

SOC 3 TYPE II

SampleManager LIMS

**Report on SampleManager LIMS
Relevant to Security**

For the Period April 1, 2023 to May 31, 2024



**KERRY L.
SHACKELFORD**
CPA LLC

Thermo Fisher Scientific, Inc.

Report on SampleManager LIMS Relevant to Security

Table of Contents

Description	Page
Section I — Independent Service Auditor's Report.....	3
Section II — Thermo Fisher Scientific's Assertion	6
Section III — Thermo Fisher Scientific's Description of the Boundaries of SampleManager LIMS	7
Overview of the Organization.....	7
Overview of Subservice Organizations.....	7
Complementary Subservice Organization Controls.....	8
Overview of SampleManager LIMS.....	9
Services Provided.....	9
Service Commitments and System Requirements.....	10
SampleManager LIMS	10
Scope of Examination and Description	11
Infrastructure.....	11
Software	12
People	14
Procedures.....	15
Data	15
Changes to SampleManager LIMS During the Period	16
Complementary User Entity Controls	17
Section IV — Thermo Fisher Scientific's Service Commitments and System Requirements	18



Section I — Independent Service Auditor's Report

To the Board of Directors and Management of Thermo Fisher Scientific, Inc.:

Scope

We have examined Thermo Fisher Scientific, Inc.'s ("Thermo Fisher Scientific's" or the "Company's") accompanying assertion in Section II of this report titled "*Thermo Fisher Scientific's Assertion*" (the "assertion") that the controls within Thermo Fisher Scientific's SampleManager LIMS¹ ("SampleManager LIMS" or the "system") were effective throughout the period April 1, 2023, to May 31, 2024, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the trust services criteria relevant to security (the "applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in *AICPA Trust Services Criteria*.

Thermo Fisher Scientific's Responsibilities

Thermo Fisher Scientific 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 the Company's service commitments and system requirements were achieved.

Thermo Fisher Scientific has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Thermo Fisher Scientific 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.

Independent Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that Thermo Fisher Scientific'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 AICPA. Those standards require that we plan and perform our examination to obtain reasonable

¹ The scope of the independent service auditor's report was limited to certain deployment options of SampleManager LIMS as described in the *Scope of Examination and Description* paragraph in Section III — *Thermo Fisher Scientific's Description of the Boundaries of SampleManager LIMS*.

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.

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

Our examination included:

- Obtaining an understanding of the system and the Company's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Thermo Fisher Scientific'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 Scientific'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.

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 Company's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions 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.

(The remainder of this page left blank on purpose.)



KERRY L. SHACKELFORD CPA LLC

Opinion

In our opinion, management's assertion that the controls within Thermo Fisher Scientific's SampleManager LIMS were effective throughout the period April 1, 2023, to May 31, 2024, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



Kerry L. Shackelford CPA LLC
Evergreen, Colorado
August 23, 2024



KERRY L. SHACKELFORD CPA LLC



Thermo Fisher Scientific
Thermo LabSystems, Inc.
300 Industry Drive
Pittsburgh, PA 15275
+1 866-823-0337
www.thermofisher.com

Section II — Thermo Fisher Scientific's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Thermo Fisher Scientific, Inc.'s ("Thermo Fisher Scientific's") SampleManager LIMS ("SampleManager LIMS" or the "system") throughout the period April 1, 2023, to May 31, 2024, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the trust services criteria relevant to security (the "applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Section III of this report titled "*Thermo Fisher Scientific's Description of the Boundaries of SampleManager LIMS*" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2023, to May 31, 2024, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria. Thermo Fisher Scientific'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 IV of this report titled "*Thermo Fisher Scientific's Service Commitments and System Requirements*."

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 April 1, 2023, to May 31, 2024, to provide reasonable assurance that Thermo Fisher Scientific's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

156F78F712C342B...

Liz Tonks
Senior Director, Engineering Delivery and Quality
Digital Science Solutions
Thermo Fisher Scientific, Inc.

Section III — Thermo Fisher Scientific's Description of the Boundaries of SampleManager LIMS

Overview of the Organization

Thermo Fisher Scientific, Inc.

Thermo Fisher Scientific, Inc. ("Thermo Fisher Scientific" or the "Company") is the world leader in serving science, with annual revenue exceeding \$40 billion. Thermo Fisher Scientific's Mission is to enable its customers to make the world healthier, cleaner, and safer. They help their customers accelerate life sciences research, solve complex analytical challenges, improve patient diagnostics and therapies, and increase productivity in their laboratories. The Company's global team of more than 100,000 colleagues delivers an unrivaled combination of innovative technologies, purchasing convenience, and pharmaceutical services through their industry-leading brands, including Thermo Scientific, Applied Biosystems, Invitrogen, Fisher Scientific, Unity Lab Services, Patheon, and PPD. For more information, please visit www.thermofisher.com.

Digital Science Solutions

Within Thermo Fisher Scientific, Digital Science Solutions partners with customers in biopharma, genomics, and other industries to deliver lab informatics solutions to derive more value and insight from their scientific data. Internally, Digital Science Solutions works in collaboration with Digital Platforms and Engineering to develop, maintain, and support Thermo Fisher Scientific's customer-facing software products, including SampleManager LIMS.

Digital Science Solutions shares responsibility with Thermo Fisher Scientific's Corporate Infrastructure & Security ("CIS") team for maintaining and supporting the IT environments hosting Thermo Fisher Scientific's customer-facing software products.

Overview of Subservice Organizations

Subservice organizations are third-party service providers (a.k.a., suppliers or vendors) whose services are relevant to report users' understanding of SampleManager LIMS and whose controls are necessary, in combination with Thermo Fisher Scientific's controls, to provide reasonable assurance that the Company's service commitments and system requirements are achieved based on the applicable trust services criteria. Thermo Fisher Scientific uses subservice organizations to achieve operating efficiency and obtain specific expertise. The following is the principal subservice organization used by the Company in support of SampleManager LIMS:

Amazon Web Services ("AWS")—

The SampleManager LIMS instances within the scope of this report are hosted in AWS data center facilities. AWS is responsible for providing cloud computing services including cloud-based virtual IT infrastructure management tools and system components. AWS' controls are necessary, in combination with controls at Thermo Fisher Scientific, to

provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria. AWS' control activities have been carved out from Section III of this report titled "*Thermo Fisher Scientific's Description of the Boundaries of SampleManager LIMS*," and the examination. Information about AWS' service commitments and system requirements, and the effectiveness of controls within their cloud computing services are described in their SOC 3 Type II report.

Thermo Fisher Scientific uses other third-party service providers, including contractors; however, they are not included in this sub-section of the report as Thermo Fisher Scientific has implemented its own controls independent of those of others that meet the applicable trust services criteria.

Complementary Subservice Organization Controls

Thermo Fisher Scientific expects that AWS will perform certain controls considered necessary, in combination with Thermo Fisher Scientific's controls, to provide reasonable assurance that one or more of Thermo Fisher Scientific's service commitments and system requirements were achieved. Such controls are referred to as *complementary subservice organization controls* and include:

Area	Control Activities Expected to be Implemented
Services	AWS is expected to provide their services as described and configured.
Personnel Screening, Security Awareness, and Training	AWS is expected to maintain the security and confidentiality of Thermo Fisher Scientific's data in accordance with contractual agreements.
Network Device Security	AWS is expected to defend the perimeter of their IT environments to prevent intrusions, disruptions, and unauthorized disclosure of Thermo Fisher Scientific's data.
Logical Access	AWS is expected to restrict logical access to their IT environments to authorized and appropriate personnel sufficient to protect Thermo Fisher Scientific's data from unauthorized disclosure.
Physical Access	AWS is expected to restrict physical access to their facilities (i.e., offices, data centers, data center service providers' facilities, etc.) to authorized and appropriate personnel sufficient to protect Thermo Fisher Scientific's data from unauthorized disclosure.

Area	Control Activities Expected to be Implemented
Media Protection and Encryption	AWS is expected to encrypt Thermo Fisher Scientific's data in the AWS Relational Database Service and protect the encryption keys as described and configured.
Logging and Monitoring	AWS is expected to preserve logged activity from the virtual IT infrastructure management tools and system components as described and configured.
Incident Response and Breach Notification	AWS is expected to report any unauthorized disclosure (breach) of Thermo Fisher Scientific's data to Thermo Fisher Scientific in a timely manner.

Overview of 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. SampleManager LIMS is maintained and supported in an ISO 9001 environment.

Services Provided

Thermo Fisher Scientific's services related to SampleManager LIMS include:

Business Analysis and Implementation—

Thermo Fisher Scientific implements SampleManager LIMS for customers and guides them through major project tasks and milestones including setting project objectives, gathering and defining requirements, configuring the system, acceptance testing the functionality of the configured instance, and deployment.

Training—

Thermo Fisher Scientific provides customers with access to the Education Center, an eLearning portal which gives customers on-demand access to interactive training material, narrated slides, demonstration videos, and quizzes. For advanced topics, the Company offers remote, instructor-led training sessions.

Support—

Thermo Fisher Scientific provides implementation support and makes the Support team available to new customers for the first three months. Post-implementation, the Company provides customers with access to the Help Center, which enables them to communicate questions, issues, and feature requests.

Maintenance—

Thermo Fisher Scientific corrects errors in the SampleManager LIMS software, periodically releases the error corrections and new features, and maintains all customer AWS IT environments (including the setup of test and production instances of SampleManager LIMS and the initial migration of the customer's configurations from test to production).

Service Commitments and System Requirements

Thermo Fisher Scientific's service commitments and system requirements are communicated through its contractual agreements with customers. The service commitments and system requirements related to the applicable trust services criteria are presented in Section IV of this report titled *"Thermo Fisher Scientific's Service Commitments and System Requirements."*

SampleManager LIMS

Thermo Fisher Scientific's SampleManager LIMS software hosted in AWS features a cloud-based laboratory information management system ("LIMS") and integrated lab execution system ("LES"), scientific data management system ("SDMS"), and electronic lab notebook ("ELN"). These integrated components allow organizations to manage their laboratory, data and procedural workflows, and connections with other enterprise systems, instruments, equipment, and customers to deliver increased compliance and productivity.

SampleManager LIMS is one of the most widely deployed LIMS in the world and has supported customers for over 30 years. The software is highly configurable and can be tailored to a customer's specific business processes and laboratory workflows. The capabilities of SampleManager LIMS are described on Thermo Fisher Scientific's [website](#).

Thermo Fisher Scientific supports several deployment options of SampleManager LIMS:

SampleManager LIMS Cloud—

Thermo Fisher Scientific manages and supports the deployment of SampleManager LIMS to auto-scalable, cloud-based IT infrastructure dedicated to the customer. The Company provisions AWS' cloud computing services, installs and configures SampleManager LIMS, and maintains the IT environment and instance.

SampleManager LIMS Self-Managed Cloud—

The customer manages and supports the deployment of SampleManager LIMS to their own self-managed cloud-based IT infrastructure. The customer provisions the cloud computing services, installs and configures SampleManager LIMS, and maintains the IT environment and instance.

SampleManager LIMS Self-Managed On-Premises—

The customer manages and supports the deployment of SampleManager LIMS to their own self-managed on-premises IT infrastructure. The customer provisions the IT infrastructure, installs and configures SampleManager LIMS, and maintains the IT environment and instance.

Scope of Examination and Description

The scope of the SOC 3 Type II examination was limited to customers using production instances of SampleManager LIMS hosted in Thermo Fisher Scientific owned and managed AWS accounts (i.e., the SampleManager LIMS Cloud deployment option). The SOC 3 Type II examination is not applicable to other deployments of SampleManager LIMS including non-production instances and instances hosted on a customer's IT infrastructure or under a customer's management.

Customer sites may include several workstation and mobile device-based IT infrastructure system components, including the Sample Manifest, Final Results Destination, Quant Studio, Thick Client Access, Web Access Client, Integration Manager, and Mobile App. The SOC 3 Type II examination is not applicable to workstation and mobile device-based IT infrastructure system components other than the Web Access Client, as they are customer owned and managed.

The scope of the SOC 3 Type II examination and description was limited to the requirements of the applicable trust services criteria and does not address the requirements of government regulations that are additional to the applicable trust services criteria, including such requirements found in the United States ("US") Food and Drug Administration regulations and the US Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security Rule.

The remainder of the description of SampleManager LIMS is limited to the SampleManager LIMS Cloud deployment option.

Infrastructure

The SampleManager LIMS instances are hosted in AWS data center facilities.

The Thermo Fisher Scientific 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.

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 Oracle database, Windows File Server shared storage, and AWS S3.

Software

Server Operating Systems: Servers run the Microsoft Windows Server operating system.

Workstation Operating Systems: Workstations run the Microsoft Windows or Apple macOS operating systems.

Other Supporting Software: Other software of significance used to support SampleManager LIMS includes:

Antivirus Software—

Antivirus software is used to protect workstations and servers against malicious software.

AWS Certificate Manager—

AWS Certificate Manager is 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 the application programming interface ("API").

AWS CloudTrail—

AWS CloudTrail is used to log, continuously monitor, and retain account activity related to actions across the AWS infrastructure.

AWS FSx—

AWS FSx is a managed file storage service used to store customer data files like a Windows File Server.

AWS GuardDuty—

AWS GuardDuty is 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—

AWS IAM is used to securely control user access to AWS services and resources.

AWS Key Management Service ("KMS")—

AWS KMS is used to store and protect certain encryption keys used to encrypt customer data.

AWS Relational Database Service ("RDS")—

AWS RDS is used to store customer data in an Oracle relational database that is managed by AWS.

AWS Simple Storage Service ("S3")—

AWS S3 is used to provide object storage through a web service interface.

Azure DevOps—

Azure DevOps is used to host the SampleManager LIMS code base and maintain a record of Software Development team activities.

Content Collaboration Platform—

The content collaboration platform is used as an “Intranet” site where policies and procedures and certain documentation are made available to all personnel who require access.

CrowdStrike Falcon—

CrowdStrike Falcon is a host-based intrusion detection and prevention system (“IDPS”) used to detect and prevent IT environment intrusions or otherwise alert appropriate personnel to potential malicious activity for follow-up.

Microsoft Active Directory—

Microsoft Active Directory is used as a directory service to authenticate corporate network users and manage group lists for access control purposes.

Microsoft Active Directory Add-on—

A Microsoft Active Directory add-on is used to further restrict the allowable composition of passwords and support length-based password aging.

Microsoft Remote Desktop Protocol (“RDP”)—

Microsoft RDP is used to connect directly to Microsoft-based virtual hosts from the internal network for administration purposes.

Microsoft SharePoint—

SharePoint is used to host the Software Development team’s SDLC and related artifacts for each release. It is also used by the Technical Operations team to store certain server access keys and digital certificate backups.

Security Information and Event Management (“SIEM”) Platform—

The SIEM platform is used to collect and analyze logged activity from the AWS-based virtual IT infrastructure system components and the SampleManager LIMS application.

Single Sign-on System—

The single sign-on system is used by Thermo Fisher Scientific personnel to access the AWS-based virtual IT infrastructure system components and customer instances of SampleManager LIMS. The single sign-on system enforces multi-factor authentication.

Slack—

Slack is used to receive notifications into a Slack channel for monitoring and response by the CIS team’s Security Operations Center (“CIS SOC”).

Software Version Control System—

The software version control system is used to store “infrastructure as code” commands necessary to deploy the AWS-based IT infrastructure system components that support SampleManager LIMS.

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”) System—

The VPN system is used by Thermo Fisher Scientific personnel to securely access the internal network and IT resources from outside Company offices and sites.

Vulnerability Scanners—

Vulnerability scanners are used to detect security vulnerabilities in the AWS-based virtual IT infrastructure system components and in SampleManager LIMS' application code base.

Application Software: SampleManager LIMS is a web-based application with a browser-based user interface. Thermo Fisher Scientific has established secure coding practices based on best practices prescribed by the Open Web Application Security Project and software engineers are trained in secure coding practices.

People

The key teams involved in supporting SampleManager LIMS include:

Digital Science Solutions Security Team—

The Digital Science Solutions Security team consists of a dedicated CIS team member who acts as a liaison to Digital Science Solutions and leaders from Quality Assurance & Regulatory Affairs, Technical Operations, Customer Support, Human Resources, Facilities/Site Security, and Engineering. The CIS team and the Digital Science Solutions Security team are responsible for the security of SampleManager LIMS.

Engineering Team—

The Engineering team is responsible for all SampleManager LIMS software development, testing, and maintenance.

Human Resources Team—

The Human Resources team is responsible for human resources-related processes, including personnel screening, orientation, training, and termination.

Information Technology ("IT") Team—

The IT team at corporate and within Digital Science Solutions manages the IT environment and resources used to support SampleManager LIMS including the Microsoft Active Directory network, VPN, and user workstations.

Product Team—

The Product team is responsible for the definition of SampleManager LIMS' functionality.

Quality Assurance & Regulatory Affairs Team—

The Quality Assurance & Regulatory Affairs team is responsible for maintaining the Digital Science Solutions quality management system ("QMS"), including standard operating procedures, the training program, and regulatory compliance for the entire organization. A member of the Quality Assurance & Regulatory Affairs team serves as the SampleManager LIMS SOC 2/SOC 3 compliance coordinator.

Technical Operations Team—

The Technical Operations team within Digital Platforms and Engineering manages the IT environment, including the AWS-based virtual IT infrastructure system components comprising each instance of SampleManager LIMS.

Procedures

The automated and manual procedures relevant to SampleManager LIMS and the transaction streams, files, databases, and output used or processed by SampleManager LIMS include security-related control activities in the following areas, among others:

- *Security Management*
- *Personnel Screening, Security Awareness, and Training*
- *Network Device Security*
- *Logical Access*
- *Protection from Malicious Software*
- *Physical Access*
- *Media Protection and Encryption*
- *Logging and Monitoring*
- *Incident Response and Breach Notification*
- *Change Management*

Data

Customer data is maintained in certain AWS-based virtual IT infrastructure system components including production databases deployed using AWS RDS, Windows file servers deployed using Amazon FSx, 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). Customer data is not stored outside of AWS.

Changes to SampleManager LIMS During the Period

No significant security-related changes were made to SampleManager LIMS throughout the period April 1, 2023, to May 31, 2024.

(The remainder of this page left blank on purpose.)

Complementary User Entity Controls

The controls designed and implemented by Thermo Fisher Scientific to achieve compliance with the applicable trust services criteria require that user entities (i.e., customers) design and implement certain controls complementary to those designed and implemented by Thermo Fisher Scientific. This section summarizes these complementary user entity controls for customer review and consideration.

Logical Access

SampleManager LIMS is customer-configurable and is capable of enforcing customer-specified password policy settings. User entities should configure SampleManager LIMS' password policy settings according to their preferences.

SampleManager LIMS is customer-configurable and is capable of automatically locking a user's session after a period of inactivity. User entities should configure SampleManager LIMS' session lock according to their preferences.

Customers should have controls in place to administer the access of their personnel to SampleManager LIMS and validate that access is updated in a timely manner for personnel terminations and changes in job responsibilities.

(The remainder of this page left blank on purpose.)

Section IV — Thermo Fisher Scientific's Service Commitments and System Requirements

Thermo Fisher Scientific's principal service commitments and system requirements generally obligate Thermo Fisher Scientific to:

- Maintain commercially reasonable and appropriate administrative, physical, and technical safeguards to protect customer data equivalent to those safeguards used to protect Thermo Fisher Scientific data.
- Limit Thermo Fisher Scientific personnel's access to customer data based on business need and provide only the minimum necessary access needed.
- Not disclose customer data to unauthorized third parties, including other Thermo Fisher Scientific customers.
- Promptly notify customers of confirmed incidents of unauthorized access to their data, if any, within 72 hours and provide support and assistance to the customer's breach investigation.
- Upon termination of the agreement and if requested, delete or destroy all customer data in its possession.
- Maintain a Quality Management System aligned with ISO 9001 standards that include policies and procedures including, but not limited to, disaster recovery, data backup and recovery, business continuity, data security, customer incident management, and change management.