360ADVANCED

SOC 3® Report on Controls Relevant to Security for Thermo Scientific™ SampleManager™ LIMS

Thermo Fisher Scientific, Inc.

June 1, 2024 to May 31, 2025

ThermoFisher
SCIENTIFIC

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™

THERMO FISHER SCIENTIFIC, INC.

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR’S REPORT

360 ADVANCED

INDEPENDENT SERVICE AUDITOR'S REPORT

To Thermo Fisher Scientific, Inc.:

Scope

We have examined Thermo Fisher Scientific, Inc.'s ("Thermo Fisher") assertion of Thermo Scientific™ SampleManager™ LIMS ("SampleManager LIMS") included in Section 2 of this report that the controls within Thermo Fisher's system were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Thermo Fisher's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Thermo Fisher uses Amazon Web Services, Inc. ("AWS"), a sub-service organization, for cloud hosting services. Thermo Fisher's assertion and description of the boundaries of the system, included in Section 2 and Section 3 of this report, respectively, indicate that certain applicable trust services criteria can only be met if certain types of controls at the aforementioned sub-service organization are suitably designed and operating effectively. The description does not include any of the controls expected to be implemented at the sub-service organization. Our examination did not extend to the services provided by the sub-service organization, and we have not evaluated whether the controls management expects to be implemented at the sub-service organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period June 1, 2024 to May 31, 2025.

Service Organization's Responsibilities

Thermo Fisher is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Thermo Fisher's service commitments and system requirements were achieved. Thermo Fisher has also provided the accompanying assertion titled "Management of Thermo Fisher Scientific, Inc.'s Assertion" included in Section 2 of this report about effectiveness of controls within the system. When preparing its assertion, Thermo Fisher is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Thermo Fisher's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Thermo Fisher's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusion about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Thermo Fisher's SampleManager LIMS system were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Thermo Fisher's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

360 Advanced

November 19, 2025
St. Petersburg, Florida

SECTION 2:

MANAGEMENT’S ASSERTION

MANAGEMENT OF THERMO FISHER SCIENTIFIC, INC.'S ASSERTION

November 19, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls with Thermo Fisher Scientific, Inc.'s ("Thermo Fisher") Thermo Scientific™ SampleManager™ LIMS ("SampleManager LIMS") system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Thermo Fisher's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section 3 of this report and identifies the aspects of the system covered by our assertion. Thermo Fisher Amazon Web Services, Inc. ("AWS"), a sub-service organization, for cloud hosting services. The description included in Section 3 excludes the applicable trust services criteria and related controls of the sub-service organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance the Thermo Fisher's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*. Thermo Fisher's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4 of this report.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Thermo Fisher's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Thermo Fisher Scientific, Inc.

Liz Tonks – Sr. Director, Engineering Delivery and Quality

SECTION 3:

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

Thermo Fisher provides science services, with annual revenue exceeding $40 billion. Thermo Fisher's mission is to enable its customers to make the world healthier, cleaner, and safer. Thermo Fisher strives to help customers accelerate life sciences research. Thermo Fisher has a global team of over 100,000 colleagues that deliver a combination of innovative technologies, purchasing assistance and pharmaceutical services through their brands, including Thermo Fisher, Applied Biosystems, Invitrogen, Fisher Scientific, Unity Lab Services, Patheon and PPD.

Overview of the SampleManager LIMS System

SampleManager LIMS is a complete informatics solution for lab, data, process, and compliance management, supporting a wide variety of process development, manufacturing quality assurance (QA) and quality control (QC) processes. With built-in additional Scientific Data Management System (SDMS), Electronic Laboratory Notebook (ELN), and Laboratory Execution System (LES) functionality, SampleManager LIMS assists businesses with managing their data, lab operations and procedural workflows.

The SampleManager LIMS Software offers the following capabilities, including but not limited to:

- Data Analytics – pre-configured dashboards that display key business and laboratory insights, including resource availability, stock information, location status, and lab performance
- Workflow Capabilities – configure, map, and simplify workflows for lab processes. Automates decisions and actions and easily adapts workflows to new methods and process changes.
- SDMS – enforces security and accessibility of both raw data and metadata throughout the data lifecycle

Sub-Service Organizations

Thermo Fisher uses Amazon Web Services, Inc. ("AWS"), a sub-service organization, for cloud hosting services. The description indicates that complementary sub-service organization controls that are suitably designed and operating effectively are necessary, along with controls at Thermo Fisher, to achieve Thermo Fisher's service commitments and system requirements based on the applicable trust services criteria.

The description presents Thermo Fisher's controls, the applicable trust services criteria, and the types of complementary sub-service organization controls assumed in the design of Thermo Fisher's controls. The description does not disclose the actual controls at the sub-service organization. Our examination did not include the services provided by the sub-service organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary sub-service organization controls.

Infrastructure

The SampleManager LIMS instances are hosted in AWS data center facilities. The Thermo Fisher network relevant to SampleManager LIMS consists of the corporate network and the AWS virtual IT infrastructure management tools and system components in scope (customer dedicated AWS Accounts and Virtual Private Clouds ("VPCs")). The corporate virtual private network ("VPN") defines network users and restricts their access to IT resources, including the AWS-based virtual IT infrastructure system components.

SampleManager utilizes a single tenant AWS environment infrastructure for customer instances. Infrastructure-as-a-Code (IaC) is used for configuration management to standardize the baseline environment configurations. Baseline Amazon Machine Images (AMIs) are maintained by the product services team to support their images used to launch a new instance. The AWS-based virtual IT infrastructure system components consist of a dedicated AWS account and a production VPC designed with a de-militarized zone (“DMZ”) to limit the footprint of the IT environment visible from the Internet. In the DMZ, the SampleManager LIMS perimeter includes an application load balancer that routes the traffic to an auto-scaling web server on the internal network and further to multiple application servers.

AWS VPC Security Groups and route tables are used to restrict traffic between the auto-scaling web server, a license server, and one or more internal load balancers, application servers, and database servers on the internal network. Customer data is maintained in an Amazon Relational Database Service (RDS) database, Windows File Server shared storage, and AWS Simple Storage Service (S3).

The following describes the in-scope components supporting the SampleManager LIMS system:

System / Application	Description	Infrastructure
SampleManager LIMS	SampleManager LIMS is a complete informatics solution for lab, data, process, and compliance management, supporting a wide variety of process development, manufacturing quality assurance (QA) and quality control (QC) processes.	Operating Systems: Microsoft Windows Server 2019 & 2022 Amazon Linux2 Networking: Cisco ASA 2500 Firewall Databases / Storage: Microsoft SQL Server 2019 & 2022 Amazon Aurora PostgreSQL Oracle 19c MySQL AWS S3

Software

Thermo Fisher’s system refers to the guidelines and activities for providing services to user entities and includes the infrastructure and software that support Thermo Fisher’s SampleManager LIMS.

Thermo Fisher uses the following software to support the system:

- Server Operating Systems – servers run the Microsoft Windows Server and Amazon Linux operating system.
- Workstation Operating Systems – workstations run the Microsoft Windows or Apple macOS operating systems.
- Antivirus Software – used to protect workstations and servers against malicious software.
- AWS Certificate Manager – used to store and protect the digital certificates used to encrypt customer data transmissions to and from SampleManager LIMS whether via the user interface (“UI”) or application programming interfaces (“API”).
- AWS CloudTrail – used to log, continuously monitor, and retain account activity related to actions across the AWS infrastructure.
- AWS FSx – a managed file storage service used to store customer data files like a Windows File Server.

- AWS GuardDuty – used to continuously monitor the IT environment for malicious activity and unauthorized behavior. It protects the AWS accounts, workloads, and customer data.
- AWS Identity and Access Management (“IAM”) System – used to securely control user access to AWS services and resources.
- AWS Key Management Service (“KMS”) – used to store and protect certain encryption keys used to encrypt customer data.
- AWS Relational Database Service (“RDS”) – used to store the customer data in an Oracle relational database and an Aurora PostgreSQL database that is managed by AWS
- AWS S3 – used to provide object storage through a web service interface.
- Source Code Management – used to host the SampleManager LIMS code base and maintain a record of software development team activities. Additionally, they are used to store “infrastructure as code” commands necessary to deploy the AWS-based IT infrastructure system components that support SampleManager LIMS.
- Content Collaboration Platform – used as an “intranet” site where policies and procedures and certain documentation are made available to all personnel who require access.
- Endpoint Detection Response Platform – endpoint protection platform (EPP) with integrated endpoint detection and response (EDR) capabilities. It monitors endpoint activity to detect, prevent, and respond to potential threats, alerting security teams to malicious behavior for investigation and remediation.
- Microsoft Active Directory – used as a directory service to authenticate corporate network users and manage group lists for access control purposes.
- Microsoft Active Directory Add-on – used to further restrict the allowable composition of passwords and support length-based password aging.
- Microsoft Remote Desktop Protocol (“RDP”) – used to connect directly to Microsoft-based virtual hosts from the internal network for administration purposes.
- Security Information and Event Management (“SIEM”) Platform – used to collect and analyze logged activity from the AWS-based virtual IT infrastructure system components and the SampleManager LIMS application.
- Notification Platform – used to receive notifications into a Slack channel for monitoring and response by the CIS team’s Security Operations Center (“CIS SOC”).
- Ticketing Systems – Azure DevOps and Atlassian Jira are used to document and manage application and IT infrastructure changes, respectively, and customer support requests, among other uses. ServiceNow is used to document and manage security incidents.
- Virtual Private Network (“VPN”) Systems – used by Thermo Fisher personnel to securely access the internal network and IT resources from outside Company offices and sites.
- Vulnerability Scanners – used to detect security vulnerabilities in the AWS-based virtual IT infrastructure system components and in SampleManager LIMS’ application code base.

People

Thermo Fisher's organization supports the framework for an effective control environment. The roles and responsibilities of key functions include the following:

- Digital Science and Automation Solutions ("DSAS") Security Team – consists of a dedicated CIS team member who acts as a liaison to DSAS and leaders from Quality Assurance & Regulatory Affairs, Technical Operations, Customer Support, Human Resources, Facilities / Site Security, and Engineering. Along with the CIS team, they are responsible for the security of SampleManager LIMS.
- Engineering Team – responsible for SampleManager LIMS software development, testing and maintenance
- Human Resources Team – responsible for human resources-related processes, including personnel screening, orientation, training and termination
- Information Technology Team – the IT team at corporate and within DSAS manages the IT environment and resources used to support the SampleManager LIMS including the Microsoft Active Directory network, VPN, and user workstations.
- Product Team – responsible for the definition of SampleManager LIMS' functionality
- Quality Assurance & Regulatory Affairs Team – responsible for maintaining the DSAS quality management system ("QMS"), including standard operating procedures, the training program, and regulatory compliance for DSAS.
- Technical Operations Team – manages the IT environment, including the AWS-based virtual IT infrastructure system components comprising each instance of SampleManager LIMS.

Procedures

INFRASTRUCTURE MANAGEMENT

Physical and Environmental Security

The physical and environmental infrastructure that is relied upon for the SampleManager LIMS system comprise of network, hardware, and facility components managed and maintained within AWS. Management obtains and reviews the annual service auditor's reports for AWS on an annual basis to evaluate the design and operating effectiveness of the controls expected to be in place.

Information Security

Network Access Controls

New user access requests are initiated by the human resources team through the Human Resources Information System (HRIS) resulting in the creation of a ticket submitted to the IT department for the creation of a network Active Directory (AD) account. Employees are then provided with a unique domain account and password. The password is configured to include password history, minimum length, account lockout duration, threshold, and multi-factor authentication. Administrative access to the domain is restricted to personnel commensurate with their job role. Additionally, logical access is reviewed on a semi-annual basis to ensure access is assigned commensurate with job roles. Accounts assigned to terminated employees are disabled or deleted upon termination.

To access the AWS production environment, personnel are assigned to the appropriate role group within AD and require a unique password with multi-factor authentication. AWS Identity and Access Management (IAM) is linked to the AD group to ensure administrative access is restricted to personnel commensurate with their job role. Additionally, an encrypted SSH connection is utilized to remotely access production resources.

Business Continuity

A Business Continuity Plan (BCP) is in place defining key personnel and the necessary steps to continue business operations in the event of an unplanned event, failure of key business processes, or a disaster. The plan outlines roles and responsibilities, recovery procedures, and communication strategies to support operational continuity. Periodic reviews and updates are performed to maintain the plan's alignment with current business functions and infrastructure.

Change Management

Thermo Fisher maintains policies and procedures to guide personnel in the development of secure software and systems. Key components of the process include development, code review, functional testing, and change authorization prior to release to production. These policies and procedures are documented and available on the company intranet to ensure employees have access to the necessary guidance.

A lifecycle management tool, Jira, is utilized to manage development projects. Both customer-initiated requests and internal strategic development features are collected and prioritized within Jira. Version control software is also in place and used to restrict access to source code as well as provide standard code repository functionality.

Application Change Management

At the initiation of the application change management process, requested application updates and features are reviewed and approved by the Product Management team before the requirements of the change are divided into separate tasks within the workflow software to be developed. Access to the integration and deployment tools, code repository, and versioning tools are restricted to personnel commensurate with their job role. Testing of changes is performed in an environment that is maintained separate from production. Code review approvals of application changes are systematically enforced to occur prior to changes being implemented to the production environment.

Infrastructure Change Management

Thermo Fisher’s IaC is stored within a code repository in GitHub. Scripts are utilized to create consistent environments within the cloud platform. Infrastructure changes are documented and approved prior to implementation into the production environment. Personnel with administrative access to the cloud environment have the ability to apply infrastructure changes to the production environment.

Endpoint Protection

The Amazon GuardDuty service is enabled to provide continuous monitoring and analysis of network traffic and system events to identify potential security threats on system resources hosted within the AWS cloud environment.

An inventory of assets is maintained to assist with the tracking and disposal of system components and system-related items. Workstations, servers, and software are maintained within their respective inventories to manage assets appropriately. Workstations are encrypted to prevent unauthorized access to data. Antivirus protection is configured for real-time malware detection and protection on employee workstations.

Incident Management

Thermo Fisher maintains a process for managing potential cybersecurity incidents according to the Incident Response Plan. Thermo Fisher stores incidents in an Incident Management System and assigns an Incident Response Coordinator for immediate threat mitigation and remediation. Once mitigation occurs, the team performs root cause analysis to reduce opportunities for recurrence and allow for continuous improvement.

Customers remain informed during potential security incidents that could impact their information as required by applicable laws, regulations and contractual requirements.

Vulnerability Management

Vulnerability scans are configured to run monthly to identify weaknesses and vulnerabilities on systems hosting the applications in scope. Patches are applied to AMIs to create a newly patched image to be pushed to the AWS infrastructure.

Additionally, penetration testing is performed on an annual basis to identify potential system security vulnerabilities. Identified vulnerabilities discovered through both active and passive reconnaissance are triaged and tracked within a ticketing system through remediation.

Data

Thermo Fisher has established a Data Classification Policy which documents the various data classification criteria. This policy is reviewed and approved by management annually and communicated to internal personnel. In addition, the Data Handling and Protection Standards define procedures for handling information assets based on their classification, including requirements for media disposal.

Customer data is maintained in AWS-based virtual IT infrastructure system components including production data bases deployed using AWS RDS and object storage deployed using AWS S3 (backup copies of customer data are maintained using AWS RDS backup snapshots which are stored in AWS S3 buckets). Data in transit is encrypted with SSL / TLS 1.2 industry standard encryption and data at rest is encrypted with AES-256 encryption algorithm. Cryptographic keys (if utilized) are stored in AWS KMS (Key Management Service).

SECTION 4:

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Thermo Fisher's management designs its processes and procedures related to the SampleManager system to meet its objectives. Those objectives are based on the service commitments that Thermo Fisher's management makes to user entities, the laws and regulations that govern the provisioning of the SampleManager system and the financial, operational, and compliance requirements that Thermo Fisher has established for the services.

Thermo Fisher's principal service commitments and system requirements may be explicitly stated within Service Level Agreements and contracts, or may be implicitly agreed to, based on the nature of the industry in which they operate. These commitments generally include the following:

Trust Services Category	Service Commitments	System Requirements
Security	➢ System access is granted to authorized personnel only ➢ Identification and remediation of security incidents / events	➢ Logical access standards ➢ Physical access standards ➢ Encryption standards