Umetrics® Studio Document

Security & Compliance Policy

2026-11-24

SARTORIUS

Contents

1 Introduction 3

2 Quality Management System – ISO9001 4

3 Information Security Management – ISO27001 5
- 3.1 Secure Development Lifecycle 5
- 3.2 Governance – Security 5
- 3.3 Threat Modeling – Security 5
- 3.4 Operations – Security 5

4 Information Security Architecture 6
- 4.1 Data Encryption 6
- 4.2 Identity Management 6
- 4.3 Access Control 6
- 4.4 Execute Isolation 6
- 4.5 Licensing 7
- 4.6 Data Isolation 7

5 GAMP 5 7

6 The Agile Development Process 9
- 6.1 Roles and Responsibilities 9
- 6.2 Governance Model 9
- 6.3 Development Process 9
- 6.4 Implementation Steps 9
  - 6.4.1 Design 9
  - 6.4.2 Risk Assessment 9
  - 6.4.3 Development 9
  - 6.4.4 Test 9
  - 6.4.5 Build and Deploy 9
  - 6.4.6 Demo 9
  - 6.4.7 Delivery 9

7 Infrastructure as a Service Architecture 10
- 7.1 IaaS Provider 10
- 7.2 IaaS Location 10

1 Introduction

The Security and Compliance Policy has been established to safeguard all data entrusted to Umetrics® Studio, developed by Sartorius Stedim Data Analytics AB (“SDA”). The policy is intended to ensure that your data remains inaccessible to competitors and other unauthorized external parties outside your organization. Security is a fundamental priority throughout the design, operation, and maintenance of the service. Accordingly, Umetrics® Studio is managed in accordance with applicable certifications and industry best-practice guidelines to support the quality, security, and reliability of the application.

2 Quality Management System – ISO9001

intertek
Total Quality. Assured.

CERTIFICATE OF REGISTRATION

This is to certify that the management system of:

Sartorius Stedim Data Analytics AB

Main Site: Östra Strandgatan 24, SE-903 33 Umeå, Sweden

has been registered by Intertek as conforming to the requirements of:

ISO 9001:2015

The management system is applicable to:

The design and development of software in the fields of Multivariate Data Analysis, Design of Experiments and Advanced Data Analytics. Provider of software and services to the life science and bioprocessing industries.

Certificate Number:
0105822

Initial Certification Date:
25 September 2020

Date of Certification Decision:
21 July 2026

Issuing Date:
28 July 2026

Valid Until:
24 September 2029

intertek

Angelique Björklund
MD, Business Assurance Nordics

Intertek Certification AB
P.O. Box 1103, SE-164 22 Kista, Sweden

In the issuance of this certificate, Intertek assumes no liability to any party other than to the Client, and then only in accordance with the agreed upon Certification Agreement. This certificate's validity is subject to the organization maintaining their system in accordance with Intertek's requirements for systems certification. Validity may be confirmed via email at certificate.validation@intertek.com or by scanning the code to the right with a smartphone. The certificate remains the property of Intertek, to whom it must be returned upon request.

3 Information Security Management – ISO27001

Sartorius Corporate Administration maintains a certified Information Security Management System (ISMS) to ensure a high level of information security for its own organization as well as for the Sartorius Group of companies and its customers, which complies with state-of-the-art technology, practice, and requirements of the internationally recognized standard for information security ISO/IEC 27001. Certificate Number: 01 153 2300658.

SDA's products are designed to support compliance with the requirements set forth in ALCOA+, 21 CFR Part 11, and EudraLex Volume 4, Annex 11. By leveraging established technologies, including data lineage and event-driven architecture, SDA can record all relevant events—together with the associated user identifier, object, data, and timestamp—in a readable and searchable format consistent with industry standards.

3.1 Secure Development Lifecycle

The Sartorius Global Cyber Resilience Act (CRA) Initiative is intended to bring all Sartorius products containing digital elements into full compliance with the CRA and to ensure that they carry the appropriate product-specific CE markings. Consequently, the implementation of a CRA-compliant Secure Software Development Life Cycle (SSDLC) program is mandatory for the development of all Sartorius software products.

In accordance with Sartorius' SSDLC requirements and the OWASP Software Assurance Maturity Model (SAMM), a Secure Software Development Life Cycle (SSDLC) program has been established to continuously assess, plan, and enhance SDA's security posture. The program is aligned with SDA's overall risk-based approach and risk management activities and is supervised by SDA's independent Quality and Cybersecurity function.

3.2 Governance – Security

To enable teams to develop, deploy, and operate data analytics features autonomously while maintaining product security, a Security Champion Program has been established, with representatives appointed from each development team. The program facilitates the resolution of issues identified through threat modeling, the alignment of security requirements and secure development practices across teams, the coordination of security controls, and the execution of offensive security testing of the system.

The Head of Product Development and SDA's Quality and Cybersecurity function are responsible for providing relevant training to Security Champions and ensuring effective, coordinated, and continuous improvement across teams.

3.3 Threat Modeling – Security

As part of the efforts to ensure compliance with the Cyber Resilience Act (CRA), information and product assets are assessed for potential risks and threats using variations of the STRIDE methodology and with incorporating Mitre At&ck in the risk assessment based on the threat modeling.

Identified threats are documented together with the corresponding mitigating security controls, offensive testing scenarios, and security requirements.

Threat modeling is conducted during Epic Refinement and on an ad hoc basis to evaluate the security implications of design decisions. The documentation is continuously updated and reviewed in response to design changes, security incidents, and relevant threat intelligence reports.

3.4 Operations – Security

Umetrics® Studio employs a cloud-native architecture built on Kubernetes. Its security measures are continuously enhanced with the objective of maintaining a Kubernetes environment that complies with the policies and controls established under ISO/IEC 27001.

Security events are aggregated for integration with Security Information and Event Management (SIEM) systems to facilitate monitoring and in-depth analysis. Suspected activities are triaged by the Security Champion Team in conjunction with other relevant threat intelligence.

Business continuity, backup, and disaster recovery are managed in accordance with Sartorius Global Procedure. Backup requirements apply to all information systems and encompass all data required for restoration in the event of a disaster. Disaster recovery backups are stored at a separate site that provides industry-standard protection. Each site's disaster recovery strategy is documented in a site-specific disaster recovery plan.

Multi-factor authentication is used to protect access to all source code. Software composition analysis tools are employed to minimize the risk of software supply-chain attacks and malware distribution. In addition, an independent third party conducts penetration testing of the software, and the results are used to continuously enhance its security.

SDA also monitors customer feedback and information relating to customer perception to assess whether customer requirements have been met. Sartorius Cloud Center of Excellence (CCoE) is a Sartorius expert team dedicated to helping Sartorius cloud products operate securely and efficiently. The Umetrics® Studio team works closely with the CCoE to promote proactive security measures and prevent incidents.

The CCoE provides guidance on designing and operating cloud-based systems and actively monitors resource usage, identifies suspicious activities, and takes appropriate action based on its findings. Together with the underlying cloud provider, the CCoE ensures that the infrastructure operates with up-to-date software and hardware adapted to the requirements of Umetrics® Studio.

All personnel involved in the development and maintenance of Umetrics® Studio are granted only the minimum level of access necessary to perform their assigned duties. The principle of least privilege applies not only to personnel access but also to the credentials assigned to the components of Umetrics® Studio. This principle constitutes a cornerstone of the information security architecture.

4 Information Security Architecture

Within the context of data security, individual customer organizations in Umetrics® Studio are referred to as tenants. A tenant may comprise a company and its subsidiaries, or any other organizational grouping deemed appropriate from a sales or contractual perspective.

4.1 Data Encryption

Umetrics® Studio uses Transport Layer Security (min TLS 1.2) on the platform's external interfaces to protect the confidentiality and integrity of transmitted data. Certificates and server configurations are reviewed regularly by independent third parties to verify that robust security configurations are maintained.

Storage encryption is used to protect data against unauthorized access resulting from physical theft. Encryption keys are managed in accordance with industry best practices and the cloud provider's security standards.

4.2 Identity Management

Umetrics® Studio integrates with customers' identity management systems through Sartorius' internal Customer Identity and Access Management (CIAM) solution, Sartorius ID. This integration provides Single Sign-On (SSO), facilitating a seamless and intuitive access experience while enabling customers to retain full control over their security requirements, including multi-factor authentication (MFA), password complexity, and general identity management.

Sartorius ID is based on Okta and its market-leading CIAM solutions, providing a robust, secure, and flexible identity foundation.

4.3 Access Control

Umetrics® Studio comprises loosely coupled, autonomous components that enforce their respective data models and trust relationships with other services. Open Policy Agent (OPA) is used to provide a cohesive access-management model that is replicated across the system's services.

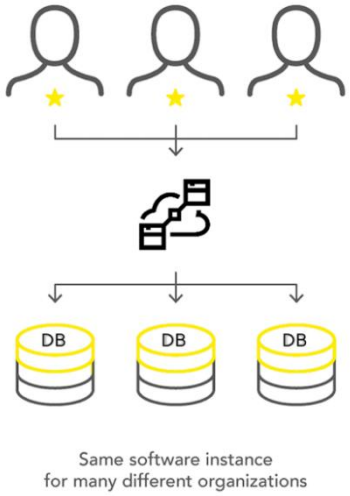
This architecture enables the definition of access policies, enforcement of record ownership, and propagation of real-time access-control lists to individual components.

4.4 Execute Isolation

User-defined functions are executed in isolation from the workloads of other tenants, thereby ensuring both equitable resource allocation and security:

- Resource-intensive workloads from one tenant do not adversely affect the performance of other tenants.
- Execution is protected by multiple layers of security controls designed to prevent unauthorized access to tenant data, including sophisticated attacks.

This protection is achieved through a range of measures, including tenant-aware job scheduling, network segmentation, and advanced operating-system-level security controls.



4.5 Licensing

Sartorius's partnership with Revenera and its software licensing solutions provides a foundation for a robust and resilient licensing system that enables flexible and secure licensing arrangements.

4.6 Data Isolation

Data records generated by end users in Umetrics® Studio are assigned a Tenant ID corresponding to the end user's organization. The records are subsequently persisted using isolation mechanisms that provide physical or logical separation between tenants, where applicable:

- **Separate data sources:** Each tenant is assigned a dedicated database or storage unit.
- **Encrypted payloads:** Sensitive information contained in a record is encrypted using a tenant-specific cryptographic key.
- **Row-level security:** Enforced by the persistence engine, this ensures that records are not visible to users outside the relevant organization. Unauthorized access attempts are denied and logged as security incidents.

The security architecture is designed to prevent data leakage between tenants and to protect against known threats, including industrial espionage.

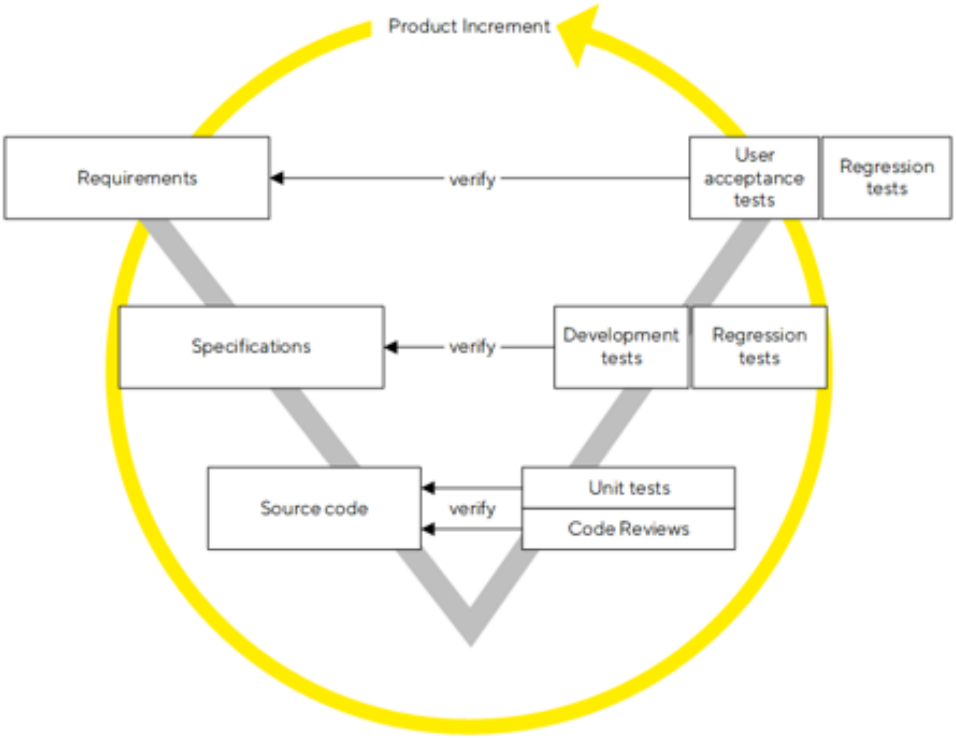
5 GAMP 5

The Sartorius Global Procedure for Agile Software Development defines the minimum standards for software development, taking into account the good supplier practices recommended in the GAMP 5 guidance.

The global procedure requires Sartorius software products to be developed under controlled quality conditions using a widely accepted, well-documented, and risk-based approach. It also promotes a common understanding of agile software development and provides guidance to development teams on meeting the requirements and expectations of customers operating in regulated environments.

Computerized System Validation (CSV) is addressed through a system risk assessment, validation plan, user requirements, traceability matrix, test plan, and test and validation report.

The illustration below provides a high-level overview of the verification model.



6 The Agile Development Process

The Agile Software Development process facilitates the continuous delivery of value through iterative cycles of planning, development, testing, and feedback. This approach enables the organization to respond effectively to evolving business and regulatory requirements.

It enhances transparency, collaboration, and accountability by involving relevant stakeholders throughout the development life cycle and regularly evaluating progress against defined objectives. Agile practices also support quality assurance and risk management by promoting frequent testing, early identification of issues, and the continuous improvement of processes and deliverables.

6.1 Roles and Responsibilities

The Software Product Development organization comprises a Process Owner, a Product Owner, and Development Teams.

The Product Manager (PM) collaborates closely with customers, other stakeholders, and the Product Development Teams.

The organizational structure is based on cross-functional Development Teams with diverse skill sets. Each team is capable of developing features throughout the entire life cycle, from design through to the delivery of functional software. Enabling teams comprising architects and user-experience (UX) specialists provide additional support to the Development Teams.

The Development Teams are supported by Software Test Engineers and Security Champions, who are responsible for maintaining a continuous focus on quality assurance and security throughout each product release. Quality Assurance is managed by the independent Quality and Cybersecurity function.

6.2 Governance Model

Sartorius' Global Idea-to-Product Procedures and Instructions govern software project management. The objective of these procedures is to provide a framework for a harmonized, controlled, and traceable process for bringing product ideas to market across the relevant project phases. They ensure alignment among the organizational functions involved in the development and commercialization of software products.

New requirements are formulated as "Epics." In collaboration with customers and other stakeholders, the Product Manager (PM) defines the content of each Epic. The PM is also responsible for determining the priority of Epics and deciding whether an Epic should be discarded.

6.3 Development Process

The product development process is structured into cycles. Each cycle is typically time-boxed to eight (8) weeks, during which the Development Teams deliver incremental value in the form of functional, tested software.

6.4 Implementation Steps

6.4.1 Design

UX/UI Designers and Architects collaborate closely with the Development Teams to align on the design of the highest-priority requirements for the current cycle.

6.4.2 Risk Assessment

Risk assessments are conducted for all requirements and used to determine the appropriate level of testing for each requirement.

6.4.3 Development

Each requirement is developed by the Development Teams, and all source code is stored in Git repositories hosted in Azure DevOps.

6.4.4 Test

Automatic tests, including unit, integration, and system tests, are implemented during the development of each feature or user story and can be executed with every build.

6.4.5 Build and Deploy

The software is built automatically whenever a developer pushes changes to a Git repository, and the automated tests are executed with each build. If all tests pass, the changes are deployed to a pre-production environment.

6.4.6 Demo

A demo is conducted after each iteration and cycle using the current software build to obtain continuous feedback from the Product Manager (PM), customers, and other relevant stakeholders.

6.4.7 Delivery

The enhanced software is released to customers

regularly, typically on a weekly schedule.

7 Infrastructure as a Service Architecture

Umetrics® Studio is a cloud-native software product that leverages the scalability, resilience, and security capabilities provided by cloud technology.

Operating a cloud environment and maintaining the associated infrastructure are not considered part of Sartorius's core business. Accordingly, Sartorius has partnered with Microsoft and uses Azure, Microsoft's Infrastructure as a Service (IaaS) platform.

7.1 IaaS Provider

Umetrics® Studio operates on Microsoft Azure, which provides the infrastructure required to operate, govern, and monitor the systems over time. Azure Kubernetes Service (AKS) forms the foundation of the Umetrics® Studio platform.

In addition to the proven AKS platform, Umetrics® Studio utilizes third-party technologies, including PostgreSQL, Docker, and Azure Blob Storage. These services benefit from the support and availability commitments provided by Microsoft. The Sartorius Cloud Center of Excellence collaborates with Microsoft Azure on relevant matters to help ensure that Umetrics® Studio remains accessible, secure, and reliable.

7.2 IaaS Location

The physical servers supporting Umetrics® Studio are currently hosted in the Azure West Europe region, located in the Netherlands.

Sartorius Stedim Data Analytics AB
Östra Strandgatan 24
903 33 Umeå, Sweden

Phone: +46 90 1848 00
www.sartorius.com

The information and figures contained in these instructions correspond to the version date specified below.
Sartorius reserves the right to make changes to the technology, features, specifications, and design of the equipment without notice.
Masculine or feminine forms are used to facilitate legibility in these instructions and always simultaneously denote all genders.

Copyright notice:
These instructions, including all components, are protected by copyright.
Any use beyond the limits of the copyright law is not permitted without our approval.
This applies to reprinting, translation and editing irrespective of the type of media used.