RSM

DAWEX

Service Organization Controls 3

(SOC3) Report

Description of
Dawex Systems relevant to Security from January 1st to December 31st, 2025

With the Independent Service Auditor's Report

March, 2026

RSM

Table des matières

Assertion of Dawex 1

Independent Service Auditor's Report 4

- Scope 5
- Service organization's responsibilities 6
- Service auditor's responsibilities 6
- Inherent Limitations 6
- Opinion 7
- Restricted use 7

Description of Dawex Systems relevant to Security 8

- Dawex Overview 9
- Description of the control environment, information communication, monitoring and Risk Assessment process 10
- Components of the system providing the defined services 12
- Design and Implementation of controls process, policies and procedures requirements 13
- Key system operations domains related to security 13

This document contains 17 pages excluding header and summary

RSM

.

Assertion of Dawex

RSM

DAWEX

Assertion of Dawex

We have prepared the accompanying Description, Description of Dawex Systems relevant to Security for the period January 1st, 2025 to December 31st, 2025 and Description of Criteria and Controls ('Description') based on the criteria in items (a)–(b) below, which are the criteria for a description of a service organization's system set forth in paragraphs 1.26 of the AICPA Guide Reporting on Controls at a Service Organization relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (the description criteria).

The description is intended to provide users with information about Dawex Systems, particularly system controls intended to meet the criteria for the security principle set forth in AICPA's TSP section 100 Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, And Privacy (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that:

a. The description contains the following information:

i. The types of services provided

ii. The components of the system used to provide the services, which are as follows:

(1) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

(2) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

(3) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

(4) Procedures. The automated and manual procedures.

(5) Data. Transaction streams, files, databases, tables, and output used or processed by the system.

iii. The boundaries or aspects of the system covered by the description

iv. For information provided to, or received from, subservice organizations and other parties

(1) How the information is provided or received and the role of the subservice organizations and other parties

(2) The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

v. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization's system

(2) When the inclusive method is used to present a subservice organization, controls at the subservice organization

vi. If the service organization presents the subservice organization using the carve-out method

(1) The nature of the services provided by the subservice organization

(2) Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

vii. Any applicable trust services criteria that are not addressed by a control and the reasons

viii. In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description

b. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and, may not, therefore, include every aspect of the system that each individual report user may consider important to its own needs.

Mr. Laurent Lafaye

CEO, Dawex

Laurent Lafaye

Certifié par yousign

RSM Paris
7 rue des Italiens
75009 Paris
France

Scope

We have examined Dawex accompanying description of its services throughout the period January 01, 2025 to December 31, 2025, based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3® Report (AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 01, 2025 to December 31, 2025, to provide reasonable assurance that Dawex'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 (AICPA, Trust Services Criteria).

Dawex uses the Dawex Data Exchange Solution (DXS) to enable organizations to create, nurture and orchestrate powerful data ecosystems. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Dawex, to achieve Dawex's service commitments and system requirements based on the applicable trust services criteria. The description presents Dawex's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dawex controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Dawex, to achieve Dawex's service commitments and system requirements based on the applicable trust services criteria. The description presents Dawex's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Dawex's controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service organization's responsibilities

In section III, Dawex has provided the assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Dawex is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; identifying the risks that would prevent the applicable trust services criteria from being met; designing, implementing, and documenting the controls to meet the applicable trust services criteria; and specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and on the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly, included procedures that we considered necessary in the circumstances.

Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented based on description criteria and the controls are suitably designed and operating effectively to meet the applicable trust services criteria throughout the period January 01,2025 to December 31, 2025.

An examination of the description of a service organization's system and the suitability of the design and Operating effectiveness of the controls involves

- Evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria and the controls were suitably designed and operating effectively, to meet the applicable trust services criteria throughout the period January 01, 2025 to December 31, 2025.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively.
- Testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met.
- Evaluating the overall presentation of the description.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent or detect and correct, all errors or omissions in providing services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls is subject to risks that the system may change or that controls at a service organization may become ineffective or fail.

Opinion

In our opinion, in all material respects, based on the description and the applicable trust services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period January 01, 2025, to December 31, 2025.
b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period January 01, 2025, to December 31, 2025.
c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period January 01, 2025, to December 31, 2025.

We noted there is no exception during our examination.

Restricted use

This report, including the description of tests of controls and results thereof in section IV are intended solely for the information and use of Dawex; user entities of Dawex 's Services for the period January 01, 2025, to December 31, 2025; and prospective user entities, independent auditors, practitioners providing services to such user entities and regulators who have sufficient knowledge and understanding of the following:

- The nature of the services provided by the service organization
- How the service organization's system interacts with user entities or other parties
- Internal control and its limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

RSM France
Member Firm Of RSM International
Jocelyn Grignon
Partner
Paris, France

Dawex Overview

About Dawex

Dawex is the technology company for data exchange, data marketplace and data hub. The mission of Dawex is to facilitate and accelerate secure data circulation between economic stakeholders, institutions, and private organizations, contributing to the development of the data economy. Dawex Data Exchange technology enables public and private organizations to operate their own data exchange solution to orchestrate a data ecosystem, source, distribute and exchange data trustfully, in compliance with regulations.

Companies in sectors such as agriculture, agrifood, automotive, banking, defense & space, energy, infrastructure, manufacturing, media & entertainment, mobility, real estate, retail, smart cities, tourism and trading are relying on Dawex expertise and technology leadership to foster innovation with impactful use cases and propel their organizations into a data-driven future.

By leveraging Dawex technology, organizations improve productivity, generate new revenue streams, develop innovative products or services, and increase their company valuation.

Custom-branded and fully configurable, Dawex Data Exchange Solution supports multiple free or monetized data exchange use cases taking place inside the organization or externally with participants of the data ecosystem, creating multiple data partnership opportunities.

The Dawex Data Exchange Solution brings the technical, contractual, financial, and regulatory compliance conditions for secure data sharing, bringing flexibility, traceability and control over the circulation of data.

Dawex technology is based on data privacy by-design and by-default. Therefore, it ensures that each organization benefits from all necessary information to comply with legal obligations and data protection regulations.

Dawex has capitalized on a rich cross-disciplinary expertise, structured best practices, and built pragmatic approaches to offer Data Exchange Advisory Services and help organizations tackle and deploy winning data exchange strategies.

Gartner, Forrester, 451Research and other renowned research firms recognize Dawex as a pioneer in the growing data economy. Dawex is a member of Gaia-X and is regularly consulted and engaged in projects at European and Institutional level on topics related to data sharing, data trading and privacy matters.

As a World Economic Forum Tech Pioneer and a member of the Global Future Council, Dawex contributes to the Data Policy work group to help define and implement forward-looking, interoperable, and trustworthy data policies.

Created in 2015, Dawex is headquartered in France, expanding business operations to Asia, North America and the Middle East. More information on: www.dawex.com

Description of the control environment, information communication, monitoring and Risk Assessment process

This section provides information about the five interrelated components of internal control at Dawex: Control Environment, Control Activities, Information and Communication, Monitoring, and Risk Assessment.

Control Environment

The objective of the control environment is to provide reasonable assurance as to the integrity and reliability of information, the protection of assets from unauthorized use, and that transactions are executed in accordance with management's authorization and client instructions.

Organizational Structure and Assignment of Authority and Responsibility

Dawex is organized around an executive team and six departments: Engineering & Research, Product & Customer Operations, Communications & Marketing, Sales & Business Development, Customer Success Management & Data Exchange Advisory, and People, Legal & Finance. This structure ensures a clear separation of responsibilities across all functions of the organization.

Governance and Oversight

The Management Board meets on a regular basis to discuss strategy, objectives, and operational performance. Meeting minutes are produced and distributed to all participants to ensure traceability of decisions and actions.

Each department holds recurring operational meetings led by its manager. Technical and security topics are addressed within the Engineering department's committee. Meeting minutes are produced and communicated to all attendees.

Service Level Agreement

Dawex defines service commitments with each client at the start of the contractual period. Service Level Indicators are monitored periodically, and compliance with contractual Service Level Agreements is overseen by the Customer Success team.

Human Resources

Dawex applies a structured recruitment process that includes management authorization, multi-stage interviews, background checks, and executive validation prior to hiring.

Upon arrival, each new employee receives a Welcome Kit covering company policies, corporate culture, and access to internal documentation. A structured onboarding program is completed during the first month, including IT security awareness training. Employee progress is tracked and formalized throughout the process.

Performance reviews are conducted three times a year. Employee training plans are formalized and approved by management, in line with Dawex's core values of pioneering spirit, customer focus, and team collaboration.

Internal Audit

The Engineering department oversees internal audit activities on security aspects. The internal auditor conducts periodic controls on the IT system, the product, and customer environments. Security policies and compliance controls are reviewed regularly with executive management.

Integrity and Ethical values

Integrity and ethical values are essential elements of the control environment, which influence the design, administration, and monitoring of key processes.

The CEOs and the management team are responsible for conveying the ethical and moral values to ensure integrity within the Team Dawex.

All employees are required to comply with all procedures and rules, as well as legal and ethical business practices, whether specifically mentioned in the different policies.

Diversity Equity and Inclusion

Dawex is composed of individuals from different countries, cultures, ethnicities, socioeconomic and academic backgrounds, genders, sexual orientations, and seniority. Our diversity brings a broad range of perspectives, which is a strength of Dawex's culture.

Treating customers fairly

Dawex seeks to maintain the highest level of professional and ethical standards when conducting business, especially when it comes to topics like corruption. We adhere to legal and ethical conduct in all relationships, including dealing with governments, government officials and private companies around the world.

Environment

Dawex is committed to behaving responsibly, and managing and offsetting our impact on the environment by:

- Minimizing waste and adopting sensible recycling policies, for example, with respect to our paper and food consumption
- Striking the right balance between remote and face-to-face meetings
- Encouraging low-carbon or carbon-free transportation options whenever possible
- Ensuring our premises meet advanced environmental certifications requirements

Control Activities

Dawex maintains a Controls Framework designed to address risks to reporting, operations, and compliance. Control activities, whether automated or manual, are applied at various organizational and functional levels to ensure management directives are carried out.

Information and communication

Information is identified, captured, processed, and reported through various internal systems as well as through interactions with clients, vendors, and employees. Security policy updates are communicated to relevant employees through internal channels.

Monitoring

Dawex monitors the efficiency of internal processes and the effectiveness of key controls on a continuous basis. Department directors are notified of internal process performance. Reporting to the Management Board is established by the Product and Engineering directors. Incidents are tracked through a dedicated management tool, and system performance is monitored around the clock.

Risk Assessment

Risk management is integrated into Dawex's governance activities. Dawex uses a recognized information security risk assessment methodology aligned with international standards as its reference framework.

The risk management process follows three steps: risk identification and classification, definition of a risk management plan with preventive measures, and ongoing risk control throughout the service lifecycle. The risk register is maintained dynamically and updated as new risks are identified or existing risk criteria evolve.

Components of the system providing the defined services

Services covered by this report

This report covers services provided to clients:

- Data Exchange Platforms (DEPs) Software Services
- DEPs infrastructure cloud services
- DEPs Support and maintenance services

Location

Software and infrastructure services are provided using certified cloud service providers. Service locations depend on client configurations and the availability zones of the cloud providers.

People

Support and maintenance services are delivered by the Customer Success, Product, and Engineering teams. Teams are organized by areas of expertise to support all clients.

Procedures

All teams are expected to apply Dawex global policies defining how services are to be delivered. These policies are accessible to all Dawex team members through the internal network.

Design and Implementation of controls process, policies and procedures requirements

Controls framework maintenance

Dawex designs, develops, and implements controls, including policies and procedures, as part of its risk mitigation strategy. Control owners are responsible for implementing controls, and management reviews are in place to ensure periodic evaluation against security commitments and requirements.

Procedures requirements

Procedures related to the Controls Framework are maintained and reviewed by dedicated control owners to ensure alignment with the related controls. Updates are made whenever control designs evolve.

Policies requirements

Dawex operates a structured policy lifecycle covering creation, review, approval, publication, and removal. Policies are proposed, drafted by contributors, and submitted for approval by designated validators before publication. During any revision or removal cycle, the current version of the policy remains in effect. Validators responsible for policy approval include members of executive management and the Head of Infrastructure and Security Engineering.

Dawex policies cover the following areas: IT management, IT security, operational instructions, and controls, reports and reviews.

Key system operations domains related to security

Physical Access

Access to Dawex office locations is controlled through individual access badges issued to employees during onboarding and returned upon offboarding. Visitor access is managed separately, with sign-in requirements and logged accesses at all locations.

Change Management

Dawex applies a structured change management process based on industry best practices, covering review, planning, approval, implementation, and validation. Changes require formal approval before implementation. Technical changes undergo code review and quality assurance validation before being deployed to production environments.

Computer Operations

Backup Strategy

Backups are performed automatically for all critical components of the Dawex infrastructure and client environments. They are encrypted both at rest and in transit, ensuring that data is never stored or transferred unprotected. Backups are replicated to a second geographic region to guarantee recovery in the event of an outage or regional failure. Retention policies are defined and enforced for all critical components, covering daily, weekly, and monthly backup cycles. All backups are restorable at any time. Restoration processes are tested periodically to ensure that both the procedures and the backups themselves remain fully operational.

Business Continuity and Disaster Recovery

Dawex maintains a Business Continuity Plan (BCP) and a set of Disaster Recovery Plans (DRP) designed to ensure the continuity of critical services and the recovery of systems in the event of a major incident or disaster. These plans cover three scopes: headquarters, Software Production, and Customer Infrastructures.

For each scope and risk scenario, the BCP and DRP define key human resources, recovery procedures, and RTO/RPO objectives. For scenarios involving Cloud Service Providers, recovery objectives are aligned with the respective CSP commitments.

Responsibilities for crisis team activation and execution of recovery procedures are clearly assigned to the Engineering and Product teams, under the supervision of executive management.

The BCP and DRP are reviewed and updated periodically to reflect changes in the system architecture, new risks identified through the EBIOS RM risk assessment process, or lessons learned from incident post-mortems.

Monitoring Stack

Systems and infrastructure are monitored continuously using a centralized monitoring and alerting stack. All applicative logs, metrics, and events are collected from multiple sources and forwarded to a centralized log aggregation system for correlation, monitoring, and security alerting purposes. Logs are retained for one year. Alerts are triggered automatically and routed to the responsible teams. Scheduled tasks and automated jobs are also monitored to ensure they complete within their expected timeframes.

Incident Management

Incidents are classified by nature and criticality. Upon detection, a team member acknowledges the alert and investigates the source of the issue. For incidents impacting customer environments, incident reports are produced and communicated to affected customers by the Customer Success team in coordination with the Engineering team.

Problem Management

When incidents require further investigation, a formal problem management process is initiated to identify root causes and implement durable fixes. Proactive monitoring is also in place to anticipate and prevent potential incidents.

Vulnerability & Patch Management

Dawex follows recognized industry best practices for vulnerability and patch management, covering detection, reporting, and remediation. Known vulnerabilities are automatically detected through code analysis. Critical patches trigger an immediate release rolled out to all customer environments. Regular penetration tests are conducted annually by a PASSI-qualified third-party auditor. Identified vulnerabilities are tracked and remediated within defined timeframes.

IT Logical Security

Security Policy

Security is a core value at Dawex. Access to information is controlled based on defined authorization levels. Sensitive communications are encrypted. Every employee has a confidentiality clause in their employment contract, while subcontractors operate under non-disclosure agreements. Dawex conforms to the European General Data Protection Regulation (GDPR).

Security awareness is an ongoing commitment at Dawex. All employees are required to complete security awareness training. Regular phishing simulations are conducted to test and reinforce employee vigilance. Monthly security talks are organized to keep all team members informed of the latest threats and best practices. A dedicated internal channel is used for IT security communication and issue reporting.

Access Management

Access to systems and data follows a full lifecycle approach, from provisioning to revocation. Access rights are granted on a need-to-know and least privilege basis, tied to the user's role and department. Each user has a unique individual account; shared accounts are strictly prohibited. Administrative and privileged access is restricted to authorized personnel only.

Upon onboarding, access rights are provisioned in line with the employee's role. Access to all business tools is managed through a centralized identity provider using Single Sign-On (SSO), ensuring a unified security control point. Multi-factor authentication is enforced at the identity provider level for all critical tools.

Throughout the employment period, user accounts are reviewed on a quarterly basis. Reviews cover active accounts against the current employee list, administrator and privileged access rights, multi-factor authentication enforcement status, and access logs including login activity, account modifications, and suspicious actions.

Upon offboarding, all access rights are promptly revoked and accounts are disabled, ensuring that former employees retain no access to Dawex systems or data.

Workstation and Endpoint Security

All corporate workstations are delivered to employees during the onboarding process and are hardened by Dawex before use. Hardening measures include full disk encryption, enforcement of corporate security policies, and installation of approved security tools. Patch management and system updates are handled centrally for all endpoints, ensuring that workstations remain up to date against known vulnerabilities.

Anti-malware protection is deployed on all workstations and managed centrally by the Dawex security team. The desktop security strategy is based on overlapping layers of defense, combining endpoint protection, application management controls, and built-in operating system security features to prevent malware

installation and enable a rapid detect-and-respond process.

All corporate assets, including workstations, accessories, meeting room equipment, and software licenses, are inventoried and managed through a centralized asset management system. This ensures full visibility over the asset lifecycle, from procurement and configuration to offboarding and disposal. Upon leaving the company, employees return their workstations, which are then securely wiped before being reissued or decommissioned. A formal quarterly review of all digital assets is conducted to ensure the inventory remains accurate and up to date.

Network Security

Network and firewall configurations are managed by a restricted group of authorized administrators. All changes follow the change management process. Network segmentation controls are in place to isolate corporate, internal, and guest environments.

Product Logical Security

Security Policy

The Dawex Data Exchange Solution (DXS) is built on "Security by Design" and "Privacy by Default" principles, meaning that security and data protection are embedded into the architecture and development process from the ground up, rather than added as an afterthought. The DXS security practices are guided by internationally recognized frameworks, including OWASP methodologies, covering web application security, cloud infrastructure, secure development practices, and vulnerability management.

Automated security testing is integrated throughout the entire development lifecycle, enabling continuous detection of vulnerabilities before any change reaches production. Code quality and security are enforced through static analysis and automated test suites at every stage. All network flows are authenticated and logged, ensuring full traceability of interactions across the DXS. Deployments follow a consistent process across all environments, reducing the risk of configuration drift between stages.

Cloud Architecture

The Dawex Data Exchange Solution (DXS) is built on a cloud-native, microservices-based architecture. This approach allows each component of the DXS to be developed, deployed, and scaled independently, reducing the blast radius of any potential incident and improving overall system resilience. The DXS is hosted on certified multi-cloud infrastructure, leveraging the reliability, availability, and security capabilities of leading cloud service providers. This multi-cloud strategy also eliminates single points of failure at the infrastructure level. Development, pre-production, and production environments are fully separated and independent, ensuring that no test or development activity can impact live customer data or services.

Network protection

Dawex implements a multi-layer network protection strategy for all internet-facing infrastructure. A Web Application Firewall (WAF) is deployed, enforcing rules aligned with the OWASP Core Rule Set (CRS), providing protection against injection attacks, cross-site scripting and protocol-level anomalies. WAF events are centralized into the monitoring stack, enabling correlation with other security events. DDoS mitigation at the network and transport layers is provided natively by the Cloud Service Providers as part of their managed infrastructure services.

Encryption and Data Protection

All data exchanged through the DXS is protected through end-to-end encryption. Data in transit is secured using industry-standard encrypted communication protocols. Data at rest is encrypted across all storage components within the Dawex infrastructure. Each file uploaded to the DXS is encrypted with a unique key, ensuring that a compromise of one key cannot expose other files. Cryptographic keys and secrets are managed through a dedicated secrets management solution, with keys owned and controlled by the solution rather than the customer.

Identity and Access Management

Access to the DXS is handled exclusively through encrypted channels. A role-based access control model is implemented, ensuring that each user can only access the features and data relevant to their role. Multi-factor authentication is supported, and sensitive actions on the DXS require explicit re-confirmation to prevent unauthorized operations.

Before gaining full access to the DXS, each new user goes through a mandatory identity vetting process. During this process, users are required to provide verified professional information, and their identity is manually reviewed by the solution orchestrator. Access to DXS features remains restricted until the vetting is successfully completed. Only fully verified users can interact with the solution, search for data offerings, engage in conversations, or publish content. This process ensures a trusted environment for all participants of the data ecosystem.

Data Segregation

Dawex Data Exchange Solution provides a native multi-tenant architecture. Data exchanged by tenants is segregated at the application level while sharing the underlying physical infrastructure.

For customers requiring higher isolation, the solution can be deployed as a single-tenant infrastructure, with complete isolation at every level from physical servers to the core application.

Development, pre-production and production environments are fully separated and independent.