skillsoft

Skillsoft Cloud Operations (CO) Services

Percipio

Hosted in the US

Revision History

Date	Version	Description	Author
7/15/2017	1.0	Description of the Cloud Operations and the Private Cloud	Cloud Ops.
5/7/2019	1.1	Updates to backup/Restore	Cloud Ops.
2/10/2020	1.2	Data Protection at rest	Cloud Ops.
5/6/2020	1.3	AWS Migration/Hosting	Cloud Ops
7/7/2021	1.4	Annual review and updates	Cloud Ops

Table of Contents

Introduction

Skillsoft offers Percipio via the Software as a Service (SaaS) Model. Percipio is accessible via the web alleviating the complexities involved in managing a web application that must be accessible over the Internet worldwide, 24/7/365.

The SaaS model our customers' IT Management no longer needs to worry about:

- Hardware costs
- Software Licensing costs
- Application monitoring
- Creation of in-house expertise to support the eLearning solution
- Dealing with application and content upgrades
- Allocation of IT staffing to perform recurring maintenance
- Security management for the application
- Backup/Restore management
- Augmentation of helpdesk staffing

Skillsoft Cloud Operations (CO) have developed policies and processes to ensure application performance while maintaining the highest security standards. Following, is the description of these processes and the overall Cloud Operations services provided by Skillsoft. For companies that are restricting the IP addresses that can be accessed from within the company, Skillsoft will provide a range of IP addresses that will have to be open for the Percipio application to work properly. More information on the IP ranges can be provided by the Account Team that supports the customer account.

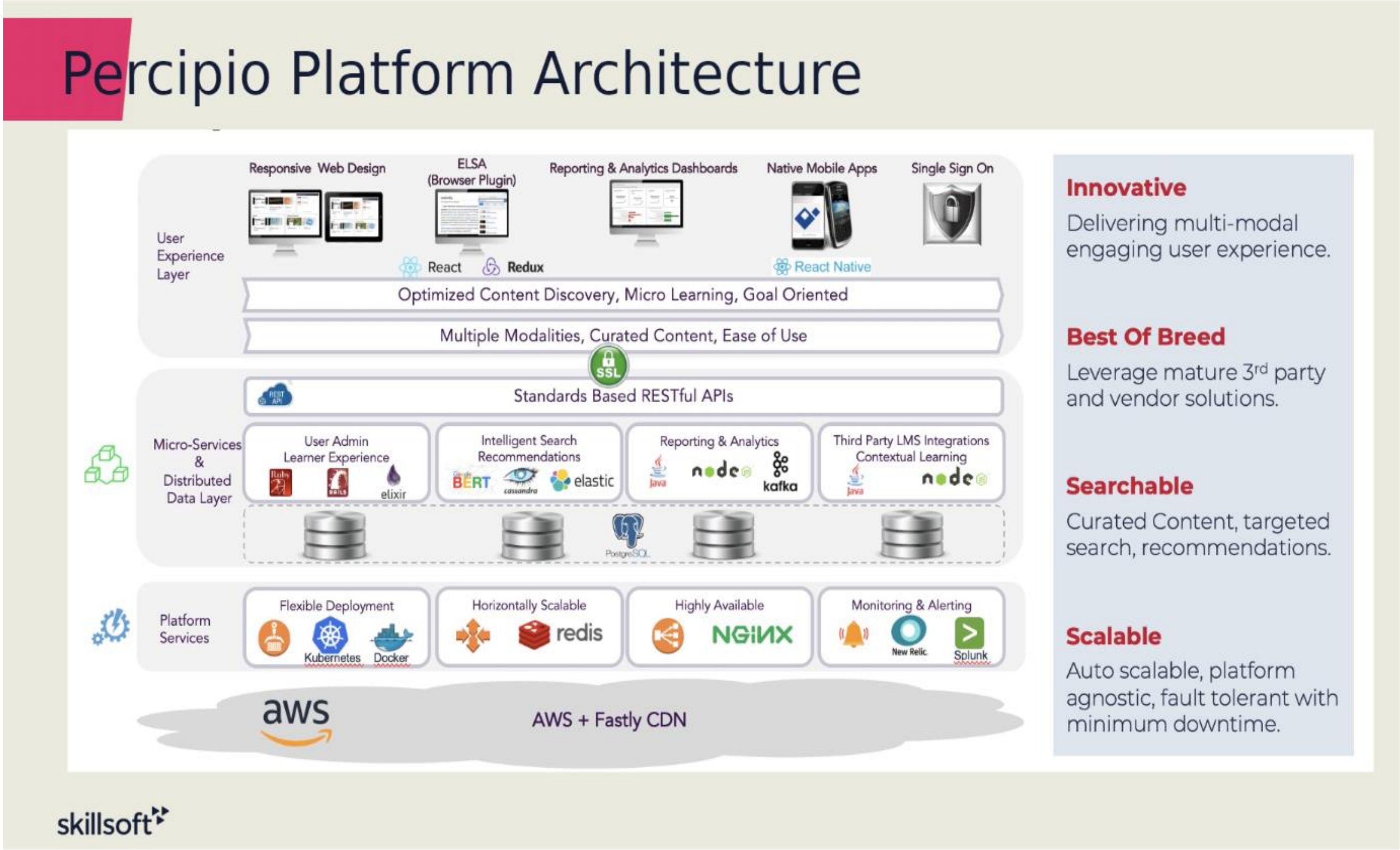
Percipio Application Description

Percipio is a web application developed on Micro Services architecture. The application uses Amazon Elastic Kubernetes Service (EKS), Docker containers, Kafka, Kubernetes, PostgreSQL databases, and Cassandra database for reporting and analytics and other technologies that are popular in the Micro Services Architecture. The Percipio application uses Java and Ruby at its core. The application uses the PostgreSQL database to store various configuration parameters as well as student credentials and student progress records. Customers are segregated in the PostgreSQL database by an organization key unique to each organization.

Percipio application uses multi-tenancy by unique identifier. All Customers use the same database and schema, but the rows of the table have a unique OrgID which is used in retrieving data for an organization. Within an organization there is a unique UserID which is used (in certain cases) to further filter the data to a single user.)

The unique identifiers are generated using the UUID v4 format (https://en.wikipedia.org/wiki/Universally_unique_identifier) – These identifier are randomly generated by software libraries complying with RFC4122 (https://tools.ietf.org/html/rfc4122#section-4.1.3).
The chances of guessing one of them is next to zero (https://stackoverflow.com/questions/4878359/what-is-the-probability-of-guessing-matching-a-guid)

Percipio - application architecture



Percipio Platform Architecture

User Experience Layer

Responsive Web Design

ELSA (Browser Plugin)

Reporting & Analytics Dashboards

Native Mobile Apps

Single Sign On

React Redux

React Native

Optimized Content Discovery, Micro Learning, Goal Oriented

Multiple Modalities, Curated Content, Ease of Use

SSL

Micro-Services & Distributed Data Layer

Standards Based RESTful APIs

User Admin Learner Experience

Intelligent Search Recommendations

Reporting & Analytics

Third Party LMS Integrations Contextual Learning

Ruby Rails elixir

BERT cassandra elastic

java node kafka

java node

PostgreSQL

Platform Services

Flexible Deployment

Kubernetes Docker

Horizontally Scalable

redis

Highly Available

NGINX

Monitoring & Alerting

New Relic Splunk

aws

AWS + Fastly CDN

Innovative

Delivering multi-modal engaging user experience.

Best Of Breed

Leverage mature 3rd party and vendor solutions.

Searchable

Curated Content, targeted search, recommendations.

Scalable

Auto scalable, platform agnostic, fault tolerant with minimum downtime.

skillsoft

PII and other user data

The application stores in its SQL database user data:

- First Name,
- Last Name
- email address.
- Activity, such as access to courses, books, audiobooks
- Time spent on Channel and Course Pages
- Collection level consumption
- Assignment status

For users/learners, the application is accessible via a Web browser on port 443. Courses launch via the HTML5 JWPlayer.

Enhanced Learning Synchronized Assistant (ELSA)

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

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

ELSA does not store or process user Personal Identifiable Information (PII). Once installed ELSA will prompt the users for their organization name i.e., companyname.Percipio.com. Once the organization is validated successfully the users will be prompted for the same user ID and password used to login into Percipio. The user is validated by Percipio via the plugin. The plugin will obtain a user unique token (JWT), which is stored in the plugin. The token will offer user's seamless login for 90 days. After 90 days the token expires. The user must re-enter their credentials.

All versions of ELSA will check upon launch if a new version is available. The Chrome version will auto-update if a new version si available in Google store. The IE and desktop application will prompt the user to download and install the new version.

Load Balancing

All current generation products achieve maximum scalability and service availability through a classic hardware load-balanced architecture. All real-time application-level components provide both horizontal and vertical scalability options and are constantly monitored against key performance criteria and are appropriately scaled on demand.
Core infrastructure components are implemented in either an active-active, or active-passive failover model.

AWS Hosting

Percipio is deployed in Amazon Web Services (AWS). The deployment is on the AWS east platform located in Virginia, U.S. Skillsoft's uses the "AWS Shared Responsibility Model" described at the following link:

https://aws.amazon.com/compliance/shared-responsibility-model/?ref=wellarchitected

Amazon Web Services (AWS) delivers a scalable cloud computing platform designed for high availability and dependability, providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is of the utmost importance to AWS, as is maintaining your trust and confidence. This document is intended to introduce AWS's approach to security, including the controls in the AWS environment and some of the products and features that AWS makes available to customers to meet your security objectives.

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

AWS offers a variety of security compliance programs including **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**

Additional information regarding AWS compliance programs can be found at:

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

Network Device Control

Description of the network, routers, switches, firewalls

Recognizing the critical nature of network and security infrastructures Skillsoft has made strategic investments in best-of -breed devices from vendors such as Cisco and F5 Networks reflecting our ongoing commitment to world-class service provision. Network infrastructures are built for scalability and fault resilience following many of the guidance's used by Internet Service providers.

Perimeter security is provided through a robust Firewall and Intrusion Detection and Prevention system. This multi-vendor, multi-layer system affords customers the greatest degree of protection from Denial-of-Service attacks and intrusion attempts while positioning Skillsoft to respond with agility to emergent threats.

All systems are built from standardized, pre-hardened images employing industry best-practices. System images are routinely reviewed to ensure responsiveness to a changing technology and threat landscape.

As a final measure Skillsoft conducts an annual, third-party security audit of our Cloud Operations environment. Skillsoft has enjoyed a very favorable assessment history with no high-risk vulnerabilities found during any assessments.

Control Program Management

Restart and recovery procedures

A comprehensive monitoring infrastructure ensures that Skillsoft Cloud Operations personnel are alerted at the earliest opportunity of service affecting conditions. Clearly articulated governances inform the assigned Cloud Operations Engineer what actions are permitted without escalation and specific details on how prescribed actions should be undertaken. In the event that a condition arises f or which there is no defined procedure, the issue is escalated to a manger immediately.

Restriction on system access

Respecting the confidential nature of the data entrusted to Skillsoft by our customers and in an effort to provide the most stable Cloud Operations environment possible, privileged access to all Public Cloud systems is restricted to Cloud Operations personnel only. Under no condition is system access granted to any party outside of Cloud Operations with the exception of service providers under a direct support or professional services contract with Skillsoft.

System documentation

Extensive documentation has been created covering all aspects of system construction, application installation and product configuration and management. These documents are constantly updated to reflect the most current policies and procedures. All documents remain under strict version control and any changes are subject to multi-party review and approval.

Protection from unauthorized access

Privileged access to all Skillsoft Cloud Operations entity is strictly controlled and available only to Cloud Operations personnel. Under no circumstance is access granted to non-CO personnel to any system. Strict and consistently enforced protocols ensure that all access is immediately suspended following any job action affecting Cloud Operations personnel.

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- v2.0 section 3.4. DSS

Overall backup strategy

System backups are not intended for the following purposes:

- Data Archival
- Protect against scenarios not directly related to the loss of data

Data backup is performed with AWS Backup which 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.

Backup Schedule

Systems will be backed up according to the schedule below:

Information Class	Frequency/Type	On Disk Retention	Offsite Retention	Comment
Percipio Relational Databases	Daily	90 Days	N/A	**Predominantly customer application data**
	Weekly	90 Days	90 Days	

Backup Media Retirement

Media will be retired and disposed of as described in the Skillsoft Digital Asset Destruction Policy.

Prior to retirement and disposal, Global Cloud Operations will ensure that:

- The media no longer contains active backup images
- The media’s current or former contents cannot be read or recovered by an unauthorized party.

Backup Verification

Daily, logged information generated from each backup job will be reviewed by the backup administrator for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimize backup performance where possible.
- IT will identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores will be done once a week in order to verify that backups have been successful

Cloud Operations will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

Data Recovery

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

In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day. Software Engineering will be involved in the restoration process of customer data via a SOW engagement.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration will be made via Skillsoft Tech Support. A ticket will be opened by Skillsoft Tech Support assigning the restoration request to Global Cloud

Operations - Hosting Support. The Restoration will be performed by Cloud Operations and Software Engineering via a SOW 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.

Slowness in Applications Performance

In addition to tracking the availability of the Public Cloud services, comprehensive measures are in place to protect against subtle or transient application latency. A redundant and geographically dispersed monitoring infrastructure provides visual, auditory and email notification f or any monitoring event that surpasses the allowable time limit. The transactional monitors emulate user activity and provide a reliable indicator of general end-user system performance.

Security Breach Management

If the Public Cloud systems or services are compromised Skillsoft Cloud Operations would immediately implement an environment lock-down blocking all inbound and outbound communication from the datacenter environment. Privileged remote connectivity would be maintained for Cloud Operations Security and Network Personnel to ensure the timeliest resolution of the issue. Every effort would be taken to close the breach, re-stabilize the systems and limit exposure of customer data. A detailed post-mortem of the events would be conducted at the earliest opportunity and shared with our customers as appropriate.

Process for communicating back to customers

Communications to the customer are affected through Skillsoft Tech Support and Learning Consultants with root cause analyses available to customers upon request.

Systems Recovery from a Service Affecting Event

Hardware Failure

Many systems in the Public Cloud Environment are hardware load balanced and the loss of a system is not service affecting. In AWS Percipio is deployed in three Availability Zones ensuring application high availability. In cases where hardware redundancy is not provided, fully configured, hot-standby systems are available for immediate use. Recovery policies and procedures are documented to enable quick response to such incidents restoring services quickly and efficiently.

Application Malfunction

Application faults are detected through continuous system monitoring and mean time to resolution in generally less than 10 minutes. Procedures for corrective actions are documented and all application faults are escalated to SW Engineering for investigation.

Network Loss

A fully redundant network infrastructure enables Skillsoft to provide the most highly available infrastructure possible. Redundancy is provided at all levels including the Internet connection. Failover tests are conducted on a regular basis to ensure that configuration modifications and patch installations do not affect the reliability of our fault tolerance.

Impaired Application Performance (i.e., latency)

Application latency is detected through continuous system monitoring and mean time to resolution is generally less than 10 minutes. Procedures for corrective actions are documented and all application latency events are escalated to SW Engineering for investigation.

Trusted Recovery

In the unlikely event that a third party needs to be involved in a system recovery, the third-party engagement will be subject to formal contract terms which are reviewed and refined by the Skillsoft legal team before engagement. Third parties directly handling sensitive information are subject to and bound by Non-Disclosure Agreements.

Disaster Recovery

Percipio infrastructure is deployed in AWS on three Availability Zones, ensuring high availability and complete redundancy. In the unfortunate case of total loss of the AWS East facility, Skillsoft implemented a Disaster Recovery Plan to facilitate the most rapid recovery possible, Skillsoft Cloud Operations has a documented an Incident Recovery Plan that details the responsible parties, the communication protocol and the steps that will be taken in the event of a disaster. Skillsoft Disaster Recovery Plan that is built on the Infrastructure as Code (IaC) and the Continuous Integration/Continuous Delivery (CI/CD) application deployment pipeline. In case of a disaster Skillsoft will deploy a new instance of Percipio application on a in different AWS region in a few hours.

Skillsoft conducts an annual D.R. test staging a rebuild of its SaaS infrastructure, application deployment and data recovery. Annual D.R. test results are available to customers upon request.

Compliance with Standard Architecture

All production systems are deployed using best of breed security practices. All systems are built from a master Infrastructure as Code (IaC) set of scripts that follow CIS security standards.

All operating systems are loaded with the most current updates and CIS configurations from the OEM. This is done using automation scripts developed in Ansible.

All systems are hardened according to NIST 800-53 Rev.4 standards enforced by our deployment of Prisma Cloud product configured to enforce the Federal Risk and Authorization Program (FedRAMP) based on NIST 800-53 foundation. Such restrictions include:

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

All systems are checked to ensure that any unnecessary or potentially exploitable services are set to be disabled at power on.

Change Management - Roles and Responsibilities

Technology managers have defined approval boundaries and act as an approving authority for adjustments that are contained to their area of purview. Changes that have a wider impact are submitted for multiparty consideration of all stakeholders. Stakeholders considering 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 VP of Cloud Operations have a final veto over all change requests.

System Configuration - Management

Adjustments to system images or configurations are strictly controlled through a multi-party review and approval process involving Management, Network and Security, System Analysts and System Engineering resources. Documentation is immediately adjusted in response to system reconfiguration.

Change Process, Testing and Approval Process

Change requests are submitted by the initiating party to the appropriate technology manager for initial consideration. The area manager will then invoke guidance of the Cloud Operations Sr. Director to determine the scope of the change and establish an approval roster. Whenever possible changes are vetted through advanced implementation in a staging environment and in some cases warrant and receive load testing by a dedicated automation team.

To ensure the quality of work, changes to the environment are verified by Cloud Operations Supervisors on an ongoing basis. The Cloud Operations Architects conduct physical audits quarterly to ensure that the environment meets the defined standards.

Configuration and Security Specification

Skillsoft employs a “most-restrictive” policy regarding all network device policies and access controls. Firewall,IDP and IDS rules are continually reviewed and monitored for suspicious events. Device configuration is standardized and heavily documented. Adjustments to configurations and policies are reflected in the associated system or device documentation.

Configuration Control

Adjustments to any device by a network engineer require the approval of the Network Manager and in some cases will additionally require the Cloud Operations Sr. Director’s approval. An adjustment to any aspect of host system configuration requires the review and approval of the Senior System Architect and in some cases the Cloud Operations Sr. Director. All configuration adjustments or changes are reflected in the associated system or device documentation.

Security, Accounts and Password Management

Password Management

Generic Usernames and Passwords use are forbidden. Administrators are granted individualized logins and empowered to manage their own passwords according to the domain enforced password policy.

Password Expiration

All user account passwords are scheduled to expire every 60 days. Passwords must meet strict complexity requirements required by Federal and DoD standards. Minimum length 14 characters and cannot be reused. Password expirations are enforced via GPOs.

Password Length and Complexity

Passwords must meet a minimum character and complexity requirements including a minimum character restriction as well as requiring non-alphanumeric characters and characters of mixed case. Password length and complexity are managed via GPOs.

Password Protection

Efforts are made to limit the communication of passwords to verbal channels and passwords are provided on a need-to-know basis. When verbal communication of passwords is not possible, username and password combinations are communicated in separate correspondences and only to the target audience. Sharing of useraccount passwords is strictly prohibited.

Physical Security Description

Physical security is provided by AWS as described at:

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

Environment - Security Description

A multi-tiered perimeter defense infrastructure ensures the greatest possible protection from unauthorized access or malicious activities. Measures include a most-restrictive firewall policy, network and pattern-matching intrusion detection and prevention systems as well as an extensive and current anti-virus infrastructure.

Systems - Security Description

All systems are constructed from standardized, pre-hardened images using industry best practices in accordance with Skillsoft specific system and software requirements. Routine and ongoing patch management is controlled via centralized patch management software ensuring a consistent and current posture.

Personnel - Security Management

Employee actions (hiring, terminations, suspensions, etc.) are fully coordinated with Human Resources and corporate IT providing immediate and coordinated responses to all Cloud Operations personnel status changes. Additionally, Cloud Operations management is apprised of all Skillsoft staff terminations should special measures be required to protect against actions of ex-employees with privileged knowledge or understanding of Skillsoft proprietary software.

Employee Laptops and Mobile devices encryption

Skillsoft utilizes file-level encryption strategy leveraging software that seamlessly encrypts files at rest and in transit based on risk-levels, as defined in the information policy. The risk factor is determined as a combination of content, context, and type of data. All customer data is defined as sensitive information and treated accordingly. For data that can potentially be copied via auxiliary devices such as USB thumb drives, CD and DVD, The IT department rolled out an Enterprise Information Protection software that will detect and prevent Skillsoft's employees from transferring customer sensitive information via mobile devices (i.e., CD-RW/DVD-RW, USB, flash drives, PDAs, cameras, mobile phones).

Access to the Public Cloud Environment

All privileged access and communication to the Public Cloud environment is secured through either client or site-to-site encryption. Site-to-site tunnels providing privileged port or service access are restricted to Skillsoft Public Cloud-Only subnets. Remote access authentication is tightly integrated with existing domain security and provides for a single point of administration. Remote access is restricted to Cloud Operations personnel. This policy is universal and comprehensive to include administration, backups, etc. Under no circumstances is privileged access afforded to SW developers, Learning Consultants, Application Engineers, corporate IT or Account Executives.

Remote Access to the Public Cloud Environment

The Public Cloud systems can be accessed only by the Cloud Operations engineers. Access to the various subsystems is segregated based on duties and responsibilities. Each engineer has a unique user ID and password that is managed via an ACL that grants access only to the systems that are under the engineer's area of responsibility. Since most Cloud Operations engineers need access to the Public Cloud environment 24/7, they have laptops however the laptops have only the operating system and VPN software on it. To access the Public Cloud environment the Cloud Operations engineers, connect remotely from their laptop to their desktop machine on Skillsoft premises, which has the VPN software that provides connectivity to the Public Cloud environment. The access is authenticated via a two-factor authentication from RSA Security. Application passwords are changed every 30 days or when an individual in Cloud Operations leaves their job role.

Third Party Annual Penetration Test

In a continuing effort to improve the security of the Public Cloud environment, Skillsoft contracts third-party security organizations to conduct annually, full penetration and vulnerability assessment of the Public Cloud Environment. Thess assessments review Firewall policies, Intrusion Detection and Prevention policies, System patch levels, vulnerability to known software exploits and brute force attacks. Assessment results are available to customers upon request.

Vendor, Technology and Platform Disclosure

As a countermeasure to intelligence gathering, Skillsoft will not release to customers under any condition the make, model or manufacturer of any network or security device in use within the Public Cloud environment. This includes release of information related to:

- Firewall related hardware/software/settings
- Intrusion Detection System related hardware/software/settings
- Network penetration testing
- Vulnerability scanning
- Network topology
- Internal IP scheme
- Operating Systems configuration and security settings
- Software vendors and version used.

Planned System Maintenance

Description of planned system maintenance schedule

Routine maintenance window operations (when service-impacting) are restricted to no more than 2 hours per week. Special maintenance windows of longer duration may be requested from time-to-time for which 14 days advanced notice will be provided.

Activities conducted in these maintenance windows may include, but is not restricted to, hardware maintenance and replacement, system patching, infrastructure enhancements and Skillsoft software releases.

Emergency Maintenance

Skillsoft reserves the right to conduct unplanned maintenance activities when a delay of said maintenance is seen to pose a significant risk to the availability and or security of the services provided. Every effort is made to coordinatethese unscheduled maintenance activities with clients in advance and to conduct these activities at the least impactful time as circumstances allow for.

Maintenance Schedule

All scheduled maintenance window activities are coordinated and planned in advance with established cut-off windows. All activities are critically examined to ensure timing and that all activities are non-overlapping.

Security Management

Maintenance activities are restricted exclusively to Cloud Operations personnel and access is strictly governed through multipart security measures.

Wireless in the office

Skillsoft provides to its employees' wireless access within Skillsoft premises. The wireless service uses WPA2 Enterprise encryption for access to Skillsoft network environments. All wireless access requires unique authentication and is logged to a central location, which is reviewed for failed access attempts. Rogue wireless 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's SW Engineering team, which consists of Scrum Masters, DevOps Managers, Squad Architect, SW Engineers and Database Developers. The SW Engineering department is divided into Squads by the various areas of expertise required by the various products and their respective software development life cycle.

QA Processes

A dedicated Quality Control team ensures all software made available to customers is of the highest quality and performance. This team has final veto authority for all software packages moving to production systems.

Qualification Processes

An extensive and comprehensive testing matrix is applied to Percipio sprints testing functionality and support for alltechnologies listed in the product compatibility matrix. New functionality is tested extensively and existing functionality is additionally tested to safeguard against regressions.

Software Rollout into Production

Following a formal release to Skillsoft Cloud Operations services, the software release package is reviewed by Cloud Operations services and deployed following CI/CD methodology. Software is initially released to an integration/QA environment for testing and load testing, subsequently software is deployed in a staging environment. Following qualification in the staging environment, the software package is deployed in production. The Micro Services architecture enables SW deployment quickly and seamlessly.

Patch (hot fixes) Management and Version Management

Continuous improvements to software occasionally result in hot fixes being available to Skillsoft's software product lines. All major and minor software releases including hot fixes are uniquely versioned and made visible to all operators. The release strategy for hot fixes deployments models that of the general software release process described above except, that deployments will be performed during production time with no disruption to users or a need of a maintenance window.

SW Engineering – Change Control

SW Engineering Process

Following the finalization of functional specifications, general software architecture is determined by the product software Architect and a Cloud Operations/ DevOps Architect assigned to each squad. In some cases, architectural considerations may result in changes to functional specifications. These adjustments are communicated back to the respective stakeholders and a final functional specification and architecture is determined. This architecture is documented and released to the DevOps manager for review, project scoping and resource assignment.

Access to Source Code

All software access and versioning are strictly controlled through GitHub, a software source control package. Accessto source code is provided on an as-needed basis and is exclusively restricted to Skillsoft SW Engineering.

Software Release Process

Authority to release software from SW Engineering to QA is restricted to the DevOps manager responsible for the product line. Authority to release software from QA systems to final qualification systems is restricted to the assigned Quality Control Engineer provided the software has meet the pre-defined acceptance criteria for release. Authority to release software from final qualification to Skillsoft Cloud Operations services is restricted to the assigned Quality Control Engineer (with QA Manager assent) provided the software has meet the pre-defined 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 and empowers Skillsoft Cloud Operations services to aggressively respond to emergent threats. All available software patches are considered by Cloud Operations architects and deployed on regular a schedule in accordance with the associated risk and the FedRAMP/NIST800-53 requirements based on severity levels.

Security and Network Devices

A dedicated team of network and security professionals continuously consider newly available patches and enhancements to network and security devices. Signature bundles for IDP and IDS devices are downloaded daily and considered for implementation on a continuous basis.

Account Controls

Access to Systems

Access to all Public Cloud Systems is restricted to Skillsoft Cloud Operations Services personnel. In select cases vendor-authorized technicians are afforded access to the systems in conjunction with hardware failure events or professional services engagements.

Access Management

System and Facility access control is governed by a select body of Skillsoft Cloud Operations Services personnel. System access is granted at a level commensurate with job function. Access to security and network devices is restricted to the Network Management team, the Cloud Operations Sr. Director, and the Senior Cloud Operations Architect. The Public Cloud Facility access is managed in conjunction with the colocation service provider through a formal ACL. Governance of this ACL is restricted to Cloud Operations managers.

Boundary Defenses

Firewalls

Skillsoft has selected best-of-breed hardware and software solutions from established industry leaders. Firewalls utilize a most-restrictive policy providing only for known traffic and require port access. Access to firewalling systems is strictly controlled and adjustments to any firewall policies is subject to managerial approval prior to implementation

Intrusion Detection Prevention (IDP)

Through granular pattern matching and event correlation Skillsoft provides comprehensive protection against known vulnerabilities and zero-day defense against emergent threats. IDP signatures are considered and updated on a continuous basis.

Intrusion Prevention System (IPS)

A redundant, active IPS implementation provides effective and proven protection against brute force and denial of service attacks. Adjustments to the IPS configuration are considered on a continuous basis.

Connection to the Public Internet

Percipio SaaS application is available through the public Internet however measures exist to ensure unauthorized access to the SaaS application do not occur. This includes username/password-only access to your Percipio site and empowering customers to perform their own application account management in accordance with their own policies via the Learning Administrator interface.

Audit Trail Protection

Logs Management

Aggressive system logging captures all events relating to system access including privileged user right use, service stops/starts, logins, and logouts. Firewall and network intelligence logs capture all f ailed access events and suspicious activities as defined by our IDP/IDS infrastructure. Comprehensive system logging and SANS/Storage management logging capture all non-standard events. Detailed application logs trap all unusual application eventsin addition to verbose web server logs. All system, security and access logs are retained by Skillsoft Cloud Operations Services for an indefinite period. All event logs are archived daily to centralized disk storage for convenient access. This centralized repository is then committed to tape and retained according to our tape retention policies as defined in this document. Access to logs is restricted to Cloud Operations personnel with the exception of application error and web logs which are shared with Skillsoft SW Engineering on an as-needed basis.

Report to customers regarding a security violation incident

Skillsoft follows a strict Incident Management process approved by its DoD and Federal customers. If a security incident occurs. Information related to the incident will be provided via Skillsoft’s Tech Support team to the customer’s primary contact. The first phase of the contact will acknowledge that a problem occurred and the status of the remediation. Subsequent updates will be sent during the remediation process. Once the incident was addressed Cloud Operations will conduct a root cause analysis and the results will be provided to customers upon the customers’ request.

Data Retention and Protection

Customers' Data – Storage

All customer data is stored within the AWS US-East-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 US-West-2 region which has been selected as the Skillsoft disaster recovery site. They are backed up daily and securely replicated to the US-West-2 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.

Customers' Data - Protection

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

Password Storage

Customers' user account passwords are hashed (and salted) securely using bcrypt

End- User Access Methods

All data access occurs through publicly accessible, password protected web systems. Direct data access is never allowed.

Personnel management

Roles and Responsibilities

Skillsoft has assembled a world-class team of IT professionals around an organizational structure that provides clear lines of accountability, oversight, and ownership without sacrificing agility and responsiveness to customers. The Cloud Operations Services team is generally divided into the following teams:

- Networking and Security
- System Architects
- Application and Systems Administrators

- Database and Data Storage Administrators
- Product Support and Customer Provisioning
- Program Management

Employee Background Checks

Skillsoft recognizes the sensitivity of the data handled by the Cloud Operations employees. To ensure the best security awareness and due diligence, Skillsoft performs background checks (subject to applicable local laws) with respect to pre-determined positions that require access to customer data. Skillsoft also checks references provided by candidates generally as part of the application process. Additionally, all Cloud Operations employees are required to review and sign a Security and Privacy Policy that details roles and responsibilities, escalation procedures and overall code of conduct within the Cloud Operations organization. All Cloud Operations employees are required to sign the policy annually, acknowledging their understanding and commitment to its guidelines.

Dedicated Cloud Operations Team

Skillsoft recognizes the unique challenges facing Service Providers and the specialized skill sets required to effectively manage and grow Cloud infrastructures. In direct response to this, Skillsoft has heavily invested in a dedicated Cloud Operations Services team whose sole mandate is to ensure the best possible experience for our customers.

Expertise Description

Skillsoft Cloud Operations Services boasts a seasoned and skilled team of technology professionals. In addition to years of industry tenure, many Cloud Operations Services personnel also carry industry certifications including certifications from the following authorities:

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

Currently Skillsoft Cloud Operations holds 54+ AWS certifications.

Personnel Training

In an ever changing and evolving technology landscape, Skillsoft recognizes the critical role training plays in the successful delivery of services. To ensure that Skillsoft has the best possible resources available to its customers, Skillsoft aggressively pursues training for all products resident in the Public Cloud Infrastructure. This included a formal training agenda for proprietary products developed by Skillsoft and generic security / privacy courses assigned to employees annually.

Capacity Management

Skillsoft takes capacity management very seriously to ensure that capacity is available for new products, new customers, customers' upgrades, and systems replacement. The Percipio application is subject to load testing validating the hardware requirements and the deployment configuration is meeting our customers' demand.

The Percipio application is deployed based on a pre-defined deployment plan that maps out exactly how the Percipio application shares the hardware and, how will the hardware be configured. The required infrastructure is pre-built and configured based on build sheets and pre-configured images scripted via Infrastructure as Code that were created by the system architects. The existing Public Cloud environment is continuously monitored for resource utilization. Since emergency situations may arise, Cloud Operations team continuously monitors systems' utilization ready to increase capacity based on demand. AWS enables Cloud Operations to utilize capacity elasticitybased on users' demand.

Third Party Service Providers

Fastly

Skillsoft uses Fastly services to stream videos on Percipio

https://www.fastly.com

Accredible

Student badging and certificates. Accredible receives learner's First Name and Last Name and training completion details, to issue a badge that displays the learner's name. https://www.accredible.com/

Practice Labs

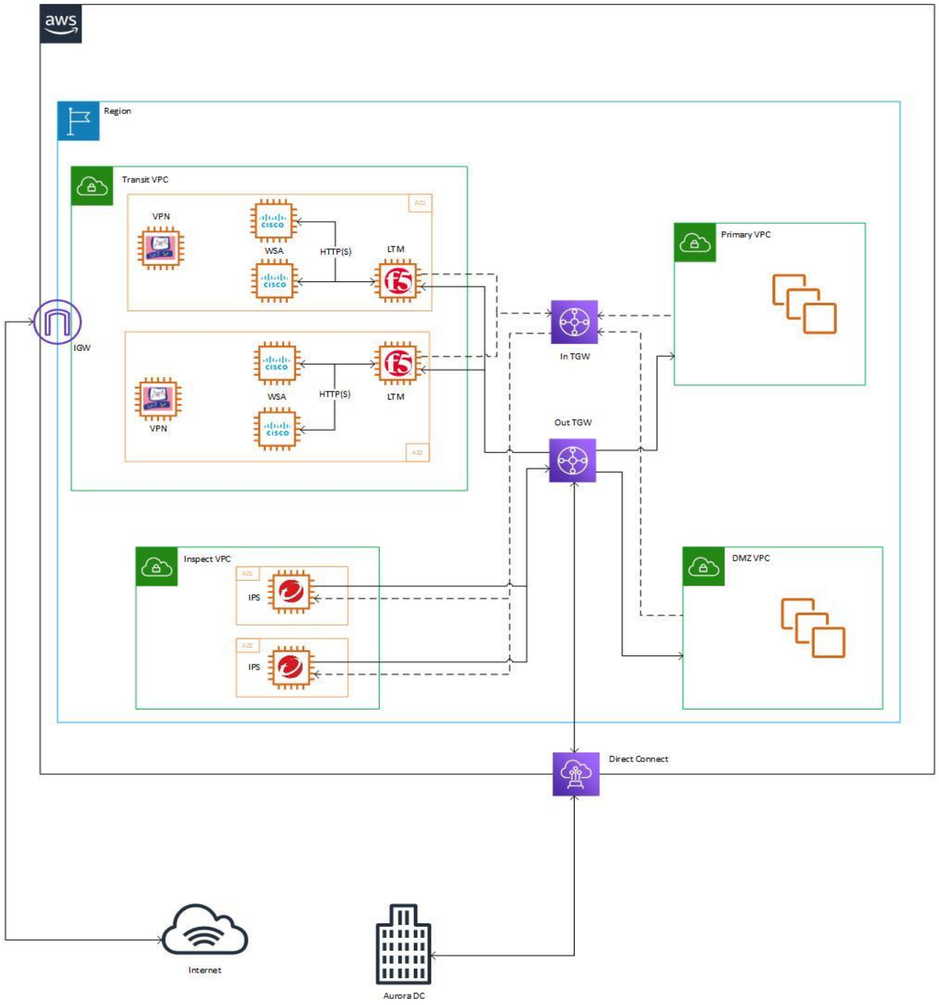
Skillsoft uses Practice Labs to provide practice labs to Percipio users. https://skills.practice-labs.com/

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


aws
Region
Transit VPC
AZ1
VPN
WSA
HTTP(S)
LTM
IGW
WSA
HTTP(S)
LTM
VPN
AZ2
Primary VPC
In TGW
Out TGW
Inspect VPC
AZ1
IPS
AZ2
IPS
DMZ VPC
Direct Connect
Internet
Aurora DC