RSM

DAWEX

Service Organization Controls 3

(SOC3, Type 2) Report

Description of
Dawex IT Outsourcing Services Systems relevant to Security from May 30 to November 30, 2021

With the Independent Service Auditor's Report

April, 2022

TABLE OF CONTENTS

This document contains 33 pages excluding header and summary

Assertion of Dawex

RSM

DAWEX

SOC 2 Management Assertion

We have prepared the accompanying Description, *Description of DAWEX Systems relevant to Security as of April 19, 2022* 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 supports 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 board 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.

Laurent Lafaye
CEO

DocuSigned by:
Laurent Lafaye
E27E71E30AB0497...

Independent Service Auditor's Report

Independent service auditor's report

RSM Paris
26, Rue Cambacèrès
75008 Paris
France
Tel: +33 (0) 1 56 88 31 20

Scope

We have examined Dawex's accompanying Description, *Description of Dawex Systems relevant to Securityas of April 08th, 2022* ('Description') based on the criteria set forth in paragraph 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), and the suitability of the design of controls described therein to meet the criteria for the security principle set forth in the AICPA's TSP section 100 *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria) from May 30 to November 30, 2021.

Dawex's responsibilities

Dawex has provided the accompanying assertion titled *Assertion of Dawex* (Assertion) about the fairness of the presentation of the Description based on the description criteria and suitability of the design 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 the Assertion.

Dawex is also responsible for providing the services covered by the Description, specifying the controls that meet the applicable trust services criteria and stating them in the description; and designing, implementing and documenting controls to meet the applicable trust services criteria.

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 of the controls described therein to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented, and the controls were suitably designed to meet the applicable trust services criteria–from May 30 to November

30, 2021.

An examination of a description of a service organization's system and the suitability of the design of the service organization's controls involves performing procedures to obtain evidence about the fairness of the presentation of the Description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the Description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. An examination of this type also includes evaluating the overall presentation of the Description.

We did perform the procedures regarding the operating effectiveness of the controls stated in the Description and, accordingly, do express an opinion thereon.

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

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important in its own needs. Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. 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 of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

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

A. Description fairly presents Dawex's IT Outsourcing Services Systems that was designed and implemented from May 30 to November 30, 2021.
B. The controls stated in the Description were suitably designed and implemented to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively from May 30 to November 30, 2021.
C. The controls tested were those necessary to provide reasonable assurance that the applicable Trust Services Criteria were met, operated effectively at the time of the review.

There is no exception identified during the audit.

Restricted use

D. This report is intended solely for the information and use of Dawex, user entities of Dawex's IT Outsourcing Services Systems from May 30 to November 30, 2021.; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's systems interact with user entities, subservice organizations, and 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 Paris

Jean-Philippe Isemann, CISA, CISM, CRISC
Partner
Paris, France

Signé électroniquement par
CONNECTIVE NV - Connective
eSignatures de la part de
Jean-Philippe Isemann
(jean-philippe.isemann@rsmfranc-
e.fr) Date : 20/04/2022 16:49:22
Signé avec le code à usage
unique : 695816

Description of Dawex IT Outsourcing Services Systems relevant to Security from May 30 to November 30, 2021.

Dawex Overview

About Dawex

Dawex is the leading data exchange and data marketplace technology company. Dawex mission 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 platform to orchestrate a data ecosystem, source, distribute and exchange data trustfully, in compliance with regulations.

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 Platform 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 Platform brings the technical, contractual, financial and regulatory compliance conditions for secure data sharing, bringing flexibility, traceability and control over the circulation of data.

Dawex approach 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.

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 a co-founding member of the Data Exchange Association. Dawex 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 has offices in France and Canada, expanding business operations to Asia, the United States 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 OUR CLIENT:

- Control Environment – sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Control Activities – are the policies and procedures that help make sure that management's directives are carried out.
- Information and Communication – are systems, both automated and manual, that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Monitoring – is a process that assesses the quality of internal control performance over time.
- Risk Assessment – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Our client's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When assessing internal control, we consider the interrelationships among the five components.

Control Environment

The objective of the control environment is to provide reasonable, but not absolute, assurance as to the integrity and reliability of information; the protection of assets from unauthorized use and transactions are executed in accordance with management's authorization and client instructions.

Dawex has an internal control process to monitor compliance with policies and procedures established by our client.

The remainder of this section deals with the rules established by management regarding the integrity, ethical values and competence of our client's employees, the policies and procedures, the risk management process and monitoring and the role of significant control groups. The internal control structure is established and updated on the basis of regular risk assessment.

Organizational Structure and Assignment of Authority and Responsibility

The Dawex organization chart is described below. It is composed of an executive team and five departments: Engineering & Research, Product & Customer Success, Com & Marketing, Sales & Business Development, and Finance, People & Legal.

Governance and Oversight

Management Board Committees

The Management Board meets every two weeks. It is composed of the members of the executive team. Guests may be invited according to the topics on the agenda. It is led by the Co-CEO. During this committee, strategies, highlights, objectives and forecasts are presented and discussed.

An agenda is shared before the meeting and a minute is communicated to all participants.

The minute includes the decisions and actions to be followed.

Department Committees

Each department has a recurring operational meeting every two weeks. It's led by the department manager.

The technical and Security aspects are managed by the Engineering department.
All incidents occurred during the previous weeks, problems management, application management and technical changes, planning and incoming subjects are discussed.

Following each committee, a minute is produced and communicated to all attendees.

Service Level Agreement

Dawex defines a scale of service needed with the client at the beginning of the contractual period.
Service commitments based on compliance with contractual indicators are made for each service. Each indicator is monitored periodically and specifically to the extent that it represents a component of the service.

Freshdesk software is used as a customer and user support management tool.

The measured indicators are defined in Freshdesk with the different parameters:
Period: period of receipt of the application or incident
Calculation formula: calculation method used to obtain the indicator
Threshold: specifies the level of service commitment made to this indicator, this is the objective to be achieved.

The Customer Success team is in charge of the user and customer support management, including the indicators calculation (Service Level Indicators) and the compliance with the contractual indicators (Service Level Agreements).

Human Resources

Hiring Process

The recruitment procedure follows 3 steps:

- Opening of the position
- Interviews
- Hiring

Opening of the position: each request for a position is first authorized by management with validation of the position and the associated budget. Once the position is defined, the People Department writes the offer, validated by the executive management, and creates the position in SmartRecruiters software (Applicant Tracking System). The validated offer is then published on several dedicated websites such as Welcome to the

Jungle or Linkedin. In exceptional cases specificity of the position, number of positions to be filled, recruitment agencies are called upon. At the same time, the choice of the "interviewers" team (3 or 4 people), trained to conduct interviews (Dawex Interviewer Pass), is made.

Interviews: Manager of the open position, assisted by the People Department, sorts through the CVs received. For the applicant whose CVs have been selected, the recruitment process follows several stages which follow one another if the interview is validated and meets a certain timing:

- Interview with the manager by visioconference call,
- then interviews with each of the members of the interviewing team that has been previously selected followed by technical tests when applicable
- then the Caliper Test (personality test) and a culture fit interview to validate that the selected applicant is in line with the company culture and has the soft skills expected in the company.
- reference taking and verification of diplomas
- final interview with the executive management

These steps are spread over 15 working days. At each interview, a report of the interview is written by the interviewer in SmartRecruiters software.
In case of rejection, the applicant is notified by email by the People Department and the information is entered into SmartRecruiters software.

Hiring: for the applicant selected, preparation of the promise of employment by the People Department, validation and signature by the executive management and sending by the manager. Signature of the promise by the applicant by electronic signature at the latest on the first day before his arrival and update of staff register at the arrival. This step must be completed within 7 working days after the validation of the application.

Onboarding

Upon arrival, each new employee is given his Welcome Kit including:

- procedures related to the company (training policy, travel policy, procedure for managing employees' personal data),
- a reminder of the corporate culture including Dawex values and a word of the executive management,
- the access to the internal documentation relating to the day to day life at Dawex

The Onboarding process: all administrative tasks related to the arrival of an employee are configured and monitored in Lucca software (People management solution).

During his first month at Dawex, the new employee is invited on Confluence (Collaborative work software) to an integration course which mixes face-to-face and

online sessions allowing him to discover the company, including:

- Presentation of internal tools
- IT Security awareness
- Demonstration of the platform, of the trust process and deployment of a platform
- Presentation of safety work tools
- Presentation of the design process and product development
- Presentation of the different departments

As soon as the session is performed, it is marked as validated in the Confluence which allows to follow the progress of the onboarding and to check when the session is complete within the delay.

At his arrival, a milestone is systematically planned with the manager and formalized in Lucca software (no later than one month since his arrival).
Another interview with the executive management is also planned in Lucca after 2 months of attendance at Dawex.

Performance review

Three times a year, employees meet their management in order to discuss and evaluate their performance (skills, achievements, training, objectives and career aspirations), to fix the objectives for the next period and to receive/ to give constructive feedback.

The interview is prepared in Lucca software (People management tool) prior to the meeting. At the end of the interview, the review is completed and signed electronically by both parties. The follow-up of the employee over a longer period of the different achievements is then facilitated and optimized as all information as the achievements, training, objectives is available in Lucca.

Training

The Dawex Training Program is based on Dawex's three core values:

- The pioneering spirit: to train with the aim of anticipation and discovery
- The customer spirit: to develop the quality of the relationship, the understanding of needs, efficiency in the solutions
- Team spirit: sharing knowledge with Dawex employees.

This program is a complement to the training sessions given during the onboarding of all new employees, which aim to introduce them to the product, the technologies used, their work environment and the company culture. In parallel to this program, Dawex employees have access to monthly Brain breaks and the opportunity to spend one day a year in the Paris or Lyon offices or in a customer location to better understand the sales and marketing challenges of Dawex.

Upon request and according to their needs, employees can have access to:

- Business training courses
- Professional conferences on topics of expertise
- Coaching sessions validated by the manager, to develop employees' soft skills
- Training in public speaking, for employees who are required to be Dawex spokespersons outside the company.

The employee's training plan is formalized in his or her various interviews into Lucca software (People management tool).
For any requested training, the training will have to be done in agreement with the manager (content and timing) and the approval of the executive management.

Internal Audit

The engineering department is in charge of the internal audit on security aspects.

The internal auditor provides on-demand control of the Dawex IT system, as well as the product and customer environments.

This service assumes the review of Information Security Policy and Security Guideline documents (that lists the solved and on-going security issues) with the CEO monthly. All periodic controls linked to security compliance are led by the Internal Auditor (Information Security Policy, User Access Management, System description, Security Guideline, etc.).
Our client formalizes procedures to describe the audit policies.
The Management can request the Audit Service to analyze IT process deficiencies and lack of documentations issues.

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 or not 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

We seek 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

We are 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 the risks that threaten the achievement of objectives related to reporting, operations and compliance).
Control activities are based on the policies and procedures that enable management directives to be carried out. They help ensure that necessary actions are taken to address risks to achieve the entity's management directives. Control activities, whether automated or manual, generally relate to the achievement of specific controls objectives and are applied at various organizational and functional levels.

Information and communication

Information and communication are an integral component of DAWEX 's internal control system. It is the process of identifying, capturing and exchanging information in the form and time frame necessary to conduct, manage and control DAWEX 's operations. At DAWEX, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, vendors and employees.
Updates to entity-wide security policies and procedures are communicated to the

appropriate DAWEX employees via the internal network.

Monitoring

DAWEX uses both, internally developed and COTS (Commercial Off-the-Shelf) applications, to monitor the efficiency of identified processes and the effectiveness of key controls. Metrics produced by these applications provide performance measurement of internal processes.
Department Directors are directly notified of internal process performance (dispatching support tickets, out of date maintenance, incidents, etc.).

Reporting to the Management Board is established by the Product & Engineering Directors. An incident management tool is used to follow the different steps of the change ('Support'). A Logging and monitoring software is used 24/7 to identify and evaluate performance.

Risk Assessment

Risk management is integrated into the governance activity of the service. Our risk management methodology is based on 3 steps:

Step 1: Risk assessment

Risk assessment consists of identifying the risks inherent to the project and classifying them according to qualitative criteria.
Risks are listed and then evaluated according to 2 criteria:

- probability of occurrence
- impact on the business

Step 2: Risk management plan

At start, Dawex and client jointly define the main project risks. Once identified and classified, a risk management plan is put in place.
This risk management plan must be integrated into the overall project planning. It defines how each risk will be monitored throughout the service. The plan specifies preventive measures to be implemented for each of the risks identified.

Step 3: Risk control

Throughout the life of the project, risks must be controlled in accordance with the validated risk management plan.

- The control must be carried out by Dawex and client according to the frequency and modalities provided

- The steering committee must ensure that the action plan defined to mitigate the risks is properly implemented
- The risk management plan is evolving and dynamic. It must be the subject of corrective actions adapted throughout the service
- The risk table must be constantly updated according to new risks that can be identified as the project progresses
- The analysis matrix is updated according to these new risks and/or the probability or impact criteria that may change.

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

The software and Infrastructure services are provided to clients using Cloud Services Providers capabilities. The locations of these services depend on DEPs' configurations and on the availability zones of the cloud service provider.

People

Support and maintenance services are provided by the Customer Success, Product and Engineering teams located in the Lyon office.

The teams are organized by skills and technologies and support all clients in their areas of expertise.

Procedures

All teams are expected to accept and apply the DAWEX global policies that define how services should be delivered. These are located on the company internal network (and can be accessed by any DAWEX team members.)

Design and implementation of controls process, policies and procedures requirements

Controls framework maintenance

DAWEX designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy: a Controls Framework is maintained and is designed to address the risks that threaten the achievement of objectives related to reporting, operations and compliance.

Control owners implement those controls and management reviews are in place to ensure that the controls are periodically evaluated against Security commitments and requirements.

Procedures requirements

Procedures related to DAWEX 's Controls Framework are maintained and reviewed by the dedicated control owners in order to ensure they are aligned with the related controls.
In case of updates needed following controls design changes, the dedicated control owner aligns the related procedures.

Policies requirements

The following describes Dawex policies workflows

New policy

1. A new policy is proposed and initiated into the IT Security Management System
2. The policy is drafted by contributors
3. The policy is proposed for approval by validators
4. If the new policy is approved, the policy is published
5. If the policy is not approved (needs for improvements), a new draft cycle is initiated
6. If the policy is rejected, it is deleted from the IT Security Management System

Policy editing

1. A policy is proposed for modification

2. The edited policy version is updated
3. The edited policy is drafted by contributors
4. The edited policy is proposed for approval by validators
5. If the edited policy is approved, the policy is published
6. If the policy is not approved (needs for improvements), a new draft cycle is initiated

Note: during the policy editing cycle, the previous version of the policy applies

Policy removal

1. A policy is proposed for removal
2. If the policy removal is approved by validators, the policy is removed from the IT Security Management System

Note: during the policy removal cycle, the current version of the policy still applies

Validators are responsible for **policies approval**, leading to publication.

The following table lists Dawex' validators for Security Policies:

Name	Responsibility
Fabrice Tocco	CEO
Laurent Lafaye	CEO
Morgane Commowick	Director of Product & Customer Success
Stéphane Vaquer	Director of Research & Engineering

These policies include:

- IT Charter
- IT Security Policies
- Instructions
- Controls, reports & reviews

IT Security Policies regroup:

- Security Policies Workflows
- Incident Management
- Change Management
- Security Awareness and employee training
- GDPR
- Online Tools

- Backup strategy
- Workstation policy
- Password policy
- User access management
- Network security
- Anti-malware policy
- Asset Management
- Physical security
- Responsible disclosure
- Data protection
- Secure communication
- Databases
- Document classification

Instructions regroup:

- Backup procedures
- Onboarding tasks
- Network & infrastructure monitoring tools
- Batch jobs
- Business Continuity Plan
- Disaster Recovery Plans

Controls, reports & reviews regroup:

- Backup Monitoring and reporting
- Application state and incident list
- User accounts reviews
- Asset reviews
- Physical access logs & reviews

Key system operations domains related to security

Physical Access

Physical Access Process

Lyon (Head Quarter)

Physical access to the building is controlled by;

- a magnetic pass (for employees)
- an intercom (for visitors)

Physical access is controlled by keys: all employees need to use their own keys in order to access the HQ.

The magnetic pass and key are delivered to by the People Department during the onboarding process. Conversely, during the offboarding process, employees return their magnetic pass and key to the People Departement.

Visitors must check-in and accesses are logged on a physical ledger.

There is no computer room.

Paris

The Paris office is managed by WeWork, where Dawex rents private offices. Control badges are individually given to employees during the onboarding process. Conversely, during the offboarding process, employees return their magnetic pass.

Visitors need to sign in at the entrance and accesses are logged.

There is no computer room.

Change Management

Our change management process is based on these ITIL recommended activities:

- Reviews
- Planning
- Approvals
- Implementations
- Validation & completion

Find Below the description of each step and its responsible team. Some small changes without impact can be pre-approved and therefore, skip some of these activities.

Reviews

After an internal member requests, a change with details like the affected systems, possible risks, and expected implementation, a person is affected to review this request.

In this step, if some additional information is needed, the reviewer asks for details to the reporter. Once all needed information is completed, change is planned.

Planning

Product Owner of each team involved in the requested change plans the change in the product roadmap with these details:

- Timeline of the implementation, with epics and/or tasks required to implement the change.
- Define the team member involved in the change (customers, developers, operations, support...), and organize communication if there is any customer impact.
- Define time estimate of each step of the implementation. This can be delegated to tasks assignees.
- Make sure testing and rollback of the change are taken into account and are part of the planned roadmap. Risks involved by the change should also be estimated.

Approval

Change approval is required before starting the implementations. A member of the product team should approve the requested change planning and implementation tasks before involved teams start working on it.

Implementations

The team members responsible for the implementation work on the change, documenting their procedures and results.

Technical change requires passing through the code review process before merging to master codebase. A staging version of the change is deployed, and QA reviewed following our development validation process.

Once the change is validated, it is deployed to the production environment according to planning and customer communication.

Validation & completion

Product team reviews and closes the implemented change. They note whether it was successful, timely, accurately estimated, within budget, and other details.

Computer Operations

Backup Strategy

All backups at Dawex are performed automatically with Infra-as-code jobs deployment. Each critical component requiring a backup comes with a dynamic backup job implementation.

Backup types:

- Native cloud/provider replication: native resilience for certain kinds of cloud services, such as S3 buckets, AWS/Google drives, Google Apps servers, ...
- Datastores: Databases dump cron jobs

- Time Machine: automated office incremental backups from sensitive mac clients
- Git clones: clone of repositories made client-side or scripted on the backup server
- Git backup repository: repository dedicated for configurations and scripts backup and versioning
- System/volumes snapshots (vms, amis): VmWare recurrent snapshots and manual instance model creation (cloud) for sensitive systems

All backups are performed daily or more frequently, depending on component criticality.
They are performed automatically with the Cloud provider backup policies, or via backup jobs running as cron jobs.

Each backup is monitored by our monitoring stack using Prometheus and DeadManSnitch:

- Backup logs are exported to our central log aggregator
- If a backup fails, an alert is triggered to our standard notification channel
- If a backup has not been done for a time > frequency, DeadManSnitch triggers to our standard notification channel

Restoration

The restore Process is part of the backup strategy. Each restoration process is tested every quarter to make sure processes and backups are fully functional.

Restore process should be done using backup dumps or volume snapshots.
To restore a database from a dump:

- Spawn a pod with datastore client (mongodb-client, postgres-client or mysql-client)
- Fetch dump from external storage location
- Import dump to the database

Batch Management

We are using different batch types in our application ecosystem. All are based on infrastructure & cloud jobs triggered by a cron or a specific event:

- Backup jobs: Runs all critical components backup.
- Logs management: Export logs to an external location for backup, monitoring and auditing in a centralized interface.
- Platform usage exports: Export logs, metrics and other data used for business logic analysis and data visualization.
- Lambda/Kinesis functions: Data flows with an event-driven serverless computing system.

- Cleanup jobs: Jobs used to cleanup resources according to retention and configuration policies.
- Keys rotation jobs: Manage security keys rotation.

Monitoring Tools

We are using these tools for infrastructure and software monitoring:

- Prometheus: Metrics based open-source monitoring solution
- Alert Manager: Handles alerts sent by client applications such as the Prometheus server
- DeadManSnitch: Cron job monitoring tool
- Grafana: Open source analytics & monitoring solution
- UptimeRobot: Website monitoring

Incident Management

Our monitoring tools described in the previous section can detect and trigger incidents to our alerting tool: Atlassian Opsgenie.

Upon reception of such incident alert, OpsGenie notifies Infrastructure team on various mediums:

- Slack channels #ops-opsgenie
- Slack channel #ops-hub-alerts
- Team members can also receive notifications via SMS, email, or push notification on Opsgenie mobile application.

Depending on the nature of the incident (transient, or permanent) and its criticity (low to critical), a team member acks the incident notification and investigates on the source of the issue.

When an incident requires further investigation, we create a ticket to identify the underlying cause of the issue and figure out how to fix it going forward. This step is described in the Problem Management procedure.

Problem Management

When an incident requires further investigation, we create a ticket to identify the underlying cause of the issue and figure out how to fix it going forward.

Problems can also be proactively detected to avoid future incidents to occur. We try to avoid relying on reactive actions and define monitoring probes and metrics to anticipate incidents from happening (Disk space size, certificates expirations, etc...).

Steps for the problem management process are described as follow:

- Prioritize: On ticket creation, we define the criticality of the problem to organize the issue in the backlog.
- Investigate: Identify the root cause and the best way to implement a durable fix.
- Document: If the problem triggers an incident, having documentation and a workaround of the error helps us identify and fix quicker, limiting the impact and downtime.
- Resolve: Implement a stable fix to make sure the problem will no longer create an incident. Some fix implementations may take some time, and in that case, we can use a temporary workaround to limit business impact while we implement the stable solution.

IT Logical Security

IT Security Policy

Principles

Security is a corporate value:

- Constant concerns through security and confidentiality internal formations and updates
- Access to different levels of information is controlled
- Data & systems access authorizations are clearly defined, limited in time
- Sensitive emails and communication are encrypted
- Every employee has a confidentiality clause in his employment contract, while subcontractors work under NDAs

Audits and responsible disclosure policy

Regular audits are internally conducted by external security experts (pentests) on our platform and its code
We encourage responsible reporting of security issues

General Data Protection Regulation (GDPR)

Dawex conforms to the European General Data Protection Regulation (GDPR), which took effect on May 25, 2018.

Policy for online tools

- Use a Dawex account to identify yourself (no personal accounts)
- Do not share online accounts
- Never ever leave a document in public access
- Do not store information permanently.

- Once an online job is finished, and especially if it is sensitive information, export the results (to a private Dawex share), then delete the related documents from the online platform

Security awareness and employee training

- All employees must follow a security awareness training
- A dedicated Slack channel is used for IT security issues & management
- Security Tips are published via Slack for all employees
- Monthly Security Talks are organized

Workstation policy

Workstations – are either MacOS based or GNU/Linux based – are delivered to employees during the onboarding process.

Hardening of these workstations is done by Dawex:

- Disk encryption
- VPN (TunnelBlick)
- Keys and secrets management (KeePassXC)
- Workstation Management (VMWare Workspace One), used to
    - Enforce security policies
    - Deliver patch management
    - Secured emailing (Thunderbird + GPG or Apple Mail + GPG)
    - Install and manager corporate tools (Slack, Zoom, KeePassXC, TunnelBlick)

During the offboarding process, workstations are returned to Dawex and are wiped out.

IT and cloud provider (Google Workspace)

Dawex relies on Google Workspace (formally Google Suite) to manage its IT Infrastructure:

- Users and groups management & security policies
- Shared resources (Google Drive)
- Office Applications (Google Doc, Sheet)
- E-mailing

Password Policy

Our password policy is the following:

- Strong passwords are mandatory
- A strong password is :

    - Long (at least 12 characters)
    - Random
    - Generated by a tool (password manager)
- Use unique passwords (one for each online service)
- A Password Manager assists in generating and retrieving strong (complex) passwords, storing them in encrypted databases or calculating them on demand.
- KeePassKC is used as a Password Manager
- Never store credentials on your web browser
- 2FA is mandatory (and enforced) to access sensitive information and tools: GSuite, GitLab, HubSpot

User Access Management

Dawex relies on Google Workspace (formally Google Suite) to manage its IT Infrastructure:

- Users and groups management & security policies
- Authentication
- 2FA is mandatory to access Google Workspace, HubSpot and Gitlab. 2FA is based on Google Authenticator or YubiKeys (IT Team)

User Accounts Review

User account reviews are managed through Google Admin Console:

- Accounts
- Groups

Reviews are scheduled:

- On a quarterly basis (full review)
- Before onboarding for new employees
- During the offboarding process

Network, VLAN and firewall management

IT infrastructures and Products was being managed in the Cloud (Google Cloud, AWS or Azure), firewalls are managed by Dawex cloud service providers

Networks, VLAN and firewall management is handled by a restricted list of administrators that are the only employees allowed to proceed to changes in configurations.

Modifications of network, VLAN or firewall configurations are following the change management process, requiring proper validation and reviews.

The network topology is the following:

- Public LAN: Dawex private internal network for corporate devices. Secured with WPA2 password and MAC addresses whitelist
- Internal LAN: Dawex public internal network. Secured by WPA2
- Guest LAN: Public hotspot for external visitors. Secured by voucher code

Anti-malware policy

Dawex employees only use MacOS or GNU/Linux workstations. Workstations are enrolled into WS1 for patch management, software and system updates. Running under MacOS or GNU/Linux and being managed by WS1, Dawex workstations are less prone to malware infection.

Our office tools (docs, slides, spreadsheets, shared Drives and e-mails) are exclusively online, via Google Workspace services. Anti-software protection is provided by Google Workspace.

Dawex desktop security policy for MacOS workstation is based on overlapping layers of defense. Services such as Workstation Management, App code signing, Run-Time protection and Protection against malware (Notarization, XProtect, Malware Removal Tool and Automated security updates) are designed to prevent malware installation and, when necessary, to provide for a quick and efficient detect-and- respond process to block and remove any malware that may have at first avoided detection.

Asset management

Workstation enrollment: All laptops must be enrolled into VMWare Workspace One (WS1), used for:

- Inventory
- Configuration
- Onboarding
- Offboarding
- Troubleshooting
- Remote assist
- Security & patch management
- Installation of corporate tools

Digital assets: on top of WS1, digital assets are managed via Snipe IT: Asset inventory tool

- Workstations (GNU/LInux & MacOS laptops)
- Accessories (keyboards, mices, screens, ...)
- Software Licences

A quarterly review of digital assets is conducted and formalized

Product Logical Security

Security Policy

Principles

The design of the Data Exchange platform is based on the following principles:

- Build a bespoke technical architecture (infrastructure and software) to bring guarantees on customers' data protection (technical, rules and regulations and business agreement)
- Apply "Security by Design" & "Privacy by Default" principles to ensure data integrity and data privacy
- Control the building and running of the "core-system": quality, scalability & security, automated deployment on preprod / prod after successful automated tests
- Consistency of deployment with the use of the same image on every stage
- Deploy only a small portion of the application (microservices)
- Static analysis of code to increase quality & automated test to help reduce bugs and regressions
- Automatic metrics to monitor system activity
- Network flows strictly authenticated and logged
- Application and API accessible through asymmetric encrypted protocols
- Streams filtered by reverse proxies and isolated by network Access Control List (ACL)
- Two factors authentication and re-validation for sensitive actions

OWASP Methodologies

We rely on the following OWASP methodologies, awareness documents, guidelines and sets of tools:

- The **OWASP Top 10** for web applications (rev 2017):
- The **OWASP Top 10** for Cloud infrastructure (pre-release):
- The **OWASP Top 10** for Docker (pre-release):
- The **OWASP ASVS** (Application Security Verification Standard) v4
- The **OWASP Testing Guide** v4
- The **OWASP Proactive Controls for Developers** (2018, v3)
- The **OWASP Dependency-check**, OWASP Dependency-track coupled with SonarQube for "A9-2013 – Using Components with Known Vulnerabilities" risks

- The OWASP Cheat sheet series project specific security topics, best practices and reference implementations (REST Security, Access Control / Authorization, Authentication, Docker Security, Injection prevention, Input validation, Key management, Logging, Multi Factor authentication, Error Handling, HTML5 security, User Privacy Protection, Virtual patching, Vulnerability disclosure, Web Service security)

Architecture and managed cloud services provider for our product (AWS)

Dawex infrastructure for our product is a cloud-native, microservice based solution that is designed to overcome the limitations of web-based architectures.

Dawex infrastructure is based on managed cloud services delivered by AWS.

Encryption, keys & secrets management

Security and efficiency are of big importance for Dawex. Day by day, we aim at maintaining the highest security standards to trade data safely and easily.

- We use asymmetric encryption protocols to store and transmit data.
- All personal and activity-related data is encrypted.
- Network flows strictly authenticated and logged
- Application and API accessible through asymmetric encrypted protocols
- Streams filtered by reverse proxies and isolated by network Access Control List (ACL)
- End-to-end encryption

Keys and secrets management.

- Key Selection: we rely on FIPS 140-2 compliant cryptographic modules for key generation
    - AES256 keys for data encryption
    - openSSH keys for accessing the Bastion Host
    - libreSSL for RSA 4096 keys (Let's Encrypt CA) for HTTPS/TLS
- Certificate Authority:
    - Let's Encrypt CA is used to issue X509-v3 certificates used for HTTPS/TLS communications
- Secrets are managed and stored using HashiCorp Vault

Password Policy

Our password policy is the following:

- Strong passwords are mandatory
- A strong password is:

- Long (at least 12 characters)
- Random

User Access Management

- Account authentication on the platform is handled exclusively via encrypted channels, using secure keys and encryption algorithms.
- A RBAC (Role-Based Access Control) approach is implemented to restrict access to authorized users
- We support two-factor authentication, and all sensitive actions require confirmation.

User Account Review (vetting process)

User account reviews are managed through Dawex Admin Console and through a vetting process.

Informations are asked to the user when he is creating his profile, including key mandatory informations :

- Profile completed including professional email – to prevent identity theft
- Company page completed including:
  - Business description
  - Company name
  - Head Office Location for legal requirements
  - Type of organization
  - Website

The orchestrator is doing a manual profile screening. He needs to verify company's and user's identity from different channels / sources.

During this process:

- User has a restricted access
- Only trusted users can access all the platform features (eg: search, conversations, offerings publishing...)
- Only trusted users can be seen on the platform
- Orchestrators can send standard or personalized messages through a support platform like Freshdesk, if connected.

At the end of the process, after the orchestrator validates his profile, the user receives an automatic account validation by email.