SARTORIUS

Compliance Information

20231012v1

Umetrics® Studio Compliance Policy

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

Abstract

Sartorius Stedim Data Analytics AB (“SDA”) operates in accordance with several certifications and best practice guidelines to promote real application quality and fitness for intended use.

Quality Management System – ISO 9001

SDA holds a certified Quality Management System in accordance with ISO 9001

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:
30 May 2023

Issuing Date:
31 May 2023

Valid Until:
24 September 2026

ISO 9001:2015 CERTIFICATION ™
intertek

SWEDAC ACKREDITERING
Accred. no. 1639
Certification of management systems
ISO/IEC 17021-1

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.

Information Security Management – ISO 27001

SDA is aimed towards an ISO27001 certification, with the basic principles in place and the road ahead defined. These principles constitute the platform to protect data security as required according to regulatory and data privacy protection requirements.

SDA product development is guided by ALCOA+, 21 CFR part 11 and EudraLex Annex 11. By using proven tools such as data lineage and event driven architecture, we can log all events together with a user identifier, object, data, and timestamp, all in a readable and searchable format.

System logs and audit trails are kept in the system and managed as any database entity, including back-up and restore. These logs cannot be altered within the system.

See the sections below to find summaries of the initiatives in the different areas.

Secure Development Lifecycle

Based on the OWASP SAMM model, we have developed a Secure Development Lifecycle program to continuously assess, plan and improve our security stance. The security program is aligned with the SDA overall risk-based approach and risk management work. The security program covers the areas Governance, Design, Implementation, Verification and Operations.

Governance - Security

To empower teams to build, ship and operate data analytics features autonomously while at the same time sustaining security of the product, we have established a security champion program with representatives from each team. This allows us to drive activities to resolve issues found from threat modeling, align security requirements and secure development best practices across teams, coordinate security controls and perform offensive security testing of the system.

Part of the security program is mandatory relevant training for security champions and continuous improvement that is effective and aligned across teams.

Threat Modeling - Security

Information and assets of our products are assessed for potential risks and threats using the STRIDE method. Identified threats are documented along with mitigating security controls, where development teams describe controls with security requirements and test scenarios.

Threat modeling is performed both during Epic (as defined below) refinement and ad-hoc to gain an understanding of the security implications of design decisions. The documented threats are reviewed as part of management review and updated based on design events, security incidents, or threat intelligence reports.

Operations – Security

Umetrics® Studio uses a cloud-native approach built on Kubernetes. The security measures are continuously improved with the goal to achieve a Kubernetes setup that complies with the policies and controls in accordance with ISO 27001.

Security events are aggregated for integration with security information and event management (SIEM) systems for monitoring and deeper analysis. Suspect activity is triaged along with other threat intelligence by the security champion team.

Business continuity, backup, and disaster recovery are handled according to a global procedure. The backup requirements are extended to all information systems and include all data that is needed to be reconstituted in the event of a disaster. The backups for disaster recovery purposes are stored in another site that provides industry-standard protection. The disaster recovery strategy of each site is laid out in site-specific disaster recovery plans.

Multi-factor authentication is used to protect access to all source code, and software composition analysis tools are used to minimize the risk of any software supply chain attacks and malware distribution. Additionally, an independent third party performs penetration testing of the software and the results are used to continuously improve the security aspects of the software.

SDA also monitors information relating to customer perception as to whether the organization has met customer requirements.

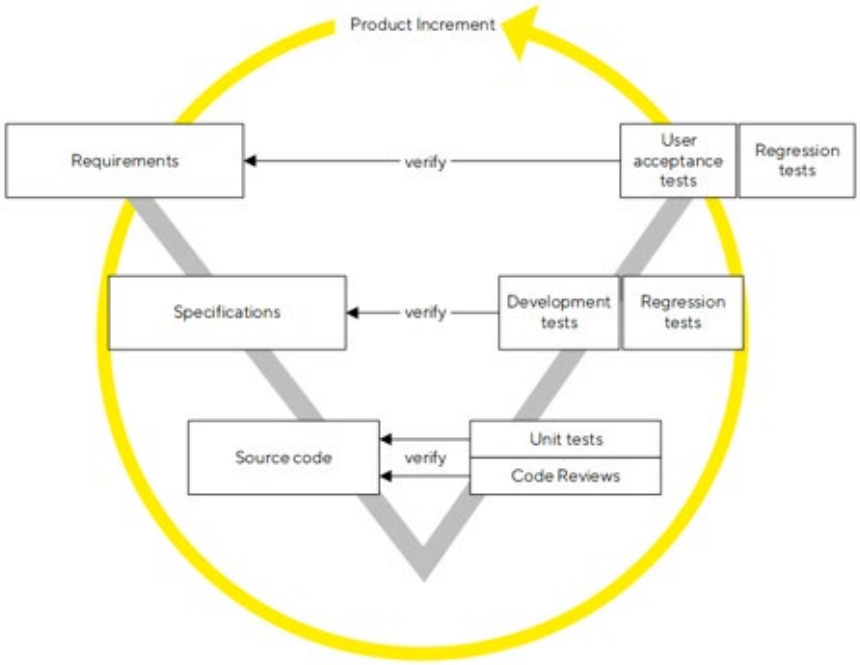
GAMP 5

SDA uses a risk-based approach in accordance with the GAMP 5 guidelines via a global procedure for agile software development. The procedure defines the minimum standards for the software development under consideration of the good supplier practices recommended by the GAMP 5.

The procedure provides that the software product is developed with control over the software quality by using a widely accepted, well documented and risk-based approach.

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

The below illustration shows a high-level view of the verification model.



The organization that develops the software consist of Process Owner, Product Owner, Development team and Quality Assurance.

The Development team has a quality and a security champion responsible for continual focus on quality and security aspects within each product release.

The SAFe & Agile Development Process

We use a software development process that is based on the Scaled Agile Framework (SAFe), which enables a scalable implementation of Agile, Lean, and DevOps practices.

Roles & responsibilities

We have clearly defined roles & responsibilities. The Product Manager (PM) is in close collaboration with customers and other stakeholders and the different product development teams.

We use a team structure where each development team is cross-functional and has different skillsets. Development teams can therefore develop any feature from design to working software. Each development team also has champions, for example Security and Quality Champions.

We also have enabling teams that consist of architects and UX specialists that assist the development teams.

Governance model

We have a clearly defined governance model via a rigid global Program Management Office (PMO) stage gate process and Program Increment (PI) planning.

New requirements are formulated in the form of "Epics". The Product Manager (PM), in collaboration with customers and stakeholders, decides what should be in each Epic. The PM decides the priority of Epics or if an Epic should be discarded.

Development process

The development of the product is divided into Program Increments (PI). The development of each PI is timeboxed to ten (10) weeks and the development teams deliver incremental value in the form of working and tested software during each PI. PI planning is a two-day event to align on priorities and scope.

PI implementation steps

Design

UX/UI designers and Architects work in close collaboration with the teams to align on the design of the top prioritized requirements in the current PI.

Risk assessment

We then assess any risks for all requirements and then decide the level of testing activities for each requirement.

Development

Each requirement is developed by the development teams and all code is stored in Git repositories in Azure DevOps.

Test

Automatic tests, for example unit, integration and system tests, are implemented during the implementation of a feature or a user story and can be executed at each build. Validation testing is also planned and automated.

Build and Deploy

The software is automatically built when a developer pushes its changes to a Git repository, and the automated tests are run on every build. If all tests pass, then all changes are deployed to a pre-production environment.

PI demo

A demo is held after each iteration and after each increment on the current build of the software to continuously get feedback from PM, customers, and different stakeholders.

Delivery

When the PM decides enough value has been reached on the increment, the software is released to customers via the global Order to Cash (O2C) process.

Sales and Service Contacts

For further contacts, visit Sartorius.com

Sweden

Sartorius Stedim Data Analytics AB
Östra Strandatan 24
903 33 Umeå
Phone +46 90-18 48 00