virtual Machine COBIT: vCenter Firewall Policy Change
DS9.3	Configuration Integrity Review	**Compliance Suite Alerts** (*Cont.*) COBIT: vCenter Orchestrator vSwitch Add, Modify or Delete COBIT: vCenter Orchestrator Create Virtual Machine COBIT: vCenter Orchestrator Delete Virtual Machine COBIT: vCenter Restart ESX Services COBIT: vCenter User Login Successful COBIT: vCenter vSwitch Add, Modify or Delete COBIT: vCloud Director Login Success COBIT: vCloud Organization Created COBIT: vCloud Organization Deleted COBIT: vCloud Organization Modified COBIT: vCloud vApp Created, Deleted, or Modified COBIT: vCloud vDC Created, Modified, or Deleted COBIT: vShield Edge Configuration Change COBIT: Windows Policies Changed COBIT: Windows Programs Accessed
DS10 Manage Problems		
DS10.2	Problem Tracking and Resolution	**Compliance Suite Reports** COBIT: DHCP Granted/Renewed Activities on Microsoft DHCP COBIT: DHCP Granted/Renewed Activities on VMware vShield COBIT: LogLogic File Retrieval Errors COBIT: LogLogic Message Routing Errors Compliance Suite Alert COBIT: LogLogic Message Routing Errors COBIT: LogLogic File Retrieval Errors
DS11 Manage Data		

Control Objective	Description	Compliance Suite Reports and Alerts
DS11.2	Storage and Retention Arrangements	**Compliance Suite Reports** COBIT: DB2 Database Backup Failed COBIT: i5/OS Restore Events COBIT: LogLogic Management Center Backup Activities
DS11.2	Storage and Retention Arrangements	**Compliance Suite Reports** (*Cont.*) COBIT: LogLogic Management Center Restore Activities COBIT: Microsoft SQL Server Backup Failed COBIT: NetApp Filer Snapshot Error COBIT: Sybase ASE Database Backup and Restoration Compliance Suite Alert COBIT: DB2 Database Backup Failed COBIT: LogLogic Management Center Backed Up or Restored COBIT: Microsoft SQL Server Backup Failed COBIT: NetApp Filer Snapshot Error COBIT: Sybase ASE Database Backed Up or Restored

Control Objective	Description	Compliance Suite Reports and Alerts
DS11.5	Backup and Restoration	**Compliance Suite Reports** COBIT: DB2 Database Backup Failed COBIT: DB2 Database Restore Failed COBIT: i5/OS Restore Events COBIT: LogLogic Management Center Backup Activities COBIT: LogLogic Management Center Restore Activities COBIT: Microsoft SQL Server Backup Failed COBIT: Microsoft SQL Server Restore Failed COBIT: NetApp Filer Snapshot Error COBIT: Sybase ASE Database Backup and Restoration **Compliance Suite Alerts** COBIT: DB2 Database Backup Failed COBIT: DB2 Database Restore Failed COBIT: LogLogic Management Center Backed Up or Restored COBIT: Microsoft SQL Server Backup Failed COBIT: Microsoft SQL Server Restore Failed COBIT: NetApp Filer Snapshot Error COBIT: Sybase ASE Database Backed Up or Restored

Control Objective	Description	Compliance Suite Reports and Alerts
DS11.6	Security Requirements for Data Management	**Compliance Suite Reports** COBIT: Active Directory System Changes COBIT: Microsoft Operations Manager - Windows Policies Modified COBIT: Policies Modified on Windows Servers COBIT: Ports Allowed Access - Check Point COBIT: Ports Allowed Access - Cisco ASA COBIT: Ports Allowed Access - Cisco FWSM COBIT: Ports Allowed Access - Cisco IOS COBIT: Ports Allowed Access - Cisco Netflow COBIT: Ports Allowed Access - Cisco PIX COBIT: Ports Allowed Access - F5 BIG-IP TMOS COBIT: Ports Allowed Access - Fortinet COBIT: Ports Allowed Access - Juniper Firewall COBIT: Ports Allowed Access - Juniper JunOS COBIT: Ports Allowed Access - Juniper RT Flow COBIT: Ports Allowed Access - Nortel COBIT: Ports Allowed Access - PANOS COBIT: Ports Allowed Access - Sidewinder COBIT: Ports Allowed Access - VMware vShield COBIT: Unencrypted Network Services - Check Point COBIT: Unencrypted Network Services - Cisco ASA COBIT: Unencrypted Network Services - Cisco FWSM COBIT: Unencrypted Network Services - Cisco IOS COBIT: Unencrypted Network Services - Cisco Netflow COBIT: Unencrypted Network Services - Cisco PIX COBIT: Unencrypted Network Services - F5 BIG-IP TMOS COBIT: Unencrypted Network Services - Fortinet COBIT: Unencrypted Network Services - Juniper Firewall COBIT: Unencrypted Network Services - Juniper JunOS COBIT: Unencrypted Network Services - Juniper RT Flow COBIT: Unencrypted Network Services - Nortel

Control Objective	Description	Compliance Suite Reports and Alerts
		COBIT: Unencrypted Network Services - PANOS COBIT: Unencrypted Network Services - Sidewinder COBIT: Unencrypted Network Services - VMware vShield
DS13 Manage Operations		
DS13.3	IT Infrastructure Monitoring	**Compliance Suite Reports** COBIT: LogLogic File Retrieval Errors COBIT: LogLogic Message Routing Errors COBIT: NetApp Filer Audit Logs Cleared COBIT: Periodic Review of Log Reports COBIT: Periodic Review of User Access Logs COBIT: Windows Audit Logs Cleared Compliance Suite Alert COBIT: LogLogic Message Routing Errors COBIT: LogLogic File Retrieval Errors COBIT: Windows Audit Log Cleared

References

“Internal Control – Integrated Framework: Executive Summary”. The Committee of Sponsoring Organizations of the Treadway Commission. Available online at: http://www.coso.org/.

“IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting”. 2nd Edition. IT Governance Institute. September 2006.

“COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models”. IT Governance Institute. 2007.

“Auditing Standard No. 5 – An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements”. Public Company Accounting Oversight Board. June 12, 2007.

“Board Approves New Audit Standard For Internal Control Over Financial Reporting and, separately, Recommendations on Inspection Frequency Rule”. Public Company Accounting Oversight Board Press Release. May 24, 2007. Available online at: http://pcaobus.org/News_and_Events/News/2007/05-24.aspx.