# Skillsoft's Cloud Operations Services

# Percipio

# Hosted in the EU

## Revision history

| Date | Version | Description | author |
|---|---|---|---|
| 27/03/2019 | 1.0 | Description of cloud and private cloud operations in the EU | Cloud Operations |
| 07/05/2019 | 1.1 | GDPR and backup/restore updates | Cloud Operations |
| 10/02/2020 | 1.2 | Data protection at rest | Cloud Operations |
| 07/05/2020 | 2.0 | AWS Hosting/Migration and updated document to v.2 | Cloud Operations |
| 09/07/2021 | 2.1 | Annual review and updates for third party vendors | Cloud Operations |
| 29/07/2021 | 3.0 | Moved to v.3 to ensure single up-to-date document | Cloud Operations |

## Introduction

Skillsoft offers Percipio according to the software-as-a-service (SaaS) model. Users access the Percipio software via the web: this simplifies the management of the web application that must be accessible via the Internet worldwide, 24 hours a day, 7 days a week and 365 days a year.

Thanks to the SaaS model, our customers' IT department no longer needs to worry about the following:

- Hardware costs
- Software licensing costs
- Enforcement
- Training of in-house experts for support related to the online training solution.
- Managing application and content upgrades
- Allocation of IT staff to recurring maintenance operations.
- Security management for the application
- Backup/Restore Management
- Increase in support staff.

Skillsoft's cloud operations (CO) department has developed strategies and processes to ensure application performance while maintaining high security standards. Below is a description of these processes and the services of the global cloud operations that Skillsoft provides. For companies limiting the IP addresses accessible in the enterprise, Skillsoft provides a range of IP addresses that must be opened for the Percipio app to work properly. If you want more information about IP address ranges, the sales team in charge of the customer account can provide you with it.

## Confidentiality

As a result of the European Parliament's decision to invalidate the Safe Harbor Privacy Principles on 24 October 2015, Skillsoft is currently offering a Data Processing Agreement (DSA) to its customers.

Skillsoft is committed to protecting your data and complies with the European Data Protection Regulation as enshrined in the applicable laws of a Member State.

## General Data Protection Regulation (GDPR)

Skillsoft has put in place the appropriate technical and organizational measures in compliance with the General Data Protection Regulation (GDPR). Skillsoft's contracts meet the strict requirements for contracts between controllers and processors. In order to meet the new liability requirements to which controllers are subject, Skillsoft maintains written records regarding its data processing activities and has put in place tools to enable controllers to exercise the right to be forgotten. Skillsoft's Data Protection Officers (DPOs) ensure the company's compliance with the GDPR.

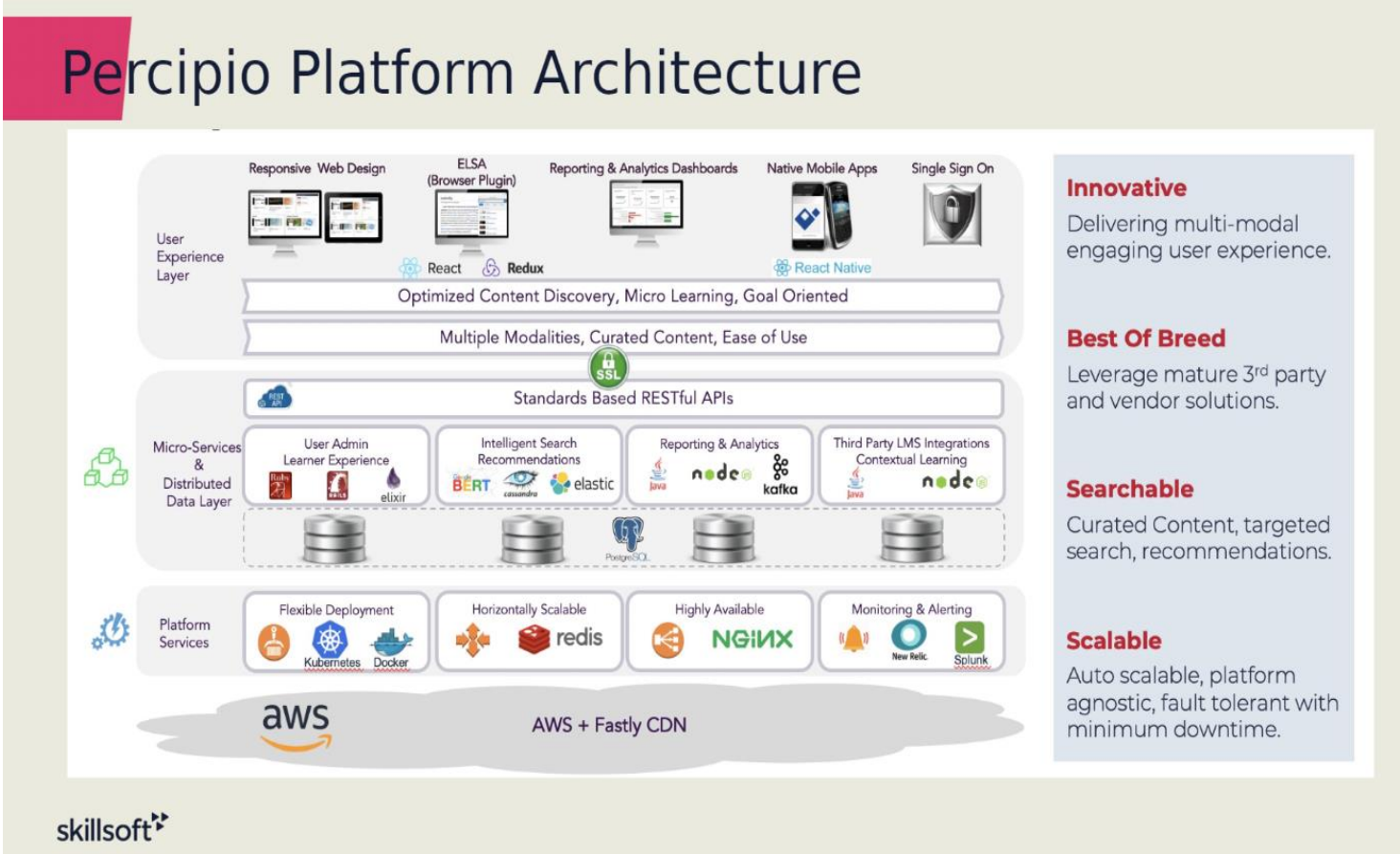
## Description of the Percipio application

Percipio is a web application developed on a microservice architecture. This application uses Amazon Elastic Kubernetes Service (EKS), Docker containers, Kubernetes, Kafka, PostgreSQL databases, and Cassandra databases for analysis and reporting. It uses other technologies that are the best in the microservice architecture. The Percipio application is also based on Java and Ruby. It uses PostgreSQL database to store various configuration settings as well as learner credentials and progress records. Customers are contained separately in the PostgreSQL database under an organization identifier that is unique to each organization.

The Percipio application uses a multi-tenant architecture with unique identifiers. All customers use the same database and schema, but the rows in the table have a unique organization identifier used when retrieving data for an organization. In the same organization, a unique user ID is used, in some cases, to further filter data to that of a unique user.

Unique identifiers are generated with the v4 UUID format (https://en.wikipedia.org/wiki/Universally_unique_identifier) . They are also randomly generated by RFC4122-compliant software libraries(https://tools.ietf.org/html/rfc4122#section-4.1.3i).
There is very little risk that these identifiers can be guessed (https://stackoverflow.com/questions/4878359/what-is-the-probability-of-guessing-matching-a-guid).

## Percipio - application architecture




## Personal data and other user data

The application stores the following user data in its PostgreSQL database:

- first name,
- last name,
- address e-mail,
- activity, such as access to courses, books, and audiobooks,
- time spent on the Canal and Course pages,
- collection-level usage and
- the status of the course.

Users/students can access the app through a web browser on port 443. The courses are launched via JWPlayer HTML5.

## Enhanced Learning Synchronized Assistant (ELSA)

ELSA is an add-on to Percipio that can be installed by the end user as a browser plugin or desktop application on Microsoft Windows. ELSA is optional. Percipio has the same features, with or without ELSA. ELSA provides quick access to Percipio search and content from any web page via the plugin or desktop application. ELSA is currently available in three versions:

1) Plugin Chrome
2) Plugin IE11
3) MS Windows desktop application

ELSA does not store or process any personal data. Once installed, ELSA prompts users for their organization name, that is, company name. Percipio.com. After the organization is validated, users are prompted to enter the same user IDs and passwords that were used to sign in to Percipio. Users are validated by Percipio via the plugin. The plugin gets a unique user token (JWT) saved in the plugin. The token allows users to easily sign in for 90 days. After 90 days, the token expires. Users must then re-enter their login credentials.

All versions of ELSA check at startup to see if a new version is available. The Chrome version automatically updates if a new version is available on Google store. The IE version and desktop application ask users to download and install the new version.

### Load balancing

All products of the current generation are extremely scalable and available thanks to a classic hardware load balancing architecture. All real-time components of the application have horizontal and vertical scalability options. They are also constantly monitored against key performance criteria and evolve according to on-demand needs. Central infrastructure components are implemented using an active-active or active-passive failover model.

### AWS Hosting

Percipio is deployed in Amazon Web Services (AWS). The deployment is done on the AWS Frankfurt platform located in Frankfurt, Germany. Skillsoft uses the "AWS Shared Responsibility Model" described under the following link: https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected

Amazon Web Services (AWS) provides a scalable cloud computing platform designed to deliver high availability and reliability and provides tools that enable you to run a wide range of applications. Protecting the confidentiality, integrity, and availability of your systems and data and gaining and maintaining your trust is of utmost importance to AWS. This document outlines AWS's approach to security, the controls that are performed within the AWS environment, and some of the products and features that AWS offers to customers to achieve your security goals.

https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card

AWS offers various security compliance programs such as **SOC 1/SSAE 16/ISAE 3402 (Formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG and PCI DSS Level 1**

More information about AWS compliance programs is available here:

https://aws.amazon.com/compliance/programs/

## Controlling network devices

### Description of network, routers, switches, and firewalls

Recognizing the critical nature of network and security infrastructures, Skillsoft has invested in the best devices from vendors like Cisco and F5 Networks. These strategic investments underscore our commitment to always provide exceptional services. Network infrastructures are designed to be scalable and fault-resistant in accordance with the many tips that Internet service providers rely on.

An intrusion prevention, detection and firewall system is responsible for perimeter security. This multi-layered, multi-vendor system provides customers with the highest level of protection against service attacks and intrusion attempts. It also gives Skillsoft the flexibility to respond to new threats.

All systems are developed from pre-re-developed and standardized images, based on industry best practices. System images are regularly reviewed to ensure responsiveness to evolving technologies and threats.

Finally, Skillsoft has an annual security audit of its cloud operations environment done by a third party. p

## Management of control programs

### Recovery and restart procedures

For Skillsoft's cloud operations staff to be alerted as soon as possible to any conditions that may affect the services, a comprehensive monitoring infrastructure has been put in place. Clearly defined governances inform the cloud operations engineer of the actions allowed without the need for escalation and give specific details about how the prescribed actions are to be carried out. If a condition appears for which there is no defined procedure, the problem must be notified immediately to the line manager.

### System access restrictions

Only cloud operations staff have privileged access to all public cloud systems to respect the privacy of the data our customers entrust to Skillsoft and to provide the most stable cloud operations environment possible. Under no circumstances is system access granted to any third party outside of cloud operations with the exception of service providers contracted with Skillsoft for professional services or direct support.

### System Documentation

Comprehensive documentation has been written and covers all aspects of system construction, application installation, and product configuration and management. These documents are continuously updated to record the latest strategies and procedures. All versions of the documents are rigorously controlled, and any changes are subject to review and approval by the parties concerned.

### Protection against unauthorized access

Privileged access to Skillsoft’s entire cloud operations entity is strictly controlled and available only to cloud operations staff. Under no circumstances is access granted to any personnel other than the CO team and this concerns all systems. Strict and consistently enforced protocols ensure that all access is suspended immediately after any task affecting cloud operations staff.

## Data protection procedures

### Data protection at rest

Data encryption at rest meets several industry regulatory compliance requirements, including FIPS 140-2 Level 2 (U.S.) and PCI-DSS v2.0 section 3.4.

### Overall backup strategy

System backups are not intended for the following purposes:

- Data archiving
- Protect against scenarios that are not directly related to data loss

Data backup is performed with AWS Backup is configured in EU-Central-1 region and is in multiple availability zones. To protect the confidentiality, AWS Backup encrypts all backups in the AWS Vault using Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with 256-bit keys.

### Backup schedule

The systems are backed up according to the following schedule:

| Information Class | Frequency/type | Disk-based retention | Off-site storage | comment |
|---|---|---|---|---|
| Percipio relational databases | Daily | 90 days | N/A | **Primarily client application data** |
| | Weekly | 90 days | 90 days | |

### Verifying backups

On a daily basis, the logged information generated from each backup job is reviewed by the backup administrator for the following purposes:

- Find and fix errors.
- Monitor the duration of the backup task.
- Optimize backup performance, if any.
- IT will identify issues and take corrective action to reduce the risks associated with failed backups.
- Random test restores will be performed once a week to verify the success of backups.

Cloud Operations will keep records of log review and test restores to demonstrate compliance with this policy for audit purposes.

## Data recovery

In the event of a catastrophic system failure, the data backed up off-site will be made available to users within 3 working days if the destroyed equipment has been replaced in the meantime.

In the event of a non-catastrophic system failure or user error, the data backed up on site will be made available to users within 1 working day. Customer data is restored with the help of the software engineering team via SOW engagement with the customer.

## Restore requests

In case of accidental deletion or alteration of information, restore requests should be made through Skillsoft Technical Support. Skillsoft Technical Support then opens a ticket assigning the restore request to the Cloud Operations - Support team. The recovery is performed by the cloud operations and software engineering teams through an SOW engagement with the customer.

## Incident Management

All Public Cloud Systems are broadly monitored f or availability from multiple physical locations. Visual and auditory alerts are generated within 1 minute of a service fault and email alerts generated within 2 minutes. Immediate action is undertaken to restore impaired services. All service affecting events are logged and analyzed by both SW Engineering and Cloud Operations resources to ensure that the event is fully understood, and steps are taken to mitigate future exposure to the event.

### Slow application performance

In addition to tracking the availability of public cloud services, comprehensive measures are put in place to protect against temporary or minor application latency. A redundant and geographically dispersed monitoring infrastructure provides visual, audio, and email notifications for all monitoring events that exceed the allowed time. Transactional monitors simulate user activity to give a reliable indicator of the overall performance of the system, from the perspective of the end user.

### Security breach management

In the event of a compromise of public cloud systems or services, Skillsoft's cloud operations team will immediately implement an environment lock to block all incoming and outgoing communications from the data center environment. A privileged remote connection will be maintained for the network and security team of cloud operations to ensure that the problem is resolved as quickly as possible. Every effort should be made to close the breach, re-stabilize systems, and limit the exposure of customer data. A detailed analysis of events should be carried out as soon as possible and shared with our customers, if necessary.

### Client Communication Process

Skillsoft's technical support team and learning consultants communicate with the customer. Root cause analyses are available if requested by the client.

## Recovering systems from an event affecting services

### Hardware failure

Many systems in the public cloud environment have a balanced hardware load, and the loss of a system does not affect services. In AWS, Percipio is deployed in three Availability Zones, ensuring high availability of the application. When hardware redundancy is not provided, fully configured standby systems are available for immediate use. Recovery policies and procedures are documented to enable a rapid response to these incidents and to restore services quickly and efficiently.

### Application failure

Application failures are detected through continuous system monitoring and the resolution time is less than 10 minutes. Remediation procedures are documented, and all application failures are sent to the software engineering team for review.

### Network loss

A fully redundant network infrastructure allows Skillsoft to provide highly available infrastructure. Redundancy is built into all levels, including the Internet connection. Failover tests are performed regularly to ensure that configuration changes and patch installation do not affect the reliability of fault tolerance.

### Impaired application performance (i.e., latency)

Application latency is detected through continuous system monitoring and the resolution time is less than 10 minutes. Remediation procedures are documented, and all application latency events are sent to the software engineering team for review.

### Secure recovery

In the unlikely event that a third party is to be involved in the recovery of a system, such involvement will be subject to official contractual terms, reviewed and clarified by Skillsoft's legal department prior to the start of the engagement. Third parties working directly with sensitive information are subject to and bound by confidentiality agreements.

### Disaster recovery

Percipio's infrastructure is deployed in AWS in three Availability Zones, ensuring high availability and full redundancy. In the event of a total loss of the AWS Frankfurt site, Skillsoft has put in place a disaster recovery plan to facilitate the fastest possible recovery. Skillsoft's cloud operations team has developed a disaster recovery plan detailing the responsible parties, the communication protocol, and the steps to take in the event of a disaster. The Skillsoft disaster recovery plan is built on infrastructure as code (IaC) and the continuous integration/continuous delivery (CI/CD) application deployment pipeline. In the event of a disaster, Skillsoft deploys a new instance of the Percipio application in a different AWS Region within hours.

Skillsoft conducts an annual disaster recovery test involving SaaS infrastructure reconstruction, application deployment, and data recovery. The results of the annual disaster recovery test are transmitted to customers upon request.

### Conformance to standard architecture

All production systems are deployed according to security best practices. All systems are designed from a set of infrastructure-as-code (IaC)scripts that follow CIS security standards.

The latest OEM updates and CIS configurations are loaded on all operating systems. This is enabled by the use of automation scripts and IaC.

All systems are strengthened to NIST 800-53 Rev.4 standards through the deployment of our Prisma Cloud product designed to apply the Federal Risk and Authorization Program (FedRAMP)based on NIST 800-53. Here are some of the restrictions to follow:

- Complex naming and password standards
- User access control settings
- Redirecting to disabled accounts.

All systems are checked to ensure that unnecessary or potentially exploitable services are configured to be disabled when powered on.

### Change Management – Roles and Responsibilities

Technology managers have a defined framework of approvals and act as the approval authority for settings within their area of competence. Changes with a broader impact are sent for review with relevant stakeholders. The stakeholders reviewing change requests are as follows:

- Network and Security Manager
- Application Services Manager
- Database Manager
- Infrastructure Manager
- Sr. Director, Cloud Operations
- VP, Cloud Operations

The Sr. Director of Cloud Operations and the VP of Global Cloud Operations have a final veto over all change requests.

### Managing system configurations

Adjustments made to system images or configurations are strictly controlled through a multi-party review and approval process involving people from management, network and security teams, system analysts, and system engineers. The documentation is updated immediately to reflect the reconfiguration of the system.

### Change process, testing, and approval process

Requests for changes are sent by the initiating party to the appropriate technology manager for preliminary study. The manager in charge then seeks advice from the general manager of cloud operations to determine the scope of the change and establish an approval cycle. When possible, changes are verified through a preliminary implementation in a staging environment. In some cases, they require and receive a load test performed by a dedicated automation team.

To ensure the quality of work, changes to the environment are continuously checked by cloud operations managers.

### Configuration and security specifications

Skillsoft applies a very restrictive policy compared to access controls and policies for network devices. The rules of intrusion detection and prevention systems and firewalls are continuously reviewed and monitored for suspicious events. Device configuration is standardized and well documented. Adjustments to configurations and policies are reflected in the documentation associated with the system or device.

### Configuration control

If a network engineer changes the settings of a device, those changes require the approval of the network manager. In some cases, it will also require the approval of the general manager of cloud operations. Any adjustment to an aspect of the host system configuration requires review and approval from the primary system architect and, in some cases, the general manager of cloud operations. Settings or changes to the configuration are reflected in the documentation associated with the system or device.

## Password, account, and security management

### Password management

The use of generic usernames and passwords is prohibited. Administrators receive individual login information and can manage their own passwords based on the password policy applied to the domain.

### Password expiration

User account passwords expire every 60 days. Passwords must meet strict complexity requirements required by DoD and federal standards. They must contain at least 14 characters and must not be reused. Password expiration is enforced through Group Policy Objects (GPOs).

### Length and complexity of passwords

Passwords must meet complexity requirements, including a minimum number of characters restriction, and non-alphanumeric character and mixed case requirements. Group Policy objects (GPOs) manage the length and complexity of passwords.

### Password protection

Efforts are being made to limit the communication of passwords to verbal channels. Passwords are provided on a need-to-know basis. When it is not possible to communicate passwords verbally, the username and password combinations are communicated separately and only to the persons concerned. Sharing user account passwords is strictly prohibited.

### Description of physical security

Physical security is provided by AWS as described here:

https://aws.amazon.com/security/?nc=sn&loc=0

### Environment – Description of security

A multi-layered perimeter defense infrastructure provides the best possible protection against unauthorized access or malicious activity. Measures include a highly restrictive firewall strategy, intrusion prevention and detection systems with pattern matching and networking, and a comprehensive and up-to-date anti-virus infrastructure.

### Systems – Security Description

All systems are built from pre-re-built images and standardized according to industry best practices and in accordance with Skillsoft's specific software and system configurations. Routine patch management is controlled by centralized patch management software to ensure consistent and up-to-date posture.

### Personnel - Safety Management

Employee-related actions (recruitment, firing, suspension, etc.) are coordinated between human resources and IT to respond immediately to changes in the status of all cloud operations staff. In addition, cloud operations management will be notified of all Skillsoft employee departures in the event that special measures need to be taken to protect themselves from the actions of former employees with exclusive knowledge or understanding of the

Skillsoft.

### Encryption of employees' mobile devices and laptops

Skillsoft uses file-level encryption policy exploitation software that consistently encrypts static and in-transit files according to risk levels, as defined in the information policy. The risk factor is determined based on the content, context, and type of data. All customer data is considered sensitive information and treated as such. For data that can potentially be copied to ancillary devices such as USB flash drives, CDs, or DVDs, IT has deployed enterprise information protection software that will detect and prevent Skillsoft employees from transferring sensitive customer information to mobile devices (i.e., CDRW/DVD-RW, USB flash drives, hard drives, handhelds, cameras, mobile phones).

### Accessing the public cloud environment

Access and communications to the public cloud environment are secured with client or site-to-site encryption. Site-to-site tunnels provide access to the service or port and are limited to Skillsoft's public cloud subnets. Remote access authentication is tightly integrated with existing domain security and provides a central point of administration. Remote access is limited to cloud operations staff. This strategy is universal and comprehensive because it includes administration, backups, and so on. Under no circumstances are software developers, training specialists, application engineers, enterprise IT, or account managers granted privileged access.

### Remote access to the public cloud environment

Only cloud operations engineers have access to public cloud systems. Access to the various subsystems is divided according to roles and responsibilities. Each engineer has a unique user ID and password and is managed through an access control list that gives access only to systems that are the engineer's responsibility. Because most cloud operations engineers require 24/7 access to the public cloud environment, they have laptops. The latter only include the operating system and VPN software. To access the public cloud environment, cloud operations engineers connect remotely from their laptop to their desktop located on the Skillsoft site that includes the VPN software that provides connectivity to the public cloud environment. Access is authenticated through RSA security two-factor authentication. App passwords are changed every 30 days or when a cloud operations employee leaves their position.

### Third-party annual penetration test

In an ongoing effort to improve the security of the public cloud environment, Skillsoft contracts with third-party security organizations to conduct an annual and comprehensive vulnerability assessment and penetration testing for the public cloud environment. These assessments examine firewall policies, intrusion detection and prevention

policies, system patch levels, and vulnerabilities to known software exploits and brute force attacks. The results of the assessment are shared with clients upon request.

### Disclosure of platforms, technologies, and suppliers

To counter the collection of information, Skillsoft will not disclose to any customer, under any conditions, the make, model or manufacturer of any network or security device used in the public cloud environment. This includes disclosing information about the following:

- Firewall settings/software/hardware
- Intrusion detection system settings/software/hardware
- Network penetration testing
- Vulnerability analysis
- Network topology
- Internal IP schema
- Operating system configuration and security settings
- Publishers and version of the software used

### Planned system maintenance

Description of the planned system maintenance schedule

Routine maintenance window operations (when these affect services) are limited to two hours per week. Special maintenance windows requesting longer may be requested from time to time. 14 days' notice will be given for these special maintenances.

Activities performed during these maintenance windows may include, but are not limited to, hardware maintenance and replacement, system patch updates, infrastructure improvements, and new versions of Skillsoft software.

### Emergency maintenance

Skillsoft reserves the right to perform unplanned maintenance activities where delaying such maintenance may pose significant risks to the availability and/or security of the services provided. Every effort is made to coordinate these unplanned maintenance activities with customers in advance and perform them at a time when it has the least possible impact as soon as the conditions are right.

### Maintenance schedule

All planned maintenance activities are coordinated and scheduled in advance in windows with defined boundaries. All activities are critically reviewed to ensure timing and that activities do not overlap.

### Security Management

Only cloud operations staff can perform maintenance activities and access is strictly controlled by multi-party security measures.

### Wireless in the office

Skillsoft provides its employees with wireless access to Skillsoft sites. The wireless service uses WPA2 Enterprise encryption to access Skillsoft's network environments. Wireless access requires single sign-on. Access logs are saved in a central location and are reviewed for failed access attempts. Unauthorized wireless network detection is performed continuously to prevent malicious activity.

Guest Wireless traffic is secured, isolated, and managed with firewall policies. Allowed ports are limited to HTTP (80), HTTPS (443), and VPN (TCP/UDP) ports.

Wireless access is separate with its own Ethernet interface on Skillsoft's firewall and does not have access to internal corporate resources. To access corporate resources, you must use the VPN.

## Production Code – Change Control

### Product development

Product-related software development is done by Skillsoft software engineers including Scrum Masters, DevOps managers, squad, architects, software engineers, and database developers. The software engineering department is divided into teams according to the different areas of expertise required by the various products and their respective software development lifecycle.

### Quality assurance process

A dedicated quality assurance team ensures that all software made available to customers is of the highest possible quality and has excellent performance.  This team has a final veto right on all software packages going on production systems.

### Qualification process

A comprehensive and in-depth test matrix is applied to the Percipio sprint testing feature and their support for all the technologies listed in the product compatibility matrix. New features are thoroughly tested, and existing features are also tested to prevent regressions.

### Putting software into production

Once officially handed over to Skillsoft's cloud operations services, the software package is reviewed by these services and deployed according to a CI/CD methodology. The software is initially released in an integration/quality control environment for testing and then it is deployed in a simulation environment. After verification in the pre-production environment, the software package is deployed to production. The micro-services architecture makes it possible to deploy software quickly and transparently.

### Hot fixes and version management

Continuous software improvements sometimes make patches available in Skillsoft's software product lines. All software releases, minor and major, including patches have a single version and this version is visible to all operators. The release strategy for patch deployments copies the strategy of the software release process described above, except those deployments are made during the production period with no downtime for users or need for maintenance.

## Software Engineering – Change Control

### Software engineering process

After the functional specifications are finalized, the product software architect and a Cloud Operations DevOps architect assigned to each team determine the overall software architecture. In some cases, architectural considerations may cause functional specifications to change. These changes will be served on the parties involved and will then be determined by a final functional specification and architecture. This architecture is documented and sent to the DevOps manager for review, project scoping, and resource allocation.

### Accessing source code

Access to all software and its versions is strictly controlled with GitHub, a software source control solution. Access to the source code is provided as needed and is restricted to Skillsoft's software engineering team.

### Software release process

Only the DevOps manager in charge of the product line can send the software from software engineering to quality assurance. Only the assigned quality control engineer has the authority to send the software from the quality assurance systems to the final qualification systems, provided that the software meets the predefined acceptance criteria for publication. Only the assigned quality control engineer (with the approval of the quality control manager) has the authority to send the final qualification software to Skillsoft's cloud operations departments, provided that the software meets the predefined acceptance criteria for general release.

## Patch Management – Process Description

### Software

A centralized patch management software suite ensures a consistent security posture across all managed systems. Skillsoft's cloud operations services have the means to actively respond to emerging threats. All available hotfixes are reviewed by cloud operations and deployed on a schedule defined by associated risks and FedRAMP/NIST800-53 requirements based on severity levels.

### Network and security devices

A dedicated team of network and security professionals continually review new patches and enhancements available for network and security devices. Signature batches for intrusion detection and prevention devices are downloaded daily and reviewed for implementation on an ongoing basis.

## Account controls

### Access to systems

Access to all public cloud systems is limited to Skillsoft's cloud operations services staff. In some cases, vendor-approved technicians are granted access to systems during hardware failures or the involvement of professional services.

### Access Management

Control of access to systems and sites is controlled by a small group of employees from Skillsoft's cloud operations departments. Access to systems is granted at a level corresponding to the person's position. Access to network and security devices is limited to the network management team, the general manager of cloud operations, and the

senior cloud operations architect. Access to the public cloud site is managed in collaboration with the colocation service provider through an official access control list. Managing this list is limited to cloud operations managers.

## Perimeter defenses

### Firewall

Skillsoft has selected the best software and hardware solutions from industry leaders. Firewalls use a very restrictive policy that filters only known traffic and required access to ports. Access to firewall systems is strictly controlled, and adjustments to firewall policies are subject to management approval prior to implementation.

### Intrusion Detection and Prevention

Through event correlation and granular search for predetermined signatures, Skillsoft provides comprehensive protection against known vulnerabilities and zero-day defense against new threats. Intrusion detection and prevention system signatures are continuously reviewed and updated.

### Intrusion Prevention System

The active and redundant implementation of an intrusion prevention system is an effective and proven protection against brute force and denial-of-service attacks. The settings made to the configuration of the intrusion prevention system are reviewed on an ongoing basis.

### Connection to the public Internet

The Percipio SaaS application is available on the public Internet. However, measures have been put in place to prevent unauthorized access to the SaaS application. This includes user-only and password-only access to your Percipio site and the ability for customers to manage their own application account according to their own policy through the learning administrator interface. The customer can choose to implement single sign-on (SSO) to ensure better protection and easy use for their users.

## Audit trail protection

### Managing log files

Intense system logging captures all events related to system access, including the use of privileged user rights, service starts/stops, connections, and disconnections. The network intelligence and firewall log files capture all access failure events and suspicious activity as defined in our intrusion detection and prevention infrastructure. Comprehensive system logging and storage management/SANS logging log non-standard events. The application-detailed log files record all unusual application events in addition to the web server detailed log files. Skillsoft's cloud operations services retain all access, security, and system log files for an indefinite period of time. All event logs are

archived daily to centralized disk storage for easy access. This centralized repository is then saved to tape and maintained in accordance with our tape retention policies as defined in this document. Access to log files is limited to cloud operations staff, except for web and application error log files that are shared, as needed, with Skillsoft's software engineering team.

### Reporting a security breach to customers

Skillsoft follows a strict incident management process, approved by its federal customers and customers associated with the U.S. Department of Defense. If a security incident occurs: Information about the incident will be provided by Skillsoft Technical Support to the customer's primary contact. The first phase of contact will be to indicate that there has been a problem and the status of the correction. The following updates will be sent during the remediation process. After the incident is resolved, the cloud operations team performs a root cause analysis. Results will be provided to clients upon request.

## Data protection and retention

### Customer Data – Storage

All customer data is stored within the AWS EU-Central-1 region that provides maximum level of data protection and integrity. They are stored in relational databases, the Kafka mail queue, and the Cassandra reporting database without any data present on web systems accessible on the Internet. Access to this data is limited to cloud operations staff. Customer data is duplicated to the EU-West-1 region which has been selected as the Skillsoft disaster recovery site. They are backed up daily and securely replicated to the EU-West-1 region. In some cases, customer data is duplicated in a controlled and secure lab environment to troubleshoot problems or for capacity planning exercises directly related to the customer. Duplicate data used in this environment is subject to a database cleanup that removes all personal information from the data before it is used in the lab. To ensure data privacy and security, the cleansing process is performed in the public cloud environment before the data is exported to the lab. AWS backup is configured in US-East-1 region and is in multiple availability zones. To protect the confidentiality, AWS Backup encrypts all backups in the AWS Vault using Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with 256-bit keys.

### Customer Data – Protection

Access to customer database systems and databases is limited to cloud operations staff. Privileged remote access is done exclusively via an encrypted and secure channel.

### Storing passwords

Customer user account passwords are hashed (and salted) securely with bcrypt

### Access methods for the end user

All access to the data is via publicly accessible and password-protected web systems.  Direct access to data is not allowed.

## Personnel management

### Roles and responsibilities

Skillsoft has built an unparalleled team of IT professionals in an organizational structure that clearly articulates the hierarchy of responsibilities, oversight, and ownership without sacrificing the agility and responsiveness required by customers.  The Cloud Operations Services team is typically divided into the following teams:

- Network and security
- Systems Architects
- System and Application Administrators
- Database and data store administrators
- Product support and customer provisioning
- Program management

### Employee background checks

Skillsoft is aware of the sensitivity of the data processed by employees in charge of cloud operations. To ensure the best security awareness and due diligence, Skillsoft conducts background checks (operation subject to applicable local regulations) of potential employees for predetermined positions that require access to customer data. Skillsoft also checks the references provided by candidates during the application process. In addition, all employees responsible for cloud operations must read and sign a privacy and security policy detailing roles and responsibilities, escalation procedures, and the overall code of conduct for the cloud operations organization. All employees responsible for cloud operations must sign this policy annually to signify that they understand it and are committed to following its guidelines.

### Dedicated Cloud Operations Team

Skillsoft recognizes the unique challenges that service providers face and the specialized skills required to manage and grow cloud infrastructures effectively.  To meet these challenges, Skillsoft has therefore invested heavily in a dedicated cloud operations services team that has the sole mission of ensuring the best possible experience for our customers.

### Description of the expert opinions

Skillsoft's cloud operations services are made up of experienced and competent professionals. In addition to their years of experience, many cloud operations services employees also have certifications from the following industry authorities:

- AWS Cloud Practitioner
- AWS Architect
- Certified AWS Administrator
- Cisco
- RedHat
- DevOps
- CheckPoint
- EMC
- GIAC
- VMWare

Currently, Skillsoft's cloud operations department has 54+ AWS certifications

### Staff training

As technologies continue to evolve, Skillsoft recognizes the critical role that training plays in successful service delivery. To ensure that Skillsoft makes the best resources available to its customers, Skillsoft spends a lot of time training on all products in the public cloud infrastructure. A formal training program has been developed for Skillsoft's proprietary products and general privacy and security courses are assigned to employees annually.

## Capacity management

Skillsoft takes capacity management very seriously to ensure that the necessary resources are available for new products, new customers, customer upgrades, and system replacement. The Percipio application is subjected to a load test that validates the hardware requirements and ensures that the deployment configuration meets the demand of our customers.

The Percipio application is deployed according to a predefined deployment plan that describes exactly how Percipio shares the hardware and how that hardware is configured. The required infrastructure is pre-designed and configured from datasheets and preconfigured images, scripted through the framework as code, and created by system architects. The existing public cloud environment is continuously monitored for resource usage. As

emergencies can occur, the cloud operations team continuously monitors system usage to increase capacity based on requests. AWS enables the cloud operations team to use capacity elasticity based on user demands.

## Third Party Service Providers

### Fastly

Skillsoft uses Fastly services to stream videos to Percipio. https://www.fastly.com

### Accredible

Certificates and badges for students Accredible receives the student's first and last name and information about the progress of their training in order to create a badge in the student's name. https://www.accredible.com/

### Practice Labs

Skillsoft uses Practice Labs to provide practice labs to Percipio users. https://skills.practice-labs.com/

skillsoft

# Appendix B

## Percipio Network Topology

AWS Pecipio Network Infrastructure | November 2, 2020

AWS Pecipio Network Infrastructure .vsdx
Maintained By SkillSoft Network Services
Last updated by Chung Ling Jee
skillsoft